13th ICCRTS: C2 for Complex Endeavors

"Information Management Processes in Support of Major Event Security"

Topic(s): Civil-Military Endeavors, Network-Centric Experimentation and Analysis

Author(s): Dr Dave Allen, Dr Renee Chow, Mr. Kevin Trinh and Dr Philip Farrell

Point of Contact: Dr Dave Allen

DRDC - Centre for Operational Research and Analysis

Canadian Forces Experimentation Centre

Shirley's Bay Campus, Bldg 4

3701 Carling Avenue

Ottawa, Ontario, K1A 0Z4

Phone: 613-990-7455

Email: Dave.Allen@drdc-rddc.gc.ca

Information Management Processes in Support of Major Event Security

Abstract

Modern threats to national security require a consolidated effort across many government agencies. In particular, to ensure the security for major public events, it is desirable to have an integrated security unit composed of staff from various agencies including: military, law enforcement (federal and provincial), as well as health and public safety agencies.

This paper looks at the information management processes required to support the operational centre of an integrated security unit. More specifically, the paper describes the set-up and analytical results obtained from an experiment designed to test specific information management processes. The considered information management processes were developed considering previous national major events as well as various relevant concept of operation documents. The effectiveness of the processes was assessed by measuring: the situation awareness of the individuals participating in the experiment, the level of information shared between the individuals, the quality of the outcomes of the processes and the time required to perform these processes.

Keywords: Interagency, information management, information sharing, business process design, situation awareness, public security, operational centre, command and control.

Introduction

In the past, national security was largely an issue of sovereignty over one's own territory. However, the threats to national security have broadened and now require a consolidated effort from many government agencies. This change requires a transformation of the military command and control structure to enable a seamless interoperability with other government departments and other partners and allied forces. Furthermore, effective information management processes are needed to support an efficient interoperability of the various agencies.

One approach to support a whole-of-government approach to the national security consists of setting-up an integrated security unit (ISU) composed of representatives from many government agencies. In 2006, the Canadian Forces Experimentation Centre set-up an experimental campaign to investigate the information management (IM) processes required to support the operational centre of an ISU. The precise scope of the campaign was focused on the operational centre of an ISU in charge of the public security during a major national event (international cultural or sporting events, G8 summit, etc.). Note that a similar study had been done by the Defence Research and Development Canada (DRDC) to investigate the information sharing processes within the Canadian Maritime Security Operational Centre, which is also composed of representatives from many government agencies (Smith and Carson 2006).

The experimental campaign was initiated by an architecture modeling of the information flow between various federal and provincial agencies involved in national security and public safety operations. This architectural work was done following the Department of Defense Architectural Framework (DoDAF) approach (see U.S. DoD 2004 for details). This work was based on information obtained through the interview of various subject matter experts. A constructive simulation of the operational centre of an ISU was then developed (Lachance and Miller 2007). The simulation model was built using ReThink™, a software application designed for business process modeling. This simulation tool was used to assess the effectiveness of specific IM processes required to support the information flow expected based on the architectural work. Resource requirements and the risk for specific task delay were assessed using the simulation model (Allen 2008). Finally, a human-in-the-loop experiment was set-up to both validate the designed IM processes and further assess their effectiveness.

This paper describes the data collection and analysis done in support of the human-in-the-loop experiment. The organizational structure of the operational centre of the ISU and the considered IM processes are described respectively in the next two sections. Following these sections, the next sections present the design of the human-in-the-loop experiment, the data analysis performed and the results obtained from the experiment. Finally, the last section provides the conclusion of the paper.

ISU Operational Centre Structure

Figure 1 displays the proposed organizational structure for the integrated security unit. The white and blue boxes correspond to staff positions while the yellow and green boxes display functional teams Since the focus is on the operational activities rather than support activities, the yellow boxes are of lower interest and the focus will be on the remaining teams (green boxes and their subordinate staff).

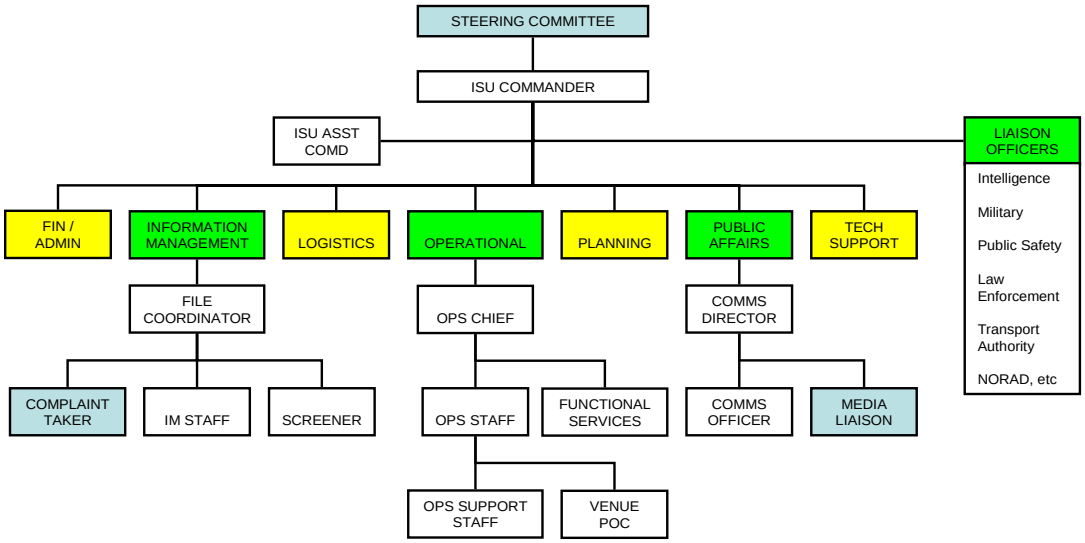

Figure 1. Proposed Organizational Structure for the Integrated Security Unit

The organizational structure, as shown in Figure 1, was developed based on interviews with subject matter experts. All the staff positions (white and blue boxes) were considered essential for the operational centre of the ISU. Note that this organizational structure does not include the staff which will provide the security at the venues where the major event is occurring. The security personnel at the venue or available to be dispatched at the venue would include quick reaction teams (QRT), emergency response team (ERT), diving teams, maritime and air services, police dog services, CBRNE (Chemical, biological, radioactive, nuclear and explosives) teams, infantry, corporate security. These various teams would include assets from various agencies (law enforcement, military, etc.). It is assumed that a Memorandum of Understanding (MOU) has been agreed upon to assign all these assets to the ISU.

