Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Integration of Space Based Radar in The Coalition Assets Surveillance Architecture - Interoperability

Rahim Jassemi-Zargani and George DiNardo

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2003-236
December 2003

Canada

Integration of Space Based Radar in The Coalition Assets Surveillance Architecture - Interoperability

Rahim Jassemi-Zargani
DRDC Ottawa

George DiNardo
Larus Technologies Corporation

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2003-236

December 2003

Abstract

The Intelligence, Surveillance and Reconnaissance (ISR) sensors have been playing an important role in war for many years and rapid advances in technology have significantly improved the operational capability of coalition military activities. Because of these advances, command and control centres receive large amounts of strategic and tactical level information from ISR assets in real-time. Therefore coalition forces are able to plan their campaigns and task their assets with more accuracy and timeliness.

Information superiority gives a great advantage to coalition forces, as we have witnessed in recent years, but managing all these ISR assets and information is not an easy task and it has raised challenges for coalition forces. Therefore, coalition countries are very interested in finding a solution to these problems. Interoperability between ISR assets and other coalition command and control centers, handling the collected information, and processing the collected information before sending it to upper level decision makers are a few of the problems identified for solution by the coalition.

In 1999, the Coalition Aerial Surveillance and Reconnaissance (CAESAR) project was started with the membership of seven nations, Canada, France, Germany, Italy, Norway, the United Kingdom and the United States to investigate the problems of interoperability between sensor assets and a single Common Ground Picture (CGP).

This report will not only illustrate the issues of interoperability and the solutions that CAESAR provides, it will also explain how a Space Based Radar sensor may be integrated into this surveillance architecture and provide valuable information to coalition forces. Canada contributed a Space Based Radar simulator to CAESAR project, to evaluate how Space Based Radar (SBR) can be interoperable with coalition assets. Additional details of the role of SBR in an ISR surveillance architecture, and the related results and analysis will be presented in follow-on report.

Résumé

Les capteurs de renseignement, de surveillance et de reconnaissance (ISR) jouent un rôle important dans les guerres depuis plusieurs années et l'avancée rapide de la technologie a amélioré de façon significative la capacité opérationnelle des activités militaires de la coalition. Grâce à ces avancées technologiques, les centres de contrôle et de commande reçoivent un important volume d'information de niveaux stratégique et tactique provenant de ces plates-formes ISR en temps réel. Ainsi, les forces de la coalition sont capables de planifier leurs campagnes et confier des missions aux différentes plates-formes avec plus de précision et de rapidité d'exécution.

Cette supériorité d'information disponible apporte un avantage certain aux forces de la coalition, comme nous avons pu en être témoin depuis quelques années, mais gérer toutes ces plates-formes ISR et ce volume d'information n'est pas une tâche facile et de nombreux challenges sont apparus pour les forces de la coalition. Ainsi, les pays de la coalition sont très intéressés à trouver une solution à ces problèmes. L'interopérabilité entre les plates-formes ISR et les autres centres de contrôle et de commande de la coalition, la manipulation et le traitement des informations recueillies avant leur transmission aux décideurs du niveau supérieur sont quelques uns des problèmes identifiés par la coalition.

En 1999, le projet de la coalition de surveillance et reconnaissance aérienne (CAESAR) fut lancé avec sept pays, le Canada, la France, l'Allemagne, l'Italie, la Norvège, le Royaume Uni et les États-Unis d'Amérique pour examiner les problèmes de l'interopérabilité entre les capteurs des différentes plates-formes et générer une seule image terrestre commune (CGP).

Ce rapport ne décrit pas seulement les questions posées par l'interopérabilité et les solutions que le projet CAESAR propose. Il explique également comment un capteur à radar spatial peut être intégré dans cette architecture de surveillance, et fournir de précieuses informations aux forces de la coalition. Le Canada a contribué au projet CAESAR par l'entremise d'un simulateur à radar spatial, afin d'évaluer comment celui-ci peut interopérer avec les plates-formes de la coalition. Des informations additionnelles sur le rôle du radar spatial dans une architecture de surveillance ISR, les résultats et leur analyse sont présentés dans ce rapport.

Executive summary

As technology progresses, the surveillance and reconnaissance sensor designs are pushed to new heights in operational capability. Today's surveillance sensors can generate gigabytes of tactical and strategic information to command and control centres in real-time for any operation. Integration of all the existing and future coalition sensors through a common network has raised some challenges. Interoperability, sensor tasking, cross-cuing, generating a common ground picture based on all sensor outputs are just a few sample challenges that multi-nation sensor integration generates. Therefore, in 1999 seven coalition nations (Canada, France, Germany, Italy, Norway, the United Kingdom and the United States) decided to solve some of these challenges by initiating the Coalition AErial Surveillance and Reconnaissance (CAESAR) project. This project concentrated on the integration of coalition sensors that provide Ground Moving Target Indicator (GMTI) and Synthetic Aperture Radar (SAR) data.

One of Canada contribution to this project is, to provide a Space Based Radar (SBR) simulator (SIMLAB) to evaluate how SBR may be integrated into an ISR surveillance architecture and provide valuable information to coalition forces

CAESAR was constructed under four groups and 20 sub-groups with more than 100 participants. The four groups are, the Project Officers group, the Operational group, Technical Interoperability group, and the Architecture group. These four groups also consist of the following sub-groups, CONOPS, TTPs, MOEs and MOPs, CAESAR Ground Picture, Cross-Cueing, Mission Planning and lessons learned for the Operations Group, Common Data Format, Common Registration, MTE tools, Cross-Cueing, Scenarios, Common Ground Picture, Mission Planning, and lessons learned for the Technical Interoperability group, Architecture Framework, Distributed Processing, Dissemination Infrastructure, and the CAESAR Ground Picture and lessons learned for the Architecture group.

CAESAR has participated annually in scheduled exercises since the initiation of the project. This report will present the results and analysis of the first two CAESAR exercises. Clean Hunter 2001, was first CAESAR simulated exercise, which it took place in June of 2001. The second exercise, Strong Resolve 2002, which took place in March of 2002, was a combined simulation and live-fly exercise. At these exercises, the Space Based Radar was successfully integrated into the CAESAR network and was the first space based radar sensor simulator to provide GMTI data within CAESAR. The results and analysis of these exercises are provided in this report.

This report provides the results, conclusions and observations on integration of coalition ISR assets and exploitation workstations. This report shows how:

- CAESAR community defined or selected a common protocol for interoperability among the coalition assets. But, these protocols and formats also need to be upgraded continuously to accommodate new sensors and exploitation workstations.

- Through the network and standard formats, coalition exploitation workstations are able to receive and process sensor data from multi-national assets and are able to generate a common ground picture based on the integrated sensor data.

- The integration of ISR assets will provide more robust surveillance architecture, which can solve some of the issues such as terrain masking and vegetation screening problems.

- The Space Based Radar simulator was integrated into the coalition network and provided valuable information for other coalition exploitation workstations.

Additional detailed results and analysis of the role of SBR in an ISR architecture will be provided in the follow-on report.

Jassemi-Zargani,R.;DiNardo,G. 2003. Integration of Space Based Radar in The Coalition Assets Surveillance Architecture-Interoperability. DRDC Ottawa TM 2003-236. Defence R&D Canada - Ottawa

Sommaire

Avec l'avancée de la technologie, la conception des capteurs de surveillance et de reconnaissance a atteint de nouvelles limites en matière de capacité opérationnelle. Les capteurs de surveillance actuels peuvent transmettre en temps réel des gigaoctets de données tactiques et stratégiques aux centres de commande et de contrôle quelle que soit la mission. L'intégration des capteurs de la coalition existants et futurs au travers d'un réseau commun a engendré quelques challenges. L'interopérabilité, l'attribution de missions aux différentes plates-formes de capteurs, la signalisation entre capteurs, la génération d'une image terrestre commune à partir des données provenant de tous les capteurs sont quelques exemples de challenges que l'intégration de capteurs appartenant à une multitude de pays génère. Ainsi, au cours de l'année 1999, sept pays de la coalition (Canada, France, Allemagne, Italie, Norvège, Royaume-Uni et États-Unis d'Amérique) décidèrent de résoudre quelques-uns de ces problèmes en initiant un projet de surveillance et de reconnaissance aérienne de la coalition (CAESAR). Ce projet focalise sur l'intégration des capteurs de la coalition, ce qui permettra de fournir des données d'indication des cibles mobiles au sol (GMTI) et de radar à ouvertures synthétiques (SAR).

L'une des contributions du Canada à ce projet est le développement d'un simulateur de radar spatial (SIMLAB) afin d'évaluer l'apport d'un radar spatial dans une architecture de surveillance ISR, et de fournir de précieuses informations aux forces de la coalition.

