



Information Processes in Support of Major Event Security

Dr Dave Allen¹, Dr Renee Chow², Mr. Kevin Trinh², Dr Phil Farrell¹

1. DRDC CORA, Canadian Forces Experimentation Centre
2. DRDC Toronto



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

Canada



Background

- As expressed by DRDC S&T Strategy:
 - During the Cold War, national security challenges were largely separate from public security issues. Today, they represent more of a single agenda.
- This change requires a **transformation** to the **military C2** to enable a seamless **interoperability** with OGDs and allied forces.
- Possible solution: Integrated security unit composed of staff from various government departments.



Outline

- Concept: Integrated Security Unit
- Experimental Campaign
- Aim of the Human-in-the-loop Experiment
- Information Management Processes
- Communication Tools
- Data Collection
- Data Analysis
- Results
- Conclusion



Integrated Security Unit

- Assumptions:
 - A major event (international cultural or sporting event or international Summit) is pre-planned.
 - A large number of government resources are required to ensure the public security at the event venues.
 - The federal law enforcement agency is the lead for public security.
 - MOUs have been drafted between government departments to share resources.
- Integrated Security Unit: Tactical and operational unit composed of staff from various government departments in charge of ensuring the public security.

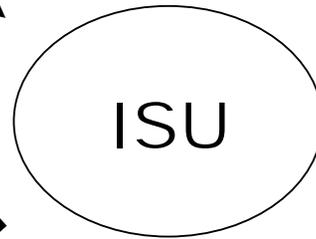


ISU Command Centre Responsibilities

Collecting
Info(Intel, Weather...)



Monitoring
Venues Security



Providing
Info(Public, OGDs...)

