LAUREA

Communication, Information Transfer and Role-Shift in a Challenging Public Safety & Security Field Operation

Turunen, Tuomas

2010 Leppävaara

COMMUNICATION, INFORMATION TRANSFER AND ROLE-SHIFT IN A CHALLENGING PUBLIC SAFETY & SECURITY FIELD OPERATION

Laurea University of Applied Sciences
Laurea
Degree Program in Security Competence

Abstract

Tuomas Turunen

Communication, information-transfer and role-shift in a challenging public safety & security field operation

Year	2010	Pages	66

Challenging criminal incidents like high-jacking of a ship in international waters or a multiple homicide in a school (e.g. a school-shooting) require effective action from all safety and security organizations involved. Many rescue and law enforcement operations require a transfer of information during a change of personnel from morning shift staff to evening shift staff, for example. This exchange is referred to as role shifting. In the case of a high-jacked ship, role shifting may become complicated as the operational area and context may change from one country to another or to international waters as the ship continues its journey. The issues of transferring information and role-shifting during a multi-actor operation is then in question. In this thesis a model for managing a complicated operational entity is constructed that addresses the issues of acquiring and disseminating facts, role-shifting, effective decision-making, and managing related risks.

In this thesis the acquisition and dissemination of facts, role-shifting and managing the related risks are studied from the perspective of different operations in the public safety field as well as from the perspective of a field actor with the writer's personal experience and experience from interviewed professionals within this context. The context of all the above mentioned is an operational entity, which in the best cases consists of planning, action and after-action phases. The operations may be in response to natural or manmade disasters that may be long-term or short-term and require decision-making delegations and role-shifts due to the dynamic nature and rapidly changing conditions and environment. The government officials working in such operations usually follow a predefined command and control model in which the decision-making is the duty of high-ranking officials. One needs information to effectively make a decision. Even in modern society an inability sometimes exists, either technical or human, that prevents the expeditious transfer of necessary information. In many time-critical, life-threatening and rapidly changing situations (an operational entity) decisions must be made in a split-second and often on the frontline. Therefore, time constraints do not allow for decision-making to follow the chain of command; decisions must be made in an ad hoc way depending on the situation.
In this thesis a model for managing a complicated operational entity is constructed that addresses the issues of acquiring and disseminating facts, role-shifting, effective decision-making, and managing related risks in a demanding safety and security field operation.

Key concepts: Role-shift, information transfer, operational entity, decision-making, communications, command & control, incident command

Contents

1 Background

In this thesis the acquisition and dissemination of facts, role-shifting and the management of the related risks are studied from the perspective of different operations in the public safety field and from the perspective of a field actor. The study includes theoretical background information, empirical data from publicly reported operations, observation data and interview data.

The operations may be unexpected and unpredictable, related to natural or manmade disasters, long-term or short-term as well as requiring decision-making delegations and role-shifts due to the dynamic nature of the situations. Communication (both human and ICT, i.e. information communication technology), acquiring and disseminating confidential information (or information in general), role-shifting and managing the related risks are issues facing organizations both in the public and private sector. Currently the organizational structures formed during operations are increasingly complex as they are often inter-organizational or international and require cooperation between several actors and involve multiple stakeholders. Organizational structures are formed in an ad-hoc or situation-driven manner in order to establish the required supportive organizational body to coordinate the operation being discussed.

How prepared are the organizations involved in a situation to acquire and disseminate facts, to transfer confidential information, to role-shift, or to manage the related risks? How are the role-transfers implemented? What happens if only one man conducts the planning of a major operation and then is killed in a traffic accident before the plan is executed? How many companies have been compromised when only one individual has been responsible for the creation or implementation of something crucial and then this individual leaves the company taking with him/her irreplaceable, undocumented knowledge? These concerns make it necessary to consider and implement contingency planning.

The purpose of this thesis is to study which of the following issues is most crucial when planning and implementing a time-critical operation:

- The acquisition and dissemination of facts
- The transfer of confidential information
- Role-shifting
- Risk management as it relates to these issues

In addition the challenge of ad-hoc organizational situations with respect to the above mentioned issues will be addressed.

An operational entity can be a law enforcement operation or a private company's publication project for a new commodity. The definition of an operational entity is somewhat challenging, because it appears that it has not been precisely defined academically. I have established some guidelines for the definition of operational entity that are presented in this thesis. In short, however, it refers to all the essential elements of an operation, e.g. planning and implementing an operation, human resources, technical resources, economic resources, and maintenance. The principles and challenges of transferring confidential information are with regard to particulars quite similar in private and public sector operations. However, The challenges in a law enforcement environment can in some situations be more critical due to the fact that human lives are often at risk.

An operational entity as it is considered in this thesis consists of three fundamental phases: Planning, Action and After-action. Some operations, in both governmental and non-governmental organizations, are re-active, even though most organizations prefer proactive measures (planning & preparations) when the goal is the best possible practice. In order to present a broad view of the issues crucial to a time-critical operation, this thesis approaches the topic from the point of view of a complete operational entity.

The transfer of confidential information is intricate, critical and sometimes problematic for several reasons. Legal, regulatory, organizational, cultural, technical, data protection/encryption, and sociological restrictions represent some reasons that may impede the transfer of confidential information in an accurate or timely manner.

The subject in total, Communication, information-transfer and role-shift in a challenging public safety & security field operation, is extensive and this thesis cannot possibly address every aspect into specific details. It will, however, provide an overview of issues and information relevant to practical common practice and, in particular, to situations where human lives are at risk and effective and immediate responses are necessary.

2 Research settings

The vast amount of literature dealing with the subject, e.g. crisis management, information transfer in the frame of reference of confidentiality and law enforcement operations, field operations of the first responders, includes very little empirically grounded knowledge regarding the acquisition and dissemination of facts, information transfer or role-shifting in an operational entity. Thus, there is an evident need to increase the knowledge in this area. The three primary research questions analyzed in this thesis are the following:

1. How must one plan an operational entity in which the transfer of confidential information (acquisition and dissemination) and role shifting are vital to the outcome?
2. How do the structures of participation organizations and their interdependencies affect role-shift situations?
3. What complications arise in communication and transferring confidential information (acquiring, disseminating or transferring confidential information) within an operational entity?

The research is based on both theoretical background studies and empirical field data. The data for this study has been collected from literature, by means of semi-structured interviews and by observation. The individuals interviewed present professional first responders from various organizations and units. They are all professionals in their field of expertise and are all within the operational entity, but they vary from intelligence to other specialized units. One notable point is that the interviewed individuals hold positions in all organizational levels and are currently involved in field operations. The experience of the interviewed individuals varies from 9 to more than 20 years of service in challenging and rapidly changing operational environments. The interview data was analyzed in terms of qualitative content analysis and systematic categorization of the data. The interviews were not recorded but written down simultaneously during the interview due to confidentiality and anonymity issues. A written report of each interview was submitted to the respective interviewed individual for verification of the written form of his point of view. Names of the interviewed individuals are not mentioned due to the nature of their work and their tasks and positions in their organizations. The interviews have been chosen as a data collection method due to the lack of published sources. Additionally, the field operators have first-hand knowledge of true needs and issues in the true context of this thesis. The published sources heavily support this understanding which is shown later in this thesis.

A large-scale exercise was arranged in Helsinki on October 29th, 2008 for first responders. The topic of the exercise was a man-made disaster and it included several organizations. There was an international observation team, which consisted of ten experienced professionals from different European law enforcement units. The observations were made as a group during two different exercises. During and after both of the exercises, all the information and findings from the observation teams where gathered together and analyzed. As a condition for permission to use the findings from this exercise in this thesis, an agreement was made that no individuals or organizations will be mentioned or otherwise identified.

The purpose of this thesis is to study what aspects of the acquisition and dissemination of facts, the transfer of confidential information, role-shifting and related issues in risk management should be considered when planning and implementing an operation. The operation is described as an operational entity, e.g. a law enforcement operation. This thesis is based on the case study method. According to Yin (2003, 13), case study is an empirical inquiry that investigates and examines a contemporary phenomenon in its tangible context, specifically when the boundaries between phenomenon and this frame of reference, the operation's context are not clearly evident. In this thesis, real-world cases and/or specific parts of real cases are used as well as a few fictional cases. All information from the real cases is based on public sources. The purpose of all the cases, fictional and non-fictional, is to clarify the context of this thesis; the operational entity, the acquisition and dissemination of facts, information transfer and role-shifting in situation-driven events. This case study is descriptive because it describes an operational entity. It is also explorative because it does not have a clear, single set outcome (Yin 2003, 15).

At the same time, quality arguments could be made about this thesis being more of a constructive case study for the following reasons: in general terms, constructions refer to a model or an entity which produces a new solution to existing problems. The usability of a construction is of great importance; the constructions implementation solves problems that emerge in business. (Kasanen, Lukka & Siitonen 1993, 244).

The pictures shown in this thesis describe various constructive solutions and risks about decision-making, role-shifting, communications and information gathering. The challenge of a constructive case study is that the target organizations, i.e. to whom the solution is aimed, have an active role in receiving and implementing any new models (Kasanen & co 1993, 246). All of the solutions depicted in the pictures included in this thesis have been confirmed as being correct? by all of the interviewed individuals in addition to being supported by the referenced sources. Hence the thesis is reliable and valid. Nonetheless, there are limitless operational entities and situations and it may be possible to identify one that might prove to be an exception. This, however, is unlikely to be a common occurrence.

The main unit of analysis in this thesis is the transfer of confidential information in an operational entity. Many hidden units of analysis can be found in this thesis, but they are left for future investigations. The main unit of analysis has been chosen for three reasons: 1) there is a real-world need for identifying the communicational issues in an operational entity, 2) there is a real-world need to explore the issues regarding role-shifting in an operational entity and 3) there is a need to develop a model to enable information transfer and reduce risk in an operational entity.

3 Defining the relevant concepts

3.1 Operational entity

What is an operation? An operation, in this frame of reference, can be anything from a private corporation's publication project for a new commodity (e.g. launching a new mobile-phone to the market) to a procedure for first responders (e.g. rescue mission for paramedics, fire department or for the law enforcement). Due to the used sources however the focal point in this thesis is more within the first responders reality. In all tasks or operations it is preferable that the task is one that can be planned in advance since the goal for the actors is to be able to have the opportunity to establish pro-active measures such as preparations, risk analysis and planning. This is however not a possibility, that the actors would often posses. Many operations for emergency first responders begin very rapidly as a reactive measure by the first responding party to someone's illegal actions or a disaster whether it is manmade or natural. Typical cases include a perpetrator committing a crime, a traffic accident, or a fire for which the first responders begin their response as a result of a 112-emergency call. That is to say, the emergency response center receives a phone call from a person witnessing a crime, and then the emergency response center gathers all the information from the caller and disseminates the needed information to the first responders in the field.

While defining the beginning of a first responder or a law enforcement emergency operation is rather easy, the ending of an operation is much more challenging to identify. Some draw the line at the apprehension of the perpetrator or to the extinguishing of a fire, but in many operations this is not the case. In this thesis, the operational entity consists of three phases: the Planning phase, the Action Phase and the After-action phase. These phases can be divided into smaller segments as illustrated in Figure 3. Planning and preparations are in crucial role, when the operation and the so-called action itself want to be conducted with the best possible outcome. The Action Phase, in short, is the conduction of the actual operation. The After-action phase is about the actions in the aftermath of the operation, such as the debriefing in order to learn from the operation with the focal point on not repeating the same mistakes next time (Interviews 2008 & 2009. If we think about the tasks in the after action phase, we quickly realize that the operation does not end when the so-called active conducting ends. There are many things that have to be done subsequent to the resolution of the emergency itself.

First of all, an investigation of some kind will likely be necessary and that begins after the action phase. An investigation concerns more of the law enforcement segment of first responders. Secondly, if one wants to learn from the incident, information must be gathered from the various phases along the way (Interviews 2008 & 2009). This information has to be analyzed and the lessons learned have to be implemented into working society and the organization levels which deal with similar issues in the future. The dissemination of the lessons learned has to be conducted expeditiously. There is a relevant risk that these lessons learned are forgotten as time passes by (Desourdis 2009).

3.2 Risk management

Risk management traditionally refers to the process of which the goal is to prevent threats and to minimize the deprivations that might occur from these threats (Suominen 2003, 27). Risk management also includes the decision-making involved to prevent or minimize hazards that have been identified by conducting risk analysis (Chong 2000, 68). It is imperative that all the possible risks are studied systematically if one wants to talk about efficient risk management. This implies a system that is in use on a daily basis or, in some cases, even more frequently. A common problem in many corporations is that risk management is considered to be something that is only dealt with by the persons in charge of security or risk management. Risk management is too seldom considered as a preventive measure rather than a compulsory action. Resources should be routinely directed toward proactive and protective measures that are often indispensable to an organization in times of crisis. Risk management should be a state of mind for all company personnel, especially for the individuals working in an operational entity. If the risk management is conducted properly, then the contingency is guaranteed (Berg 2001, 44).

The risks should be managed in a real-time manner and then constantly assessed, re-evaluated and defined. It would be ideal if all the factors could be analyzed as soon as they appear or as soon as the situation or the circumstances seem to change. If one could succeed in this, then it might be possible to be more proactive than reactive. This type of proactive action should be performed at all organizational levels so that any individual should be able to act accordingly in any given situation. A simplified example: If an employee discovers an unlocked door that he knows should be locked, he should lock it instead of leaving it for security personnel to handle.

3.3 Information

In this thesis, the information means facts provided or learned about someone or something, especially in an operational entity. In the underlining meaning of the word, information is the act of informing or giving form or shape to the mind, as in education, instruction or training (New Oxford American Dictionary).

Furthermore, to specify the meaning of information, the following definition is used: "when the data is being refined further and associated with other facts and presented in the manner appropriate to the context it becomes Information" (Rantanen 2003, 8). Information is a broader concept than data; it also emphasizes the attributes describing the data so that it can take a factual form. Information is more understandable than mere numerical or symbolic descriptions. The precise definition of information for a native Finnish speaker, as the author of this thesis is, is somewhat challenging due to the fact that there is only one word in Finnish, "tieto," to describe data, information and knowledge (Rantanen 2003, 8). Keskinen (1999) tries to avoid making distinctions between these concepts and refers to them by the acronym DINK—data, information and knowledge (Rantanen 2003, 8). This is also more than reasonable assumption in the context of this thesis since it would be nearly impossible, as well as unnecessary, to make the distinction between the three.