Le projet CAESAR a été réalisé par quatre groupes et 20 sous-groupes, totalisant plus de 100 participants. Les quatre groupes sont le groupe des agents de projets, le groupe des opérations, le groupe de technique d'interopérabilité et le groupe architecture. Ces quatre groupes sont divisés en sous-groupes, tels que CONOPS, TTPs, Moes and MOPs, image terrestre CAESAR, signalisation entre capteurs, planification de mission, et aussi des groupes formés à partir des leçons à retenir pour le groupe des opérations, pour le format commun des données, la planification de mission, ainsi qu'à partir des leçons à retenir pour les groupes de technique d'interopérabilité, du cadre d'architecture, du traitement distribué, de l'infrastructure de dissémination et de l'image terrestre commune CAESAR, et finalement à partir des leçons à retenir pour le groupe architecture.

Depuis le début du projet, CAESAR a participé annuellement des exercices planifiés. Ce rapport présente les résultats de l'analyse des deux premiers exercices. L'exercice « Clear Hunter 2001 », réalisé au mois de juin 2001, fût le premier exercice de simulation. Le second exercice, « Strong Resolve 2002 », réalisé en mars 2002, était la combinaison de simulations et d'un exercice en vol temps réel. Au cours de ces exercices, le radar spatial fût intégré avec succès au réseau CAESAR. C'était la première fois qu'un radar spatial délivrait des données GMTI pour le projet CAESAR. Les résultats et l'analyse de ces exercices sont décrits dans ce rapport.

Ce rapport fournit les résultats, les observations et les conclusions sur l'intégration des plates-formes de la coalition et sur l'exploitation des stations de travail d'exploitation. Ce rapport montre comment :

- la communauté CAESAR a défini ou sélectionné le protocole commun d'interopérabilité pour dialoguer avec les autres plates-formes. Il s'avère que les différents protocoles et formats doivent être mis à jour afin de pouvoir intégrer de nouveaux capteurs et stations de travail d'exploitation.

- à travers le réseau et les formats standards, les stations de travail d'exploitation peuvent recevoir et traiter les données provenant des capteurs de plates-formes multinationales, et générer une image terrestre commune.

- le simulateur de radar spatial fût intégré dans le réseau de la coalition et fournit des informations importantes aux autres stations de travail d'exploitation de la coalition.

Des résultats et analyses détaillés additionnels sur le rôle d'un radar spatial dans une architecture de surveillance ISR sont également reportés.

Jassemi-Zargani, R.;DiNardo, G. 2003. Integration of Space Based Radar in The Coalition Assets Surveillance Architecture - Interoperability. DRDC Ottawa TM 2003-236, R & D pour la défense Canada - Ottawa.

Table of contents

List of Figures

List of Tables

1. Introduction

Information superiority has been one of the key advantages in any military mission. Most of the nations have been developing more complex surveillance sensors to achieve this superiority. But, the integration of the different nation's sensors to achieve information superiority to support coalition nations joint mission has been a challenging problem that coalition nations are currently facing.

Coalition nations developed or are developing different types of surveillance and reconnaissance sensors and the sensor data must be compliant with a common network in order to share information among the nations. This is necessary to provide a common ground picture for command & control centers and decision makers based on all data received from different sensors. This integration is essential to make the surveillance architecture more robust for persistent surveillance over a theatre of operation.

Interoperability among all the sensor platforms, exploitation workstations and mission planning workstation are just a few examples of the issues that have to be considered for designing or setting up any surveillance and reconnaissance architecture. Therefore, seven coalition nations have gathered to solve some of these problems under the CAESAR project. These nations have contributed either a national asset or an exploitation workstation. Each nation's sensor has an important role in the CAESAR surveillance architecture and Canada is contributing a space-based sensor for this architecture to satisfy the needs of supporting a coalition mission.

Integration of the sensors, real-time network design, shared database and creation of a common ground picture has been investigated by different researchers or organizations to improve the ISR architecture. The organizations such as, NATO Consultation, Command and Control Agency (NC3A) have been investigating the integration of ISR assets since 1995 with collaboration of Supreme Headquarters Allied Forces Europe (SHAPE) and several other nations [10]. They have been working on developing a NATO Alliance Ground Surveillance (AGS) testbed., so all the NATO countries can integrate their assets into this testbed and share their data with other nations. Also researchers such, Gene Layman et al provides an overview and benefits of using Defence Information Infrastructure Common Operating Environment (DII COE) and High Level Architecture (HLA) for an interoperable C4I simulation environment [1]. Adelantado and his colleagues from the French Aeronautics and Space Research Centre (ONERA) are investigating the multiresolution modeling and simulation with HLA [2] to improve the interoperability among the ISR asset simulators.

The effectiveness of space-based surveillance sensors in conjunction with other ISR assets for collecting strategic information verses tactical has been used limitedly. This report will show the concept of a new generation of space-based radar constellation, which can generate tactical and strategic information and provide this information to all coalition nations through the common network and communication protocol.

Space-Based Surveillance (SBS) architectures have been investigated by many researchers from different nations or by collaboration of multiple nations such as, Canada, the United

Kingdom and the United States under the Tri-Lateral Technology Research Development Program (TTRDP)[3]. This report will also show the designed SBS satellite constellation and the implementation of that constellation into the overall surveillance architecture. A more detailed analysis of SBR role in the ISR surveillance architecture will be provided in the follow-on report.

2. Interoperability

Coalition nations are rapidly deploying advanced sensor data systems and the ground processing capability to exploit this data. Despite these advances, a single nation will not be able to field sufficient sensors to fully support a large scale military operation. Technical interoperability between various coalition sensors and ground processing workstations can be achieved through the standardization of network and protocol formats. The CAESAR project has defined and developed the methods and standards to interconnect these various sensors and ground exploitation systems to allow the sharing of data and intelligence in a real-time shared networked environment. The following sub-sections will provide the definition of interoperability, a description of the testbed that was used for testing the network and new protocols, and the interoperability issues and lessons learned.

2.1 Definition

INTEROPERABILITY: the ability of two or more systems or components to exchange information and to use the information that has been exchanged [4].

Within CAESAR technical interoperability requirements provide for two differing application protocols and formats to conform incoming simulated data and outgoing sensor processed data. Distributed Interactive Simulation (DIS) for simulated entity truth data being provided to the nation sensor simulators and the NATO AGS Pre-exploitation data format (EX) data exchange protocols to transmit and share processed sensor data. The DIS protocol is exclusively used for simulated entity creation and distribution, whereas the EX application protocol may be used in both live and simulated operations.

The User Datagram Protocol (UDP) multicasting protocol is the underlying transmission protocol used by both DIS and EX to transmit data packets over the network. Though, DIS does not implicitly specify UDP as the transmission protocol it is assumed that DIS data transmission is a many to many transmission model therefore requiring the use of UDP. The NATO EX protocol standard has been developed within the capabilities and limitations of the UDP specification and the many to many multicast transmission model.

The following subsections will provide a more detailed description of the CAESAR application protocols and the transmission layer UDP protocol.

2.1.1 NATO AGS Pre-exploitation Data Format (EX)

The NATO EX protocol format was developed to address the shortcomings of the current NATO STANAG protocols and to support the protocol format being used for both real-world and simulated operations. The shortcomings of existing NATO protocols are two fold. First, present NATO protocols have not considered radar data, which is the primary sensor data of the Alliance Ground Surveillance (AGS) Sensors. Second, the type of the data being transmitted either, early stage raw sensor data, that is sensor data before any significant processing has been performed, or late stage "exploited" data, data that has been significantly processed and where operational information has been extracted (usually by a human in the loop). A protocol that supports an intermediate stage or a "pre-exploitation" level format was not available.

The NATO EX protocol format was formulated to support AGS radar data and the intermediate stage data as generally provided by AGS sensors. The NATO EX provides for the representation and transmission of intermediate stage Synthetic Aperture Radar (SAR) imagery data, Moving Target Indicator (MTI) data and other AGS specific data and CAESAR specific communication data packets (FreeText, Radar Service Requests etc.). A "pre-exploitation" level data format is data that has been processed to be of use to an analyst. In the case of MTI data this is radar data after it has gone through detection processing. Further information may then be extracted from the data stream, such as position, radial velocity, radar cross-section, and perhaps some form of classification or target size. In the case of SAR imagery data the data has been processed to be "geo located" and corrections for platform motion, and image quality may be performed.

2.1.2 Disbriuted Interactive Simulation (DIS)

Distributed Interactive Simulation (DIS) IEEE 1278.1 is the name of a family of protocols used to exchange information about a virtual environment among computer hosts in a distributed network environment that are simulating the behaviour of objects in that environment. The simulated objects are capable of physical interactions and can sense other objects within the simulated environment. DIS was developed by the U.S. Department of Defence to implement systems for military training, rehearsal and other purposes. The basic architecture concepts of DIS are an extension of the Simulator Network (SIMNET) developed by the Advanced Research Project Agency (ARPA). The current release of DIS is IEEE 1278-1A 1998 version 6. The basic architecture concepts of DIS are:

No central computer controls the entire simulation: DIS uses a distributed simulation approach in which the responsibility for simulating the state of each entity rests with separate simulation applications residing in host computers connected via a network.