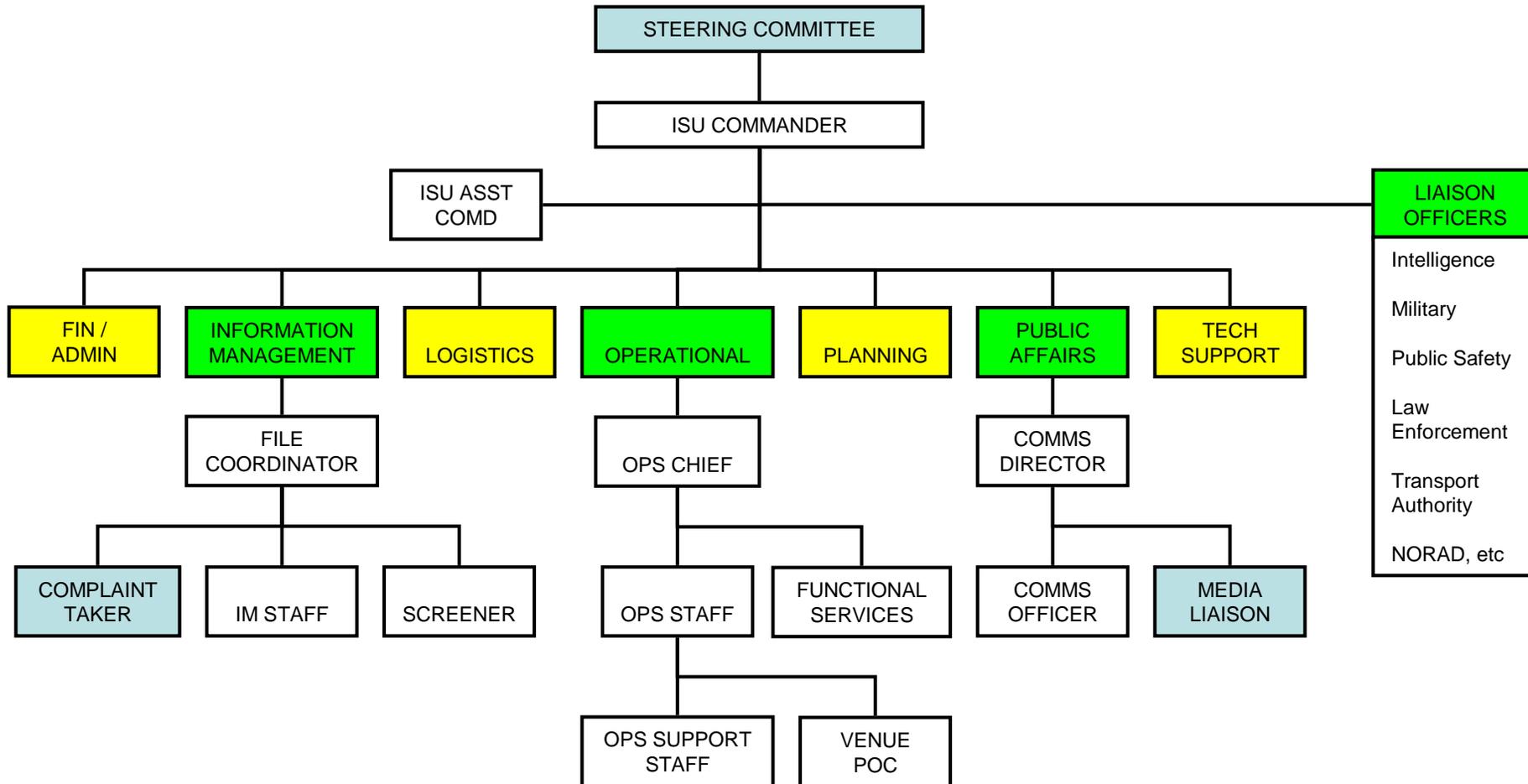


Directing
Resources





ISU Command Centre Organization





Aim of Experimental Campaign

- In November 2005, the Canadian Forces Experimentation Centre set-up an experimental campaign with the aim of:
 - Identifying deficiencies in how the agencies work together and share information;
 - Provide recommendations on how to enable agencies to work collaboratively to collect and analyze intelligence and other information to develop a solid awareness in their area of responsibility



Overview of Experimental Campaign

- Using the DoDAF operational views, determine the required info flow between the various organizations involved in major security operations.
- Determine and model a set of Information Management processes supporting the required info flow.
- Analyze the developed model to assess the resources requirements.
- Perform an human-in-the-loop experiment to validate the developed model.



DoDAF Operational Views

- The Operational Views were developed based on SMEs interview and CONOPS documents (Canada Command CONOPS, PREOC CONOPS).
- The output was a set of 9 IM processes:
 - Situation Report
 - Maintain Situation Awareness
 - Incident Report
 - Incident Response Planning
 - Request for Information
 - Request for Assistance
 - Transfer of Authority
 - Handover
 - Public Affairs



Situation Report Process

<p>WHAT</p> <ul style="list-style-type: none">• A regular-interval report declaring current status of security, own forces, operations, locations, and event situation.• Provides the current status picture of own forces / assets / domain within overall situational awareness.• Synonymous with current status report, routine report, etc.	<p>WHY</p> <ul style="list-style-type: none">• Provides higher-level authority with updated status information from its venues and own forces to facilitate the development and maintenance of a common operating picture.• Ensures own force readiness (<i>no news is not always good news</i>).• Provides the baseline current status information used to brief the Cmdr and maintain situational awareness (SA).	<p>WHEN</p> <ul style="list-style-type: none">• Regular pre-determined intervals.• Nominally once per day• Timings dependent on primary means of venue SITREP transmission.
<p>WHERE</p> <ul style="list-style-type: none">• From active venues to higher-level authority.• Consolidated within the ISU Command Centre.	<p>WHO</p> <ul style="list-style-type: none">• Venue responsible for timely transmission of a status summary.• ISU Ops Section consolidates Venue status summary into baseline situation brief.• ISU Planning Section produces the operational plan for the next 24 operational hours.• ISU Ops Chief responsible for brief to ISU Cmdr.• ISU Cmdr to provide guidance based on ISU Situation Brief.	<p>HOW</p> <ul style="list-style-type: none">• Through transmission of pre-determined status summary requirements (template) from venue to ISU Ops Section.• An electronic dashboard will be used to keep track of individual venue site status.