At the top of the organization structure of the ISU is a steering committee. This committee's role is mostly strategic and therefore it was not considered within the modeling and experimental study.

The ISU Commander has the role to lead the ISU. This Commander will be assigned by the agency that has the lead for the major event security (likely a federal or provincial law enforcement agency).

The ISU Commander is assisted by the Assistant Commander and by liaison officers from the various agencies involved within the major event security. These agencies would include intelligence agencies, law enforcement agencies other than the one leading the major event security, military agencies, agencies in charge of public safety (e.g., first responders), and agencies owning or in charge of critical infrastructures (e.g., airports, power central, etc.). Note that the role of these liaison officers is to ensure a good flow of information between the agency that they represent and the ISU. However, the liaison officer for a given agency might not be the only representative from this agency within the ISU. For example, there could be military representatives within the information management section as well as military liaison officers.

The rest of the ISU is divided into seven sections: Financial and administrative, information management, logistics, operational, planning, public affairs, and technical support. The financial and administrative, logistics and technical support sections provide a support role to the overall security operations and were not investigated within the modeling and experimental work.

Although it can be argued that the information management section is largely fulfilling a supporting role, this section was included within the study due to the expected close involvement between this section and the operational section. The IM section is composed of a File Coordinator, some IM staff, Screeners and Complaint takers. While this work was being done, the role of the Complaint takers had not been clarified and is discussed in this paper. The role of the other staff within the IM section is clarified in the next section where the processes are described.

Since our focus is on the operational activities, the operational section is of primary concern to us. An Ops Chief is leading this section composed of Ops Staff, Ops Support

Staff, Venue Points of Contact (POCs) and Functional Services managers. The role of these staffs is clarified in the next section.

Finally, the last section of interest is the Public Affairs section. This section is in charge of liaising with the public and more specifically in charge of all press conferences. The Communication Director leads this section and supervises the work of a team of Communication Officers and Media Relations Officers.

Information Management Processes

As mentioned previously, the aim of the experimental campaign was to investigate the IM processes required to support the operational centre of the ISU. The architectural (DoDAF) work as well as concept of operation documents (Emergency Response Program 2001, Department of National Defence 2002, U.S. Joint Forces Command 2006) were used to select the IM processes. However, before introducing the selected processes, it is worth describing what is meant by process and how it differs from approach or method.

Within this paper, an approach is defined as an attitude or manner (modus operandi) to perform some task. An example of an approach is an effects-based approach to operations. Different processes can be used to implement this approach and the approach simply specifies that the focus is on the intended effects regardless on the planning method chosen to develop courses of action.

A method is defined as a way of accomplishing specific tasks. It can be very specific mentioning the specific tools one shall use. For example, there are different methods to write a text. One can first write down an outline of the text describing the main ideas of each section and each paragraph within each section and then write down the content of each paragraph. Furthermore, one can use a pencil or a computer or a combination of both (first writing down using a pencil and then typing the text on a computer). Each method will have their pros and cons.

A process is defined as a collection of interrelated tasks, which solve a particular issue. It is more global than a method and specifies the goal to be achieved. It can very specific by associating given resources and methods as well as specifying the time allocated to each task. There were nine IM processes investigated within the experimental campaign. These processes were named as follows:

- Situation Report (SITREP) process;
- Maintain Situation Awareness (SA) process;
- Request for Information (RFI) process;
- Incident Report (IR) process;
- Incident Response Planning (IRP) process;

- Request for Assistance (RFA) process;
- Transfer of Authority (ToA) process;
- Handover (HO) process;
- Public Affairs (PA) process.

Within the simulation model, these nine processes were described in details with specified resources and time allocated to each task. However, for the human-in-the-loop experiment a more succinct description was provided to the experimental participants. The succinct description of the nine processes is given in the following sub-sections. For the more detailed definition of the processes, the reader is referred to the simulation handbook (Lachance and Miller 2007, 35-78).

Situation Report Process

As mentioned previously, a process consists of a set of tasks and an intended goal. Therefore each description of the nine processes will provide both a description of the set of tasks and of the intended goal of the processes.

The Situation Report (SITREP) process has two main goals: preparing and providing a summary of the situation to higher authorities; and, developing and distributing the commander's directions. The main tasks consist of: 1) The staff at the venue sends their status summary to the operational centre; 2) The Ops staff consolidates the status summary from all venues with information from other sources to produce a situation brief; 3) Simultaneously, the planning staff produces the operational plan for the next 24 operational hours; 4) The situation brief and the next operational plan are then combined by the Ops Staff to produce the draft Commander directions which are reviewed at the commander's daily meeting that will be attended by the chief of each section as well as the commander, assistant commander and liaison officers; and, 5) The revised commander directions are distributed internally and externally by the IM section. The SITREP process focuses on the operational level rather than tactical. The information shared within the SITREP process is mostly about patterns and trends with regard to the overall operation. Figure 2 provides a concise overview of the process.

