Observations on the Dissemination of ISR Data Employing Network-Enabled Capabilities in the Coalition Environment

A paper submitted for the Coalition Interoperability Track of the Command and Control Research and Technology Symposium

John Mahaffey (Author, Point of Contact)
Trond Skaar (Co-Author)
NATO Consultation, Command and Control Agency, The Hague
PO Box 174
2501 CD The Hague
Netherlands

Observations on the Dissemination of ISR Data Employing Network-Enabled Capabilities in the Coalition Environment

John Mahaffey (Author, Point of Contact)
Trond Skaar (Co-Author)
NATO Consultation, Command and Control Agency, The Hague
PO Box 174
2501 CD The Hague
Netherlands

> ***The commander must work in a medium which his eyes cannot see, which his best deductive powers cannot always fathom, and with which, because of constant changes, he can rarely become familiar.***
>
> **Carl von Clausewitz**
> **On War**

Abstract

Intelligence Surveillance and Reconnaissance (ISR) systems provide key capabilities to the coalition and national command authorities for intelligence collection, exploitation and battle management. ISR systems support the full range of component commanders at all levels of command. Further, both coalition and national command authorities may employ exploited and pre-exploited ISR information in the development of politico-military options for military and civil operations within an area of operations (AO). As a result, ISR information provides a critical piece of information for both military commanders and their civilian counterparts operating in the same AO and will likely be in demand for contingency operations from disaster relief to military conflict. This paper will present the key findings of experimentation employing network enabled databases and ISR management tools for dissemination of ISR data and information. Subjects to be addressed include but are not limited to information security and cross domain data transfer, network resource allocation and tools provided for review and minimization of bandwidth requirements, tasking and management of ISR systems by end users outside of traditional networks, communications capabilities and limitations realized through collaboration functions and web enabled applications as well as ISR command and control in an open network of multiple end users.

Keywords

Command and Control, C2, Coalition, Collaborative Tools, Intelligence Surveillance and Reconnaissance, ISR, Network Centric, Network Enabled, Security Theatre Collection Management, TCM, Time Sensitive Targeting, TST,

Introduction

In a Combined Air Operations Centre (CAOC) in Northern Europe, a Time Sensitive Targeting (TST) Cell has assumed responsibility of a peace enforcement operation in West Africa. As a concept of “reach-back”, the Northern European CAOC will be required to process incoming command and control (C2), targeting and intelligence information, then disseminate targeting decisions in near real time (NRT) to deployed commanders in the field. The fleeting nature of TSTs means that this process must be completed in minutes, not hours or days.

To accomplish this, the CAOC TST Cell requires reliable, accurate and actionable information. This information required by the TST Cell will include but not be limited to raw or pre-exploited data from Intelligence Surveillance and Reconnaissance (ISR) systems operating in the area of operations (AO), C2 direction from the Joint/Combined Joint Forces Commander (JFC/CJTF), and weaponeering, targeting information from subordinate units in the AO. The TST Cell in turn disseminates targeting results and recommendations to the JFC/CJTF and C2 direction to subordinate commanders. In essence, the TST Cell, physically removed from the AO, must act as if it is right there; in the AO with commanders in the field and at the Joint Headquarters with the JFC/CJTF. Information then is the critical component to success.

This can be accomplished a myriad of ways; local and wide area networks (LAN/WAN), tactical data links, web enabled data bases as well as simple radio and satellite telecommunications provide much of this capability today. Unfortunately, implementation of these capabilities is imperfect; especially in the area of coalition operations. Interoperability, the key component of a network, is often degraded and potentially lost to the asymmetrical implementation of technical and operational standards by a coalition of forces and nations. In other words, coalition systems may be speaking the same language, but cannot fully understand each other.

But the mission must continue, fully integrated or not. The TST cell will support the CJTF and subordinate commanders, coalition ISR forces will participate in the operation and commanders in the AO still need information and direction. The challenge then, is to provide support with the systems provided with a minimum of technical and operational modification. So how does the commander make the system work? What can the commander do to provide required information from systems at the tactical level through the operational level to the strategic levels of today’s war-fighter? One answer lies in the development capabilities for the retrieval, storage, exploitation and dissemination of ISR data and information through network enabled databases as well as on-line ISR management and collaborative tools.

Capabilities based in part on network centric technologies provide one solution to the problem. These technologies include but are not limited to network-enabled databases, system management applications and collaborative tools. An example of this capability is the multinational Coalition Aerial Surveillance and Reconnaissance (CAESAR) Project. The

CAESAR project is comprised of Aerospace Ground Surveillance and Reconnaissance (AGS&R) ISR systems from seven NATO nations. The project, underway since 2001, has successfully developed and validated capabilities for the dissemination of ISR data and information over multiple channels. These channels include information broadcast on local and wide area networks, tactical data link, instant messaging and storage/retrieval from web-enabled data bases. CAESAR ISR data and information includes ground moving target indicator (GMTI) data, synthetic aperture radar (SAR) and photographic imagery, link 16 "J" series messages and textual reports. This data is available to the end-user both near real time and archived. The focus of this paper is on the development and validation of web enabled technologies for the management of and the collection and dissemination of this ISR data and information.

This paper will present the key findings of experimentation employing a capability developed during the CAESAR project called CAESAR Shared Data (CSD) as a web-enabled database and theatre collection management (TCM) tool for dissemination of ISR data and information. This paper will also provide details on the development of the CSD as a network enabled capability for coalition ISR operations. Subjects to be addressed include but are not limited to information security and cross domain data transfer, TCM and collaborative tools as well as integration of ISR data, information and sensors for the common operating picture (COP) for commanders both within and outside of the dedicated ISR network.