Maintain Situation Awareness

<p>WHAT</p> <ul style="list-style-type: none">• Defined as knowing what is going on around you, situational awareness is the ability to identify, process, and comprehend the critical elements of information with regards to overall mission accomplishment.	<p>WHY</p> <ul style="list-style-type: none">• The maintenance of SA allows for synergy between organizational components and stakeholder agencies.• SA allows for concurrent planning activity to take place.• An agency requires suitable situational awareness to effectively carry out its mission.	<p>WHEN</p> <ul style="list-style-type: none">• The process of maintaining effective situational awareness is a constant task of the agency and its organizational components.• Constantly updated common knowledge information base, accessible to stakeholders, is synonymous with the maintenance of effective situational awareness.
<p>WHERE</p> <ul style="list-style-type: none">• The IM Section of an agency leads its efforts in maintaining effective Situational Awareness.• Each stakeholder agency needs to make their SA (common knowledge base) accessible to valid RFIs from other agencies.	<p>WHO</p> <ul style="list-style-type: none">• The IM Staff is responsible for the common knowledge base but all organizational components are responsible to ensure that the common information holdings are updated and as accurate as possible.• In a multi-stakeholder environment in which the ISU finds itself in, effective SA depends on all stakeholders maintaining SA and contributing to a common knowledge base.	<p>HOW</p> <ul style="list-style-type: none">• Operational SA is updated primarily through:<ul style="list-style-type: none">– Status summary from venues– Intelligence reports– OGD SITREPS and public safety domain information• A geographical dashboard reflecting SA would allow rapid visual SA assessment of the venues environment.



Incident Report Process

<p>WHAT</p> <ul style="list-style-type: none">• A non-scripted report triggered by the occurrence of an incident deemed significant.	<p>WHY</p> <ul style="list-style-type: none">• Used to inform higher-level authority (ISU) of an existent or potential non-routine situation.• Maintenance of Situational Awareness (SA), and potential to reveal hidden pattern of incidents.• Potential requirement for additional assets to be assigned, or the potential redistribution of own assets to solve incident.	<p>WHEN</p> <ul style="list-style-type: none">• Initiated at the discretion of the on-scene security authority.
<p>WHERE</p> <ul style="list-style-type: none">• From the on-scene security authority to the ISU Ops Section.	<p>WHO</p> <ul style="list-style-type: none">• Initiated by the On-scene Security Authority.• IR passes through the ISU Ops Section, who performs incident analysis.• IM Staff to update situational awareness (SA)	<p>HOW</p> <ul style="list-style-type: none">• Via communication means available.• Initial IR normally through voice communications; therefore log must be kept of incoming voice communications.



Incident Response Planning

WHAT

- A plan that contains objectives, strategies and assignments for one or more asset groups, for a designated time period, location, or objective.
- The IRP addresses the policies, priorities and resource requirements to address designated objectives, as well as coordination directions.

WHY

- The response plans are developed to maximize own force response by enhancing coordination among specific organizational components.
- The response plans minimize the reaction time required to mobilize own assets in a coordinated fashion towards an objective and effect a desired outcome.

WHEN

- Contingency plans for potential-case scenarios developed pre-event and held at the ISU.
- IRP activation normally triggered by an IR; or within the ISU Ops Section as a result of intelligence forecasts.
- Automatic IRP activation for designated occurrences / events may be pre-approved by the ISU.

WHERE

- Initiated and activated within the ISU Ops Section.

WHO

- The ISU Planning Section modifies the appropriate contingency plan to reflect the current situation and particulars.
- Cross-agency tasking requires consultation with appropriate OGDs and intelligence.
- The ISU Comd or designate approves IRP activation.

HOW

- An IRP activation is issued to tasked units via the most appropriate means.



Request for Information

WHAT

- The RFI is a 'formal' process to collect information from various stakeholders to help guide decision-making and to aid in the maintenance of effective situational awareness.
- An RFI is used to solicit relevant information from multiple sources for input towards various key business processes.

WHY

- A 'formalized' RFI process allows for the tracking of key information requirements to ensure fulfillment in a timely manner.

WHEN

- Anytime key information is required and not held within own information resource holdings.
- If the required information cannot be found internally, a RFI is triggered towards another unit or agency.

WHERE

- The collective information holdings of an agency are known as its common knowledge database.
- A RFI can be directed to both internal organizational components, or externally to stakeholder OGDs.

WHO

- The ISU IM Staff is responsible for maintaining the ISU knowledge database, and ensuring 'seamless' data retrieval.
- The Intel Officer will feature strongly in any intelligence-related information requests.

HOW

- A 'formal' written request via electronic means will ensure that the RFI can be tracked and fulfilled in a timely manner.
- The ISU IM Section must maintain a RFI log to ensure key information requests do not go unfulfilled.