Autonomous simulation applications are responsible for maintaining the state of one or more simulation entities: Simulation applications are autonomous and generally responsible for maintaining the state of at least one entity and (in the case of CAESAR) several entities. The total number of entities for which a simulation application is responsible for is limited only by the capabilities of the simulation.

A standard network protocol is used for communicating truth data: Each simulation application communicates the state of the entity to other simulations on the network using a standard network protocol in multicast mode. The receiving simulation is responsible to unpack and decode the entity.

Changes in the state of an entity are communicated by its controlling simulation application

Perception of events or other entities is determined by the receiving application

Dead reckoning algorithms are used to reduce communications processing: A method of position/orientation estimation is used to limit the rate at which simulations must issue state updates for an entity.

2.1.3 User Datagram Protocol (UDP)

The UDP protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed and is regarded as a best effort transmission protocol. The underlying transmission protocol is the Internet Protocol (IP). A complete explanation and description of the UDP and IP protocol is provided by RFC768 [12] on the Internet RFC/STD/FYI/BCP Archives web site [5].

2.2 NATO AGS Capability Testbed (NACT)

To investigate the technical aspects of interoperability NC3A has developed and implemented, NACT, at the NC3A headquarters, The Hague, Netherlands. The NACT, with support of the NC3A, SHAPE and the CAESAR coalition nations, consists of NATO and nationally supplied hardware and software that allows simulation and operational systems to interconnect for the purpose of enhancing research and development efforts in the area of interoperability. The NACT allows CAESAR to perform experiments, provide demonstrations and participate in various simulators based and live fly exercises. The NACT has allowed participants to recreate an accurate representation of simulated platform and sensor pairs so that interoperability of sensor data and exploited data can be demonstrated, evaluated and improved. At the moment the NACT supports systems (simulated or operational) from the seven CAESAR coalition nations and NATO NC3A simulators and NATO data formats.

The NACT, and NC3A, provides a secure facility, computers, software, networking hardware and software, network administration, data collectors and processors, and additional data and support structures to facilitate interoperability operations and exercises. The NACT also provides a controlled switching capability and subnet network structure that allows connection to other NATO laboratories. Other laboratories that the NACT can be connected to include TMD development and operations, Air Surveillance, C2 development and Electronic Warfare and Logistics Management. Additional systems interconnected to the NACT include: Integrated Command and Control (ICC) system for Air Forces, NATO's SEW dissemination network, TMD Target Refinement and Nominations (TRAN) tools and live and simulated Recognized Air Picture (RAP) production capabilities.

In June 2003, the Common Shared Data Database (CSD) was integrated into the NACT. The CSD provides a shared repository for GMTI data, SAR imagery data, and exploitation products as contributed from coalition nation sensors, simulators and exploitation workstations. The coalition nations may use the CSD data to initialize their internal data stores and processes, to recover from system outages and to complement their data store from other coalition system data products. The CSD also provides a mechanism for coalition systems to examine data for which their own particular system does not have the capability to collect or render. The ability to geo-locate, render and display SAR imagery data is one example of CSD capability. Additionally, the CSD may be used to support other CAESAR objectives including the generation of a Common Operational Ground Picture (CGP).

The CSD is comprised of an underlying data model and the software and network interfaces enabling access to CSD data. The CSD may be accessed by an arbitrary number of application systems either directly using defined APIs or through a web client. Direct access to the CSD is through a common set of Distributed Computing Services. The Common Object Request Broker Architecture (CORBA) is the standardized mechanism used to exchange data across different platforms.

The NACT network as shown in Figure 1 is subdivided into two primary networks which are further subdivided into subnets with packet forwarding through the subnets allowing sensors and exploitation systems on the configured subnets to retrieve and share data and exploitation product information. The primary networks are:

Truth Data DIS network:

This network utilizes the DIS protocol to generate all exercise target and sensor position data. The data is provided in DIS Protocol Data Units (PDU) format cells encapsulated in the Internet Protocol User Data Protocol (UDP/IP). This network operates at 100 Mbits /sec on an unshielded twisted pair network (100Base-T). The DIS network provides all target truth data, sensor platform DIS position information and other DIS PDU as specified by CAESAR (DETONATION, START, STOP etc).

Exploitation NATO EX network:

The NATO EX protocol is used to export all CAESAR GMTI, SAR and communication data .The data is provided in EX format cells encapsulated in UDP/IP packets. This format is used for all exercise sensor processed data (GMTI, SAR etc) exported to CAESAR exploitation/tracking stations and to receive EX packet instructions and requests (RSR) and FreeText.. This network operates at 10 Mbits/sec on an unshielded twisted pair network (10Base-T).

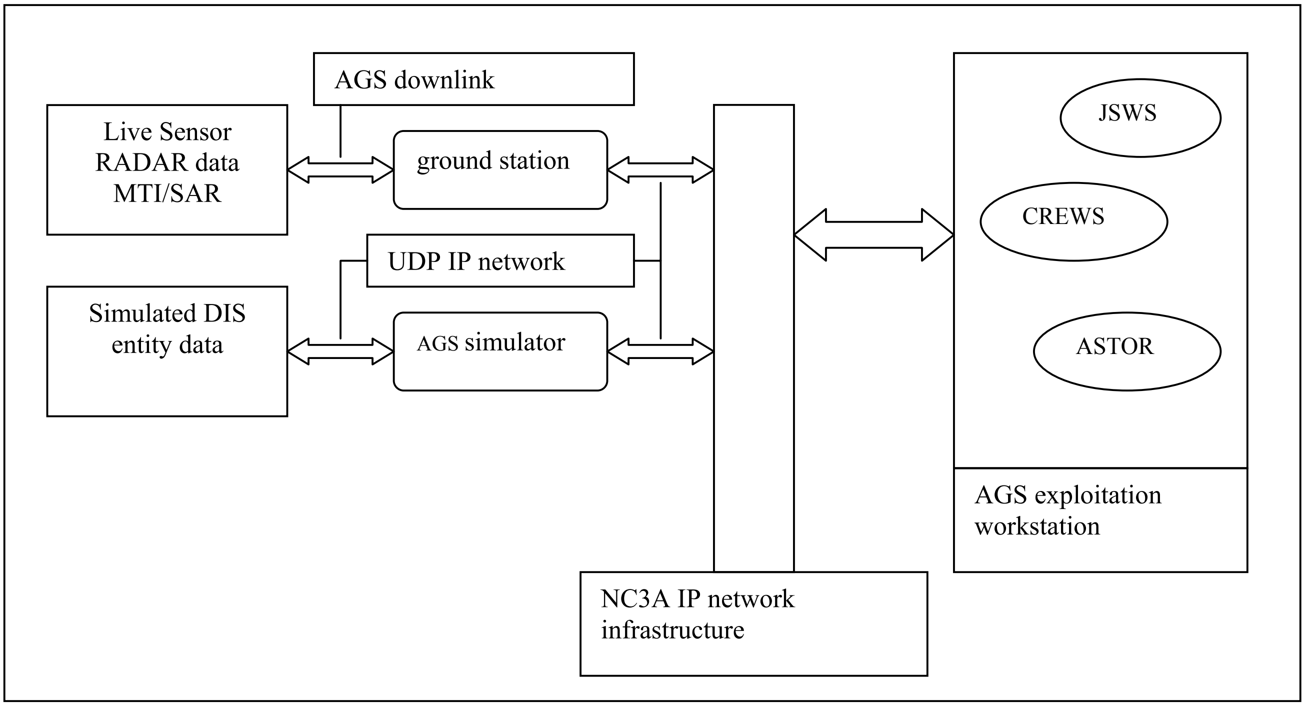

Figure 1 NACT Architecture

2.3 Interoperability Issues and Lessons Learned

The Lenk paper, Formats For The Representation of AGS Pre-Exploitation Data Types [6], outlined the problems of existing data formats and proposed the use of a new data format, to process pre-exploitation data as provided by AGS sensors. Through development and participation in various CAESAR exercises and integration tests a number of issues and problem areas were identified in the EX format protocol, DIS and the use of UDP as a multicast transport for pre-exploitation data.

2.3.1 EX Version 2.01

Using a multicast best effort data protocol UDP, allows for the possibility of lost and or corrupted data. There is no mechanism to automatically detect errors and retransmit data as provided for under TCP, a connection oriented protocol. The individual systems must provide for error checking and fault resolution. The CAESAR mechanism assumes that data will be retransmitted within a short time frame, this scenario is valid for air platforms but is not realistic for non-geosynchronous/geostationary space based platforms. The loss of transmitted data is not recoverable under the current mechanisms.

Best effort data protocols do not guarantee the delivery of packets in a first sent first received order, it is possible for packets to arrive out of order. The EX format has assumed that data arrives ordered. Special efforts must be performed by the receiving workstations to reassemble EX packets into an ordered packet list and processed.