3.4 Confidential information

Confidential means something that is intended to be kept as a secret. Confidential information is knowledge that is privileged, "confidential" and restricted (New Oxford American Dictionary). Confidential information is everything concerning the operation or the participants (Interviews 2008 & 2009). According to one interviewed individual (Interviews 2008 & 2009) it is possible that when two or more pieces of public information are put together, it becomes confidential information.

According to the interviews (Interviews 2008 & 2009), it is commonly understood within the working societies of the interviewed individuals, that confidential information is formed from the mission-critical facts. However, it is of utmost importance that the individuals involved in an operation do not to speak to anyone about the operation or share any information about the operation. (Interviews 2008 & 2009). The challenge can be in a situation where two or more clusters from different organizations are collaborating in an operational entity, e.g. the different organizations are working together in a same law enforcement operation. There are numerous examples in history of large-scale rescue, military and law enforcement operations that have gone bad when the participants have not successfully shared information (Desourdis 2009 & The 9/11 Commission Report 2003).

Confidential information can be, and should be in some cases, divided into different segments. This technique is used, for example, in outsourcing software industry operations (i.e. software development) to other countries or several partners/subcontractors. Each segment forms a piece of the whole but without the other pieces it is not possible to complete the puzzle and gain a full understanding of the entire project. Figure 1 illustrates this concept of segmentation.

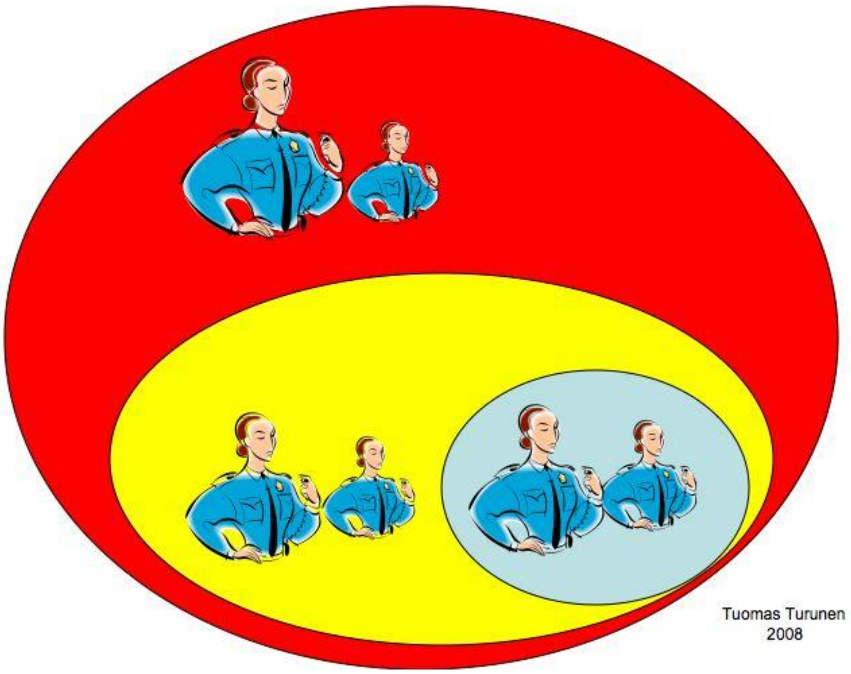

Tuomas Turunen
2008

Figure 1

Segmentation of information

Confidential information is divided into different sections in an operational entity.

Dividing confidential information into different segments is quite demanding. The areas of responsibility in the operational entity define, to a great degree, the need for sharing and dividing information. The segmentation of information is closely related to the different sectors that are within the operational entity.

There is an issue within information segmentation –how to manage all the pieces of information, how to manage the so-called big picture. In many cases, there is only one person, a designated leader, for each of these segments. This leader controls the information and has access to it (Interviews 2008 & 2009). If the leader is taken away from the equation, meaning that he/she will not be available for a reason or another, the question is who else can access the information. Hence it might more convenient to have two (or more) persons having access to the information. Additionally it can be underlined that some global and extremely successful companies, such as Google, IMAX Corp and GUESS?, are managed by “shared leadership" (Alvarez, Svejenova & Vives 2007). The advantage in this is dual: the areas of responsibility can be divided and/or shared. If they are shared, then the risk of losing the information with the event of losing one leader is less likely, due to the fact that the other leader should still have the same knowledge. Hence instead of just one commanding officer, there are two commanding officers in the figure one.

One major challenge is to ensure that the mechanisms are in place to allow an operation to continue even if a key individual is disengaged for a reason or another or if a database, communication network or information transfer-system collapses for any reason. No system should be implemented without being properly tested (Interviews 2008 & 2009). Critical systems such as processes and ICT should have back up systems that are also properly tested.

Many ICT-systems, such as the GSM and TETRA/C2000-networks, work almost perfectly under normal circumstances and under normal workload conditions. However, even these high-standard systems can face insurmountable problems during large-scale incidents —problems so big that the systems collapse (Ministry of Justice 2009, 29). The whole operation is in most cases much more demanding if the communications, i.e. the radio and GSM network, are not functioning properly or at all (Interviews 2008 & 2009).

3.5 Information transfer

In this thesis the information transfer refers to transferring information between individuals even if the information is momentarily stored into a database, repository or memo of some kind. The information can be transferred between individuals face-to-face (so called face-time) or by various types of networks and communication devices (phone, video conferencing, etc.), thus relying on ICT infrastructure as an enabler. In this frame of reference, the information transfer refers to transferring also situational awareness, situation status information, relaying instructions, giving orders, setting guidelines, receiving orders, acknowledging guidelines, and sharing learned lessons (Interviews 2008 & 2009). Within the concept of security management, the demands for information transfer and the needs for correct information and documentation have emphasized (Mäkinen 2007, 104).

According to Rogers, information transfer or knowledge transfer is an attempt by an entity to copy a specific type of knowledge from another entity (Leyland). Leyland does not view the transfer speed or extent to be important; the focus should be on ensuring the desired result, which is to incorporate the new information with the information already existing within an organization. In an operational entity, however, the transfer speed plays a crucial role especially in rapidly changing environments. Decisions are made based on information, preferably correct information, and it must be available as quickly as possible. Time-criticality and real-time transfer and response are essential in this context. As an example consider a fire in a huge congress hotel. A fire in a hotel is extremely time-critical. The fire must be extinguished as quickly as possible in order to save human lives as well as property. The time-criticality in this context is that there is a limited amount of time to consider the various courses of action. Information from the hotel, which is on fire, must be transferred to the first responders as quickly as possible. In order for the fire department to act expeditiously, the information regarding the location of the fire within the hotel must be correct and precise.

3.6 Role-shift

There is very little empirical scientific knowledge regarding decision-making, delegation and especially role-shifting in unexpected and unforeseen situations. There are also not too many studies regarding multi-organizational, international, or multi-actor operations, which can occur during a major crisis or emergency.

In some cases, when information is transferred the role is also shifted from one person to another. For example, a transfer of information and role may occur in a situation where an evening shift manager relieves a daytime shift manager. Ideally, the day shift manager updates the evening shift manager’s information by reporting the progress and possible changes in the construction project, i.e. situation. In other words, the situational awareness, the knowledge and the “role” are transferred simultaneously.

There are different kinds of role-shifts such as:

- Intra-organizational Role Shift. The role is shifted within an operation from one person to another within the same organization. The persons involved are from the same organizational level or are both trained to lead and command such operations.
    - The role-shift can be conducted for many reasons. Here are a few examples:
        - The operation occurs over a long period of time and the duration of the operation makes it necessary to shift the role.
        - The person assuming a specific role is unable to continue working for whatever reason making it necessary to shift the role to another individual.

- Compulsory Role-Shift. Different role is shifted within an operation. A person receives or assumes a different role within the same organization.

    - A specific role becomes necessary in an operation and someone is required to assume the role, which is not originally his/her task.
    - This can be, and usually is, a situation where something unexpected, or unforeseen, happens or some kind of an incident occurs after which the prevailing and functioning party has to assume a new role. In this case, the new role may be something quite different from the everyday tasks of the prevailing actor.
    - A compulsory role shift, the role-shift described here can go "upwards" or "downwards" in the command chain. This refers to vertical movement in the organizations hierarchy.
    - This compulsory role shift can be a situation where the leader has to take a performer's role or the performer has to become the leader of the situation. This is illustrated more accurately in Figure 2 "Role-shift".

- Inter-organizational Role Shift. Same or different role in a different organization.

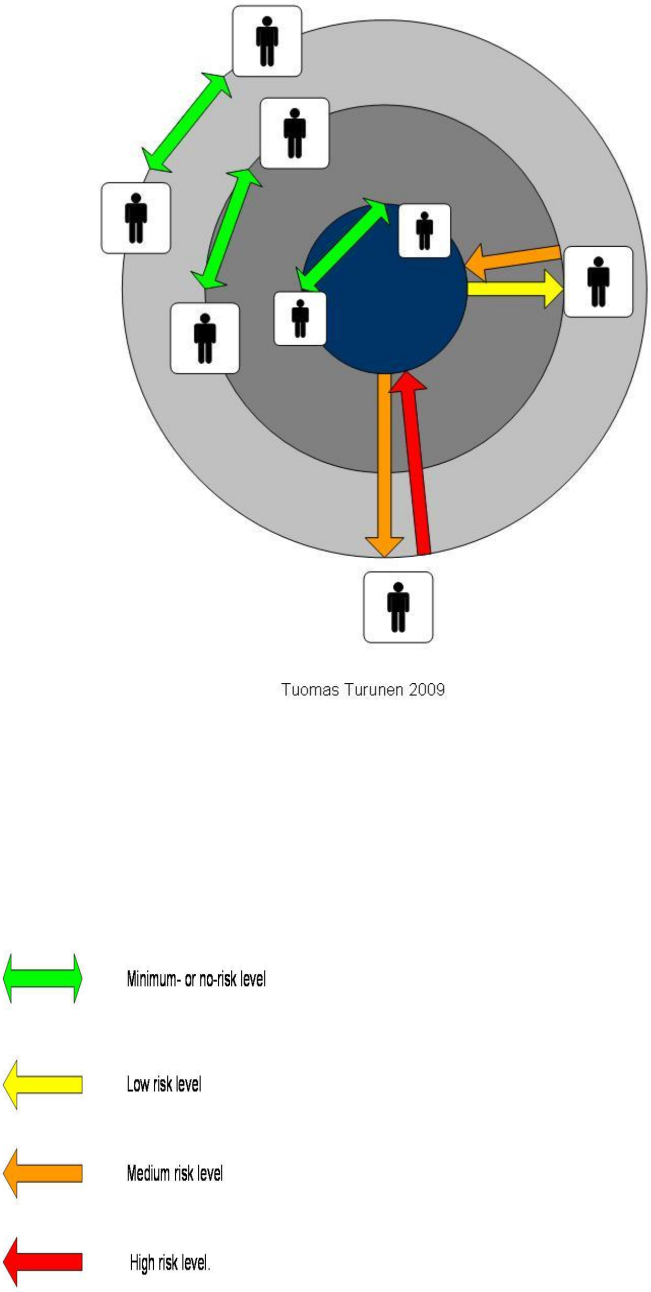
    - In multi-organizational operations it is possible that role-shifts have to be made across organizational borders. This happens quite seldom, because it is a situation, which can be extremely challenging and it is generally unwanted occurrence. Additionally, the risk level in this is rather high from the starting point and it sometimes includes legislative issues. However, this is an issue which has to be considered for the following reasons:
        - In the case of complex and massive emergency, there is always more than one organization as an actor.
        - At times, the participating authorities are conducting almost the same roles or organization A is in a supportive role giving

executive assistance to organizations B and/or C. For example, paramedics are giving executive assistance to police or police is providing security to a doctor, who is evaluating an aggressive patient.

  - Many of the current law enforcement and rescue operations in the present engage elements and participants from various countries and organizations. These executors come from different cultures. While this is not a major concern, the individual organizations' culture, guiding legislation or means of conducting a given tasks may vary and can present challenges.

- The issues in the above example are the following:
  - Potential language problems: If the participants are from different countries, they may or may not have a common language. To have a common language is an asset, but it is far from enough; the operational language has to be the same also for all participants. English is the most common operational language in the international organizations, such as the United Nations, International Criminal Court, NATO and the Europol. According to some of the interviewed persons (Interviews 2008 & 2009), who have in depth experience in international and inter-organizational operations, the common language is far from enough, because the level of English can vary, and often does, enormously between participants. Hence the biggest problems can occur because of communicational issues such as misinterpretations. To succeed in this topic, one needs to conduct proper planning, agreements and training between the participating organizations and countries so that the terminology in the operational environment is the same for all the participants.

- To succeed in this, the participants have to agree on the above mentioned issues in all organizational, operational and administrative levels. This is a goal that is not easily achieved but is necessary to succeed in the search of the best possible practice.



Tuomas Turunen 2009

Figure 2 Role-shift

Role-shift within the same organization.

The innermost circle represents the management level of the organization or the operational management, depending on the context. Whichever the case, the innermost circle represents the people in charge. The ring in the middle represents the deputy or middle management level of the organization and/or the operation. The outermost ring is the operator level. This level represents the individuals conducting the operation in the field, on the front line (e.g. the front line firefighter).

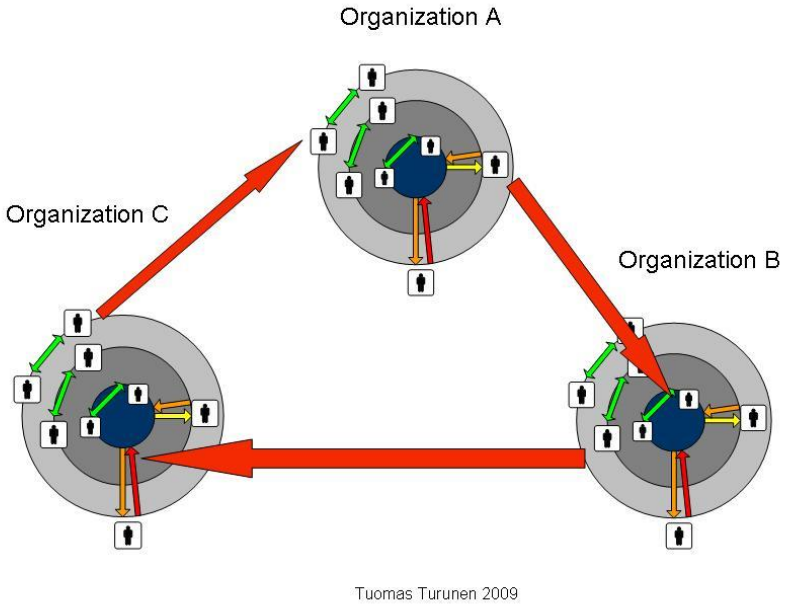
The green arrows describe a role-shift within the same organizational level. The color green is used to indicate a low level risk within the role-shift. The yellow arrow is used to indicate a role-shift from an upper level to the next level downwards. The color yellow indicates an increased level of risk. The risk is considered rather small in scale because the upper level supposedly manages the tasks in the lower level. While not true of every organization, in many operational organizations the manager has, at some point in his/her career, taken care of the deputy manager's position. Regardless, this role-shift has an increased risk level compared to the role-shift within the same organizational level because the tasks and job-description are different from the normal duties (Interviews 2008 & 2009).