Intelligence Surveillance and Reconnaissance (ISR) systems provide key capabilities to the coalition and national command authorities for intelligence collection, exploitation and battle management. ISR systems support the full range of component commanders at all levels of command. Further, both coalition and national command authorities may employ exploited and pre-exploited ISR information in the development of politico-military options for military and civil operations within AO. For example, imagery from infrared imaging systems may be used by military commanders for the targeting of vehicles in hostile area and by their civilian counterparts to locate refugees hiding in rugged terrain as part of disaster relief operations. As a result, ISR information provides a critical piece of information for both military commanders and their civilian counterparts operating in the same AOR and will likely be in demand for contingency operations from disaster relief to military conflict.

The ISR system of systems provides NRT information to the intelligence staff via dedicated ground stations and/or voice and data links. This information may include data or information that is correlated with on-board and/or off-board intelligence information. Additionally, information that has been exploited and/or fused with intelligence information may also be provided through suitably equipped exploitation stations. Commanders without direct access to the ISR ground exploitation stations may obtain information in the form of Link-16 ground or air tracks or textual messages relayed via voice, facsimile and/or electronic media such as e-mail and other Internet Protocol (IP) based protocols. In this case, the data link and/or textual report serve as a surrogate for the actual ISR data and information [CAESAR TTP, 5.3, 2005]. This in turn provides opportunities for the employment of a multilayered approach to C2ISR architecture development.

There are however, challenges associated with retrieving, exploiting and disseminating ISR data and information. For one, because most current and near term ISR systems are nationally owned and operated, dissemination of their information is often limited by national infrastructure and security restrictions. Many ISR systems rely upon an infrastructure of sensors and dedicated ground stations that are both complex and expensive to operate.

National information security requirements further restrict direct access to ISR data and information. This is especially true of coalition operations where multiple national forces may support operations under a central command. So this is the primary challenge; how to provide coalition commanders and civilian authorities access to near real time and archived ISR data and information for military and humanitarian operations within the AO.

ISR Operations and Management

Within a CJTF, the demand for ISR data and information generally outstrips the available resources. For this reason, those ISR assets declared to the coalition are generally under the overall control of the CJTF intelligence directorate (J2). The J2 will normally provide prioritization and validation for all ISR collection requirements through the collection coordination intelligence requirements management (CCIRM) process. The CCIRM cell will prioritize and resolve conflicting requirements in accordance with CJTF Direction & Guidance, as well as assign requirements to appropriate ISR asset(s) or, in the case of requirements that can not be satisfied with available assets, assign them to a higher HQ. In order to be effective the ISR architecture must be flexible enough to accommodate NRT modifications to planned collection and exploitation requirements [Ross, 2003]. Note however, that within the coalition, a number of national ISR systems will remain solely in the hands of their national commanders. This is especially true for the smaller ISR systems attached to units below the component level. Some examples of these assets include the Canadian Sperver Tactical Uninhabited Aerial Vehicle (UAV) and Coyote ground surveillance systems. While these systems remain under their national command, their data and information may be provided to a wider group of commanders and components through network centric data bases and data links.

The ISR architecture developed to support a coalition operation should further be both technically and operationally flexible enough to incorporate new ISR assets as they become available and to compensate for the losses of ISR assets due to technical, operational and political reasons. In order to provide this capability the ISR architecture must set specific baselines for technical and procedural entry into the network. These baselines include common data formats (data and text) and common operational procedures (i.e. Tactics Techniques and Procedures [TTPs]) [Ross, 2003]. The employment of network enabled databases employing common data formats may provide additional interoperability where systems are not capable of joining the dedicated ISR network directly.

Network Enabled Databases

Coalition ISR dissemination is complicated by a host of issues. These include but are not limited to non-interoperable systems, irregular levels of system and procedure implementation across coalition partners as well as national and coalition security restrictions. In order to be effective, multinational intelligence architecture must be planned and established for every multinational operation in order to unite the national intelligence cells of participating coalition members in a common effort. This can be accomplished through the employment of coalition LAN/WANs using systems such as Battlefield Information Collection and Exploitation System (BICES) and Combined Enterprise Regional Information Exchange System (CENTRIXS) [JP 2-01, 2004]. Where these systems are unavailable for technical and operational reasons, a dedicated network may be established for specific operations.

Databases resident on these networks may provide systems with both connectivity and authority to access and download ISR data and information.

This is however, not without cost. CAESAR systems like most NRT capable ISR systems require a complex and expensive infrastructure of dedicated ground data stations in order to collect, analyze, exploit and disseminate the data and information collected by their sensors. Exploitation and dissemination of this data and information is a critical component to time sensitive operations.

To address some of these problems, the CAESAR project created the Coalition Shared Database (CSD) in order to reach a larger number of commanders and end-users. The CSD provides users with a single interface through which they can search for Link 16 tracks, GMTI, SAR and other imagery as well as products based upon exploited data. Data produced by the CAESAR sensors and exploitation stations is gathered by the CSD, automatically tagged using metadata inherent in the data standards, and then stored in the database. This data is then available for search by time, geographic region, platform type, data type and other parameters [Kreitmair, 2005]. To further enhance interoperability the CSD metadata is attempted harmonised with the International Organization for Standardization (ISO) standards, especially the ISO 191xx series (standardization in the field of digital geographic information).

Net Enabled Database Employment - CSD

The CSD has been designed to provide the following capabilities relating to the availability and operational use of CAESAR data [SADP, 2005]:

- Members of the CAESAR community may use the CSD to initialize national system databases and complement their databases with information from other coalition members' systems.
- The CSD can be used by systems that have suffered communications failure or been offline for a period of time. It will allow these systems to return and catch up with missed data that has been captured by CAESAR assets during that time. In the same way, assuming sensor collection has continued during this time, the offline ground station may then publish their data to the CSD for others to access.
- The CSD supports the generation of the CAESAR Ground Picture (CGP). It will provide access to GMTI, SAR and other data to not only CAESAR participants, ranging from exploiter to consumer, and can also be available to other 'disadvantaged' users, users that cannot process the standard message formats used within CAESAR, through standard Web browser interface. It will also allow historical data to be accessed and used in support of other CAESAR program objectives.
- A key benefit of the CSD is it removes the reliance on the broadcast mechanism currently used within CAESAR to disseminate data. The transmission of imagery in this way puts a huge strain on the networks. The CSD provides a more efficient means to access only the imagery of interest, reducing image sizes by enabling requests for image 'chips' and providing subscription mechanisms to assist the user.