Request for Assistance

<p>WHAT</p> <ul style="list-style-type: none">• A formal request from an organizational component for additional federal resources to fulfill an assigned task and/or satisfy an objective.	<p>WHY</p> <ul style="list-style-type: none">• To facilitate the sharing of resources across agencies which were not accounted for in pre-event Memorandum of Understandings (MOUs), or Service Level Agreements (SLAs).• There are post-event fiscal issues associated with cross-agency tasking and operations.	<p>WHEN</p> <ul style="list-style-type: none">• RFA initiated when own resources cannot optimally fulfill an assigned task.• If pre-event planning is comprehensive, the use of RFA will necessarily be minimal.• An RFA normally follows an IR and IRP activation, or an Intelligence forecast.
<p>WHERE</p> <ul style="list-style-type: none">• A RFA can be initiated by any security or public safety organizational component involved within the designated event.• The RFA will be routed to the federal agency or agencies having authority over the additional resources usually going through the Government Operation Centre (GOC).	<p>WHO</p> <ul style="list-style-type: none">• In most cases, RFA discussions will take place and decisions made within the ISU Ops Coordination Group (<i>sic. Steering Committee</i>).• The agency, from whom assistance has been requested, will base its decision on its resource allocation requirements and plans.	<p>HOW</p> <ul style="list-style-type: none">• In most RFA cases, pre-approved MOUs / SLAs will be activated to meet the need, amended to reflect the current situation / particular event.• The Steering Committee (Crisis Cell) may become involved should an issue require higher-level resolution / adjudication.



Transfer of Authority

<p>WHAT</p> <ul style="list-style-type: none">• The Transfer-of-Authority-to-Higher-Level process is a formal process for an agency to relinquish its assigned tasks to a higher authority.	<p>WHY</p> <ul style="list-style-type: none">• A lack of designated authority held by an agency may trigger the requirement for a formal ToA to higher level, due to the gravity of the security and/or public safety situation.• RCMP HQ requested that this COBP be modeled due to the inherent fiscal implications associated with ToA to higher authority.	<p>WHEN</p> <ul style="list-style-type: none">• With proper games preparation and planning, this process (ToA to higher level) should not come into play as a functioning requirement of the ISU – unless an acute security or major public safety event should occur.
<p>WHERE</p> <ul style="list-style-type: none">• The decision will be made at the Steering Committee (Crisis Cell) or higher level, in consultation with Provincial and Federal – level agencies and ministries; and with input from the Comd ISU.	<p>WHO</p> <ul style="list-style-type: none">• The decision to activate ToA to higher level will go through the Steering Committee (Crisis Cell).	<p>HOW</p> <ul style="list-style-type: none">• A high-level decision process at the Steering Committee (Crisis Cell) or higher-level of authority.



Handover Process

<p>WHAT</p> <ul style="list-style-type: none">• The Handover process is used by the ISU to formally transfer the lead for the management of a security threat to a consequence manager.• Since in most cases, the crisis management and consequence management overlap, this process is mainly for formally informing the other agencies about the wrapping up of the crisis management operation.	<p>WHY</p> <ul style="list-style-type: none">• The ISU gives up the lead when the security threat is considered to be reduced to an acceptable level and no longer requires the ISU's lead• The IPSU requested that this COBP be retained (for fiscal, liability and legal reasons).	<p>WHEN</p> <ul style="list-style-type: none">• The process is initiated as required.
<p>WHERE</p> <ul style="list-style-type: none">• HO is initiated in the ICC• The decision will be made at ISU COMD level, in consultation with the IPSU, Municipal, Provincial and Federal – level agencies and ministries, as required.	<p>WHO</p> <ul style="list-style-type: none">• ISU COMD and Ops Chief will initiate the process based on the current situation.• ISU Planning Staff will coordinate and plan the handover with the new Lead Agency or IC as appropriate	<p>HOW</p> <ul style="list-style-type: none">• A Handover will not be restricted to a particular format. The requirement is for the time and place of Handover to be recorded and confirmed by all parties.