The orange arrows are used to indicate a role-shift made either upwards in the chain of command or downwards in the chain of command if more than one organizational level is passed. One of the interviewed individuals (Interviews 2008 & 2009) pointed out that a new leader who assumes a position across the managerial border due to a role-shift might actually have fresh and functional ideas about how to lead the operation. While this might be true in some cases, it should not be tested in a time-critical and/or life-threatening situation due to the possible risks.

The red arrow is used to indicate a role-shift from a lower level to an upper level when more than one organizational levels are passed. The risk level has to be considered rather high, when several organizational levels are crossed, e.g. CEO of a large business company assuming the role of low-level sales person within extremely short amount of time.

The colors are not meant to tell the ultimate truth regarding the risks or the risk values. They are, however, indicating guidelines and they are meant to be taken as recommendations concerning risks within role-shifts. This should also create an understanding, that the role-shift is an unwanted situation –yet often needed. There are actual cases involving a role-shift situation that would have been characterized with a red arrow (high risk), but the outcome of the operations were still successful due to the competencies of the single participants who assumed the role upward over hierarchical and/or organizational levels (Interviews 2008 &

2009). This outcome, however, cannot be considered typical and should not be relied on in standard practice since role-shifts have to be performed with the lowest possible risk level. It follows that during a role-shift another person should replace one individual with the education, training and most importantly, the competence to fulfill the required tasks whatever they might be.



Tuomas Turunen 2009

Inter-organizational Role-Shift

Figure 3

Inter-organizational Role Shift. Role-shift from one organization to another. Note that this model also applies to a role-shift within an organization when roles are shifted between different units.

An inter-organizational role shift is not necessarily a major concern in an operational entity but it is still an issue, which has to be carefully considered due to the cross-border nature of many operations in the modern day world (Interviews 2008 & 2009). An inter-organizational role shift, this concept has to be planned and its risks, with all the possible scenarios, have to be analyzed in the pursuit of excellence. Such analysis, however, can be impossible in time-critical, rapidly changing, ad hoc situations. Hence, all the planning, agreements and courses of action ought to be conducted in advance as much as possible.

Frontex is the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union—the agency for external border security in the European Union. Frontex has experience in multicultural and multi-organizational operations where actors and participants come from different countries. Its responsibilities are to co-ordinate activities of the national border guards in ensuring the security of the EU's borders with non-member states (Frontex).

The following paragraphs describe the context of this chapter:

Operation called "Indalo 2007" conducted by Frontex (Frontex). The operation's focus was to target illegal migrant boats from Algeria and Morocco to the Spanish coast of Levante. The main nationalities of these illegal immigrants were mainly Moroccans, Algerians and the people from the so called sub-Saharan countries in Africa.

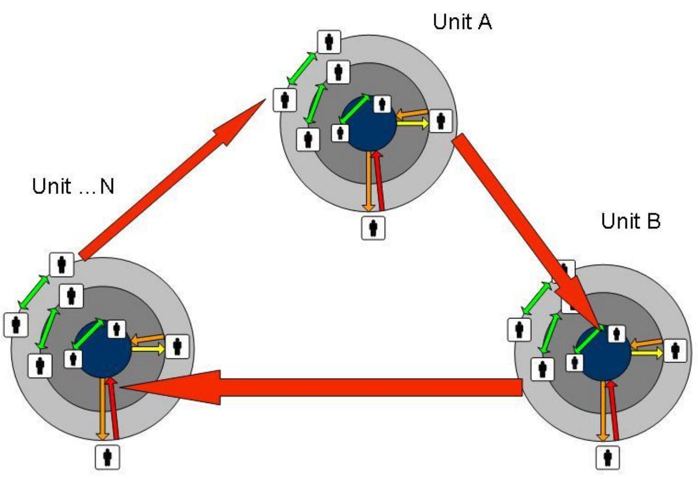
There were seven different countries from the European Union as participants in the operation Indigo. The operation lasted for three weeks and it cost 1, 7 million Euros. It is not known if the preparations are included to this sum. It gives nonetheless the impression, that the operation has to be decently funded and resources are required if results are wanted to be seen as in this operation.

Budget (EUR): *1,700,000*
Implementation: *30/10-20/11/07*
Hosting Member State: *Spain*
Participating Member States: *Germany, France, Italy, Spain, Malta, Portugal, Romania*
Operational resources: 5 c*oastal patrol boats, 3 offshore patrol vessels, 3 aircrafts, 2 helicopters, 10 experts*
Total number of incidents: *22*
Illegal migrants intercepted: *309*
Illegal Migrants detected in operational area: *180*
Illegal migrants detected out of operational area: *165*
Facilitators arrested: *4*

(Frontex)

The role-shift between different between organizations, in this frame of reference between organizations from different countries and cultures, can be demanding. On a smaller scale the issues arise when roles are shifted between different units in the same organization in the same operational entity. For example, organization A is conducting an operation. The operating units are A, B and C. The areas of responsibility are divided between the units but for some reason these areas are changed. This is an undesired situation (Interviews 2008 & 2009). The expectations of the society and the stakeholders in the private sector are high towards the caretakers of the incident. Everybody has the right to expect that the best and the most applicable persons are used in order to conduct the best possible practice (Interviews 2008 & 2009).

Role-shift in the same organization between different units



Tuomas Turunen 2009

Intra-organizational Role Shift

Figure 4

The role-shift can be, and often might have to be, conducted within the same organization between units who have been trained to do different kinds of tasks or they are not interconnected. The units' areas of expertise are different from each other and the methods of conducting work vary from each other. In such a situation when role-shift is needed between units, the risks are usually high (Interviews 2008 & 2009).

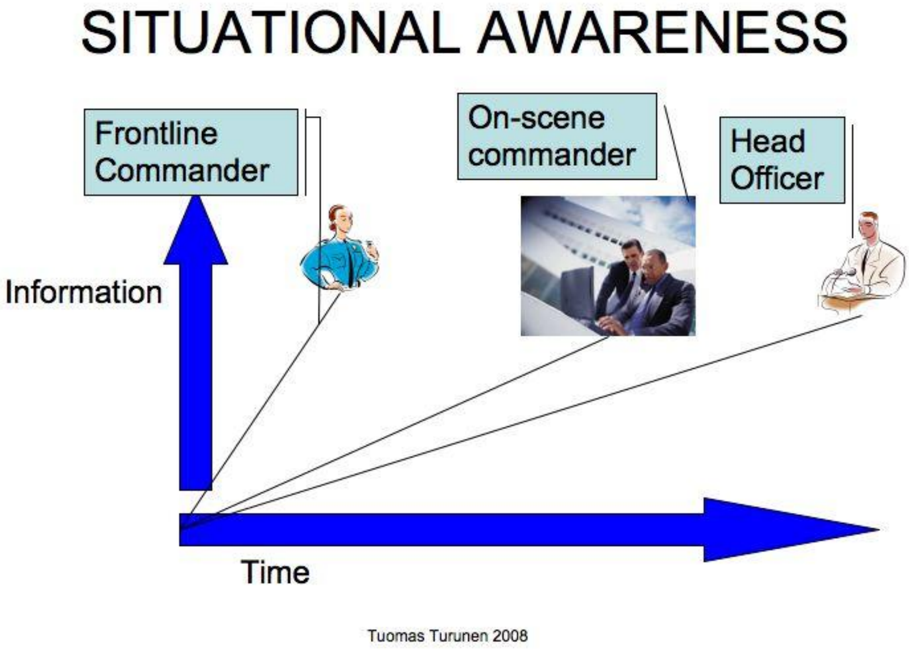
Normally, in an operational entity, the actions of these units can be planned and coordinated to work with each other so that each unit performs it's own task. However, in a time-critical and rapidly changing environment these so-called "originally planned" tasks cannot always be conducted by the unit, which was intended to perform them. This can be the case for various reasons, e.g. the unit suffers from a sudden and unforeseen ineptitude or a dilemma of some kind, which is causing problems. Hence, another participating unit or units might have to complete tasks that were not originally assigned to them or are outside of their area of expertise. This requires participants to quickly adapt to the prevailing situation. Once again, the quality and the competency of the individuals are emphasized (Interviews 2008 & 2009). The good, or even excellent, skills of an individual are not always enough to achieve success due to the fact that it is not just an individual but a whole team, who conducts the task. Proper training and preparation of the entire team is a necessary element for success. The key to success or to make things a lot easier if the preparedness and training are in order. This requires good quality training and in this context, the training includes communications and the transfer of confidential information with the focus on transferring situational awareness. Experience plays an important role in all this. Conducting any operations is infinitely easier and the results more predictable if the participants have solid experience with the business in question.

3.7 Contingency planning

In a law enforcement or business environment, situations in which the continuity depends on one individual should be avoided. The commander of an operation is responsible for analyzing the risks associated with contingencies of an operation. The outcome of an operation can be disastrous if key players are removed from the operational entity for any reason. The organization should be build so that no matter what happens today, the tasks can be carried out also tomorrow. For example, a CEO of a car factory is very interested in the fact that no matter what happens today, the factory will be able to produce cars also tomorrow and the days after. An organization’s procedures should be established so that business can be carried out regardless of the players in place. Contingency planning for crises big or small is a rising priority, especially in an operational entity (Myers 1999, 1).

According to Myers (1999, 31) there is a constant need for cost-effective solutions when it comes to contingency planning. The probability of a situation arising that requires a contingency plan is low, therefore, organizations are often unwilling to allocate resources to contingency planning. One Detective Chief Inspector who was interviewed, however, says that when human lives are at risk, it isn’t an issue of cost-effectiveness only effectiveness. A small saving can become a disastrous expense when the potential risk becomes a reality (Interviews 2008 & 2009).

3.8 Situational awareness



AdSa. Ad-hoc Situational Awareness

Figure 5

in 1) Time-critical and 2) Life-Threatening situations. In some cases it takes more time for those not on the front line to achieve an up-to-date situational awareness.

Situational awareness within the context of this thesis means that it consists of the following increments: location, amount and quality of personnel, location of other actors and bystanders, location of the theatre, weather/temperature affecting the operation, operational abilities, resource allocation, decision-making history, and condition of the actors (e.g. remaining time of operational capability before shift).

- Location of the theatre
- Weather conditions
- Terrain
- Location of the personnel
- Amount of the personnel
- Quality of the personnel

- Operational abilities of the personnel
- Location of the actors and possible bystanders
- Quality of perpetrators (if perpetrators occur in the operation)
- Quantity of perpetrators
- Previous and current actions of the perpetrators
- Other resources (budget for the operation)
- Decision making history

The *location* refers to the location of the operation be it in a city center or in mountainous terrain. The location can, and usually does, determine partly the course of action. For example the location of fire affects in to the decision-making; there is a huge difference between courses of action of the rescue department if a fire is in a large hotel or if it is in a farm building used for storing grain. When thinking a situation from a military commander's point of view, the *location and amount of personnel* is crucial information for the leader. Without such knowledge it would be impossible to assign tasks to different units efficiently. The location of the bystanders can also be more than relevant, should those exist in the theatre. Usually there are plenty in urban terrain. Additionally the location of perpetrators also is more than relevant should there be perpetrators in the operation in question.

The *weather* refers to the weather conditions in the area of the operation. Should the weather conditions be extremely difficult, e.g. the harsh environment of the Norwegian Lapland in the wintertime, it has immense effect to the operational abilities of the participants. Hence the weather can be of great importance in situational awareness.

The *terrain* refers to the stretch of land with the focal point on its physical features. There are relevant differences between mountainous terrain and an archipelago as simplified examples of different kind of operational terrain. This is due to the fact that different kind of methods of operations and logistical solutions are required in different kind of terrains, e.g. road transportations offer limited solutions to operations, which take place in archipelago.

The *quality of personnel* refers to the skills, previous experience and knowledge of the personnel, especially regarding the current situation. The operational abilities are a bit similar to the quality of personnel, but still there are distinguishing differences. The quality of personnel can be of a high standard, but still their operational abilities can be poor. This can be the case because of injuries or lack of tools needed for the task.

The *quality of perpetrators* refers to the professionalism of the perpetrators, e.g. are the perpetrators members of organized crime group capable of extreme actions or are the perpetrators teenagers conducting their first act of crime. There are several similar relevant issues between the perpetrators and the other participants, i.e. law enforcement, which play an important role in the context of situational awareness. *Previous and current actions of the perpetrator* are of great significance as well as the capabilities, when making decisions about course of action from the law enforcement's point of view (Police Act).

The *other resources* refers to additional, yet relevant factors in the operation and especially when creating situational awareness. These factors are situation dependant. They can be, for example, the economical resources or the available parties giving executive assistance. The economical resources have straight influence to the amount and quality of personnel and/or equipment that can be used and it also affects the amount of time that can be used for the operation.

The *decision making history* refers to actions (and decisions) made by the participant(s) involved in the operation, e.g. the decisions made by the rescue department from the beginning of the operation. The decision-making history has a relevant meaning in situational awareness. Without this information, it would be quite challenging to have a clear and a thorough understanding of the situation. It must be pointed out, that there are several situations where there is no prior decision making. This requires acting accordingly. To be more precise, in unforeseen and/or unexpected situations e.g. life-threatening and time-critical situations, there are hardly ever any of the above-mentioned factors to be used in creating the situational awareness. In addition it has to be mentioned, that the above-mentioned definition or description of factors of situational awareness is not fully comprehensive, but it gives a compendious understanding of the concept of situational awareness. (Interviews 2008 & 2009).