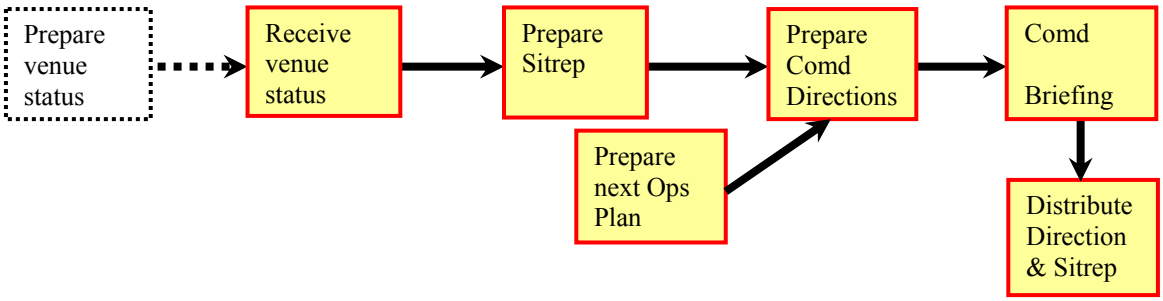

Figure 2. Overview of the Set of Tasks within the SITREP Process

This SITREP process has the advantage of having similarities to both the Battle Rhythm process usually performed within a military task force headquarters (U.S. Joint Forces Command 2006) and with the situation report process performed at emergency operation centres (Emergency Response Program 2001, 47-48).

Maintain Situation Awareness

The maintain SA process is an important process to ensure that the stored information about own resource activities and about threats are kept updated. The blindness to changes over long period of time is a current operational issue that this process should help mitigate. The main tasks of the maintain SA process consist of: 1) The IM Staff receives the new information; 2) The screeners log the information in the relevant databases and determines any required additional actions (for example, displaying the information on an electronic easel); 3) The IM staff requests additional information or clarifications if required; and, 4) The information is sent by the Ops Chief to the Commander or liaison officers if it is judged important to them. Figure 3 provides a concise overview of the process.

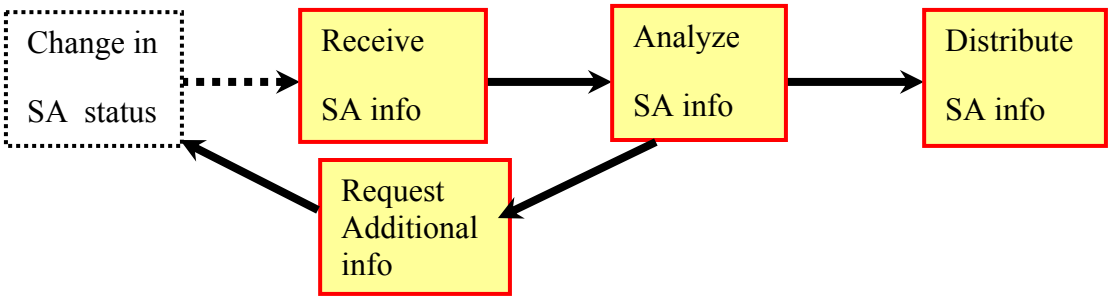

Figure 3. Overview of the Set of Tasks within the Maintain SA Process

Although many operational centres have methods to support a good SA, few have a precise process in place. Within military operational centres, the SA process is sometimes called Knowledge Development (U.S. Joint Forces Command 2006, Chapter 4). Within emergency centres, tools for maintaining SA include whiteboards, flip charts, electronic easels and possibly digital projectors (Emergency Response Program 2001, 39-40). However, there is often no specific process required for maintaining SA.

Request for Information

The request for information (RFI) process is a formal process for managing information requests. The tasks within the RFI process consists of: 1) An ISU staff member or one from another organization fills in a formal RFI form to request the information needed; 2) The IM staff receives the RFI; 3) The screener prioritizes the RFI and associates a tracking number with it; 4) The IM staff queries the database to look for an answer; 5) If the requested information is not available within the database, an Op staff tasks an internal resource or requests the information from an external organisation depending on where the information is the most likely to be found; 6) The Op staff analyzes the received information; and, 7) The screener provides the information to the person requesting it and closes the RFI. Figure 4 provides a concise overview of the process.

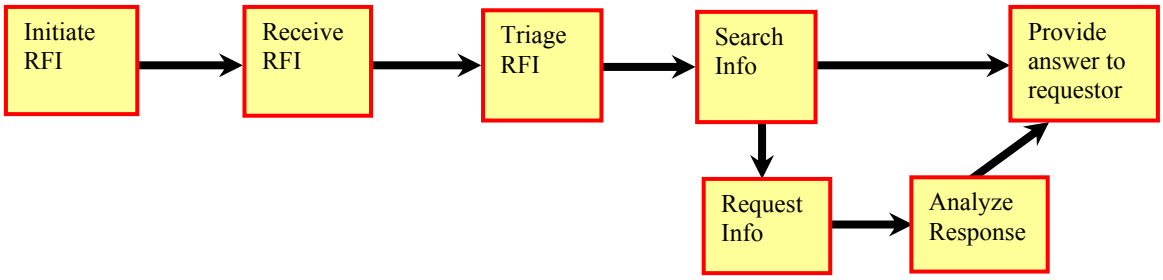

Figure 4. Overview of the Set of Tasks within the RFI Process

The RFI is a common process used during military operations to manage the request for information (U.S. Joint Forces Command 2006, Chapter 4, 24-25). Although, typical emergency centres do not require a specific RFI process, memorandum forms are to be used for internal communications (Emergency Response Program 2001, 43). The memorandum forms will - similarly to the RFI - keep track of who requested information, his or her functional position, and the date and time the information was requested.

Incident Report

The aim of the incident report process is for the venues staff to inform the operational centre on incidents that happened or that are happening. The main tasks of the incident report process are: 1) The venue staff formulates an incident report; and, 2) The venue staff sends the incident report to the operational centre. Different communication tools can be used to communicate the incident report depending on the situation. If the incident is minor and the venue resources can deal with it, a written incident report could be simply logged into a web-based portal. If the venue staff is dealing with a major incident that requires additional resources, a verbal incident report could be transmitted by radio or phone. Figure 5 provides a concise overview of the process.