In order to ensure the widest distribution of the CSD capability, it has been web enabled. Currently, there are two methods by which systems access CSD Data: using a client fully integrated in the exploitation system (often called a "thick client") or a Web browser based client (often called a "thin client").

- A thick client is a software application on an exploitation workstation that allows the user to query all CSDs on the network without invoking a new application. This method allows the receiving application (i.e. C2 system) to query and receive ISR data seamlessly without the need for operator intervention. As a result, ISR data and information is fed automatically into the application for further exploitation and display.
- Thin client access comprises a stand-alone web browsing capability to query each CSD on the LAN/WAN individually for data and information. The workstation operator must request coalition J-6/G-6 or the individual CSD administrator for the uniform resource locator (URL) of the CSD when using the thin client. The thin client allows any authorized PC to access and visualize ISR data and information that has been uploaded to any CSD on the requisite network.

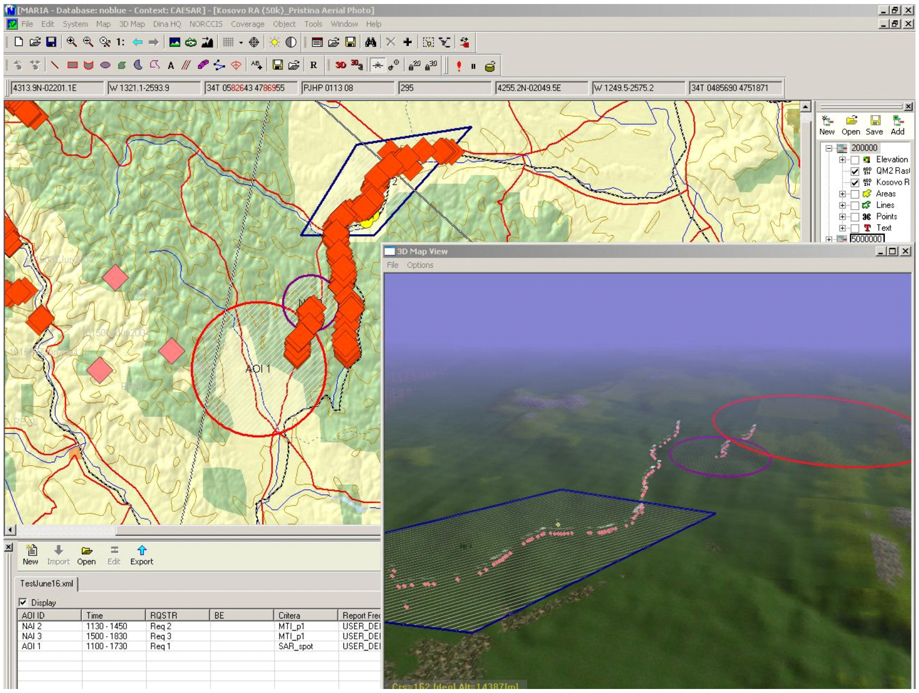
There are two basic mechanisms to retrieve the data; query or subscription. Workstation operators can retrieve ISR data and information from the CSD using the query mechanism. The query mechanism allows the operator to specify search criteria such as time and geo-location for moving target indicator (MTI), imagery, tracks and supporting data. Supporting data criteria are product dependant such as filtering on a single sensors collection plan. The subscription mechanism allows the workstation operator to subscribe to the CSD based upon his search criteria. Once subscribed, the user will either be notified that data is available or the data will be automatically forwarded to the user depending on user subscription selection.

Theatre Collection Management Tools

The CSD was initially designed as an ISR data archive resident on ground and exploitation stations within the CAESAR network. As shown previously, the CSD collects, archives and disseminates ISR data and information to other systems on a specific network. This in turn has enabled a wider array of commanders and staffs to access both NRT and archived ISR data and information. The result is an expanding need for this information at command and exploitation nodes both inside and outside of the traditional ISR network. This in turn complicates the management of an already complex the ISR system of systems.

The requirement for a dedicated ISR manager was realized during Strong Resolve 2002. ISR assets provided to SR 2002 included an US Air Force E-8C Joint STARS, a French Army HORIZON and the Canadian RADARSAT. The E-8C was assigned to the J2 through the Joint Forces Air Component Commander (JFACC). The HORIZON was assigned to the Allied Mobile Force – Light (AMF-L) G2 and the RADARSAT remained a national asset receiving tasking from the J2 through a Canadian Liaison Team. The mission of the ISR manager was to review and coordinate requests for information (RFIs) then translate them to individual collection requirements for each ISR system. This position was required to ensure ISR collection requirements were correctly assigned and to ensure that CJTF approved objectives for collection and targeting were met. Within NATO this position is currently held by the Theatre Collection Manager.

The TCM task was complicating by the lack of automated connectivity between the theatre collection manager at the J2 and individual commanders and ISR systems in the field. In order to assist the TCM with ISR management capabilities, dedicated TCM tools were developed. Currently implemented TCM tools provide the ability to manage ISR system collection requirements during the planning and execution process. These include real time management of ISR system collection plans, orbits and planning functions such as terrain or route screening. Figure 1 depicts the integration of NRT Link 16 tracks and the current ISR collection plan on the Norwegian Command and Control Information System (NORCCIS). Note that the ISR information displayed is being uploaded to a resident CSD before being integrated into the NORCCIS common operating picture (COP). Employing the CSD on the NORCCIS, the TCM can visualize current ISR data and information in relation to an ISR system's collection requirements. Using this information and the resident TCM tolls, the TCM can then maximize the ISR system's capability to provide information to the supported commander by modifying or adding ISR system collection requirements.