Description of roles in figure 5:

- Frontline commander or the officer closest to the situation in the field
  - Physically on the frontline
  - Has physical contact, proximity, to the incident
    - Sees and hears the prevailing situation authentically
  - Co-ordinates and commands the personnel on the frontline
  - Fulfills the tasks given by the on-scene commander
  - Uses means given by on-scene commander to accomplish the objectives

- On-scene commander
  - Is near the immediate action, but does not necessarily have visual contact with the scene

- Assigns tasks to the frontline commander
- Establishes rules and guidelines to direct the actions of the Responsible for the implementation of the operation on the field
- Co-operates with participating organizations
- Provides (additional) resources
- Provides situational awareness to all levels of the operational entity
- Makes the overall decisions on the scene

(Kuker 1999, 9-13, Emergency Management & Public Health; Rake 2003; Loflin 2009)

According to Rake (2003) the on-scene commander is the person, who has the overall command on the scene of the crisis situation, even if, or when, other levels of decision-making exist. Loflin (2009) and some other authors use the term incident commander. This is equivalent to the on-scene commander. Regardless of the term used, the prevailing issue is whether the on-scene command has an adequate level of situational awareness to make appropriate decisions. As previously noted, communication channels can be out of order, for a reason or another, causing the on-scene commander to be unaware of the prevailing situation.

- The head officer
    - Is located in the head quarters of the organization.
    - Establishes general guidelines for the operation
    - Provides additional resources
    - Manages public relations
    - Provides situational awareness to the management of the organization

Situational awareness is essentially connected to the role-shift. A role-shift refers to the transferring of related contextual information, or situational awareness, from one person to another when a new person assumes the same role or when a new organizational body takes charge of the operation. The contextual information refers to all relevant issues including the information from the planning phase, intelligence information, capacity, skills and experiences of the operating personnel, and information about the tasks conducted during the operation so far if the context information is viewed broadly. Transferring the context information can be very demanding especially if there is a limited amount of time or no time at all for a face-to-face discussion. It is preferable that a role-shift, information transfer and the updating of situational awareness be conducted in a face-to-face manner referred to as face-time. (Interviews 2008 & 2009)

Situational awareness varies enormously between operation participants in rapidly changing environments. The difference between information levels varies greatly depending on the role of the participant. The frontline leader or even an ordinary officer has, in many cases, the most up-to-date situational awareness of the actions on the front line if the situation is time-critical (Interviews 2008 & 2009). The situational awareness of the on-scene commander and his/her superior officers is significantly different from the actual situation during the action phase. Depending on the situation, communication capabilities, and individuals involved it takes time for the on-scene-commander to gain a clear understanding of the circumstances.

The challenge is to transfer the information and the situational awareness from the front line to the on-scene commander, without consuming time (Interviews 2008 & 2009).

A
c
c

According to one on-scene commander, "I got a clear view of what had happened after the action was over" (Observation 29.10.2008). I had no chance of making decisions, because everything happened so fast. All the decisions were made by the people in the front line" (Observation 29.10.2008). This model concerning situational awareness and decision-making applies especially to time-critical and life-threatening operations. Most actions of the responding officers must be started ad hoc even though standard operating procedures have been predetermined, i.e. the marching order has been trained and/or written in advance. The responsive action of the first responders is initiated from outside of the first responding organizations and would not otherwise occur.

It is important to recognize that the risk assessment illustrated in Figure 5 does not apply to situational awareness for all possible scenarios. The associated risk can sometimes be exactly the opposite of what is illustrated—the best view of the situation may be in the operations center. The challenge is to create a system that transfers the situational awareness in real time to all participants, who *de facto* need the information, regardless of their physical whereabouts.

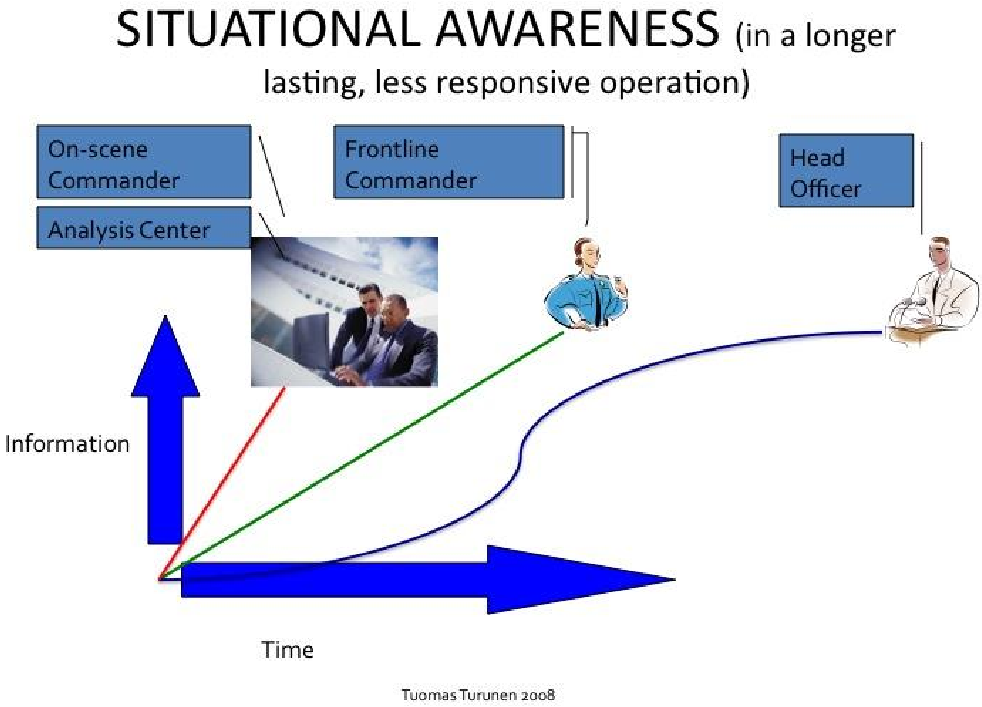


Figure 6 ANSA (Analysis Center Situational Awareness)

The Picture above describes the situation mentioned in the previous paragraph – there are situations, where the best situational awareness is not in the front line, but in an analysis center or another place or position. The operating parties in figures 5 and 6 are the same, with an additional analysis center, which is connected with the on-scene commander. The connection between the analysis center and the on-scene commander should work flawlessly and in real-time (Interviews 2008 & 2009).

In figure 6, the analysis center and the on-scene commander learn about critical information concerning the incident. At this moment and time, the "front line commander" or the officers in the field do not have a clear situational awareness. The best situational awareness is with the on-scene commander/analysis center. An example of this: The analysis center/ on-scene commander receives information, that the perpetrator, who has been unknown until this time, is called J.D. and is wearing a red jacket. This information is transferred to the front line commander and/or the field operators, so that they can do the required actions (Interviews 2008 & 2009).

When the first responders know the situation or incident beforehand, they have more time to plan and react to the forthcoming event (Interviews 2008 & 2009). Hence it can be said, that situation is less responsive and longer lasting compared to the incident described in Figure 5.

It is imperative to understand the prevailing situation in order to make the right decisions. If the decision-making party does not have a clear understanding of the situation, the results may be devastating. During the 9/11 attacks on the World Trade Center Towers in New York City the situation was chaotic. Emergency calls overwhelmed the emergency response center. According to the 9/11 Commission Report (295), the emergency response center was *"plagued by the operators' lack of awareness of what was occurring"*. The callers from inside the Towers were told to remain where they were and wait to be rescued. Many of them were put on hold and the emergency call was further transferred to a superior officer in the emergency response center. The lack of information inside the emergency response center combined with instructions that callers maintain their position and wait for rescuers to arrive may have resulted in numerous casualties during this horrible act of terror (the 9/11 Commission Report, 294-296).

4 Operational entity – examples

The majority of law enforcement operations are reactive meaning that officers respond to a situation that has already occurred. The general objective, however, for law enforcement is to prevent unlawful acts from happening in the first place. This objective can in many occasions be accomplished with proactive measures.

There are many occasions when the authorities, the police or the rescue department, have the ability to plan and prepare in advance for an operation. An example of this: an apprehension of an international organized crime group or a large athletic event such as the World Championships in a specific sport.

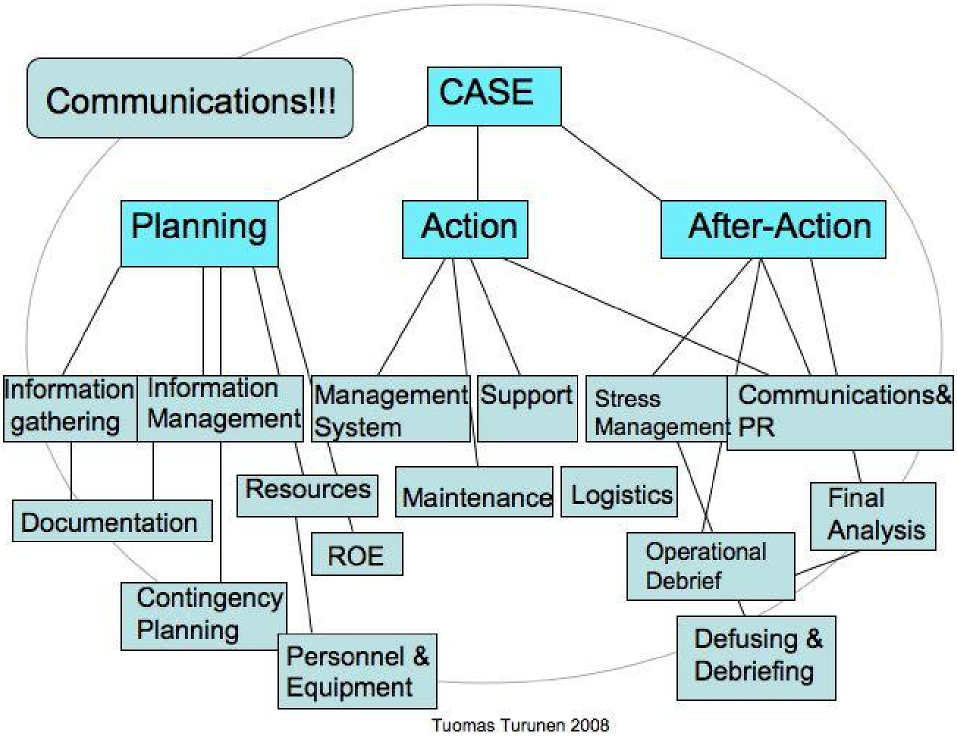
The Planning Phase occurs prior to the actual event and during this phase many things need to happen. Continuing with the sporting event example, information must be gathered, e.g. number of participants and spectators, possible threat scenarios –such as the accommodations and event venues must be inspected so that safety and security plans can be made, resources must be evaluated and gathered, cross-organizational planning must occur between organizers, police, customs, border guard, private security companies, the list is vast. It is clear, that public-private sector partnerships must be established and they are of high importance. There is also a great deal of other situation dependant issues.

The Action Phase occurs during the event itself and there are a considerable number of tasks to be conducted during this phase. Proper preparation, usually, ensures that all essential and important tasks during the action are assigned. One of the most crucial elements of the Action Phase during the "event" is to ensure that all of the key players have a real-time perception of the prevailing situation (Musashi 1993, 98). This can be referred to as situational awareness. In order to succeed in accomplishing the tasks during the event, one must have the ability to act according to the situation. This is not always easily accomplished, if ever, and is entirely dependent on the skills of the involved individuals and organizations. It sets the demands for flexibility, resilience and key competencies for individuals and within an organization. If the nature of the event changes rapidly and radically, different resources may be required with regard to both individual and organizational skills.

The After-Action Phase begins after the event itself has ended. It has been said, that this is the point when much of the action should start, even though it feels like everything is over and nothing needs to be done (Interviews 2008 & 2009). Information regarding actions during the event should be gathered together from different sources and should be analyzed properly so that individuals and organizations can learn from their experiences. These different sources are situation dependant, but they can be one or more of the following: different organizations, bystanders, media, and other open sources, e.g. Internet. One of the most crucial things is to gather the information from all the organizational levels.

As described above, the operational entity can be divided into three phases:

1) The Planning Phase
2) The Action Phase
3) The After-Action Phase



Tuomas Turunen 2008

OPEN (Operational Entity).

Figure 7

The operational entity is divided into planning, action and after-action phases.

Planning phase

- Information gathering
- Information Management
- Documentation
- Contingency Planning
- Resources
- Rules of Engagement (ROE)
- Personnel and Equipment
- Plan
    - Emergency plan
    - Primary plan
    - Alternative/additional plans
- Communications
- Logistics

Action phase

- Conducting action plan
- Management system
- Maintenance
- Resources
- Support
- Communications
- Public relations
- Logistics

After-Action phase

- Communications
- Public relations
- Operational debrief
- Stress management
- Final analysis
- Distribution of lessons learned

An operational entity can be described with a mind-map as illustrated in Figure 7. This is just an example and the contents of the boxes can and should be changed according to the needs of the user. It cannot be highlighted enough, that communications is extremely important in all the phases of the operation (Interviews 2008 & 2009).

4.1 Illustrative example cases

In this thesis there are fictitious example cases of operational entities presented. The examples are more or less varying from unexpected and unpredictable incidents to foreseen acts of organized crime. The imaginary case can be related to natural or manmade disasters, varying from long-term to short-term operations. Some require decision-making delegations and role-shifts due to the dynamic nature of the situations and also because of the international and inter-organizational environment and context. The purpose of these examples is to enlighten the context.

4.2 Case 1

Case 1 is a fictitious law enforcement operation. There are several organizations from several EU-countries working together including customs, police—both local and national—and border guards. A law enforcement unit in Scandinavia has learned that a band of internationally organized criminals are planning to traffic narcotics from the Mediterranean area into two or three of the Scandinavian countries. The perpetrators are planning their operation carefully by conducting reconnaissance in the operational area several times over several months before the actual delivery of the narcotics.

Different law enforcement units exchange confidential information in a short period of time. Several police and customs units are collaborating with each other over the borders. Conducting an operation of this nature raises questions regarding:

- Who has the overall command;
- How planning, action and after-action phases are coordinated; and
- What types of communications are necessary in order to maintain the operation without great difficulties?
- What kinds of channels or ways are used to transfer confidential information?
- Is the dissemination of the information centralized to a single party?
- Is this party known to all the operational participants, especially the ones obtaining reconnaissance information?
- Is the information dispersed among the participants equally?

- Is the information sent to the operational participants as soon as possible?
- Risks within the case of role-shift? According to the interviews (Interviews 2008 & 2009) the meaning of personal contacts are of great importance especially in international operations. When a person is changed during the operation, there is a risk that some participants are more reluctant to continue the collaboration in the same level.