Not all AGS sensor capabilities have been implemented in the EX version 2.01 protocol format. For example, SBR is able to provide true target velocity, as opposed to radial velocity, but this is not available within the EX format. The EX format and EX parameters have been formulated, primarily, for airborne platforms and their sensors. Aspects of EX do not support or address space based platforms and sensors or non-moving platforms and sensors.

The EX format document allows for imagery data to be transmitted in multiple imagery formats (TIFF, GeoTIFF, GIF, etc). Pixel stream data has been well tested and is implemented in all CAESAR compliant exploitation workstations. Observed at Strong Resolve 2002, the pixel stream imagery data format, though well suited for small image data files is not robust for large image data files within the CAESAR network implementation and a best effort, lossy, network protocol [11].

Given the above observation, image data formats other than pixel stream was observed to be operationally difficult to implement within the CAESAR communication network [11]. The use of UDP does not guarantee that required header and data format parameters, required to reconstruct the image, will be delivered and or delivered in the correct order. Pixel stream data, by its format, allows the receiving workstation to reconstruct parts of the image from the EX header parameters. Missing areas are processed differently by each receiving workstation but, importantly, the complete image is not lost due to packet loss.

From exercise observations the EX format and UDP network protocol did not reliably transmit large imagery data files [11]. The large data SAR image from RADARSAT1 could not be transmitted to all workstations using EX format pixel stream and the UDP network protocol. To provide operational access the imagery data was stored on an external data store and workstations requiring access to the imagery data would use a connected protocol (FTP over TCP/IP) to retrieve the data. This limitation underlies the difficulties with best effort protocols (UDP) and multicasting requirements.

NC3A is currently investigating STANAG 4607 to address the shortcomings of the EX version 2.01 data format.

2.3.2 DIS

The simulation community and the Defence Modeling and Simulation Office of the U.S. Department of Defence have addressed the DIS protocol limitations and difficulties. The High Level Architecture (HLA) has been developed to address these limitations and issues.

Limitations and disadvantages of DIS, as it pertains to the CAESAR implementation are:

- DIS incorporates limited packet timestamps and requires strict time synchronisation between simulators

- Transmission of DIS packets over large distances or multiple sites is difficult

- Packet latency is not addressed within the standard but must be supported by the application

- DIS requires packet retransmission to address the issue of packet loss, increasing network traffic. For large entity simulations network traffic is unnecessarily increasing the probability of UDP packet loss.

2.3.3 UDP

The CAESAR data network (Exploitation and Truth Data) has been designed and implemented using multicast and the UDP protocol over IP. UDP, as described above, is a simple unreliable protocol used to implement multicast requirements. As defined in RFC768 [12], UDP was designed to transmit messages to multiple interconnected network computers with a minimum of overhead. Limitations and disadvantages of using UDP are:

- A UDP packet may be lost or discarded in several ways, including failure of the underlying communication mechanism

- UDP implements a checksum over the data portion of the packet. If the checksum of a received packet is in error, the packet is dropped without notification. This error is observable during the transmission of large imagery data [11]

- Each UDP socket stores a limited queue of received packets. Arriving datagrams that do not fit within this limited capacity are discarded without notice

- UDP does not guarantee that packets are delivered in the order they were sent.

- UDP may generate duplicate packets during the communication process

- UDP packets are given low priority on a routed network. If the network is busy and needs to drop packets, UDP packets are dropped first. Router and node design and network configuration is important to improve the proper and reliable transmission and reception of UDP packets

- If a router allows multicast packets to be sent to all subnets more than once, network traffic increases drastically. Multicast message are sent to all subnets on a routed network. Routers are not aware which subnets have responders to the multicast data, therefore data is sent to all subnets.

3. Space Based Radar

Space-Based Radar (SBR) surveillance concepts have been generating interest among many nations for several decades. Only recently, technological advances have combined to make a SBR surveillance system a near-term reality. Canada has pursued this concept under national programs, such as the Radarsat2 project, or under international programs, such as the Tri-lateral Technology Research and Development Project (TTRDP).

TTRDP was formed by collaboration of the United States, the United Kingdom and Canada to characterize and investigate the military value, technical feasibility, and potential cost of space-based surveillance (SBS) systems for maritime, land, and aerospace defence applications.

Radarsat2 is a Canadian National asset, which will be testing the GMTI detection concept from space. The first stage of space integration into an ISR surveillance architecture was conducted based on Radarsat2 sensor and platform model. The second stage of the SBR integration is based on the proposed SBR surveillance architecture developed through the TTRDP program. This multi-satellite constellation was designed with the requirements of; nearly full coverage of the earth, specific response times and revisit rates.

3.1 The Space Based Radar Concept

The main applications for this concept are wide area land & maritime surveillance, early warning and deep look over the theatre. The concept design is driven by the need for the primary radar sensor to provide GMTI capability, and also provide SAR imagery. [7].

There are two concepts that have been considered for this analysis; first concept that was used for integration into the ISR surveillance architecture was Radarsat2, which represents a single space asset. The second concept was based on the concept Alpha from the TTRDP project. This design concept has been driven by requirements of the constellation of spaceborne GMTI sensors [7].

3.2 GMTI Sensor Design

The Radarsat2 satellite GMTI concept is considered as a first stage for integration of space based assets into an ISR surveillance architecture. The Radarsat2 satellite parameters are provided in Table 1 and details of the concept is provided in reference [8].

The second concept was based on the concept Alpha constellation design, which was based on the GMTI sensor mode requirements. Table 2 shows the Concept Alpha GMTI parameters as defined by the Concept Alpha Team [7].

Table 1 Radarsat2 parameters

SYSTEM PARAMETERS	CURRENT ASSUMPTIONS
Constellation	1 Satellite
Orbital Altitude	798 km
Orbital Inclination	98 degrees
Antenna Size	1.37 x 15 m
Frequency	C band (5.4 GHz)
Incident angle	20 – 49 degrees
Field of regard (at broadside)	500 km (2000 km accessibility swath)

Table 2 Concept Alpha parameters

SYSTEM PARAMETERS	CURRENT ASSUMPTIONS
Constellation	36 Satellites 12 Orbital Planes
Orbital Altitude	1100 km
Orbital Inclination	85 degrees
Antenna Size	2.5 x 32 m
Frequency	X band (10.0 GHz)
Incident angle	20 – 80 degrees
Field of regard (at broadside)	2200 km

4. Simulator Model

The simulator model selected for these exercises is the Simulation Laboratory (SIMLAB), developed at DRDC-Ottawa to study the concept of SBR surveillance architecture with other ISR assets (Figure 2).

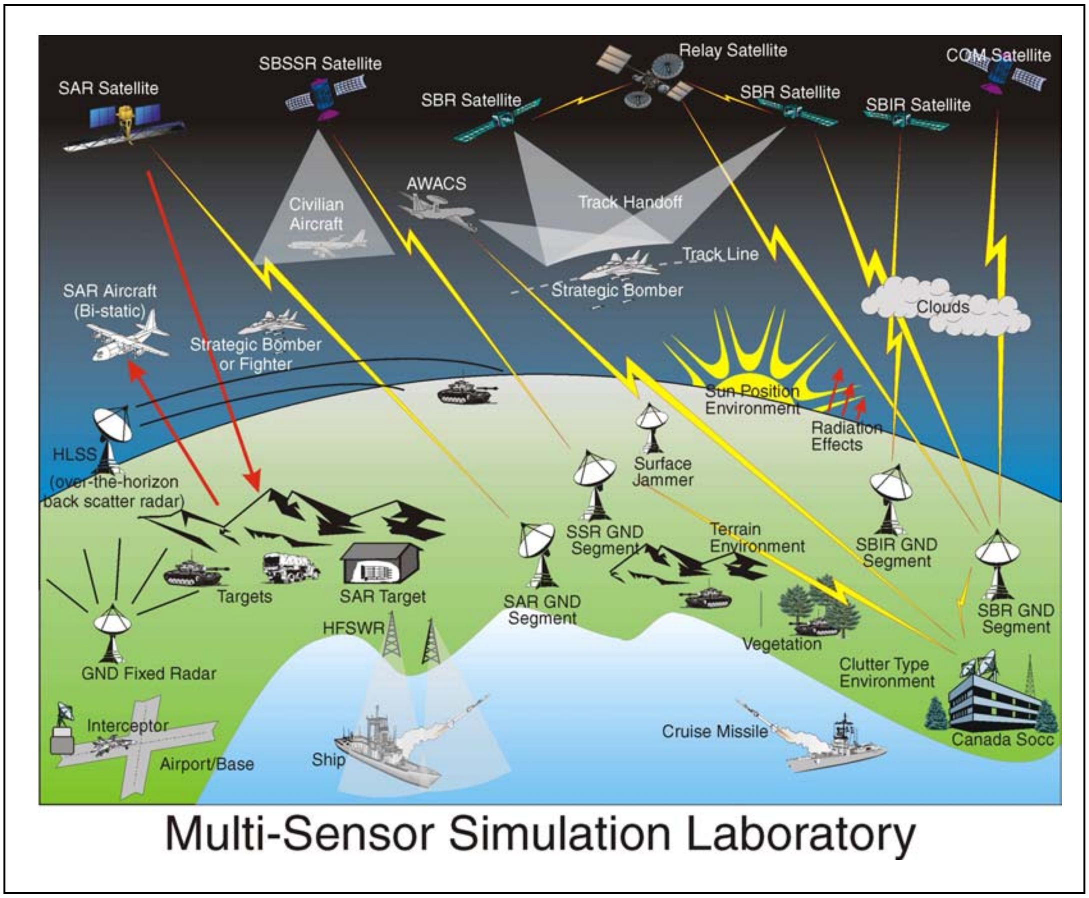

Figure 2 Multi-Sensor Simulation Laboratory SIMLAB

4.1 SIMLAB

AASTRA Aerospace developed the Space-Based Radar (SBR) Surveillance Simulation Laboratory (SIMLAB) in the late 1980s for the Department of National Defence (DND) of Canada [9]. This simulator was developed to model and analyze SBR surveillance architectures. The simulator contains four major groups of library models, as shown in Table 3.