[MARIA - Database: noblue - Context: CAESAR] - [Kosovo RA (50k)_Pristina Aerial Photo]

4313.9N-02201.1E | W 1321.1-2593.9 | 34T 0582643 4786955 | PJHP 0113 08 | 295 | 4255.2N-02049.5E | W 1249.5-2575.2 | 34T 0485690 4751871

TestJune16.xml

☑ Display

AOI ID	Time	RQSTR	BE	Critera	Report Fre
NAI 2	1130 - 1450	Req 2		MTI_p1	USER_DEI
NAI 3	1500 - 1830	Req 3		MTI_p1	USER_DEI
AOI 1	1100 - 1730	Req 1		SAR_spot	USER_DEI

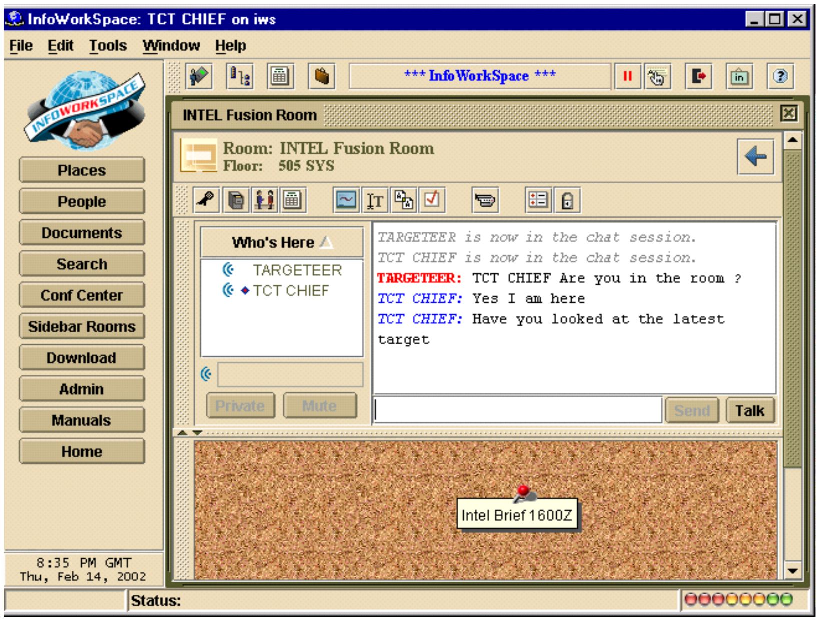
File Edit System Map 3D Map Dina HQ NORCCIS Coverage Object Tools Window Help
New Open Save Add
200000
Elevation
QM2 Rast
Kosovo R
Areas
Lines
Points
Text
5000000
AOI 1
3D Map View
File Options
New Import Open Edit Export

Figure 1 NORCCIS Integration of ISR Collection Plan and Link 16 Tracks

Collaborative Tools

Experience with time sensitive operations such as TST has revealed the need for a robust set of collaborative tools for employment within a network centric environment. These tools provide the commander with rapid, accurate access to multiple sources of information. Within a network, these tools may provide the ability to coordinate directly between numerous databases such as intelligence, targeting, weaponeering and C2. New Web-based tools such as secure "chat rooms" for coordination and information sharing, video teleconferencing for command and control, and e-mail for coordination and tasking, are combat-tested in operations in the Balkans [AFDD 2-5, 2002], Afghanistan and Iraq. These tools should be able to coordinate with multiple agencies, commands and staffs in real time over a common network.

One collaborative tool that shows great promise for the employment of ISR data and information across a network is *chat* or Instant Messaging (IM). Using IM, a supported commander can coordinate with one, several or all of the agencies and commanders managing the ISR system. This is especially evident in area of TST and other time sensitive operations such as Theatre Missile Defence (TMD) and Suppression of Enemy Air Defences (SEAD). IM provides a dedicated medium for real time coordination and collaboration similar to a dedicated radio frequency. Instant messaging is also similar to e-mail, but differs from email in that its primary focus is **immediate** end-user delivery. Figure 2 depicts IM capabilities with the ability to post messages and arrange meetings for specific users.



TARGETEER is now in the chat session.
TCT CHIEF is now in the chat session.
TARGETEER: TCT CHIEF Are you in the room ?
TCT CHIEF: Yes I am here
TCT CHIEF: Have you looked at the latest target

Figure 2 Collaborative Tools - IM

The CAESAR Technical Interoperability Experiment (TIE) 2004 provided the first opportunity to implement and use a IM capability between individual systems across a network. The IM capability used was Jabber, a widely used IM protocol that has been approved by the Internet Engineering Task Force (IETF) to become an Internet standard. Jabber allows real time communications through IM capabilities and interactive management of ISR systems. These capabilities provided collection management and direct communications with ISR systems resident on the network. Jabber supported theatre level track management as well as ISR system management through the rapid dispersal of sensor service requests from commanders to their ISR systems directly, During TIE 2004, ISR workstation operators were extremely enthusiastic about using instant messaging as a means of communication with other workstations and CAESAR participants. They would like to see this technology further implemented in future exercises/experiment [Lee, 2004].

IM provided excellent opportunities for coordination and collaboration for the employment of ISR systems. However, like all media, there were problems. Like a radio frequency, IM may become overloaded with users, causing confusion and reducing the ability of the commander to coordinate quickly and effectively. Further, it can be used to transfer files and URLs to files to a large population of network systems. For example, transfer of a URL to a 1 MB file to 50 subscribers on the network could result in the sudden movement of 50 MB of data on the LAN/WAN. This would in many cases, cause the network to become overloaded, thereby reducing or eliminating critical ISR data and information already on the network. The solution to this problem lies with the implementation of operational and technical procedures to manage IM participation. Using the above example, an IM message notifying all 50 users that information is available for review at a specific data base would allow the users to first decide if they need the information, then to review it before downloading. This would serve to self-limit the amount of data and information moving throughout the network in response to IM announcements. It should also be noted that usage of caching mechanisms could reduce the total WAN transmissions, and hence limit this problem.