4.3 Case 2

Case description. Two perpetrators commit an AMOK-situation, in other words a school shooting or an active shooter incident. According to the Wikipedia the word amok is of Malayan origin and it is transferred by Oxford Advanced Dictionary as "*mad with uncontrollable rage*". Amok-situations can occur in different kinds of environments, such as shopping centers, schools, governmental facilities and so on. As an example, in 2001 in Switzerland, in the city of Zug, a man entered a governmental building killing 14 politicians and wounding 10 people before killing himself (BBC). All this happened in about ten minutes (BBC). Regardless of the theatre of the amok case, all the amok-cases share very similar challenges for the first responders. The challenges are the following:

- Achieving situational awareness from the scene to the first responders
- Locating the perpetrators
- Locate the facility or the operational environment
- Locate the participating units and entities from different organizations, e.g rescue department, police, civil guard etc. both in- and outside the facility
- Acquire maps of the theatre or the floor plan of the facility
- Gathering (relevant) information
- Disseminating information
- Allocation of resources
- Decision making
    - Who has the best situational awareness?
    - Who has the ability to make the decision?
    - Who has the authority to make the decision?
- Communication

    - Risk of ICT-overload
    - Risk of GSM-network overload
    - Possibility of sending documents, images and/or video from and to the frontline?
        - In order to facilitate situational awareness
    - Number of joint radio channels between organizations?
- Shared on-scene command post between organizations?
    - In order to facilitate situational awareness and to decrease the amount of radio traffic
- Collaboration between organizations?

5 Issues regarding the transfer of information and communication capabilities

As pointed out earlier, there are various reasons why confidential or conceptual information for the operational entity is not transferred to the parties for whom that information is vitally important. Conceptual information includes all the information concerning the operation as well as seemingly irrelevant information because such details could later on become relevant information within seconds.

In the corporate world, most of the information concerning project details is classified because companies do not want competitors to gain the advantage. Trade secrets are carefully guarded and the transfer of information is something to be avoided. However, in time-critical and life-threatening public safety operations in which several authorities including governmental bodies and private actors cooperate, the transfer of information may be complicated by legal limitations, confidentiality issues and a mixture of different organizational cultures. Furthermore, the transfer of information is a highly people-oriented activity in which personal characteristics affect the success of the transfer (Interviews 2008 & 2009).

There are several reasons why information is not transferred in an operational entity, although, necessary information should be transferred efficiently, quickly and reliably especially in time-critical and life-threatening situations. Necessary information may be in several repositories as well as undocumented tacit knowledge, thus, making the acquisition of information a challenge. The reason for not transferring the information can also be of course a human error (Interviews 2008 & 2009).

The baseline in an operational entity is that the information needs to be secured and protected. One may ask, why is this. It is due to the fact, that decision-making without information is more than difficult. Additionally, in several countries there are privacy laws, which dictate the information, stored and sent, concerning individuals within law enforcement context need to be encrypted. The operation at hand dictates the need for the information transfer. In some operations the need for information is greater than in other operations. More specifically, in some operations a) the need is greater on the front line than in the command post or b) the need is greater for the commander than for the first officer on the scene. The need for information is dictated entirely by the situation. Herein lies the challenge. How do the participating organizations and individuals know where the most crucial information is located and how is that information transferred in order to enable a swift response and continuity of the operation? In some cases the information has to be transferred between organizations as well as within the organization at all levels. Because of this, it is imperative that the information transfer process works flawlessly. According to the interviews (Interview 2008 & 2009), all critical systems have to be field-tested before being implemented.

5.1 Legal issues

In most governmental situations where cross-organizational cooperation is required, the legal issues must be carefully considered. There are many national-, EU- and international laws and treaties that must be checked thoroughly when conducting operations in this frame of reference. All the possible scenarios should be analyzed from the juridical point of view in regular bases in order to minimize the legal gaps in the case of actual critical incident. For example, are the laws and the agreements, not to mention the practical part, in place between neighboring countries concerning the use of digital law enforcement radio network for mutual emergency response tasks, e.g. a train accident in the border of two or more countries. There are some examples of this subject, in general and not specifically concerning radio network, such as the international crisis of M/S Estonia. M/S Estonia sank in the Baltic Sea in September 1994 claiming 852 lives being one of the deadliest maritime disasters in the late 20th Century. One of the most critical issues was a communicational issue (Onnettomuustutkinta). The incident was not initially treated as a large-scale disaster and the requests for executive assistance did not apparently reach the right parties (Onnettomuustutkinta).

5.2 Sociological and Cultural Issues

Most employees want to be good at what they do. They want to be important to the organization and to the working society. Many people want to come up with new ideas and monopolize those ideas in order to make themselves irreplaceable to some extent. It often happens that a subordinate presents an innovation idea to his/her superior and, after a period of time, the superior presents the subordinate's innovation as his/her own. Once this happens, the subordinate is unlikely to present another idea to the same superior. Because these types of situations are common, people are inclined to keep their own ideas and information to themselves.

According to Leyland (Leyland), a multicultural environment creates some challenges for the information transfer process. People with the same ethnic or cultural background share information with each other more easily than with individuals in other cultural groups. In other words, there is a cultural border, which sometimes creates an obstacle for information transfer process.

The differences between the cultures of organizations themselves also present challenges during the transfer of information and communication. Hierarchical structures, the level of formality, the used concepts and perception of individuals concerning the information exchange. During international operations cultural issues may be further emphasized. Political viewpoints, religion etc. can pose conflicts and barriers. Moreover, even the gender of a person can unfortunately result in a conflicting situation (Interviews 2008 & 2009).

5.3 Technical issues

Technology can be either a great enabler or, in some cases, a hindrance in information transfer and communication. Information communication technology solutions present a wide spectrum of different systems that can be used for the previously mentioned purposes. However the systems may not always be:

- Available
- Usable
- Ergonomic
- Reliable

(Interviews 2008 & 2009).

The 9/11 Commission report is highly critical of the Federal Bureau of Investigations (FBI) information system on several points. Because the FBI's information systems were in such a poor state, field agents usually did not know what investigations agents in their own office, let alone in other field offices, were working on. The officers of the Federal Bureau of Investigation conduction analysis did not possess easy access to the relevant information concerning the threat targeting the United

States. As a result of this, it was nearly impossible to develop an understanding of the threat from international terrorist groups. (Frontline).

6 Planning phase

There is an old saying that proper preparations prevent poor performance. Planning plays a crucial role for an operational entity. Planning takes a thorough understanding of the operational environment, available resources and capability as well as risk analysis of possible threats. Although the planning phase is of great importance, there is another old saying that once the action starts, all plans are thrown into the bin. While this is not always the case, it reveals how difficult it is to plan properly. It is nearly impossible to take everything into account, especially when one seldom has all the correct information about the relevant factors. However, it is still not an option to leave the plans undone. The planning phase plays a very important role, which is to prepare the participants for the operation as well as for possible complications (Interviews 2008 & 2009). In this frame of reference, the preparation refers to both psychological and physical sides of the process of making ready. These are the possible scenarios or events that might occur.

If the participants have analyzed all the possible and imaginable risks and scenarios thoroughly and they have conducted all the preparations as well as possible, then it will be much easier for them to adjust their own actions according to the actual situation. There is always the x-factor, e.g. the scenario or incident, which could not have been predicted or it did not occur to any participants' mind, which we cannot know, but we must do our best to prepare ourselves for everything –even for the unexpected and unforeseen.

Time-criticality has an important role in the planning phase. How much time does one have for planning? Usually it is good to have a well-prepared schedule and deadlines for the planning phase. The time-management in the planning-phase is emphasized. The goal for the best possible practice in the planning phase is to create the best possible plan under the given time. This can be compared to the time-line demands in project management where the delays can be economically disastrous (Pelin 2008, 107-109). According to one of the interviews (2008 & 2009), the planning should be conducted with the utmost exactness when human lives are involved –hence such an operation can hardly be compared with a solely economical operation. It can be reasoned that the economical operations have consequences, which may reflect to individuals' welfare, but no-one hardly gets killed or seriously injured.

The time-criticality should not always be considered as a negative factor. Sometimes it is an advantage that there is not much time to plan (Interviews 2008 &

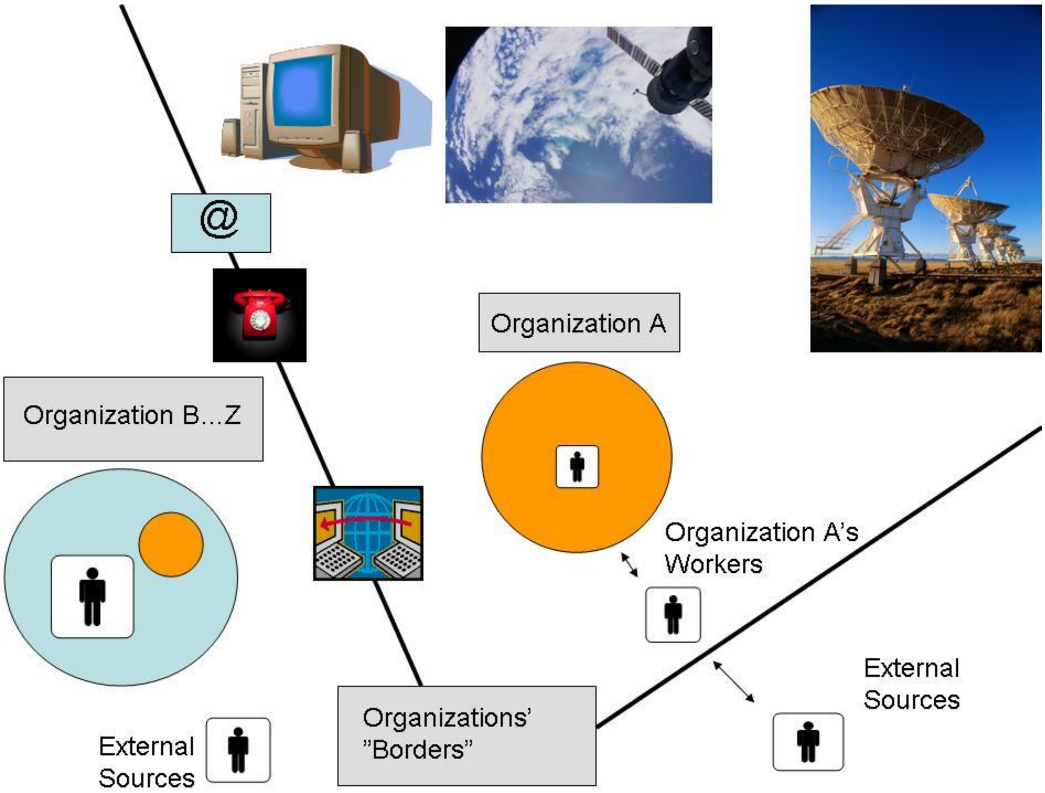
2009). This depends of the nature of the operation. If the working society that is conducting the operational entity with a short planning timeframe is professional and the preparations for quick-starts are decently planned and tested, then it is not a problem to succeed in the operation.

The lack of time should not be used as an excuse to leave the decisions unmade or to refuse of conducting the operation (Interviews 2008 & 2009). This concerns especially the leaders in charge of working societies and operational leaders. Karl Von Clausewitz (Clausewitz 2002, 42-44) has written about coup doiél. According to Clausewitz coup doiél is about seeing and understanding the situation as it is and the ability to act accordingly within a blink of an eye. This has been studied in various military academies.

One tool for the planning phase is the Work breakdown Structure (WBS). This system has been successfully used in managing several projects (Pelin 2008, 93-106). According to Pelin, the project planning should be divided into smaller pieces or work packages. A leader or a person in charge has to be named for each package. The challenges appear again in the forms of transferring the information and keeping up the contingency.

6.1 Information gathering

Information gathering has a crucial role in each and every operation. According to different persons who were interviewed to this thesis, the ability of an organization to use the gathered information is often quite limited (Interviews 2008 & 2009). The problem is not to get information, but the problem is to get the correct and essential information from the information flow, to get it analyzed and to get it to the people who need it in order to carry out the tasks as well as possible.



INGA (Information Gathering). Tuomas Turunen 2009.

Figure 8

In picture four, the organization A is gathering information for an operation. The organization A ought to already know the existing information within the organization. This includes the information within the personnel and in databases or in an information repository. Unfortunately this has not always been the case even in high-quality intelligence units (The 9/11 Commission Report).

Organization A is gathering the information from inside its own organization. All the information gathering should be conducted by a certain team or individuals trained for the task (Interviews 2008). “All the information should come in the organization to the same unit, center or team, and all the information should be analyzed and passed on to the field from the same place” (Interviews 2008).

Information is also gathered from various sources, also outside the organization if it is possible and/or needed. The used methods differ between organizations in question. The picture four illustrates an organization, A, which uses external organizations and individuals and other open source methods in order to gain the best possible situational awareness concerning the operational entity. This has to be conducted by trained professionals, analysts, instead of other, non-trained personnel, conducting an ad-hoc analysis (Interviews 2008 & 2009).

6.2 Information management

The information should usually be segmented, especially in bigger operations as shown in Figure 1 on page 12. It is however imperative to have an operational structure, where all the information is gathered, analyzed and managed. There has to be “someone” who is on top of the situation 24/7. Usually the personnel responsible for their segments are not very fond of sharing information (Interviews 2008 & 2009). This can be due to many things, like sociological, cultural, legal and/or technical issues, which are presented in chapter 5.

Before the 9/11 terrorist attacks upon the United States, the authorities of the United States had a lot of information concerning the perpetrators and the attacks to come. The biggest problem was that the information was shattered across all the different security agencies such as the CIA, FBI, NSA and so on. Also the people in charge of the national security had peaces of this information. The challenge was, that in the USA they did not have a common centre for all this information where all the information from different sources would have been put together, analyzed and passed on to the decision making parties. According to the 9/11 Commission Report (258), on July 5th, 2001, representatives from many authorities discussed about the al Qaida threat. The attacks were imminent according to the intelligence information. The representatives were apparently told not to disseminate this information further on to the individuals who conduct the work on the field. (The 9/11 Commission Report 256-260). It can be said that these actions did not improve the possibilities of impeding or hindering the Al-Qaida attack against the United States in September 2001.

The CIA gave an order in June 2001 to all its station chiefs to share all information concerning al Qaeda with their host governments (The 9/11 Commission Report, 256). These station chief were all working outside the United States. It is very demanding to share information between different organizations, not mention information exchange and/or sharing between countries and nations. Although there seemed to be a lot of information about the oncoming attacks, there was a lack of implementation to actual executions to disrupt such plots (the 9/11 Commission Report, 259). The domestic agencies did not have directives or a plan how to respond to the threats (the 9/11 Commission Report 264). It can be said, that even the correct information is pretty much useless, if one doesn’t know what to do with it.