Table 3 SIMLAB Library Module

SURVEILLANCE SYSTEMS	TARGET TYPES	COMMAND AND CONTROL	ENVIRONMENT
SAR Satellites	Bombers/Fighters	Sector Operations	Weather Visibility
SSR Satellites	Cruise Missiles	Control Centre	Terrain Following
SBR Satellites	Civilian Aircraft	Communication Links	World Map
SBIR Sensors	Ships	Ground Segment	Clutter
AWACS	Vehicle	Interceptor Aircraft	Jamming
Ground-Based Radar		Interceptor Weapon	Environment
High-Level Surveillance Systems		Delivery	
HFSWR			

SIMLAB is capable of producing numerous detailed simulation results with regard to target detection and tracking, beam dwell time, instantaneous grazing angle, coverage of targets within the Area of Interest (AOI), and many others. This simulator is capable of modelling multi-satellite constellations, and it can handle multiple theatres of coverage simultaneously. SIMLAB was developed based on very detailed models for surveillance systems. For example SBR satellite has more than 100 input parameters. SIMLAB is also capable of modelling different types of Space Based sensors, such as SAR and IR , and antenna apertures types such as Phased Array, Rotating Reflector and others with detailed parameters [3]. This lays the foundation for a very detailed and extremely versatile software simulation. SIMLAB is an engineering level simulator, which can calculate the Probability of detection (Pd) of the targets based on the target velocity, returned signal from the target, clutter background, and noise parameters. In addition to detection, it also contains algorithms for tracking the targets.

4.2 Simulator (SIMLAB) Interface Design

Several modifications were necessary for the SIMLAB simulator to meet the requirements of the CAESAR project. These modifications enabled the simulator to support receiving external simulated entity data broadcasts from a real-time DIS network data source and to output simulated moving target indicator (MTI) data to a real-time exploitation network.

The design principles were based on two criteria:

- Minimize the modifications to SIMLAB to support CAESAR
- Provide flexibility to support a variety of communication and network requirements.

Resulting from these two criteria and the primary objective for flexibility, the design consisted of external bridges communicating with SIMLAB through shared memory tables and data queues. Through this design, the SIMLAB software is not restricted to a single external communication protocol, providing transparency to SIMLAB. As Figure 3 shows, (SIMLAB

Interface Overview) the SIMLAB communication capability consists of approved software interface mechanisms to communicate with the mandated CAESAR network protocol requirements, DIS and NATO EX. As mentioned earlier the CAESAR requirements consists of a dual network implementation, a simulation network and an exploitation network. Both networks utilize the User Datagram Protocol (UDP) and the Internet protocol (IP) as the underlying network transmission protocol.

The communication processes consists of two separate bridges, the DISBRIDGE and the EXBRIDGE, as shown in Figure 3.

The DISBRIDGE is the interface between SIMLAB and the CAESAR simulator network. DISBRIDGE verifies the incoming data; transforms the data to the SIMLAB required co-ordinate system, and data format and outputs the transformed data to the shared entity table, which is accessible by SIMLAB.

The DISBRIDGE process is also able to dynamically generate and filter targets based on the dynamic target lookup library and the DIS PDU input received in real-time and constraints specified by the operator. This process helps to minimize the data lookup requirements of SIMLAB and improve real-time response

The EXBRIDGE process is the interface between SIMLAB and the CAESAR exploitation network. SIMLAB processes DISBRIDGE entity information and outputs detection data (MTI) to a shared UNIX interprocess communication queue (IPC). EXBRIDGE retrieves this processed MTI data from the shared IPC Queue and transforms and formats the data to the CAESAR MTI EX protocol format packet structure EXBRIDGE then transmits the EX MTI detection packets onto the CAESAR exploitation network wrapped within UDP network packets.

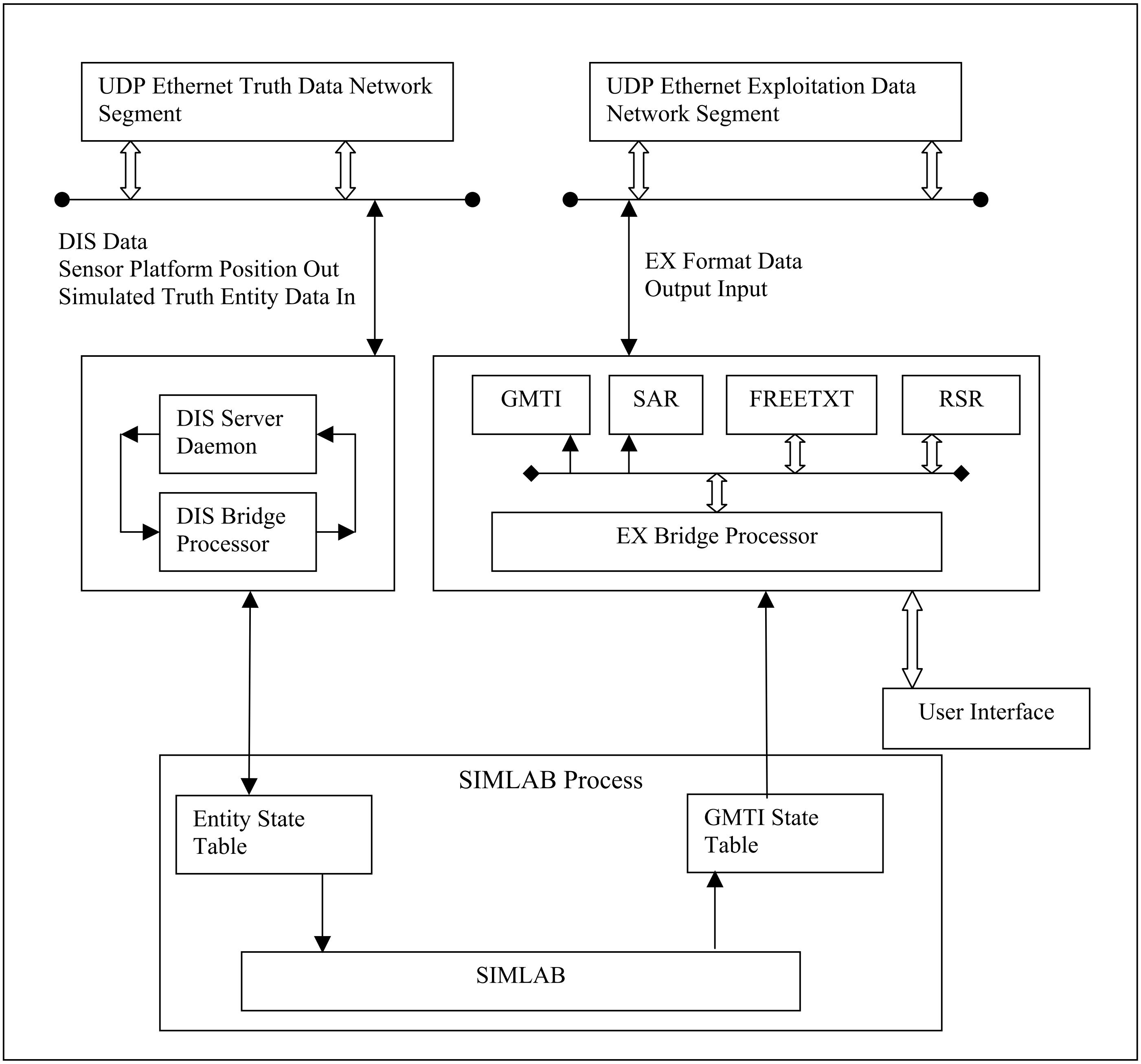

Figure 3 SIMLAB Interface Overview

5. Simulation Results and Analysis

Since 2001, there have been a number of simulation and live exercises conducted, under the CAESAR umbrella, to investigate interoperability issues. The Space based radar simulator was involved with these exercises and the results and analysis of two CAESAR exercise are provided in this section.