Employment of IM can function as an enabler for reducing the bandwidth requirements by pointing operators to the CSD for new data and information. Another mechanism for achieving operator notification of new data and information in the CSD is to use the inherent subscription and notification capability in the CSD interface. Through notification mechanisms the systems adopted a “pull” versus “push” concept for large imagery files such as SAR. Previously large images being “pushed” though the network exceeded the available bandwidth. By using IM or the inherent notification mechanism to alert system operators that new imagery was available on the CSD, the operators could go to the CSD, view thumbnails of the imagery and decide if any of the imagery was needed. Other IM based ISR management functions included the ability to send a sensor service request (SSR) and system reports such as joining reports, mission reports and the Size Activity, Location and Time (SALT) report. By employing IM for these functions, the opportunities for receipt and acknowledgment of system requests and direction provided increased efficiency in the overall management of the ISR system [Mahaffey, 2005].

There are a number of other collaborative tools required for successful collaboration. Currently there is an effort to develop a coalition collaborative tool for TST. This tool, based upon the NATO Joint Targeting System (JTS) will integrate ISR data and information from the CSD, targeting information from the JTS, C2 information from the NATO Integrated Command and Control (ICC) for Air Operations System as well as nationally provided data bases on weaponeering, collateral damage and other national capabilities. Each of the aforementioned databases provides critical input to the collaborative process.

United States Forces Korea (USFK) has developed a web-based TST site capability primarily designed to post TSTs, their prosecution status, and battle damage assessment (BDA). This web site also provides a central location containing links to battle rhythm related data, commander’s guidance, and legacy electronic documentation. This capability provides NRT information to the theater’s targeting positions and cells. All TST-related positions can access the TST web site via the web browser using a number of C2 and targeting applications. These include the Joint Targeting Toolbox (JTT) and the Global Command and Control System (GCCS) [JWC, 2002].

Another collaborative tool under development is the US Air Force/Central Command Network-Centric Collaborative Targeting (NCCT) advanced concept technology demonstration (ACTD) aims to integrate ISR sensors (Joint STARS, AWACS, Rivet Joint and others including UAVs) to produce a common picture of the air battle space with the focus including the timely detection of time-critical targets. NCCT seeks to obtain the synergistic sum of the individual system’s intelligence-gathering capabilities. It is not dissimilar in concept to the Navy’s Cooperative Engagement Capability (CEC) venture [Pustam, 2004]

Security

For most ISR systems, security is often the defining issue on the sharing of data and information within a coalition. The coalition network may be comprised of a number of coalition and national networks, or security domains. These domains are designed to ensure the protection of nationally secure information while allowing dissemination to authorized communication, command and intelligence nodes within a coalition network. Ideally, all coalition participants would operate on a single network, providing data and information to commanders and their staffs as required. Unfortunately, national security requirements often supersede coalition information requirements within a coalition. For this reason, it is important to provide controlled access to the coalition network. Or when that fails, provide rapid relay of required data and information from one network to another (i.e. "air-gapped").

During the Joint War-Fighter Interoperability Demonstration (JWID) 2004 CAESAR experimented with employment of the CSD as a method of ISR data and information dissemination to multiple commanders across two secure domains. During JWID 2004, ISR data was successfully disseminated between secure domains through the use of the Information Exchange Gateway (IEG). Through the use of the IEG, two separate CSD systems as well as other national and NATO web search and ISR exploitation applications (i.e. the Spanish search box web crawler and the German incident control and reporting utility system (ICARUS) and multinational intelligence centre (MNIC) ISR exploitation databases) were able to download and exploit data and meta-data across the security boundary between the red and the blue domains [Kreitmair, 2005]. This capability provides a potential solution to coalition cross domain data and information dissemination.

The Multilayered Network

Within the network, ISR data and information can be transmitted in NRT to suitably equipped and network enabled ground stations for processing and exploitation. Some systems broadcast this data to a large number of users, while others use point-to-point links to send the data to only one ground station. When correctly connected to a LAN/WAN, ground and exploitation stations may provide pre-exploited and exploited ISR data to air and ground based systems via Link-16 and network enabled data bases. Ground based exploitation systems with the capability to receive and exploit data from other systems may enhance or improve existing information through the use of advanced exploitation algorithms. Some exploitation systems and web-enabled databases also have the ability to interface with C2 systems. Select airborne and land based ISR systems also have on-board surveillance and exploitation capabilities. However, in order to properly exploit these capabilities the ISR system architect and/or TCM must find and exploit the least common denominator among the participating systems.

What is a common denominator? According to the Miriam Webster Dictionary, a common denominator is a common multiple of the denominators of a number of fractions. How does this relate to interoperability among C2 and ISR systems in a coalition? First, the common denominator among systems relates to those systems that are similar in capabilities and requirements. For example, Link 16 as a tactical data link provides the ability to transmit and receive commonly formatted messages between systems with common capabilities (i.e. Link 16). In order to transmit and receive this information, the participating systems must be capable of doing so. In other words, if the Link 16 implementation on system A is not the same as system B, the results will be something less than fully interoperable.

Given the differences in systems, implementation, doctrine, funding and a host of other requirements, C2ISR systems obviously face a number of hurdles in becoming fully interoperable. This in turn leads us to the next question. Given a requirement for coalition participation in a CJTF operation, how can the commander integrate all of the available systems? The answer lays with the least common denominator. According to the same dictionary, the least common denominator is the least common multiple of two or more denominators. In an integrated system this means that each participating system must have some capability common with the whole network. Essentially, there must be a way for each system to talk to every other system on the network. For example, if system A cannot receive and exploit system B's Link 16 ground track, a work around may be arranged through transmit of the track information across a secure radio frequency or through free text messaging on an IM application. As a result, it is highly likely that the ISR network will be resident on systems that are interoperable on multiple layers.