Figure 5. Overview of the Set of Tasks within the Incident Report Process

Since this process is focused on activities happening at the venue rather than within the operational centre, it was considered outside of the scope of the experimental analysis. Therefore, the tasks associated with this process were performed by the experimental control team rather than by experimental participants.

Incident Response Planning

In response to an incident report received from a venue, the operational centre staff may initiate the incident response planning process. The aim of this process is to allow the operational centre to guide the response to an incident and possibly dispatch additional resources or specialized teams. The tasks within the incident response planning depend on the seriousness of the incident. For all incident reports, the initial tasks consist of: 1) The venue POC receives the incident report;

2) The Ops Chief and the Ops staff analyze the incident; and, 3) The Venue POC and ISU Ops Staff monitor the evolution of the situation. If additional resources are required at the venue then these additional tasks are performed: 4) the File Coordinator and Ops Chief develop objectives and tactical assignments for an immediate response; and, 5) The Ops Staff and Functional Services manager distribute the tactical assignments for requesting the additional resources. Finally, if detailed planning is required, four additional tasks are performed: 6) The Ops Staff issues a heads-up; 7) The Ops Chief, File Coordinator, Planning staff, IM staff, and liaison officers develop specific course of actions using contingency plans; 8) The ISU Commander appoints an incident commander; and, 9) The incident commander reviews and approves the developed course of actions. In addition, the incident response planning can trigger, simultaneously with the development of a course of actions, a Request for Assistance (RFA) process. This process is described in the sub-section below.

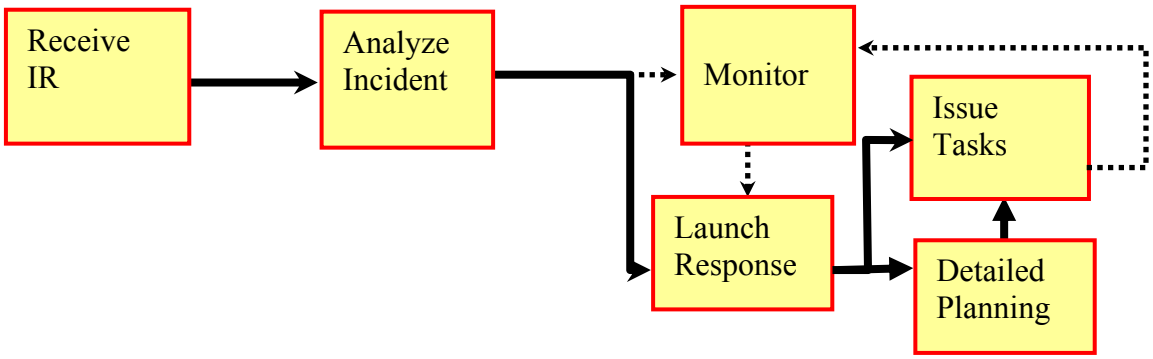

Figure 6. Overview of the Set of Tasks within the Incident Response Planning Process

Request for Assistance

The request for assistance (RFA) process will be used in response to a large-scale incident when the resources nder the authority of the ISU will not be adequate to respond to the incident. The goal of the RFA is to request additional resources from specific federal or provincial agencies. These resources could include military and law enforcement regular units as well as special services units.

The RFA process is triggered by the incident response planning process. Following the receipt of an incident report and the dispatch of resources for an immediate response within the incident response planning process, the RFA process might get triggered. The RFA process consists of the following tasks: 1) The ISU Assistant Commander with the liaison officers from the relevant agencies write down a request for assistance; 2) The ISU Commander approves the request; 3) The Ops Staff transmit the request to the relevant agencies; 4) The external agency upon receipt of the request analyzes their resources available and writes a RFA response; 5) The response is sent back to the Ops Staff who receives it; and, 6) The ISU Assistant Commander and File Coordinator analyze the response received from the external agency and can trigger an update of the developed courses of action. Although not explicitly modeled, the ISU Assistant Commander also informs the Steering Committee about any request for assistance. Figure 7 provides a concise overview of the process.

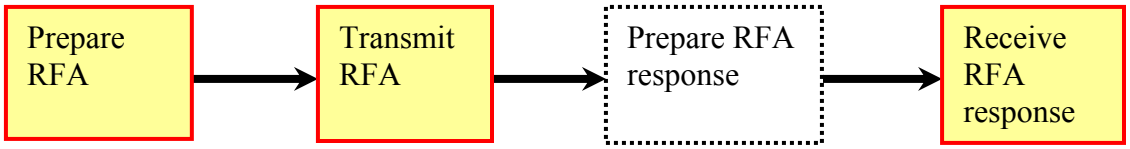

Figure 7. Overview of the Set of Tasks within the Request for Assistance Process

Transfer of Authority

The transfer of authority (ToA) process will be used by the ISU to give away the lead of a portion of an incident response to another agency (for example, transferring the lead for further investigation or transferring the incident response for incident extending beyond the venue of the major event). The aim of the process is to ensure the clarity of the transfer to all and keep track of the transfer to ensure that any related fiscal implications to the transfer are acted upon. The tasks within the ToA process consist of: 1) The Commander, the Ops Chief and the File Coordinator analyze the need for the transfer; 2) The Planning staff draft a ToA plan; 3) The plan is transmitted to higher authority with a proposal for the new lead agency; and, 4) The ISU Commander oversees the transfer of authority. Figure 8 provides a concise overview of the process.