According to Ambassador Cofer Black, coordinator for counter terrorism, the intelligence sharing was a reality between U.S. agencies before the 9/11, but it has to be made much easier than it was. As a result of these issues, the Terrorist Threat Integration Center (TTIC), the Terrorist Screening Center (TSC) and the other security agencies such as the CIA, FBI, Homeland Security and so on are meeting every day with each other to analyze and share information. Black agrees with the 9/11 Commision Report, which states that the law enforcement agencies have to move from a "need-to-know" to a "need-to-share"-based system. (Black & The 9/11 Commission Report).

Information management is not only an issue in operations concerning national security, but also concerning much more smaller case scenarios in everyday law enforcement environments –also in Finland. Sharing the information is a challenge, but another challenge is the amount and the location of the information. First of all, it does not have to be big or inter-organizational operation, where there is a lot of information coming from several directions and all the information is put on to one individual's shoulders. The arrangements or the organization should be build so that too much pressure would not be put on to (ICT-Solutions and) individuals. Each system should have a functioning back-up system or two (Interviews 2008 & 2009). This requires good resources or efficient allocations of resources. It also requires a thorough risk analysis on the vulnerabilities and "pressure points" of the system. In other words, it needs to be found out which points and/or individuals get the most pressure. The goal is to have a minimum amount of pressure points.

Secondly, the location of the information is a challenge that needs to be surmounted. The information needs to be in a place, where all the individuals whom might need it, will also be able to get it whenever they need it. According to the Interviews (2008 & 2009) the problem is to find a place where to keep the information so that only the right people will access the information from whatever location and whenever it is needed. Hence there is a need for portable and mobile solutions.

The challenge in information management is also the fact that the confidential information is transferred even when it should not be. The confidential information can be misused intentionally or accidentally. One of the biggest challenges for the domestic and international law enforcement tasks is the information leakage (Interviews 2008 & 2009).

The Media plays also an important role in the information management. Actually, it plays a crucial role, which might become paramount at all the phases of the operational entity. Eric Lichtblau (2006), a well-known American journalist, became aware of the United States' National Security Agency's super-secret Terrorist Surveillance Program and it's highly classified information gathering methods and – capabilities (Goldsmith, 2008). According to Goldsmith (2008), Lichtblau was first about to reveal these security agency's methods and capabilities in an article, which was to be printed in the New York Times, but the " White House pushed back hard first with meeting hosted by the president's senior counterterrorism officials, and then with an extraordinary plea from president Bush himself". The Terrorist

Surveillance Program was an unlawful program of information gathering, e.g. phone-tapping, Internet and e-mail-surveillance conducted by the Bush-government (Goldsmith 2008). The author of this thesis is not taking any sides in this matter, but underlining the fact that the leakage of information to Media or any other external party might cause challenges to information management in any part of the operational entity.

6.3 Communications in planning phase

According to WordNet, which is the Princeton University's large lexical database of English, "*communication* is defined as the activity of communicating, activity of conveying information. It is something that is communicated by or to or between people or groups. "A connection allowing access between persons or places".

The communication is more than crucial in the operational entity and so it is also in the planning phase. It is of utmost importance that the correct information is not only available to the right people, but that it is also usable and understood. It is more than often, when the information changes during the planning phase. Hence, it is paramount for the attending parties to communicate with each other. The often rapidly changing environment, rapidly changing circumstances and changing information about the context at hand put enormous pressure to communications, if the best possible outcome of the operational entity is the goal.

As it has been described in this thesis, the operational entity is usually a task for a team or several teams, depending on the organization and the context. Communications is a necessity for teamwork. According to one of the interviewed field officers, the outcome of the planning improves when there is efficient communication between the participants throughout the planning phase (Interviews 2008 & 2009). This seems to be the case especially in operations, where there are a great amount of participants from different work groups with different areas of expertise as their responsibility. It is remarkably easier for the person in charge to collaborate directly with the experts concerning the possibilities, risks and challenges in the planning phase. The additional value is that again the situational awareness improves between participants and the risk for misinterpretations decrease.

6.4 Information transfer in planning phase

Information transfer in telecommunications is defined as the process of moving messages with the user information from the sender to the sink (the place in computing, where the message gets written out to) (Wikipedia). This thesis is not concentrating into ICT-solutions (Information and communication technologies), but it is an area, which cannot be left totally out either. Furthermore, the information transfer is a crucial part of this context –the operational entity. The information transfer is closely connected to communications and in this frame of reference there hardly can be one without the other.

As it can be seen in the figure 7 (Information gathering), information for the operation is and can be received and gathered from several locations, by several means and by several actors. The information is, or can be, gathered passively or actively. In other words, eyewitnesses etc can give the information to the law enforcement or first responders in general. The demand of rapid information flow puts enormous pressure to the organization. Therefore the organization's structure should enable all information transfer to and from all directions (Carter 2004, 4).

6.5 Role-Shifting in the planning phase

The concept of role shifting has not been extensively studied. Nonetheless, the role-shift is an everyday task in numerous professions and working places and work sites. In everyday life, the metro- or the bus drivers are changed several times.

An example from a fictional law enforcement operation's planning phase: *A law enforcement operation is being planned and the planning phase takes for six months. The operation is a high-risk arrest with five police teams including over 40 operators working in the field. There are also other law enforcement organizations involved and the total number of participants is well over one hundred.*

One individual conducts all the planning for the 40-man unit and he/she does not share any information with anyone, but only some hours before the operation.

The person planning the operation does all the reconnaissance for the operation and does not let anyone else in to the operation's area prior the task. The same person liaises alone with other organizations involved in the operation. This person makes notes to his/her own notebook and is the sole person controlling the operation's planning. None of the information is saved into a database etc.

All the participants start rolling into the operation's area. The teams that are planned to conduct the apprehension take their positions from the terrain. At this point all the teams are briefed about the plan. According to the plan, the apprehension is supposed to be conducted in position A.

However, the on-scene commander makes a decision to make the apprehension in position B, which has not been previously taken into account by the tactical teams because all the critical information had not been shared.

The tactical teams arrive to the place B and try to apprehend the perpetrators. There is a surveillance team at the place B, but the tactical teams learn this at the last minute. The leader of the tactical teams would like to use the surveillance team as an asset, but he does not have the locations of these officers.

The overall command of the operation transfers the needed information to the leader of the tactical teams. The tactical leader takes control of the situation, but three of the seven perpetrators manage to escape in to the woods. The tactical leader starts to co-ordinate the search-patrols, but he is injured severely by the shots fired by the perpetrators. It takes a lot of time for the next officer to gain control of situation and the tasks, which the wounded officer in charge had already started.

It is quite easy for the above-mentioned example to picture some major risks and non-contingencies in the information management and transfer. What if the person planning the operation gets injured or dies prior to the task? What if and when the information needs to be transferred to another place in a time-critical situation? Can the information be altered by accident and so on.

There is a “five-rights-rule” concerning information, information transfer & management and situational awareness:

- The right information
- To the right people
- To the right place
- In the right format
- At the right time

(Source unknown)

Information is needed in decision-making and the information needs to be correct. The information has to be available or at hand for the people who need it. Therefore the information has to be in the right place and/or it has to be transferred there. This requires that the information is in a transferable format and that there is a working communications system, which allows the transfer.

If we take a closer look into the case, which is above mentioned, we have the following findings:

- The right information was not available to the right people. This means that the leader of the tactical teams did not have a real-time situational awareness. He/She would have needed the same information with the on-scene commander or the leader of the surveillance teams.

- The information was not in the right place. The person in charge would have needed the information in the field. Also the information of the rapidly changing operational environment (the escape of the two perpetrators) should have been transferred with all the context-information to the on-scene commander in an intelligible form. It often requires more, than just verbal communication to understand the situation at hand.

- The information might have been in a right format, but the transfer of the information combined to a role-shift showed the non-contingency of the transfer. The new leader had to start almost from the beginning.

6.6 Documentation

In order to keep up with the information of the operation, the documentation of the information is imperative. The information has to be stored into a safe place, but it must be also accessible. This is very challenging, but not impossible. No system or operation of any kind should be dependable on one individual. This applies also to the documentation. The documentation should be restored in a place, where it can be accessed easily, and only by the people who have the authorization for it. In reality, this requires a sophisticated documentation system, which is reliable and can be accessed wirelessly –also from the outside of the office (Interviews 2008 & 2009). This is due to the fact that the vital information might come when ever and from wherever. The demand for instant and real-time information transfer is often required in emergency management and also in commercial projects.

In order to learn from operations and the issues from the past, the lessons learned (and the context information) have to be documented and once again, they have to be accessible to the individuals, who need the information. A simple example of this: *international guests are coming to visit the University. One person from the university has all information about the schedule of the visitors' flights. All this information is in his/her e-mail, but not anywhere else. The university has promised to arrange the ride from the airport. On the day, when the visitors are arriving, this person with the arrival information does not come to work and cannot be contacted by phone.*

The documentation usually has a paramount role in the role-shifting. Especially in cases, where the role shifting is done in an ad-hoc way, without prior notice. Also the context of the information can be and in many cases is vital. If the contextual information has been documented, it can help the person in the new role to cope with the situation (Interviews 2008 & 2009). This is in the cases, where the roletaker has time and possibilities, e.g. the access to the documents, to familiarize oneself with the situation and the immediate operational history.

7 Action phase

The action phase can begin from the initiative of the private company, corporation or law enforcement actor or by the actions of the customer or the perpetrator in the law enforcement scenario. In some law enforcement or emergency management cases however, the action phase can start in a more responsive way e.g. by a phone call to the emergency response center. According to Hellenberg & Visuri (2009, 19), the additional governmental, rescue and law enforcement authorities can receive information about an on going or already happened crisis situation or a law enforcement operation either through official and confidential channels or from the media. It is imperative for all operation participants to get correct information about the current situation in the operation (Hellenberg & Visuri 2009, 19). With today's information technology, the information of disasters will most likely reach the media and the large audiences rather quickly. The bystanders, victims of disasters, eye-witnesses etc. send pictures and videos about incidents to media and therefore the information is available in open sources e.g. the internet almost in real time. The information flow can be enormous.

Correct and up-to-date information is needed in order to make decisions. If one does not have information, it is easier to fall into ineptitude in decision-making. In some cases the best and most up-to-date source of information, also for the law enforcement community, can be obtained from the open sources.

If the action phase has to be conducted as a responsive action, it is more likely that there will be the following issues in carrying out the operation:

1. The lack of or the limited amount of time
2. The importance of the values or the social order in stake
3. The uncertainty of the situation at hand, that is the situational awareness
4. The element of surprise

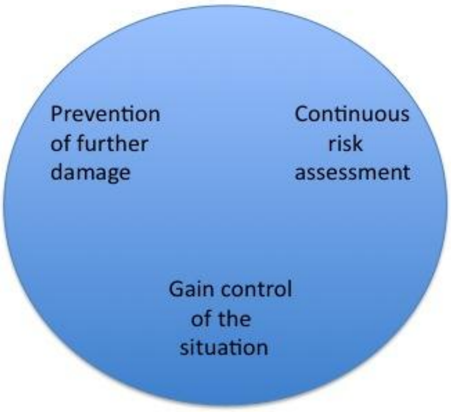
(Nikula & Hellenberg 2009, 21)

According to the Finnish Ministry of Justice's Investigation Commission of the Jokela School Shooting (Ministry of Justice 2009) in major disasters no authority can work alone, but co-operation is needed between actors. The operational parties should not merely trust on their own resources. Besides, a few organizations possess all the needed areas of expertise in a large-scale event, not to mention a large-scale disaster. Information sharing and training at organizational levels is required in order to achieve a working relationship between the actors. This means the actual and operational interoperability between the first responding organizations. Also in reality and in the field –not only on the paper in the form of an agreement.

When the action-phase lasts for a long time, the costs rise remarkably –at least in the majority of the cases. This affects to the resources and not always in a positive way from the field operator's point of view. The costs are usually cut down, if the wanted results are not met in time. (Patric, Murray, Burke & Kayyem 2007, 4). This could mean diminishing personnel and/or equipment, which might lead into unwanted results, e.g. compromising the safety and security of the surroundings or the participating parties.

The goal of the action phase depends on the situation at hand. What is the nature of the operation? Is it to put out a fire in a ferry bout or in a farmhouse? Is it to stop the actions of an active-shooter in a shopping mall or to solve a domestic disturbance situation?

All in all, the following can be said about the goals of an action-phase. There are many things to be taken care of. For this purpose there are various checklists and procedures created by first responders, governmental officials and management books authors (Burke 2007, 193-194, 294). However, the problem or the risk with checklists is that sometimes they might diminish the amount of thinking of the person interpreting the checklist. In other words, sometimes it is challenging to act according to the situation. It can be easier from time to time to read the checklist and to conduct the tasks in the order of the checklist. In most cases this might actually work. However, there are numerous situations, where the checklist or at least the order of the things to be done, have to be fitted in the situation. This is challenging. Therefore, the author of this thesis prefers to present these "to do-lists" as a circle. The purpose of this is to present the same vital things in a way which will make the user to think about the most suitable action for the situation. The danger or the risk in this is that this model requires more from the end-user, but then again, it is meant for people who make these decisions for a living.


Prevention of further damage
Continuous risk assessment
Gain control of the situation

Tuomas Turunen 2009

7.1 Management System

With “Management System” in this thesis is referred to the ways of controlling the execution of operational entity. The definition is derived by the author of this paper from the definitions of management and operational systems, which refer to managing operations with and/or without computer software and giving directions to operational activities (Wordnet).

The operational management is one of the key elements in all kinds of operational entities. It is imperative for the success of the task to have a management system that works regardless of the location or the individuals involved. The operational management system has to be clear without a doubt to all participants and it has to be planned, trained, analyzed, implemented and tested beforehand in order to work also in the most challenging environments (Interviews 2008 & 2009). If this is done ad hoc, the success of the operation cannot be taken for granted.

Operational entities management system is as close to a project management system as possible; in theory the liabilities of projects from different areas share the same challenges –from the management’s point of view. The “boxes” described in the figure six, OPEN –the operational entity, vary between different kinds of projects, but they all still ought to be there.

7.2 Maintenance

One of the key-issues in each and every operational entity is the maintenance. The importance and the role of the maintenance are imperative, especially in large-scale operations and those of long duration. If the maintenance does not work or cope with the demands of the operational resources and the prevailing situation, the outcome will most likely be undesired. Here in the context of maintenance, the operational resources include such things as human resources, logistical resources and supplies.