In other words, ISR data and information will be moving along networks supported by the LAN/WAN, tactical data link, voice and data telecommunications and even potentially, by personal runner. For this reason, the over all ISR network should be both flexible and redundant at critical nodes such as the TST cell.

The Multilayered Network – the WAN/LAN

The 21st century war-fighter has access to multiple networks. These networks include the traditional WAN/LAN that exists at most commands. These networks include but are not limited to CRONOS, SIPRNET, CENTRIX and BICES. If dedicated secure networks are not already in place, they can be created through the use of telecommunications internal to the command. This can be done by building and/or contracting dedicated communications architecture and providing secure crypto capabilities at the transmitting and receiving nodes. Given enough bandwidth and security, the coalition LAN/WAN may provide access to the dissemination of ISR data and information through standard ISR workstations. In this case, raw or pre-exploited data and information may be made available from the ISR system to a larger group of commanders for analysis and exploitation [Mahaffey, 2005].

Because bandwidth is a finite resource operational and technical procedures should be applied to promote the optimal usage the network. These procedures should be based upon the commander's requirements and should provide prioritization for data and information dissemination according to operational need. For example, dissemination of Link 16 tracks and GMTI use smaller amounts of bandwidth on the network. Imagery on the other hand may use significant amounts of bandwidth for fairly small products [Mahaffey, 2005]. By establishing priorities for ISR data dissemination, the commander, through the TCM can ensure that priority operations such as TST may be executed without the loss of ISR data due to limited bandwidth. This certainly does not diminish the need for imagery dissemination. The commander will likely need a full range of ISR data and information products for operations. This is where an NRT database such as the CSD excels. By storing the imagery in NRT, and providing an interface to download the imagery on request, the CSD provides the commander with the ability to manage both immediate and planned ISR requirements. Further, exploitation tools such as "image chipping" allow the commander the opportunity to choose what parts of the imagery are most critical to operations, further reducing bandwidth demands on the network.

Figures 3 and 4 provide examples of a detailed image and additional information that can be obtained from the search results. The example shows a search result that provides a thumbnail, an associated overview picture, and a set of metadata that describes the image: e.g. file title, URL address, the date when the image was acquired, geographic position information and a short annotation. The overview picture (1024*1024 pixels JPEG within an NSIF file) is only 270 kB in size, while the complete picture is about 56 MB. Based on the search results, the user can either view or download a selected file, or request a smaller "chip" of the image to be generated and provided by the CSD server, as shown in Figures 4 and 5. The chipping function reduces bandwidth requirements and increases access to desired information. Images are provided in STANAG 4545 (NSIF) format and GMTI data is provided as STANAG 4607 data [Kreitmair, 2004].