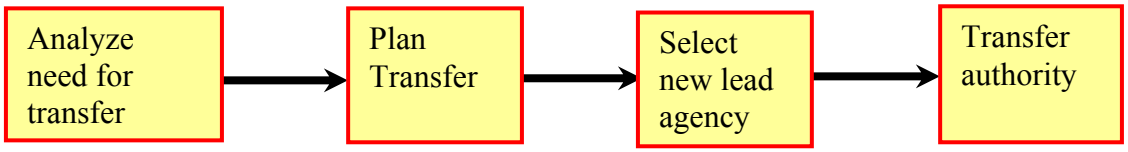

Figure 8. Overview of the Set of Tasks within the Transfer of Authority Process

Handover Process

The aim of the handover (HO) process is very similar to one of the ToA process, but the situation leading to the handover process is very different. A handover is performed when the response to the crisis management is completed and there is no more threat to the public security. In that situation, the ISU will handover the authority to a consequence management agency. The tasks included within the handover process are also similar to those of the ToA process, but the main difference is that higher authorities above the ISU are not involved. The precise tasks consist of: 1) The Commander, the Ops Chief and the File Coordinator analyze the completion of the incident response; 2) The Planning staff and the relevant liaison from the consequence management agency develop a handover plan; and, 3) The Commander oversees the handover. Figure 9**Error! Reference source not found.** provides a concise description of the process.

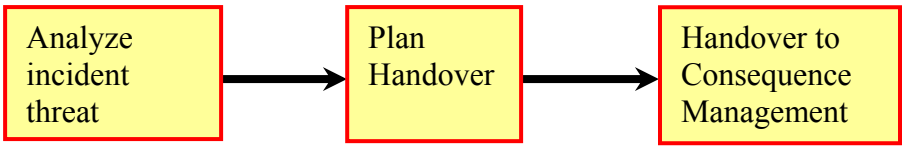

Figure 9. Overview of the Set of Tasks within the Handover Process

Public Affairs Process

The Public affairs (PA) process is an important one that specifies the interface between the ISU and the public. The tasks within the public affairs process consist of: 1) The media relations officer reviews the severity of newly received information; 2) The communication officer reviews the current consultation plan; 3) The communication officer updates the media lines (media lines are pre-planned key messages to communicate to the media about a particular subject area, designed to provide a timely and coordinated response to an event or issue) to develop a media briefing; 4) The communication director approves the media briefing; 5) The Commander approves the media briefing; and, 6) The media relations officer delivers the media briefing to the media. Figure 10 provides a concise description of the process.

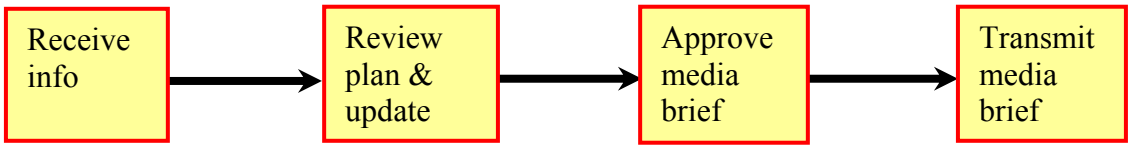

Figure 10. Overview of the Set of Tasks within the Public Affairs Process

Note that this public affairs process is simpler than the one used within military operation centres or emergency operation centres. For a military operation, public affairs are closely linked with information operations (IO) and both processes have to be synchronized and integrated to some extent. Within an emergency operation centre, public affairs go beyond informing public of the current situation and include communicating public warnings and alerts, as well as communicating the need for specific resources, e.g., call for volunteers, heavy equipment operators, etc. (Emergency Response Program 2001, 44)

Design of the Experiment

Experimental Aim

Explicitly, the aim of the experiment was to:

- Validate the modeled IM processes; in other words, verify that the triggers, the implementation and the outputs of the processes are as modeled;
- Identify unforeseen impacts related to the implementation of the IM processes; and,
- Measure the effectiveness of the IM processes to meet the required interagency information sharing.

The validation of the modeled IM processes will allow us to identify the limitations of the ReThink simulation. Furthermore, the simulation could be upgraded based on results from the experiment to better represent reality.

Experimental Hypothesis

The hypothesis of the experiment is that: The IM processes identified and developed through modeling and simulation are realistic and feasible in terms of providing greater interagency situation awareness and improved incident management capabilities during major event security operations.

Experimental Data Collection

The testing of the hypothesis requires the measure of the degree of adherence to the IM processes (verifying that the IM processes are realistic) as well as the measures of the operational centre staff situation awareness and the quality of the incident management. Therefore, at least three quantities need to be measured:

- The adherence to the IM processes: Expected trigger, task flow, resource-to-task association, and output;
- The quality of the incident management; and,
- The participant's situation awareness.

To properly test the hypothesis, one should have two groups: one where the IM processes are implemented and one where the group has either a different set of IM processes or does not have specific processes and must self-organize. This way, one could verify if the designed IM processes lead to greater situation awareness and improved incident management. Unfortunately, due to the lack of time and resources only one group was available for a short period of time and an alternative approach to test the hypothesis was required. The selected approach was to compare the situation awareness between the experimental participants and the experiment control team – it is expected that the control team staff, who were aware of the details of the scenario, would have a very good SA and the degree to which the experimental group matches the control group would shed light on the effectiveness of the IM processes. With regard to the quality of incident management, the subjective assessment from the participants was used.

Explicitly, the data collected during the experiment supported the assessment of the following measures:

1. Level of adherence to the business process: Observing and categorizing the tasks performed by the ISU staff and determining the trigger for the task.
2. Quality of incident management: Measuring the effectiveness of the processes to support the incident management.
3. Situation awareness: Measuring the participant's situation awareness and the completeness of the information logged into the portal.

The required data will be collected through observation of the staff tasks, monitoring the activities on all computers and distributing surveys to the experimental participants as well as to some staff from the experiment control team.

Experimental Setting

The 26 experimental participants consisted of members of national, provincial and municipal security agencies, members of the Department of National Defence (DND), as well as members of Public Safety agencies. The participants were selected based on their training to fill specific roles within the experimental ISU.

A computer network was set up linking all participants with one another as well as the experiment control team. Each participant had a computer and two monitor screens. A web-based portal – called the Incident Management System (IMS) - was set-up on the network server and the participants also had access to various Office applications (Outlook, Word, Internet Explorer, Power Point, and Excel). The participants could also communicate between them using a soft phone (Cisco Softphone).