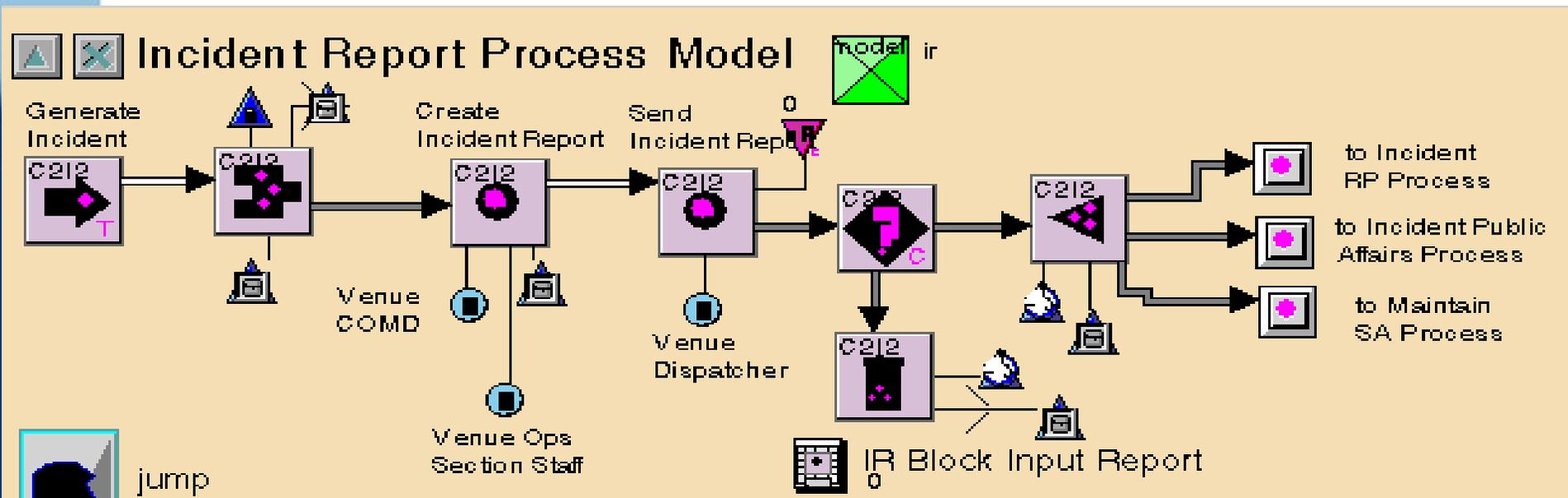
Public Affairs Process

<p>WHAT</p> <ul style="list-style-type: none">• This process deals with the preparation and dissemination of public information regarding games domain security issues.• The PA staff functions as the media point of contact and assists with intergovernmental communications and liaisons.	<p>WHY</p> <ul style="list-style-type: none">• Public Affairs is a vital component of operations that provides the interface between security operations and the public.• Public Affairs 'feedback' into the maintenance of effective situational awareness is an important aspect of ops.• Modeling is required to ensure that the ISU can effectively function in a demanding public info environment.	<p>WHEN</p> <ul style="list-style-type: none">• Pre-emptive public affairs news releases and background information for the public.• Reactive public affair / public information releases in response to incidents, or information requests from media.
<p>WHERE</p> <ul style="list-style-type: none">• The PA section within the ISU will mirror the ISU Ops Section at all levels.• A PA consultative presence needs to be in place throughout the entire decision-making process.	<p>WHO</p> <ul style="list-style-type: none">• The ISU Comd is the release authority for games domain security-related public affairs / public information releases.• The ISU Comms Director is responsible directly to the ISU Comd for all PA-related issues.	<p>HOW</p> <ul style="list-style-type: none">• PA matters are executed through an ISU PA section that mirrors the levels and functions of the ISU Ops Section.



Process Modeling

- The processes were detailed and modeled using ReThink G2 software.
- The simulation model was analyzed by assessing the risk of time delays for the accomplishment of the required tasks





Human-in-the-Loop Experiment

- The human-in-the-loop experiment was executed over 4 days, from the 20 to 23 November 2007.
- Aim:
 - **Validate** the modeled 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 processes;
 - Measure the **effectiveness of the processes** to support the incident response and meet the required interagency information sharing



Experimental Settings

- A team of 26 collocated experimental participants from various agencies manning the ISU Command Centre.
- A team of 14 experiment controllers feeding the experimental injects.
- A team of 4 analysts collecting the data.
- Each individual had access to a computer with 2 monitors.
- A single network was linking all individuals involved into the experiment.
- A web based portal was used as knowledge base repertory.
- Communication tools included emails and a soft phone.
- The experiment was preceded by 1 day of training.