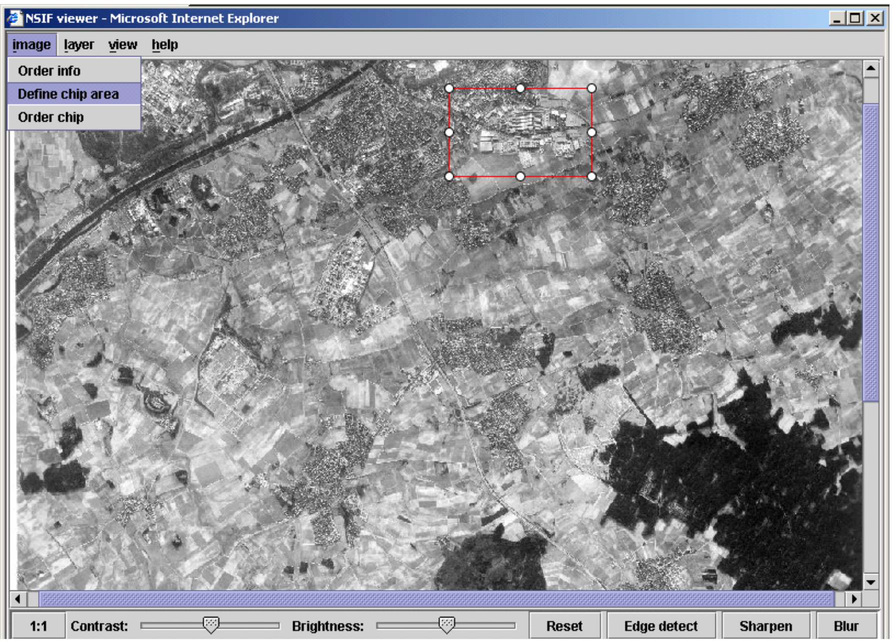


Figure 3 Definition of Chip Area

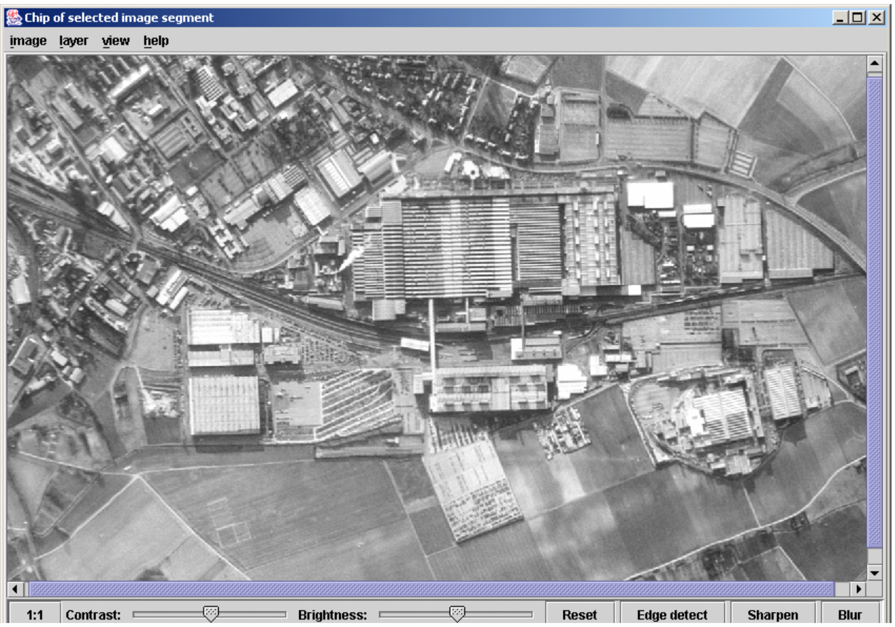


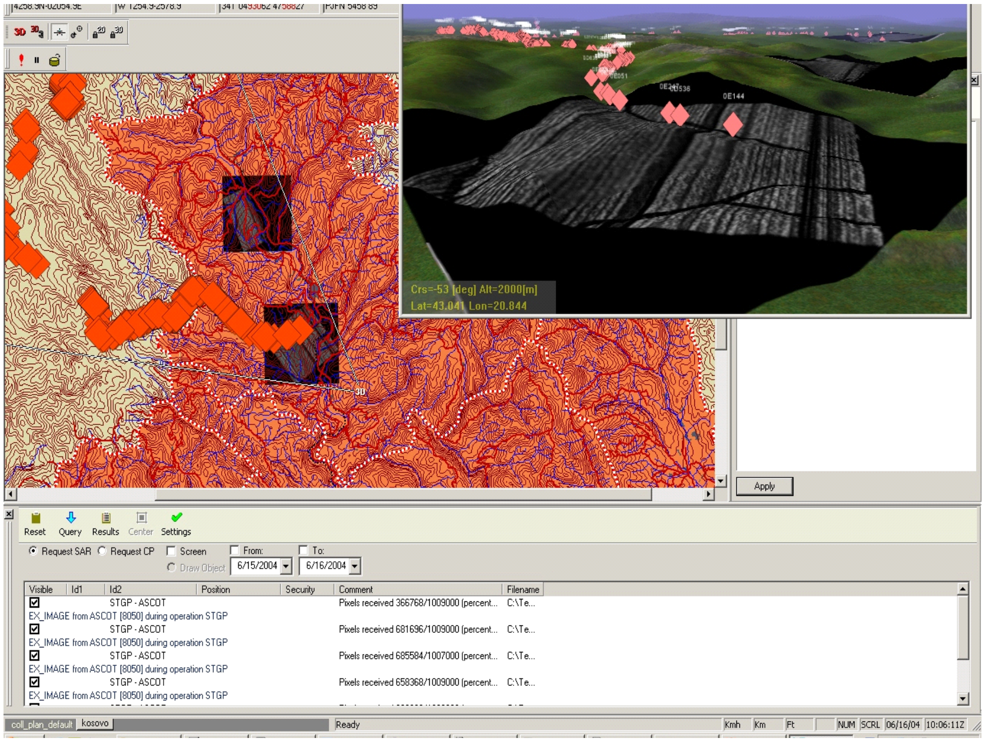
Figure 4 Chipped area

The chipped area is selected from the overview image and the CSD server will then generate a new NSIF image which will be delivered to the client. While the total image has a size of 56 MB, the selected area is only 0.95 MB [Kreitmair, 2004].

The Multilayered Network – Data Link

In some cases tactical data link may provide the only option for the dissemination of NRT ISR data and information to a wider network for many C2 and ISR systems. This is especially true for C2 information systems such as NORCCIS and ICC. As described earlier, tracks and points derived from ISR data may be employed as an ISR data surrogate. Figure 6 depicts link 16 tracks being forward told from a GMTI capable ISR system integrated into the NORCCIS COP together with synthetic aperture radar (SAR) imagery.

Like other ISR data and information, tactical data link data may be collected, archived and disseminated by ISR data bases. By cross-cueing archived and NRT tactical data link data with ISR imagery, data and information, the commander may provide a more accurate COP. The data depicted in Figure 6 is being downloaded from a CSD on the network. Using this picture, the commander can visualize current movement based upon NRT GMTI against archived imagery and geographic information system data.



● Request SAR ○ Request CP □ Screen □ From: 6/15/2004 □ To: 6/16/2004
○ Draw Object

Visible	Id1	Id2	Position	Security	Comment	Filename
☑		STGP - ASCOT			Pixels received 366768/1009000 (percent...	C:\Te...
EX_IMAGE from ASCOT [8050] during operation STGP						
☑		STGP - ASCOT			Pixels received 681696/1009000 (percent...	C:\Te...
EX_IMAGE from ASCOT [8050] during operation STGP						
☑		STGP - ASCOT			Pixels received 685584/1007000 (percent...	C:\Te...
EX_IMAGE from ASCOT [8050] during operation STGP						
☑		STGP - ASCOT			Pixels received 658368/1009000 (percent...	C:\Te...
EX_IMAGE from ASCOT [8050] during operation STGP						

coll_plan_default | kosovo | Ready | Kmh | Km | Ft | NUM | SCRL | 06/16/04 | 10:06:11Z

Figure 6 NORCCIS COP with Link 16 and SAR Imagery

This capability is not without some drawbacks. First, tactical data link track data is only as good as the system and/or the operator performing the tracking. This may provide significant limitations for targeting options against targets derived from ISR data and information and disseminated via tactical data link. For this reason track quality becomes a critical component in the exploitation of tactical data link as an ISR surrogate. A higher track quality should equate to a higher degree of accuracy for the track and the ISR data. Unfortunately, this may not be true. The higher track quality may only be an indication updates by the operator. This may or may not be accurate. As a result, a commander intending to engage a target based upon the J 3.5 track would be required to provide other more accurate methods of identification. Second, each system implements their tactical data link differently. At the technical level this may not seem a major problem if all that is needed is a simple track or point message. At the operational level however, it may cause a great deal of confusion. For example, implementation of the Link 16 J 3.5 ground track varies from system to system. The NATO E-3 AWACS may see a J 3.5 track from the E-8C Joint STARS with a recognizable track number, identity and track quality. An F-16 may see the same track as an icon but not the track number. This limits methods for the transfer of targeting data to the F-16 by the Joint STARS and/or the AWACS.