To master the maintenance in an operational entity is somewhat of a challenge. This is related to the several things e.g. the duration of the operation, as mentioned above, but also such factors as the terrain, traffic communications, or the density of population. In some areas the climate can also play a challenging role for the participants of the operation. The more demanding the terrain and the climate, the more the operation usually depends on the maintenance (Sun Tzu 1998, 133, 138).

7.3 Communications in the action phase

The communications in the action phase are very demanding. The more the participating organizations, the more demanding the communicating gets. The more the participating countries, the more demanding the communicating gets. (The 9/11 Commission Report, Ministry of Justice 2009 and Nikula & Hellenberg)

To succeed in communications is somewhat challenging in many situations and especially in rapidly changing and life-threatening situations such as in a large-scale disaster. There are many factors that have influence on the matter. Depending on the nature of the action and the quality of the participants.
The following topics have influence to communications in the action phase. The list is not fully comprehensive, but these factors, qualities or the lack of them are emphasized in the action phase:

- Number of participants
  - Their skills, e.g. experience, stress management skills
- Number of organizations
  - Their abilities to collaborate, e.g. their experience in working jointly together
- Technical means of communication, e.g. radio network, GSM-network, other ICT-solution.
  - The reliability and the dependability of the network
  - Also between different participating organizations

7.4 Information transfer in the action phase

The need for information transfer in the action phase varies between different kinds of operations. The need for information transfers usually increases the more the longer the operation lasts (Interviews 2008 & 2009). In the case of a high jacked ship, which is cruising in the international waters, the information transfer is needed over borders and between private and law-enforcement actors.

According to Kennedy (2009), the most important thing in communicating in an acute crisis situation, like a school shooting, is to deliver the correct information to the right people as fast as possible. In Kennedy's context the information needs to be transferred to teachers and first responders so that they can act according to the situation. Kennedy also states, that the needed information can also be transferred by e-mail, visual electronic displays, faxes, pop-up messages and so on. This is true to some extent, but what if and when the network collapses or is otherwise not in use? The only option is to build information transfer and communication networks that endure a lot of pressure.

7.5 Role-Shift in the action phase

Role-shifting is usually a lot easier, when there is a great amount of time to it. In other words, if person A is transferring his/her tasks to person B and they have no time pressure, e.g. they are not in a hurry, the role-shifting is a lot easier compared to a situation where person B has to take the role instantly, without a seconds notice. However, the lack of time, demand for speed and action are often typical qualities for the action phase. As mentioned in the Role-Shift chapter 3.5, there are things that have to be or should be transferred "with the role". It is a question of transferring the situational awareness with all the needed contextual information. Due to the above mentioned, the role-shifting in the action phase can often be extremely challenging.

The three most important things, the key factors to success in the action phase are speed, decisive action and the element of surprise. The activities have to be conducted with such a speed, that the possible obstacles, natural or manmade, cannot hinder the wanted outcome from the actions of the first responders. The surprise, as well as speed, is needed in order to gain control of the situation. (Gollner 2008).

All organizations consist of individuals. There abilities are emphasized in role-shifting. The needed skills can be enhanced with training. This dilemma or the issue of needed capabilities is very old and it is briefly dealt with in the next chapter.

7.5.1 Strategic Intuition

To succeed in receiving or taking a role in a role-shifting situation requires good qualities and experience from the new "player" in the role. So-called strategic intuition is often needed. This topic has been discussed in Europe since the times of Napoleon, but even longer in Japan and China. For some reason this matter of great importance has not been studied as largely among the first responders as it has been within the military.

According to Clausewitz (2002, 42) to succeed in the unexpected events of a battle, one has to have the ability to make the correct decision in a blink of an eye. This is referred to as *Coup d'oeil*, which is an old French term from the times of Napoleon. It is more of "mental" than a "physical" ability to see the situation at hand and act according to the situation –sometimes even against the prior plans. (Clausewitz 2002, 42-43).

Clausewitz wrote the above mentioned in the beginning of the 19th Century. Miyamoto Musashi (1993,16 & 82) wrote about the very same thing in Japan in the 17th Century. In battle one needs to "understand the moment" regardless of everything else. (Musashi 1993). Sun Tzu (or Sun Tzi depending on the source) wrote very thoroughly about the same topic about 2000-2500 years ago (Sun Tzu 1998, 74). The same context is conversed on many other Chinese strategy classics as well.

According to the interviews (Interviews 2008 & 2009) the challenge of being able to act according to the situation stays the same even in today's operational environment. This ability can be trained and it is the task of the persons' responsible for training to create exercises, which force the people in the exercise to think about the prevailing situation and act according to that particular moment.

8 After-action phase

After-action phase is the last phase of the operational entities phases, which is described in this thesis. The after-action phase is crucial. If the "lessons learned" is conducted with care and good quality, it will serve all the three phases in the future (planning, action and after-action phase). This means that if all the information about the conducted operation is properly gathered and analyzed, there is a great opportunity to conduct the next planning, the next action and the next after action phase even more efficiently and with better results as a whole.

8.1 Communications in the After-action phase

The after-action phase can sometimes be the most important phase within the operational entity. This is due to the fact, that by doing everything as well as possible in this phase, it will serve all the other phases in the future –the next planning-, action- and after action phase. Sometimes organizations and individuals within forget the need for after-action phase. The participants might occasionally think that the operational entity ends when the action ends. (Interviews 2008 & 2009).

I
n

To communicate with the participants, especially after an inter-organizational event, is of utmost importance (Interviews 2008 & 2009).

In large-scale events there is most likely a need to communicate with other important parties, e.g. the media. This is a challenging and an important task, which is left for future studies. However, real-time and reliable co-operation is needed with the media. According to the Finnish Ministry of Justice's Jokela report (Ministry of Justice) it is *extremely important to ensure proper communications as part of situation management and to inform the families of those involved, the local population, and any organizations involved in the crises in one way or another as soon as possible*. This goes for all the phases in the operational entity, but as the first responders' primary goal is to prevent further damage and organize a rescue operation, the communications with the external parties might sometimes be somewhat of challenging (Ministry of Justice).

8.2 Information transfer in the After-Action phase

The demand for information transfer in the after-action phase can occur especially in cross-organizational collaboration. It might be advantageous for several parties to conduct also cross-border information exchange. This should not only be limited into case studies in the sense of learning organization, but also expanded into planning and acute disasters.

8.3 Role-Shift in the After-action phase

The role-shift in the after-action phase can mainly concern the people in charge of the after-action phase. As in other role-shifts, the transfer of correct situational awareness emphasizes. The after-action phase should normally have adequate amount of time to conduct the role-shift, should it be used for one reason or another.

8.4 After analysis

The after analysis has a very important role in the operational entity. The after analysis prepares for each and every part of the operational entity, if it is done thoroughly, critically and objectively (Interviews 2008 & 2009). The results of the after analysis give new ideas how the next planning-phase should be conducted. It also provides information for the upcoming action-phases and how they should be dealt with. What went wrong and why? In what areas can we improve and in what areas we did too much and why did we do it…

There are many operations to my understanding where the after analysis was made very poorly or not at all. As a result of this many individuals have been trying to develop the after analysis system. Just because they want to share their unfortunate experiences so that the next one in the same role would not have to go through the same mistakes. There is an old military phrase about not being able to remember anything. This phrase refers to the unpleasant, yet almost universal fact that nobody seems to learn nothing from anything.

The after-action phase is crucial. If the "lessons learned" is conducted with care and good quality, it will serve all the three phases in the future (planning, action and after-action phase). This means that if all the information about the conducted operation is properly gathered and analyzed, there is a great opportunity to conduct the next planning, the next action and the next after action phase even more efficiently and with better results as a whole. (Interviews 2008 & 2009).

According to one of the interviews (Interviews 2008 & 2009), the challenge with the after-analysis is the implementation of the findings from the analysis. All the participants, even at all organization levels, agree to the findings and agree that the issues have to fixed, there is no guarantee that these findings are taken into practice.

8.5 Stress management

Stress management in this context has a wide, yet relevant meaning. One of the most important things in leading a police unit, running a store or managing a big factory is to maintain the ability to keep the core process running. For example, the owner/CEO of a car manufacturer should be interested in the fact that no matter what happens today; the factory will be able to make cars also tomorrow, the day after and the days after that. The core process in a law enforcement environment is to take care of the operations also tomorrow –regardless of today's tasks and regardless of their effects to the working society. The operational entity has to be managed in a way, which enables the unit and/or the participants to conduct operations day after day –if needed.

Stress management (or crisis management) is an important part of work welfare. It is "a good to know fact" for the field operators that the higher and the highest command has taken these things into consideration. In other words, the field officers know, that the management level has a contingency plan also for the personnel, in the case of a serious emergency, e.g. a casualty within the working society. The field officers know, that if something goes wrong, no one is left behind or left alone with his/her problems. There can be several things, which might have to be taken care of, such as the preparations for interrogations, court hearings, healthcare and insurance issues. Sometimes these tasks can be too challenging for an individual to carry out. Hence the support and co-ordination from the organization are more than welcome. According to the interviews (Interviews 2008 & 2009), these issues trouble the minds of the field officers -both consciously and subconsciously.

Crisis management (and Critical Incident Stress Management) is a tool for leadership. It is a lot easier to lead people, if you know at least the basics of traumatic situations and the trauma healing process. Also if one thinks about contingency planning or cost-efficiency, then crisis management system should be taken into account. Why? It is not just a cliché, that the workers are the most valuable resource in an organization. If there are no employees left or they are not in an operational condition, there is no one left for the managers to lead nor is there anyone to conduct the operations.

Critical Incident Stress Management according to Everly and Mitchell:

1) Pre-crisis preparation
    a. Stress management training
        i. For individuals and organizations
2) Disaster or large-scale incident, e.g. school and community support programs and staff advisements
3) Defusing
    a. Small group discussions
    b. Assessment
    c. Triage
    d. Symptom mitigation
4) Critical Incident Stress Debriefing (CISD)
    a. 7-phase, structured group discussion
    b. To mitigate acute stress symptoms
    c. Assess the need for follow-up
    d. Provide psychological support
5) One-on-one crisis intervention/Psychological support

   a. Throughout the whole crisis spectrum

6) Family crisis and/or organizational consultation
7) Follow-up and assessment for additional treatment

(Everly & Mitchell).

The education and training of the operators take years. The training is *very* expensive and the commanders obviously want to have the field operators in a working condition for as many years as possible. Therefore it is cost-efficient to make preparations for critical incident stress management. Risk management and quality management can be added into this concept very easily. The risk management is obvious, but it is also about managing the issues and leading the personnel with good quality. One of the focal points in several quality standardisation systems is work welfare and preparations for crisis management.

To lead the incident, working society and organization in crisis and in the aftermath one needs to have the basic knowledge in stress management. Training in stress management is needed in all levels of the organization, due to the fact that all organizational levels are involved in crisis situations –especially in the large-scale ones.

Communications and co-ordination play an important role also in the stress management as a part of the operational entity. It is imperative that all the stress management occasions, e.g. defusing and follow-ups, are co-ordinated properly. The information concerning the employees working condition has to be transferred to the decision-making parties. This is quite challenging and it definitely requires a so-called case-officer, who is in charge of the so called after action issues, for example the stress management and the issues within. There are many issues to be dealt with in this phase. Therefore it is of high importance that there is a designated case-officer, who has not been involved in the operation’s action phase. This is because an “outsider” is needed; that is a person who is familiar and competent in the context in question, but has not him/herself been directly affected by the situation. (Interviews 2008 & 2009).

8.6 Final analysis

The final analysis and the usage of the analysis in training and improving the overall conducting of operational entity have probably the most important role. There is no use to extract all the slightest details of “rights” or “wrongs”, decisions or events, if nothing is learned from them (Interviews 2008 & 2009). The best possible practice involves learning the lessons from adverse events. Without transferring the learned lessons into the upcoming tasks, the risks cannot be reduced (Cowan, 2003). It is also very important to make sure that the results of the analysis are implemented into action. It is not enough to arrange education about the new findings or information, which have been discovered from a field operation –as an example. It is as important for the people in charge to make sure and to confirm that the new information is internalized and taken into everyday practice (Interviews 2008 & 2009).

8.7 Defusing & Debriefing

8.7.1 Defusing

Defusing is an old military term, which means disarming a bomb or another explosive. It also refers to deactivating and making ineffective, especially when it comes to the explosives. Psychologists and several other workgroups such as the first responders, who encounter stressful and traumatic situations, have adopted the term defusing. In the context of operational entity, especially within large-scale disasters, the (psychological) defusing is used to describe the methods used after a possibly traumatic incident, which has possibly occurred to the participants in the operational entity. The purpose of defusing is to easy the trauma symptoms with the individuals involved in the traumatic situations, to gain the working condition if it is lost and to evaluate the possible needs for further treatment. In other words, the purpose is to normalize the situation. (Saari 2003, 149).

The defusing has to be conducted by a trained individual. Within the working societies of first responders, a trained peer more and more often conducts the defusing. This is due to the fact, that it is easier for a fire fighter to talk to another fire fighter, who is used to the same working conditions and is familiar with the challenges within. It appears to be so within the context of law enforcement and the first responders, that defusing is used more and more, while the more thorough psychological debriefings are conducted rather seldom. (Saari 2003, 149-153).

According to some of the interviews (Interviews 2008 & 2009), the psychological defusing plays an important part in traumatic incidents. Hence it has to be taken into the operational entity as an important part, should it be needed.

8.7.2 Debriefing

Psychological debriefing is an ”in-depth defusing”, which is lead by a trained professional, e.g. a psychologist. Psychological debriefing might be needed when the defusing itself was not conducted or it was not effective. Debriefing has four objectives, but the primary objective is to help the individual, and hence the working society, to cope with the situation and to regain the working condition. (Saari 2003, 156-158).

The psychological debriefing should be arranged when the operation has been:

- Sudden, unforeseen and
- The situation has been traumatic and shocking
- Long-lasting and stressful
- Physical injuries
- Death

(Saari 2003, 173).

In conclusion, the psychological after-action measures emphasize, if the operation has traumatic features in it. In the modern day world of the security and first responding professionals, the defusing and the debriefing play a role of great significance. The minimum requirement for contingency planning, when it comes to operational entity and the after-action phase, is to have preparedness for psychological counter measures, should they be needed.