5.1 Clean Hunter Exercise 2001

Clean Hunter exercise was a live-fly NATO exercise conducted near central Europe in June 2001 [9]. Since no live fly ISR assets were scheduled, the Theatre Missile Defence (TMD) part of this exercise was simulated. Therefore, the SBR simulator and other CAESAR sensors simulator participated in this exercise to fulfill this role. All the detection reports from CAESAR assets were sent to allied exploitation workstations through the NATO CAESAR network to support the TMD cell. Section 5.1.1 will show some of the results from this exercise.

5.1.1 Simulation Results for Clean Hunter Exercise

The SBR sensor and orbit parameters for this exercise were modelled based on the Radarsat2 Sensor. The details of the model are provided in section 3.2. Figure 4 shows the detection results by SBR sensor for different days of the exercise. The detected target's parameters such as location and speed were broadcast through the exploitation network in NATO EX format. The coalition exploitation workstation received the SBR data and integrated the data with other coalition assets such as, JSTARS, HORIZON, Global Hawk, Raptors, ASTRO and CRESO.

As the results in Figure 4 show not all the detection attempts were successful, and that is because a large percentage of these targets were moving at a very low speed, below the Minimum Detectable Velocity (MDV) threshold of the SBR. Also, some of these targets were deep into clutter and they were not detectable.

The variation in the detection attempts on different days also caused by the limitation of the sensor field of view and pre-defined orbital parameters. The AOI was not always covered fully by the sensor

At Clean Hunter 2001 SBR simulator (SIMLAB) was interoperable for the first time with other coalition assets simulator and Exploitation workstations through CAESAR network. These results show the successful application of the SBR to detect ground moving targets and broadcast the results to other coalition nations through the NATO EX protocol.

Figure 4 also shows that there was only single or dual passes per day and sometimes, no passes over the AOI. These results show, that a single satellite cannot provide continuous coverage over an AOI, therefore it can only provide limited tactical or strategical information to the coalition command and control centre.

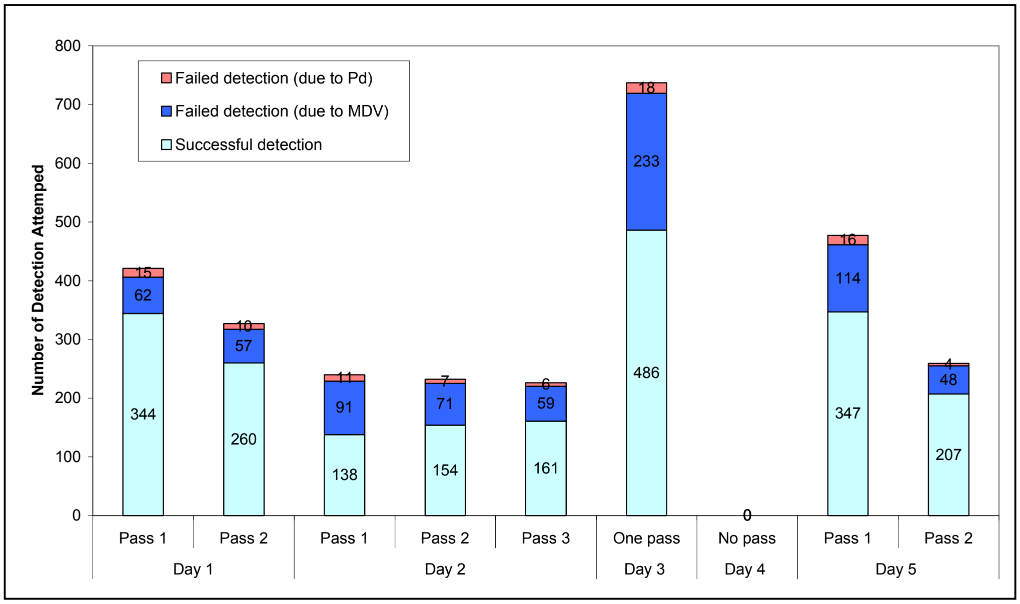

Figure 4 Detection Results from Clean Hunter Exercise 2001

5.2 Strong Resolve Exercise (2002)

Though CAESAR participation in the Clean Hunter 2001 exercise was well received it was observed that while the CAESAR concept appeared accurate, it was not possible to assess the timeliness that would be available from live fly sensor systems and that participation in a live fly exercise would be more revealing. Strong Resolve 2002, a large-scale live fly exercise was chosen to evaluate CAESAR concepts within a live exercise scenario. During Strong Resolve 2002, CAESAR, provided near real-time data from the French HORIZON GMTI sensor and the US Joint STARS GMTI sensor. SAR imagery of the area was provided by RADARSAT1. Data was down linked to a central point and processed by various CAESAR assets into the NATO EX format and made available to the exploitation workstations.

Due to scheduling conflicts, weather conditions and platform down time, the simulated exercise was kept running to keep the operators on alert and to solve any inoperability issues between the sensors and the exploitation workstation. The results presented in sub-section 5.2.1 are representative of the simulated exercise portion of the Strong Resolve exercise.

5.2.1 Simulation Results for Strong Resolve Exercise

There are three sets of results provided in this report from the Strong Resolve exercise. First, the results of an early stage of the conflict, where there were only a few moving targets in the AOI, which was located at higher latitude. The second stage is when there are more activities in the AOI and the third stage when the activities in the AOI were at maximum.

The concept Alpha constellation design from the TTRDP project was selected as the model for the Space Based Surveillance (SBS) architecture. The details of this concept are provided in sub-section 3.1. This concept provides more frequent coverage over the AOI, which is a valuable complementary asset to the other ISR coalition assets. The increase in the number of satellite and the higher inclination angle of the satellite orbit, allows the SBR satellites to have more frequent passes over this particular AOI located at higher latitude.

This test was also conducted to evaluate the interoperability issues in the NATO CAESAR network. This SBS provided much more frequent coverage over the AOI, and therefore broadcast a large amount of valuable information about moving targets position and their velocity in the AOI through the network.

Figure 5 shows the coverage statistics of the AOI by the Concept Alpha SBS architecture, which provides an average of 4.13 minutes coverage per satellite pass and gaps of 6.8 minutes between satellites, passes. These results represent the early stage of the war, when there were not many moving targets at the AOI (Figure 6).