A day of training preceded the experiment. The training day started with a two-hour overview presentation of the whole campaign of experimentation, the expectation from the experiment and an overview of the scenario background. This presentation was followed by a two-hour training session on the soft phone and the web portal (IMS). Finally, there was a one-hour session to review the IM processes. Note that various participants had been involved in the design and development of the IM processes and had a good knowledge of them. Also, since the participants had used the Office applications on a regular basis, only a very short overview of the tools was given.

The experiment ran for three and half days. The experiment control team, which was located in a separate room than the participants, fed the participants various types of information: incidents details, intelligence and weather reports, etc. Some of the inputs were provided to inform the participants of the situation at the venue, while other information requested decision being made by the participants. At the end of each experimental day, the participants were requested to answer an electronic survey. Participants answered the survey independently with no interaction between them. After the survey, the group of participants was invited to provide verbal feedback.

Experimental Scenario

The scenario was based around a generic international major event. The scenario included a wide variety of routine security events as well as some select security and/or public safety incidents of a more serious nature that will trigger processes like the IRP, RFA, ToA and HO processes. More specifically, the threats included epidemic, terrorist groups, anarchist groups, environmental disasters, bomb threats, threats against critical infrastructure, black market activities, as well as other suspicious activities. A threat analysis was part of the background-reading package and included fictitious international and domestic organizations that wish to disrupt the major event for their own purposes as well as possible environmental and public safety threats. Each incident was supported by a quantity of representative information typical of the level of information that will be expected by the various security agencies.

Data Analysis

IM Processes Validation

As mentioned previously, the IM processes was validated by comparing the similarity between the triggers, implementation and outputs observed during the experiment with the modeled processes. More explicitly, the data captured for the IM validation was analyzed as follows:

- Following the reception of new information by the participants, the outputs of tasks produced by the participants were used to determine the processes that have been triggered.
- The list of triggered processes was then compared with the expected triggered processes that had been determined while developing the experimental scenario.
- The tasks observed by the analysts during the experiment as well as those observed from the monitoring tool were used to compare the implementation of the processes with the modeled processes. To ensure the validity of the interpreted observations, the participants were surveyed with regards to their involvement within the various processes.

The output of this analysis was a comparison between the modeled processes and the observed processes. Reasons for observed differences were also investigated by considering the context within the operation centre at the moment when the considered trigger was received.

Quality of Incident Management

The quality of the incident management was assessed through the surveys distributed to the experimental participants. The participants were requested to assess the adequacy of each process to support the incident management and were requested to identify factors hindering the incident management. The assessment from each participant was correlated with various factors (the participant's situation awareness, workload, degree of involvement within the processes, satisfaction with the overall received information, satisfaction with the received training and guidance, satisfaction with the tools available, and amount of experience within an operational centre). The computed correlations were used to further identify possible factors impacting on the satisfaction with regard to the quality of the incident management.

Situation Awareness

Endsley's definition of situation awareness was considered for the experiment. Explicitly, situation awareness was defined as (Endsley 1988, p. 97): "The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future". This definition implies a three-level situation awareness. The first level corresponds to perceiving cues or elements of information from the environment within a volume of space-time. The second level corresponds to the comprehension of the meaning of the cues. This implies

being able to decipher the relevant cues and to assess the correlations between the various received cues. This second level corresponds to building evidence (evidence is obtained when a certainty value is assigned to the meaning of cues). This ability requires induction or diagnostic inference. The third level corresponds to anticipating the evolution of the situation. This ability requires foresight.

To determine the participants' situation awareness, we designed a total of 27 questions each with a choice of 4 answers. The questions were divided into three topics: threat or incidents details (Red SA), external agencies information (Green SA) and operational centre own information (Blue SA). In addition, different questions were designed to assess the different levels of situation awareness. Specific questions about cues (e.g., the location of an incident or the name of an anarchic group) were designed to assess the level 1 of situation awareness (level-1 SA). Questions requiring to assess the meaning of a decision or to identify correlations between cues were designed to assess the level 2 of situation awareness (level-2 SA). Finally, the level 3 questions assessed the knowledge of the participants with regards to the intent of various actors and the potential consequences related to specific incidents (level-3 SA).

The situation awareness was analyzed by comparing the participants' results to the SA questions with the results of the experiment control team. The experiment control team had a good level of situation awareness due to their involvement in the designed of the scenario. Therefore, the experiment control team was used as a reference group with an assumed high level of situation awareness. Effective information management processes should support the experiment participants to develop a level of situation awareness similar to the one of the experiment control team.

Experimental Results

Due to the limitation on the size of this paper, only the main results from the experiment are provided here. The sections are subdivided into three sub-sections: adherence to the IM processes; quality of the incident management; and, situation awareness.

Adherence to the IM Processes

As summarized in the appendix, there was good testing of the Incident Response Planning process, for which most modeled tasks were observed. The SITREP and Public Affairs processes were also frequently observed; however, the sequence of performed tasks was significantly different from the modeled ones. The Transfer of Authority and Handover processes were observed only a few times each but showed many similarities to the modeled processes. Finally, no formal processes for the Request for Information, the Maintain Situation Awareness and Request for Assistance processes were observed. Possible causes for the observed disparities include the lack of familiarity of the experimental participants with the processes, the lack of tools to support specific processes (e.g., RFI) as well as the need to adapt the participants' role to meet the workload.

Quality of the Incident Management

The effectiveness of the IM processes in supporting incident management was assessed by asking the experimental participants to score on a scale from 1 to 5 their level of satisfaction with the IM processes (1 meaning totally unsatisfied and 5 totally satisfied). The results from these questions are displayed in Figure 11. Note that the participants could also answer 'uncertain of effectiveness' (not displayed here).