9 CONCLUSIONS AND FUTURE RESEARCH

9.1 CONCLUSIONS

The operational entity is an extremely vast concept, that engenders diverse, situation and context dependant, approaches. It is however, self-evident, that the overarching approach to the operational entity is convergent in several challenging public safety and security field operations. The field operation or the operational entity should consist of the planning, the action and the after-action phases-whenever this is possible –as it has been presented in this thesis. This is due to the demonstrated fact that planning and preparations are often more than beneficial prior to conducting any operations. The action-phase itself can start as a responsive measure to any variety of incidents, however, the execution of the action-phase is much more effective, and the possible outcomes are more predictable, if the planning and operational procedures are in place before the commencement of the action-phase. The after-action phase, when executed as described *supra*, prepares effectively for the next planning, action and after-action-phases. In other words, the operational entity should prepare the participants for future operations regardless of this fact pattern. This should be the case even if the next similar operation should occur several years from the prior operation. Hence the documentation and the availability of the lessons learned have to be established and archived. There are several variable factors in the operational entity, which have to be taken into account as it has been presented in this thesis. The changing of organizations, organizational structures, working societies, operational environments and conditions, will continue to be dynamic, yet the operational entity concept remains consistent. In order to master and manage the operation with its multiple unique aspects, not to mention the entire entity, is very demanding --especially in large-scale inter-organizational and international operations.

The constructs created in this thesis, concerning operational entity, information transfer and role-shifting are heavily supported by interviews. The OPEN-construct (operational entity) has been approved and implemented by a multinational organization as a project management model for large operations. The construct of the operational entity was presented to the organization in October 2008. The target organization adopted immediately this model and started the implementation in November 2008. The organization's core activities are in the areas of defence and security. According to the Marketing Director of the organization, this construct has improved the project management of the organization and has been implemented in various projects. This speaks to the validity of a working construct. It also suggests that this construct works in the field and in practice, and not only in a theoretical frame of reference.

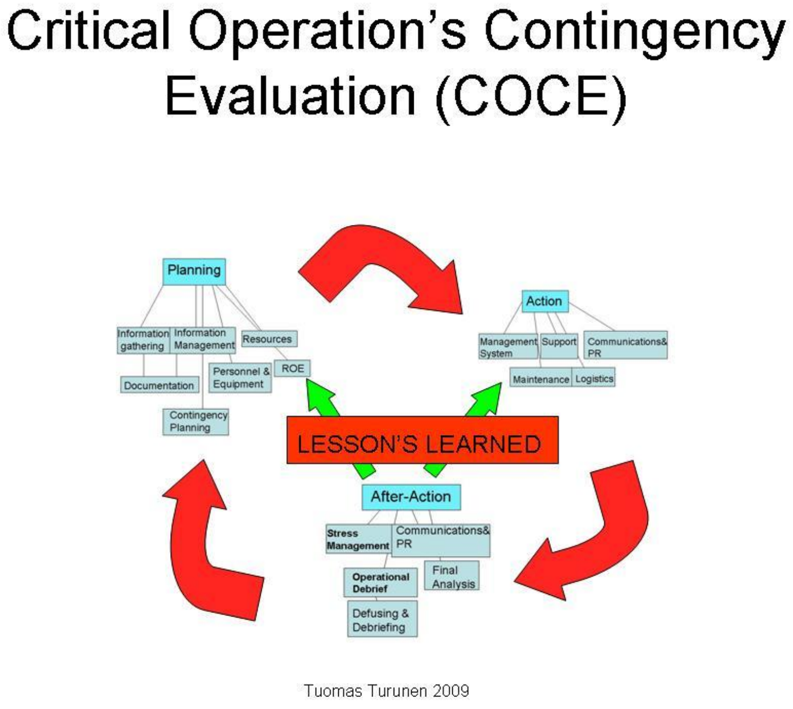
The observation, interviews and the published sources, especially the 9/11 commission report, support the construction of situational awareness and decision making in time-critical and life-threatening situations. There have been, and will unfortunately be, several public safety and security field operations where the decisions must be made in the frontline without transferring the decision making to a higher ranking party, detached from the frontline, and thus lacking the situational awareness in this frame of reference.

The communication, to wit the acquisition and dissemination of facts, is without doubt an extremely essential factor in all phases of the operational entity. The information communication technology and the secure transfer of confidential information are in close contact with the communications. The baseline in communication in an operational entity is that it must be reliable and dependable, that is to say that the means of communication exist and are functional regardless of the challenges provided by the operational environment, participants or any other variables within the operational entity. The communications are not only about technological solutions, but more of information sharing between participants –especially in planning- and after-action-phases. This applies also for the action-phase. The efficacy of information communication technology seems to be more of a challenge during the action-phase compared to the other phases. The challenges in information sharing and –transferring in the action- and after-action phases appear to be more dependant upon human factors, e.g. negligence and unwillingness to share information, territorial barriers, etc.

The role-shift is a very interesting and important, yet a little studied, subject in the area of public safety and security field operations. The construct of role-shift in an organization and the construction of inter-organizational role-shift seem to be somewhat groundbreaking. Hence the Laurea University of Applied Sciences has used the role-shift construction in the application process for the European Commission seventh framework program.

There is a need for flexibility and resilience in both individual and in organizational contexts. There is a need for a clear vision and goal concerning the operation and its unique requirements. However, during the course of an operation, one is likely to encounter various obstacles. To overcome effectively these obstacles one has to be able to act according to the situation at hand. The individual skills are paramount, but so are the other areas as well, which enable the individuals to work as teams and as organizations. Hence, the communications, organizational structures, management systems must facilitate and support making things possible that are needed to succeed in operational entities. This is achievable and it does not necessarily require a new system, but what is requisite is to have the right people in the right positions, doing the right job, in the right places.

In conclusion, the main finding is the following Critical Operation's Contingency Evaluation (COCE). The majority of operations, in all sectors, should consist of 1) the planning phase, 2) the action phase and 3) the after action phase. The effectiveness of communications and information sharing between the participants' are essential to the success of an operation. It is imperative, that all the information is gathered afterwards as soon as possible, analysed and archived, for future reference. Most important is to establish a didactic process and practice for learning from the findings. This learning has to be continues at all organizational levels. Otherwise the risk of repeating the same mistakes is unacceptably high. In some operational context's, this means casualties, material loses and unnecessary increases in costs. The lesson's learned from the final analysis and the post mortem of the after-action phase should be implemented directly into the next planning, the next action and into the next after-action phase, which is shown with the green arrows in the picture below. The red arrows describe the importance of continual information gathering, analysing and learning.



Critical Operation's Contingency Evaluation (COCE)

Tuomas Turunen 2009

COCE

Figure 9

9.2 FUTURE RESEARCH

The operational entity in the context of challenging public safety and security field operations is more than fascinating subject within first responders and other security and military professionals worldwide. Unfortunately there seems to be an emerging need to master these large-scale disasters, man-made and natural, in a more integrated international and inter-organizational environment than exists presently. This thesis answers several questions concerning acquisition and dissemination of facts, transfer of confidential information, role-shifting and managing the related operational risks. However, it also offers a considerable amount of more detailed subject matter for future research, that should be engaged in a more granular manner in order to further comprehend possible issues, risks and solutions within this context.

The information transfer and the secure transfer of confidential information is inextricable with operational communications and it is a subject that offers an interesting and challenging context for any future studies, especially between different but adjacent organizations, public and/or private.

One of the most interesting future research areas, according to some of the interviews (Interviews 2008 & 2009), is the concept of the role-shift. The role-shift study could be conducted within context of first responding authorities. It would be advantageous and beneficial if the studies were conducted in the field, rather than in a theoretical context. The observations could afford additional information to the findings of this thesis.

10 Sources

Alajärvi, K., Herno, L., Koskinen, H. & Yrttiaho, L. 1995. Työelämän viestintä. Porvoo: WSOY.

Alvarez, J., Svejenova, S., Vives, L. 2007. "Leading in pairs". Summer 2007 issue of MIT Sloan Management Review.

BBC. Referred to 12.12.2009. http://news.bbc.co.uk/onthisday/hi/dates/stories/september/27/newsid_2539000/2539769.stm

Berg, K-E. 2001. Yrityksen riskinhallinta. Helsinki: Yliopistopaino

Black, C. Referred to 28.12.2008. http://www.state.gov/s/ct/rls/rm/2004/35683.htm

Burke, R. 2007. Counter-Terrorism for Emergency Responders. 2nd Edition. Florida: CRC Press

Carter, D.L. 2004. Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies. Refered to 10.10.2009. http://www.intellprogram.msu.edu/Carter_Intelligence_Guide.pdf

Clausewitz, C. 2002. Sodankäynnistä. Smedjebacken: Fälth & Hässler

Cowan, J. 2003. Functioning as a team? The role of NCEPOD reports in clinical risk management. Clinical Governance: An international journal. Refered to 12.11.2008. http://nelli.laurea.fi:2086/Insight/viewPDF.jsp?contentType=Article&Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/2480080210.pdf

Chong, Y., Y. 2000. Managing project risk –Business risk management for leaders. Great Britain: Pearson education limited.

Desourdis, R. 2009. Achieving Interoperability in Public Safety and Emergency Response IT/Communication Systems. Refered to 20.9.2009. http://www.ptc.org/ptc09/images/papers/PTC09_Desourdis_Full%20Paper.pdf

Emergency Management & Public Health. Referred to 20.5.2009. http://www.mass.gov/Eeohhs2/docs/dph/emergency_prep/how_emergencies_are_handled.pdf

Everly, G. & Mitchell, J. [www-document]. A Primer On Critical Incident Stress Management. Referred to 11.9.2009. http://www.icisf.org/about/cismprimer.pdf

Frontex. Referred to 15.12.2009 http://www.frontex.europa.eu/examples_of_accomplished_operati/art15.html

Frontline. [www-document]. Referred to 14.5.2009. http://www.pbs.org/wgbh/pages/frontline/shows/knew/could/911commission.html

Goldsmith, J. 2008. The New Rebuplic. Referred to 10.9.2009. http://nelli.laurea.fi:2100/pdf9/pdf/2008/NRP/13Aug08/33339573.pdf?T=P&P=AN&K=33339573&EbscoContent=dGJyMMvl7ESeprA4zOX0OLCmrlGeprRSr6y4SbeWxWXS&ContentCustomer=dGJyMPGqtU%2B2rq5NuePfgeyx44Dt6fIA&D=afh

Gollner, M. 2008. Speed, Action, Surprise –Das Einsatzkommando Cobra. Printed in the EU.

Hellenberg, T. & Visuri, P. 2009. Preventing Terrorism in Maritime Regions –Case Analysis of the Project Poseidon. Aleksanteri Papers 1:2009. Helsinki University

Interviews 2008 & 2009.

Kasanen, E., Lukka, K., Siitonen, A. 1993. The constructive approach in management research. Journal of Management Accounting Research, 243-264.

Kennedy, M. American school and university Mar2009, Vol. 81 Issue 7, p16-16
http://www.nelliportaali.fi:80/V/T6UYA5APA242GNTC9JFRV4BYXLJ4UF89TVDRA2L9Q4AD4MYEFL-09189?func=meta-3&short-format=002&set_number=040849&set_entry=000008&format=999

Kuker, T., M. 1999. On-Scene Commander's For Responding to Chemical and Biological Threats. Referred to 19.15.2009.
http://transit-safety.volpe.dot.gov/training/Archived/EPSSeminarReg/CD/documents/weapons/OSCG_NDPO.pdf

Loflin, M. 2009. Incident Commander Check List: A Quick Reference Guide. Referred to 15.9.2009.
http://nelli.laurea.fi:2100/pdf23_24/pdf/2009/FEN/01Aug09/43739513.pdf?T=P&P=AN&K=43739513&EbscoContent=dGJyMNXb4kSeqLE40dvuOLCmrlGep7RSs6y4S7CWxWXS&ContentCustomer=dGJyMPGqtU%2B2rq5NuePfgeyx44Dt6fIA&D=afh

Leyland, M., L. 2006. The role of culture on knowledge transfer: the case of the multinational corporation. Journal: The learning organization.
http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Articles/1190130304.html

Ministry of Justice. 2009. Investigation Commission of Jokela School Shootings. Referred to 20.5.2009.
http://www.om.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=OMJU%202009%202%20Jokelan%20koulusurmat%20132%20s.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1243790105463&blobheadername1=Content-Disposition&ssbinary=true&blobheader=application/pdf

Musashi, M. 1993. Maa, vesi, tuli, tuuli ja tyhjyys. Keuruu: Kustannusosakeyhtiö Otavan painolaitokset.

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita Prima Oy.

Myers, K., N. 1999. Manager's guide to contingency planning for disasters –Protecting vital facilities and critical operations. Printed in the United States of America: John Wiley & Sons.

New Oxford American Dictionary. 2005. A computer software.

Nikula, P. & Hellenberg, T. 2009. EU Crisis Coordination Arrangements and Decision-Making- Case of Maritime Terrorism in the Baltic Sea. Aleksanteri Papers 1:2009. Helsinki University

Observation 29.10.2008. Joint-Operations Exercise of the Finnish Army, Police and Rescue Department.

Onnettomuustutkinta. Referred to 12.12.2009.
http://www.onnettomuustutkinta.fi/estonia/chapt20.html

Patric, D., Murray, T., Burke, K., & Kayyem, J. 2007. The Commonwealth of Massachusetts State Homeland Security Strategy. Referred to 16.5.2009.
http://www.mass.gov/Eeops/docs/helpus_helpyou/state_homeland_security_strategy_092307.pdf

Pelin, R. 2008. Projektihallinnan käsikirja. 5. Uudistettu painos. Jyväskylä: Gummerus Kirjapaino Oy.

Police Act. 493/1995. Referred to 20.11.2009.
http://www.finlex.fi/en/laki/kaannokset/1995/en19950493.pdf

Rake, E. 2003. Emergency Management and Decision Making: Taxonomy, models and future research. Emergency Management, vol. 1, No 4.

Rantanen, H. 2003. Managing Emergency Response With the Help of Information Technology. A Feasibility Study from a Finnish Perspective. Licentiate thesis: The University of Kuopio

Saari, S. 2003. Kuin Salama Kirkkaalta Taivaalta –Kriisit ja Niistä Selviytyminen. Keuruu: Otavan Kirjapaino Oy.

Sundholm, E. 2003. The M/S ESTONIA Disaster and the JAIC: When Answers Lead To Questions.

Sun Tzu. 1998. Sodankäynnin Taito. Viides painos. Helsinki: Tietosanoma Oy.

Suominen, A. 2003. Riskienhallinta. 3. painos. Helsinki: WSOY.

The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States –First Edition. Printed in the USA: W.W. Norton & Company, Inc.

Wordnet. Princeton University word lexiton. Refered to 10.10.2009.
http://wordnetweb.princeton.edu/perl/webwn?s=communication

Yin, R., K. 2003. Case Study Research, Design and Methods, Third Edition. Printed in the USA: Sage publications limited.

11 Picture Directory