Experimental Scenario

- A major event scenario involving a very large public (hundreds of thousands) and extending over several days was considered.
- The event was spread over a few venues where the ISU was responsible for public security.
- Considered threats included:
 - Anarchist and terrorist groups;
 - Black market activities;
 - Threats against critical infrastructure;
 - Bomb threat;
 - Environmental disaster;
 - Suspicious activities.



Data Collection

- Data was collected through computer monitoring, surveys distributed at the end of each experimental day, and observations obtained by the analysts.
- The data required for the following assessment was collected.
 - Level of adherence to the business process: Observing and categorizing the tasks performed by the ISU staff; determining the triggers of the processes; and, assessing the completion of the outputs of the processes.
 - Quality of incident management: Measuring the effectiveness of the processes to support the incident management.
 - Situation awareness: Measuring the participant's situation awareness and the completeness of the information logged into the portal.



Observation Collected

Inject ID	Task Observed	Inputs Used	Who	Date	Time	Duration	Device Used	Trigger	Output	Comments



Questions of Surveys

- The participants amount of Operational Centre experience and the similarity of their role during the experiment with their day-to-day job.
- The participants' satisfaction with the amount of training received.
- The participants' amount of workload during each day of the experiment.
- The participants' frequency of usage of the various communication tools and their satisfaction towards these tools.
- The participants' satisfaction towards the amount, quality and timeliness of the received information.
- The participants' perceived frequency of direct involvement within each process and their satisfaction of the effectiveness of the processes.
- The participants' situation awareness.