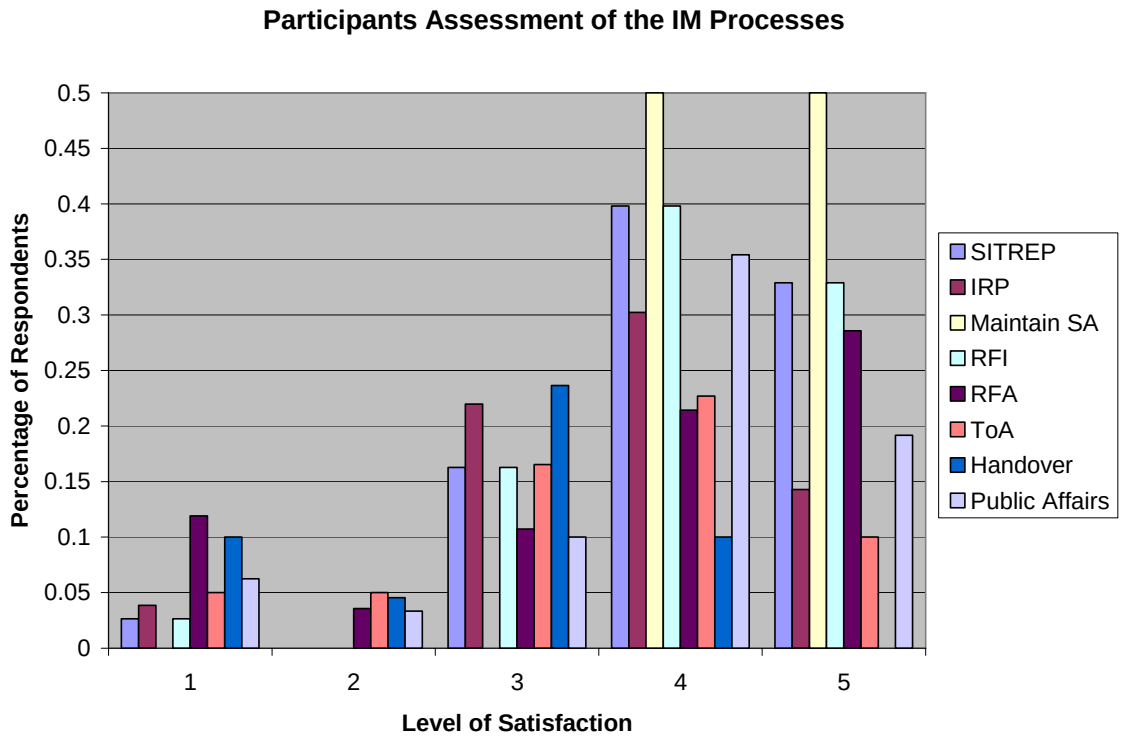

Figure 11. Assessment of the Effectiveness of the IM Processes by the Experimental Participants.

The satisfaction with regards to the Maintain SA process is largely inconclusive since only two staff responded. This is not surprising since this process was not observed during the experiment. Therefore, the participants could not assess the effectiveness of this process. Overall the satisfaction with all processes was very positive with all modes at 4 or 5 (except for the Handover process). The processes with the lowest satisfaction are the RFA and Handover processes. These processes required a higher level of coordination with other agencies. The difficulty in establishing this coordination could explain the lower level of satisfaction.

Various types of correlations were computed to assess factors that impacted on the participants' satisfaction with the IM processes. These factors included: the participation in the processes themselves; the amount of workload; the satisfaction with regard to other processes; the satisfaction with regard to the overall amount of information and the quality of the information; the satisfaction with regard to the amount of received

guidance and training; and, the participant's SA. Among all the considered correlations, only the following were statistically significant:

- The participants with a higher satisfaction towards the SITREP process also had a higher Blue SA (correlation: τ_b= 0.588) and Green SA (correlation: τ_b= 0.75). There are two possible explanations for this fact: Either the participants with good Blue and Green SA found the SITREP more comprehensive or some participants developed a better Blue and Green SA from the SITREP output and therefore were more satisfied with its effectiveness.
- The participants with a higher satisfaction towards the RFA process also had lower level-1 SA (correlation: τ_b= 1.0), level-2 SA (correlation: τ_b= 0.714), and Green SA (correlation: τ_b= 0.667). These correlations are indicative that the RFA process, which was not fully fulfilled, was problematic and the participants who were more aware of other agencies situation (Green SA) were more aware of this problematic.

Situation Awareness

The situation awareness of the participants was computed and the individual score varied from 37.5% to 100% correct answers with an average of 72.4%. Table 1 displays the situation awareness (SA) of various groups. The score for the three different levels of SA, the three different types of topic as well as the overall average SA for the group are displayed. The first row displays the average score for the experimental participants. The second row displays the average score for the experiment control team. Finally, the third row displays the average score for six staff members within the operational section, which is a sub-group of the experimental participants.

Table 1. Situation Awareness Average Score for Various Groups

	Level-1 SA	Level-2 SA	Level-3 SA	Red SA	Green SA	Blue SA	Overall SA
Participants	81.25%	63.8%	60.0%	73.8%	70.6%	72.7%	72.4%
Experiment Control	73.7%	83.3%	66.7%	71.1%	85.7%	66.7%	71.4%
Operational Section	89.2%	77.8%	66.7%	84.4%	78.6%	85.7%	82.1%

Although some differences between the various groups' average SA can be observed, a t-test was used to verify the statistical significance of the differences. An independent sample t-test was used to compare the results between the participants SA and the experiment control SA while a dependent sample t-test was used to compare the participants' SA with the operational section's SA. No significant difference between the participants' SA and the experiment control's SA were obtained. These results support the conclusion that the IM processes were effective to support a good situation awareness of the operational centre. However, a significant difference between the operational section's SA and the participants' SA was obtained for the Level-1 SA (t value of 2.50), the Green SA (t value of 3.39) and the overall SA (t value of 2.64). The increased SA of

the operational section is easily explained by the fact that the human learning process is more effective through active intervention than through passive observation (Perales and Catena 2006). In other words, the operational staff's important decision-making role based on incoming information supported their SA.