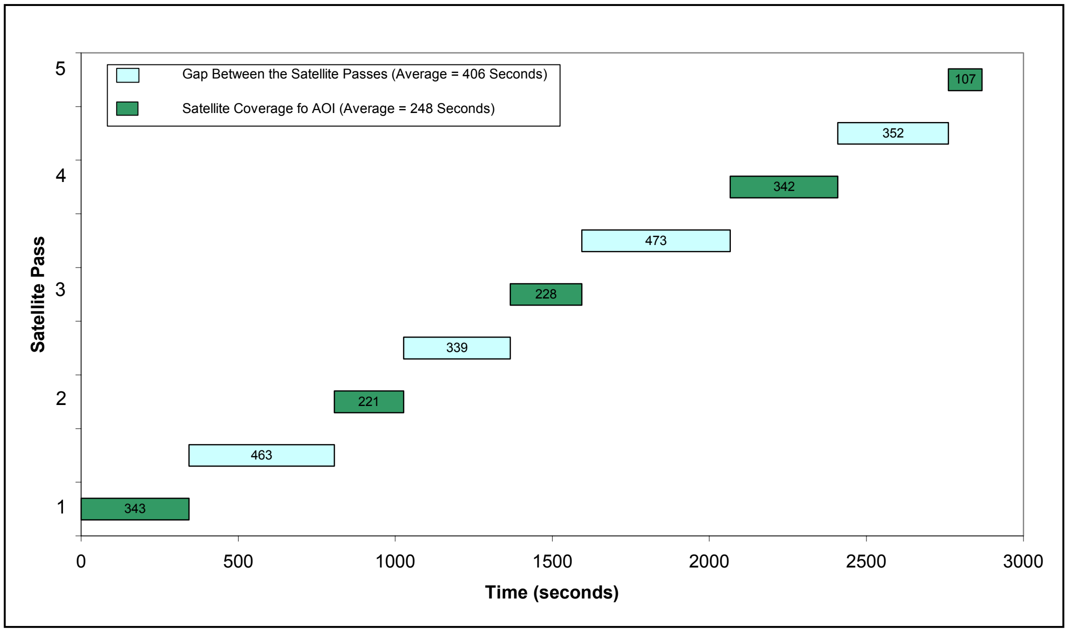

Figure 5 Coverage Provided by SBR in Strong Resolve Exercise

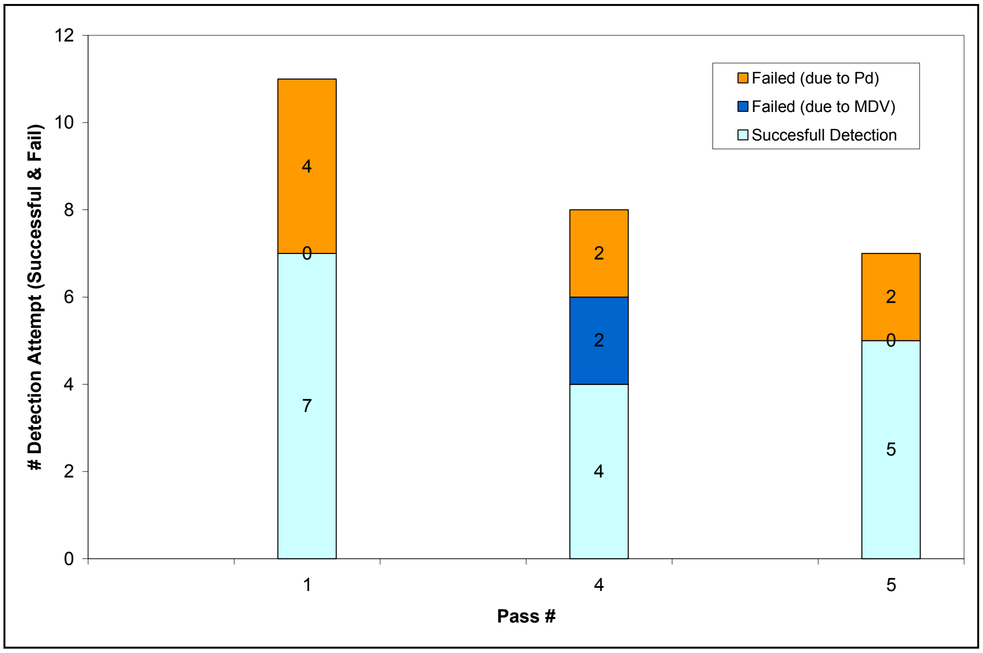

Figure 6 Detection Attempts by SBR in Strong Resolve 2002

Figure 7 shows the results from the second stage of the conflict in the AOI. Only four passes over the AOI with an average of 3.42 minutes per satellite pass has been shown. Figure 7 also shows that this concept can provide more frequent coverage over the AOI.

Figure 8 shows that there was more activity in the AOI than the day before. Therefore, SBR was able to detect more ground moving targets on this day, even though the average pass over the AOI was less than the day before. All the successful detections were broadcast to all other coalition nations exploitation workstations. This figure also shows that a large number of targets are moving at very low speed or they are not moving at all. The SBR Minimum Detective Velocity and the integration of detection reports into other ISR assets will be presented in more detail at in follow-on report.

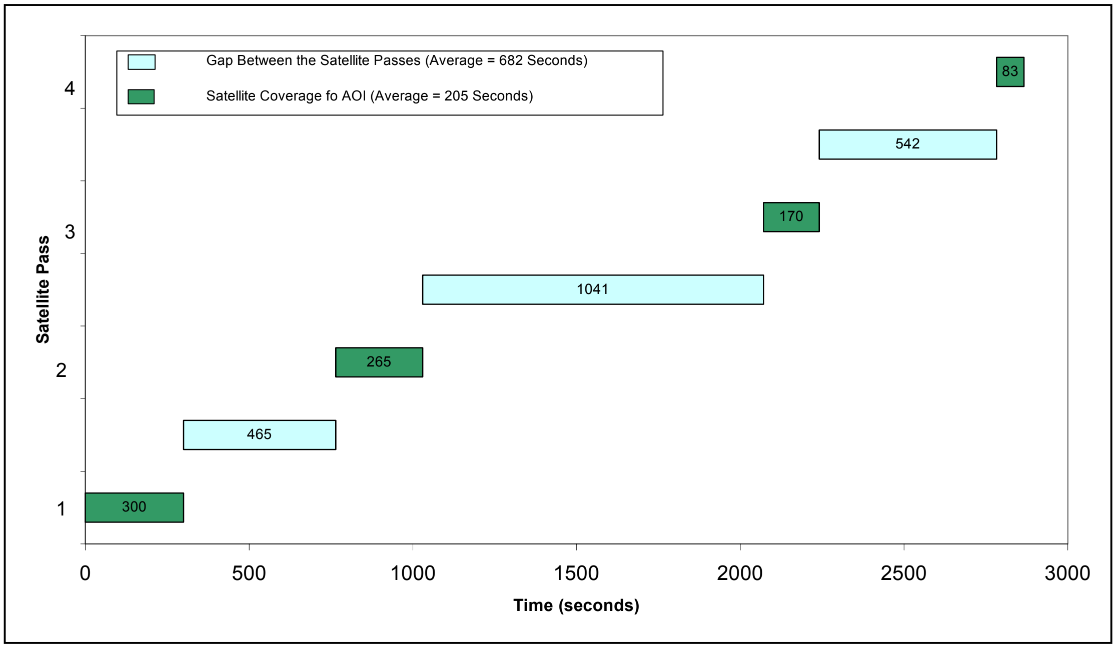

Figure 7 SBR Coverage for Strong Resolve Exercise

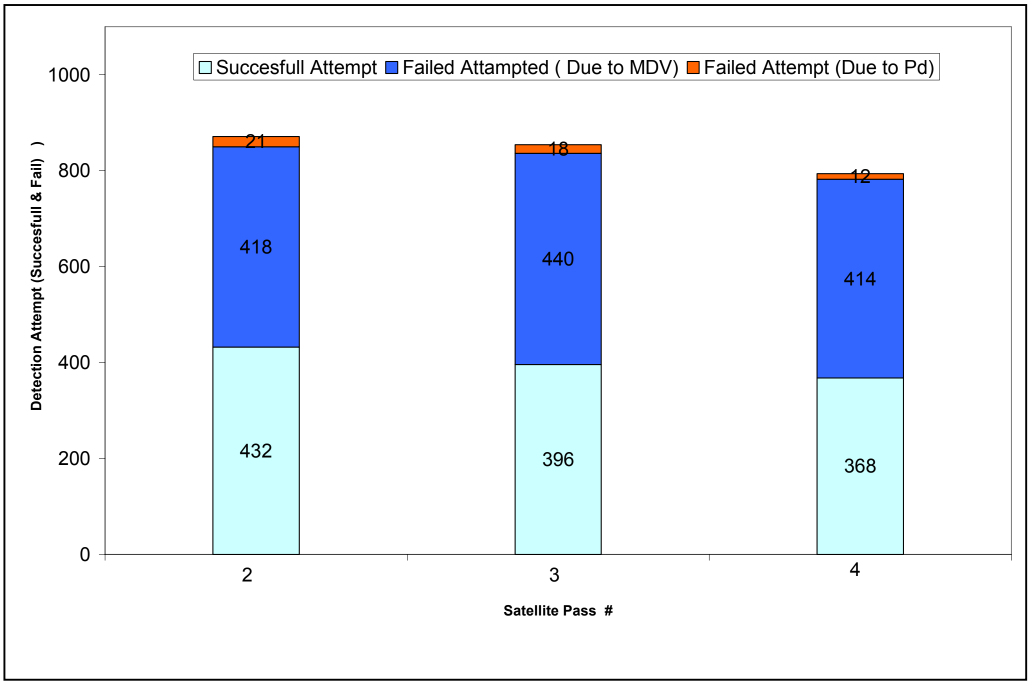

Figure 8 Detection Analysis of SBR

Figure 9 shows the single pass of the satellite when there were large amounts of activity in the AOI. As shown in the figure the SBR had over 1000 detection attempts in 303 seconds coverage, but only 358 of the these attempts where successful. Therefore, only 358 detection reports were broadcast through the CAESAR network to other coalition workstations. This shows that the SBR can handle a large number of target activities within the area of interest, but that the Minimum detectable velocity is still an issue for SBR.