Results



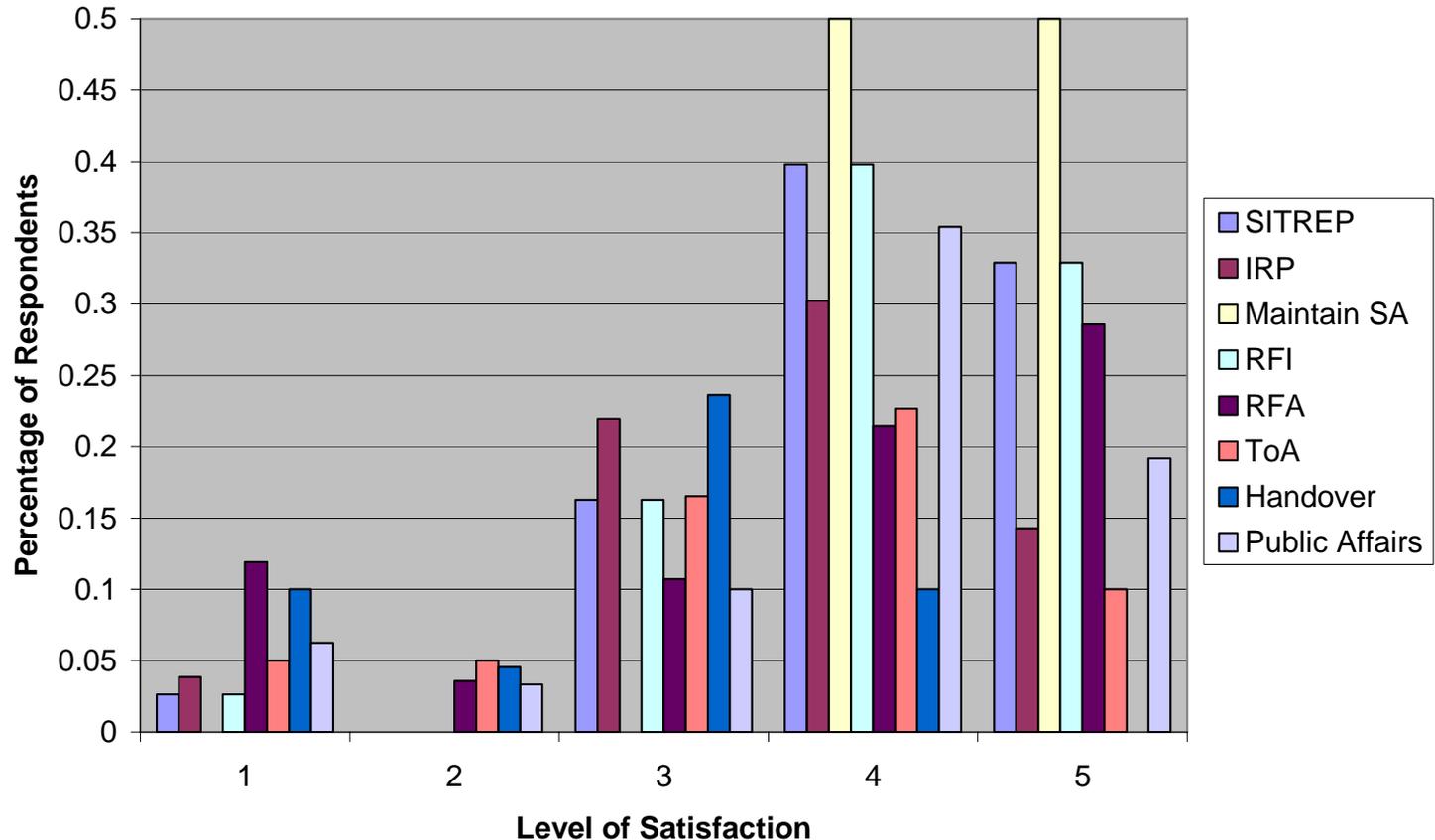
Validation of the processes

- All expected tasks from model were observed.
- In some situations, short cuts were observed and tasks were omitted or done in parallel rather than serially.
- Main differences between model and observations:
 - Triggered processes sometimes differed but mostly highlighted limitations of the model.
 - The resources assigned to the tasks was more flexible than modeled.
 - Additional tools would have been required to support some processes (RFI and RFA).



Effectiveness of the Processes to support Crisis Management

Participants Assessment of the IM Processes



- Lowest satisfaction with processes requiring a larger amount of interagency interaction: RFA and Handover.



Situation Awareness

- Three levels of situation awareness for three different topics were measured:
 - **Level 1:** Knowledge of cues, perception of elements of information.
 - **Level 2:** Comprehension of the meaning of the cues, capable of building evidence of meaning (requires induction and diagnostic inference).
 - **Level 3:** Anticipating the evolution of the situation (requires extrapolation and predictive inference).
 - **Red topic:** Info concerning threat or incidents
 - **Green topic:** Info concerning other organizations
 - **Blue topic:** Info concerning own decisions and resources



SA Results

- The participants overall SA varied between 37.5% and 100%.
- There was no statistical significance between the participants SA and the experiment control SA.
- The participants within the Ops Section has a significant Level-1 ($t=2.5$), Green ($t=3.4$) and Overall SA ($t=2.64$) higher than the other participants. **Active intervention helps learning!**

	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%



Correlations

- Higher centrality ($\tau_b=0.47$), closeness ($\tau_b=0.43$) and coreness ($\tau_b=0.50$) implies higher workload.
- Staff with more Ops Centre experience were likely more dissatisfied with the timeliness of the info ($\tau_b=-0.71$) but more satisfied with the quality of the info ($\tau_b=0.54$).
- Staff having indicated spending more time in face-to-face conversation had a higher SA ($\tau_b=0.48$). No significant correlation exist for time spent in formal meetings or communicating by phone or email.
- Staff feeling more overwhelmed with the amount of info had a lower SA ($\tau_b=-0.78$).
- Staff with a higher SA also had a higher centrality ($\tau_b=0.47$), closeness ($\tau_b=0.47$) and coreness ($\tau_b=0.53$).



Conclusion

- The experiment allowed to validate the model processes and should be used to update and improve the model.
- The participants involved in the experiment were capable of reaching a SA similar to the experiment control team who was well aware of the content of the injects. This is indicative of the adequacy of the processes and tools.
- The Ops Section had a particularly high SA most likely due to their involvement in responding to the incoming information.
- Being involved in the information sharing implies higher workload.
- Face-to-face conversation were effective to support higher SA.
- Direct involvement with many strong groups is effective to support higher SA.
- Ideal ISU structure and its interaction with the national level should be further investigated.

DEFENCE



DÉFENSE