The Multilayered Network – Text

Text or voice networks provide the ability to work around integration and interoperability issues caused by network and/or system interoperability and integration non-compliance. These options include free text messaging via formal messages, e-mail and telecommunications including radio, telephone and facsimile [Mahaffey, 2005]. In some cases, text messaging may be the only method of data and information transfer for sensor system that is not resident on the network. For example, a Special Forces reconnaissance team may forward textual observations to the network via a PDA and a satellite communications system. These messages, like all other data in the database, should be registered with location, time and description. This will enable reports to provide additional information to the COP. If the team is unable to connect directly to the network, their text messages may be forwarded by a receiving station in the AO. In this example an E-3 AWACS may take the message via VHF radio and convert it to free text on the Link 16 network. The report is then be forwarded to a CAOC for entry into the COP.

Conclusion

Recent history provides assurance of the following assumptions: First, coalition operations are going be the norm, not the exception. Second, each operation, from conventional military operations to disaster relief requires accurate, reliable and actionable intelligence to be effective. Third, ISR systems will provide a large proportion of the NRT and archived data and information that comprises the intelligence, coalition commanders will require. Given these assumptions, the commander's ability to access ISR information, rapidly and reliably becomes a critical factor in the successful completion of the coalition mission. But as previously noted, there are problems associated with ISR data and information dissemination in the coalition environment. These include non-interoperable system integration, national and coalition security restrictions and the introduction of new and unfamiliar ISR systems and capabilities at multiple levels of command, across multiple components. As a result, the old J2 control of all ISR assets paradigm has been broken. What is required is a network centric view of the ISR system as a system of users (commanders), suppliers (sensors) and archives (databases). This network enabled ISR system of systems enables a wider array of commanders and staffs to retrieve, exploit and disseminate ISR data. These new systems and users drive increased requirements for management of ISR systems, both pre-planned and in real time. Network enabled capabilities such as the CSD provide support to these requirements.

Continued development of network-enabled applications such as the CSD for employment in multilayered network provide the basis for a network centric capability to retrieve and disseminate ISR data and information to the full range of commanders and staffs, regardless of data and information type, operational mission or network. Without these capabilities, ISR systems will inevitably fall into the old model of "stove-piped" systems thereby significantly reducing the utility and effectiveness of the ISR system as a whole.

References

[AFDD 2-5.2, 1999]
Air Force Doctrine Directive 2-5.2, Intelligence Surveillance and Reconnaissance Operations, 21 April 1999

[CAESAR TTP 5.3, 2004]
GMTI/SAR Capable ISTAR Tactics Techniques and Procedures, Operations Working Group, Version 5.3, July 23, 2004

[JP 2-01, 2004]
Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004

[JWC, 2002].
United States Joint Forces Command Joint Warfighting Center, Office of the Secretary of Defense, Joint Warfighters Joint Test and Evaluation, Commander's Handbook for Joint TST, 22 March 2002

[Kreitmair, 2004]
Kreitmair Thomas, Ross Joe, Dissemination of ISR data in the Coalition Aerial Surveillance and Reconnaissance (CAESAR): Results and the Way Ahead Command and Control Research and Technology Symposium, San Diego, June 2004

[Kreitmair,2005]
Kreitmair, Thomas, Hoekstra Wim, Mahaffey John, NC3A Technical Note 1044, Provision of Aerospace Ground Surveillance (AGS) Data to Operators, February 2005

[Lee, 2004]
The Coalition Aerial Surveillance and Reconnaissance (CAESAR) technical integration experiment 2004 (TIE04) lessons learnt report – Operations working group (OWG) perspective 4-15 October 2004

[Mahaffey 2004]
Mahaffey, J.L., "Observations in allocation and tasking of Joint Level Intelligence Surveillance and Reconnaissance (ISR) systems in support of Coalition Operations", Command and Control Research and Technology Symposium, San Diego, June 2004, NATO Unclassified

[Mahaffey, 2005].
Mahaffey, John L, Observations in the Dissemination of Intelligence Surveillance and Reconnaissance (ISR) Data and Information within a Coalition Environment DRAFT, March 2005

[Pustam, 2004]
Pustam, Anil, Networking Air Power; Military Aerospace Technology Online, Volume: 3 Issue: 1, Mar 06, 2004

[Ross, 2003]
Ross, Joseph, Lee, Paul, Kreitmair, Thomas, Mahaffey John, Technical Note 986, Proposed Overarching NATO Intelligence, Surveillance And Reconnaissance Architecture and its Relationship to The NATO Alliance Ground Surveillance Core Capability, (Revision 1) December 2003

[SADP, 2005]
GMTI/SAR Capable ISTAR System Architecture Design Principles (SADP), Architecture Development Working Group, Version 4.0 Draft A, February 14, 2005

Biography

John L Mahaffey is a Senior Scientist with the Command and Control Systems Division, NATO Consultation, Command and Control Agency, The Hague, The Netherlands. He provides operational concept analysis and system architecture development for the integration and interoperability programs for multinational C2 and ISR systems and applications.

Trond Skaar is a Senior Scientist with the Command and Control Systems Division, NATO Consultation, Command and Control Agency, The Hague, The Netherlands. He provides technical support to the development and implementation of network enabled database architectures and system applications for multinational C2 and ISR systems and applications.