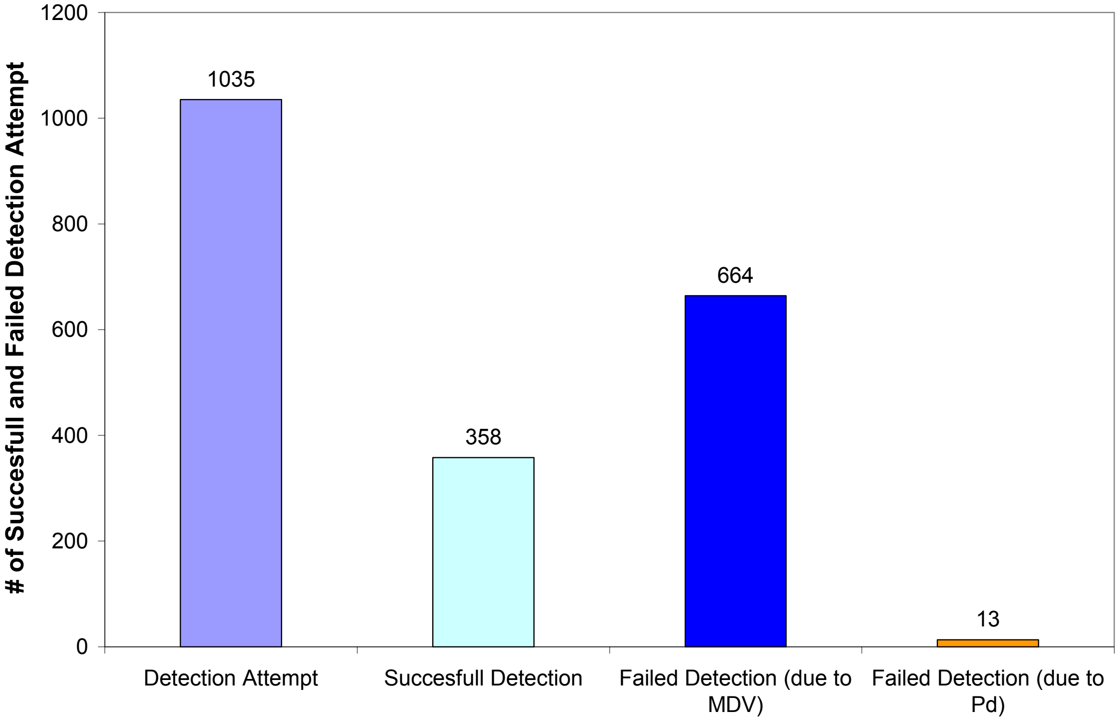

Figure 9 Detection Status for single pass 303 seconds

6. Conclusions and Recommendations

CAESAR was created to study and improve interoperability issues among coalition assets. This project has improved the common standard network protocols, formats and sharing of data to establish ideal interoperability among coalition assets. Interoperability allows the command and control centre of coalition forces to task surveillance assets with more accuracy and provides the ability to cue other sensors to complement each other.

Terrain Masking and vegetation screening have always caused problems for coalition force sensors; therefore with a robust surveillance network and application of sensor integration, most of these issues have been solved. A collection manager is able to task all the sensors more efficiently to help overcome terrain masking and screening problems.

Through this network and format standard, coalition exploitation workstations are able to receive and process sensor data from multi-national assets and are able to generate a common ground picture based on the integrated sensor data. Exploitation workstations are also able to generate more robust tracks on the targets based on the detection reports from the multiple sensors.

Space Based Radar was successfully integrated into the CAESAR network and was the first simulated space based radar sensor to provide GMTI data within CAESAR. SBR simulator (SIMLAB) was able to generate GMTI detection reports and broadcast them using the NATO EX format and network protocols. All the coalition exploitation workstations were able to receive the SBR data and integrate the GMTI information with other assets detection reports to generate a common ground picture. SBR improved the ISR Surveillance architecture by providing a capability for wide area search; deep looks behind enemy lines and the ability to complement other assets, when these other coalition assets were in a shadow area or off station.

NATO EX or other NATO STANAG protocols and formats also need to be upgraded continuously to accommodate the new sensors and exploitation workstations. Further investigation is required into the role of space-based radar in an ISR Architecture.

7. References

[1] Layman Paper – http://www.dodccrp.org/6thICCRTS/Cd/Tracks/Papers/Track3/113_tr3.pdf

[2] Multiresolution Modeling and Simulation with the High Level Architecture Martin Adelantado, Stéphane Bonnet, Pierre Siron , 12e European Simulation Symposium, 28-30 September 2000, Hambourg, Germany

[3] R. Jassemi-Zargani, B. Preiss, Modelling and Simulation Analysis of Concept Alpha (TTRDP) Constellation Design, DREO Technical Memoranda, DREO TM 2000-100, November 2000, 35 pages.

[4] Institute of Electrical and Electronics Engineers, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

[5] http://www.faqs.org/rfcs

[6] Lenk, Peter J., "Formats For The Representation of Alliance Ground Surveillance (AGS) Pre-Exploitation Data Types – Version 2.01", NATO C3 Agency Technical Note 732, October 1998.

[7] Concept Alpha Team, Concept Alpha Description and Performance, TTRDP Report, March 2000

[8] http://www.space.gc.ca/asc/eng/csa_sectors/earth/radarsat2/inf_tech.asp

[9] Simlab Documentation, DRDC Ottawa

[10] Ross, Joseph, "The Coalition Aerial Surveillance and Reconnaissance (CAESAR) Approach to Enhancing the Interoperability of Coalition Ground Surveillance Systems" NATO C3 Agency Technical.

[11] Strong Resolve Lessons Learned Final Report CCSD-CAESAR-11, Modified: 8/29/2002, Strong Resolve Evaluation Team

[12] RFC 768 User Datagram Protocol, Postel J. August 1980

[13] Institute of Electrical and Electronics Engineers, IEEE Standard for Distributed Interactive Simulation – Application Protocols IEEE 1278.1 95, New York, NY: 1995.

List of symbols/abbreviations/acronyms/initialisms

DND	Department of National Defence
AGS	Alliance Ground Surveillance
AOI	Area Of Interest
ARPA	Advanced Research Projects Agency
ART	Average Revisit Time
ACR	Area Coverage Rate
C2	Command and Control
CAESAR	Coalition Aerial Surveillance and Reconnaissance
CF	Canadian Forces
CGP	Common Ground Picture
CONOPS	Concept of Operation
CORBA	Common Object Request Broker Architecture
CSD	Common Shared Database
DIS	Distributed Interactive Simulation
DII COE	Defence Information Infrastructure Common Operating Environment
DRDC	Defence Research and Development Canada
EX	NATO AGS Pre-exploitation data format
FOV	Field of View
GMTI	Ground Moving Target Indicator
HFSWR	High Frequency Short Wave Radar

HLA	High Level Architecture
ICC	Integrated Command and Control
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISR	Intelligence, Surveillance and Reconnaissance
MDV	Minimum Detectable Velocity
MOE	Measurement of Effectiveness
MOP	Measurement of Performance
MTE	Moving Target Exploitation
MTI	Moving Target Indicator
NACT	NATO AGS Capability Testbed
NATO	North Atlantic Treaty Organisation
NC3A	NATO Consultation, Command and Control Agency
ONERA	Office National d'Etudes et de Recherches Aerospatiales
RSR	Radar Service Request
SAR	Synthetic Aperture Radar
SBIR	Space Based Infra-Red
SBR	Space-Based Radar
SBS	Space-Based Surveillance
SEW	Shared Early Warning
SHAPE	Supreme Headquarters Allied Forces Europe
SIMNET	Simulation Network
SIMLAB	Simulation Laboratory
SSR	Secondary Survellance Radar

RAP	Recognized Air Picture
TCP	Transmission Control Protocol
TMD	Theater Missle Defence
TRAN	Target Refinement and Nominations
TTP	Tactics, Techniques and Procedures
TTRDP	Tri-Lateral Technology Research and Development Program
UDP	User Datagram Protocol

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa,
Ottawa, Ontario, K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Integration of Space Based Radar in The Coalition assets Surveillance Architecture - Interoperability (U)

4. AUTHORS (Last name, first name, middle initial)

Jassemi-Zargani, Rahim; DiNardo, George

5. DATE OF PUBLICATION (month and year of publication of document)

December 2003

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

36

6b. NO. OF REFS (total cited in document)

13

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

DRDC Ottawa, 3701 Carling Avenue, Ottawa, Ontario, K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15eo13

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC Ottawa TM 2003-236

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

The Intelligence, Surveillance and Reconnaissance (ISR) sensors have been playing an important role in war for many years and rapid advances in technology have significantly improved the operational capability of coalition military activities. Because of these advances, command and control centres receive large amounts of strategic and tactical level information from ISR assets in real-time. Therefore coalition forces are able to plan their campaigns and task their assets with more accuracy and timeliness.

Information superiority gives a great advantage to coalition forces, as we have witnessed in recent years, but managing all these ISR assets and information is not an easy task and it has raised challenges for coalition forces. Therefore, coalition countries are very interested in finding a solution to these problems. Interoperability between ISR assets and other coalition command and control centers, handling the collected information, and processing the collected information before sending it to upper level decision makers are a few of the problems identified for solution by the coalition.

In 1999, the Coalition Aerial Surveillance and Reconnaissance (CAESAR) project was started with the membership of seven nations, Canada, France, Germany, Italy, Norway, the United Kingdom and the United States to investigate the problems of interoperability between sensor assets and a single Common Ground Picture (CGP).

This report will not only illustrate the issues of interoperability and the solutions that CAESAR provides, it will also explain how a Space Based Radar sensor may be integrated into this surveillance architecture and provide valuable information to coalition forces. Canada contributed a Space Based Radar simulator to CAESAR project, to evaluate how SBR can be interoperable with coalition assets. Additional details of the role of SBR in an ISR surveillance architecture, and the related results and analysis will be presented in follow-on report.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Interoperability, Sensor Fusion, Intelligence, Surveillance, Reconnaissance