Conclusion

This paper describes a human-in-the-loop experiment performed to assess specific processes to support the information management within the operational centre of an integrated security unit in charge of the public security during a major national event. A specific hypothesis was drafted to guide the experiment. The adherence to the information management processes, the assessed effectiveness of the processes as well as the experimental participants' situation awareness were all measured to test the hypothesis. The SA results provide the most convincing evidence that the IM processes were effective at supporting the operational centre information sharing. Further work are planned to further investigate the interagency information sharing and more specifically the RFA, Handover and Maintain SA processes that were not observed as expected during the experiment.

Reference

Allen, Dave. 2008. *Modeling Information Management Processes for Major Event Security*. Department of National Defence, DRDC CORA, Technical Report TR 2008-XX

Emergency Response Program. 2001. *PREOC Operational Guidelines*.

Department of National Defence. 2002. *CF Operational Planning Process*. Joint Doctrine Manual B-GJ-005-500/FP-00, J7 DLLS 2

Endsley, M.R. 1988. *Design and evaluation for situation awareness enhancement*. In Proceedings of the Human Factors Society 32nd Annual Meeting. Vol. 1, pp. 97-101. Santa Monica, CA: Human Factors Society.

Lachance, Patrick, and Jordan Miller. 2007. *CF-OGD Interaction Model for Major Event Security Operations – Simulation Handbook*. CAE PS (Canada) Inc.

Perales, J.C, and A. Catena. 2006. *Human Causal Induction: A Glimpse at the Whole Picture.* European Journal of Cognitive Psychology, Vol. 18, pp. 277-320.

Smith, Pete, and Neil Carson. 2006. *Maritime Security Operations Centre East – Preliminary Work and Information Flow Analysis*. Department of National Defence, DRDC CORA, Technical Note TN 2006-01

U.S. Department of Defense. 2004. *DoD Architecture Framework Version 1.0*

U.S. Joint Forces Command. 2006. *Effects-Based Approach to Multinational Operations – Concept of Operations with Implementing Procedures*. Version 1.0, Suffolk, VA: United States Joint Forces Command, Joint Experimentation Directorate.

Appendix A

Process	**Validation Comment**
Situation Report (SITREP)	This process was observed but with some adjustments. The File Coordinator was in charge of ensuring the completion of this process. The observed tasks included: • Determination of the SITREP request inputs (File Coordinator and IM Manager) • Request of SITREP inputs (File Coordinator) • Development of requested inputs (Comms Director, Liaison officers, Venues staff, Ops Staff, Plans Staff and Functional Services) • Development of Commander's brief (IM staff) • Review of Commander's brief (Ops Chief) • Update to Commander's brief (File Coordinator) • Commander's meeting • Update of Commander's brief to include Commander's direction (File Coordinator) • Distribution of the Commander's brief (File Coordinator)
Incident Response Planning (IRP)	This process was observed with minor adjustments. This process was generally followed and was well facilitated through the web portal. The activities within this process were under the lead of the Ops Chief. The observed tasks included (not all these tasks were performed for all incidents): • Receiving incident details (Venues POC or liaison officers) • Logging incident into the incident management system - IMS (File Coord, IM Manager or Screener) • Requesting updates on incident (self-coordinated by Venues POC, Ops Staff, Functional Services, liaison officers) • Logging updates into IMS (Venues POC, Ops Staff, Functional Services, liaison officers) • Reading IMS updates (All) • Discussing required resources (Ops Chief with Ops Staff and Functional Services) • Dispatching additional resources (Functional Services, Ops Staff, or liaison officers) • Issuing tasks (Functional Services, Ops Staff) • Updating the Commander of situation (Commander and Ops Chief) • Discussing Course of Action (Ops Chief with Ops Staff, liaison officers and Functional Services)
Maintain Situational	The formal process was not followed. Three types of information were received by the participants: status report for the Commander's brief, incident updates and

Process	Validation Comment
Awareness (SA)	intelligence report. Most of this received information was in response to requests: Request for Commander's brief inputs (SITREP process) or incident updates (IRP process). Only the incoming intelligence reports were neither triggered by the SITREP process or the IRP process. Some information within the intelligence report regarding on-going incidents was logged into IMS by the File Coordinator. This is the only observed task that could be considered part of the Maintain SA process.
Request for Information (RFI)	The formal process was not followed. In most cases, the desired information was informally obtained. There were a number of PA queries that were handled by the Comms Director but the formal RFI tracking process as developed was not used. The intelligence liaison officer also maintained an intelligence-related RFI tracking list but did not use the formal process as developed.
Request for Assistance (RFA)	The formal process was not observed. Injects designed to trigger this process resulted in the experimental participants taking a course of action other than RFA to manage the incident. However, the operational staff were very responsive to RFAs coming from the Urban Domain.
Transfer of Authority (TOA)	This process was observed with some adjustments with regards to the tasks performed. The observed tasks include: • Discussion of changes with regard to the incident (Ops Chief, Ops Staff) • Updating the Commander (Ops Staff, Commander) • Requesting transfer to higher authority (Commander, Higher authority) • Informing ISUstaff of transfer of authority (All) • Updating IMS incident information (Screener)
Handover (HO)	This process was observed but not as often as expected. For many incidents, the operational staff dispatched additional resources but did not need to perform the handover process upon completion of the crisis management. Most performed handover processes were with the Urban Domain, which was requested to complete relevant investigation. The observed tasks include: • Discussion of changes with regard to the incident (Ops Chief, Ops Staff, Functional Services) • Propose handover (Ops Chief) • Update of IMS (File Coordinator, IM Manager or Screener)
Public Affairs (PA)	Process observed and partially validated. Main steps of the process were followed but not completed in detail, most likely due to lack of resources (only the Comms Director was involved in the experiment) or workload. • Discuss PA query (Comms Director with Ops Chief, Ops Staff, File Coord, or external source) • PA task logged into IMS (IM Staff)