Hans Liwång, M.Sc. and Licentiate in Shipping and Marine Technology, in Ph.D. program, Swedish National Defence College and Chalmers University of Technology, hans.liwang@fhs.se.

Marika Ericson, LL.M. in Law, in Ph.D. program, Swedish National Defence College and Uppsala University, marika.ericson@fhs.se.

Martin Bang, M.Sc. in Pol. Sci., in Ph.D. program, Swedish National Defence College and Finnish National Defence University, martin.bang@fhs.se

AN EXAMINATION OF THE IMPLEMENTATION OF RISK BASED APPROACHES IN MILITARY OPERATIONS

Key Words

Security risk management process, risk analysis, threat assessment, risk awareness, military intelligence, legal assessment

Abstract

Today several nations utilise risk based approaches in military planning. However, the discussion on limitations with the approaches in regard to aspects such as uncertainties, the nature of the threat and risk to civilians is limited.

The aim of this work is to identify important challenges when applying risk based approaches to military activity. This article discusses risk based approaches in general and their military applications. Five generic quality requirements on risk analysis are presented from research in risk philosophy. Two military application areas for risk analysis: military intelligence, and risk management in legal assessments are analysed in relation to the presented quality requirements on risk analysis.

From the analysis it is clear that risk analysis is an integral part of the decision-making analysis and cannot be separated in time, space or organisationally from the decision-making process in general. Defining the scenario to analyse, including the time span, is a central task in risk analysis and will affect every aspect of the risk estimation. Therefore, the principles for scenario definition must be communicated and continuously updated throughout the organisation. Handling the uncertainties throughout the process is also important, especially if the aim is a resilient military system.

1 Introduction

In 1916 British General Fuller published a journal article entitled "The Principles of War, With Reference to the Campaigns of 1914–1915." His article was a description of modern principles of war described as crucial to successful military planning and actions. According to the theory the principles represent the most important nonphysical factors that affect the conduct of military operations at all levels. The principles of war are today reflected in the doctrines for many nations and security is one of the principles. Security is achieved when measures are taken to protect the forces. Appropriate security allows for freedom of action by reducing vulnerability to the enemy's actions (NATO, 2007; University of Cincinnati, 2004).

Today several nations utilise risk based approaches to analyse the level of security in operations. Examples of military risk management approaches include the NATO Comprehensive Operations Planning Directive's (COPD) description of the role of risk analysis in military planning, the US Department of the Army (2006); the US Marine Core Marine Corps Institute (2002); and the Swedish Armed Forces (2009a) risk management methods for military operations and specific methods for IT security (RTO/NATO, 2008); force protection (DCDC, 2010; NATO, 2007); and antagonistic threats (Swedish Armed Forces, 2009b). In the article "Risk: misunderstanding or military misnomer" Tomes (2012) discusses the strength of risk thinking in military organisations but also problematizes how the risk concept is implemented today. Tomes' article gives rise to important questions on the risk based approaches which are not addressed in military doctrines. For civilian risk based approaches there exists an important discussion on the strengths and weaknesses of approaches and tools (see for example Frosdick (1997); Hansson (1993); Hubbard (2009) and Kunreuther (2002)). However, for military approaches the discussions on problems or limitations with the approaches are limited.

The aim of this study is to increase the understanding of risk analysis in the military context and thus increase the quality of risk analysis as a decision support. The overarching research question is: what challenges can be seen when applying risk based approaches to military activity? The research is based on five generic quality requirements of risk analysis presented by Hansson (1993, 2012):

1. The decisions options, as well as the system/scenario studied, must be finite and defined.

2. The analysis must be able to identify the negative outcomes of the studied hazard.
3. From the analysis it must be possible to objectively describe the consequences of the hazard.
4. It must be possible to obtain/assess the probabilities with reasonable accuracy.
5. It must be rational to keep the expected outcome (the risk i.e. the probability times the consequence) as low as possible.

Two application areas for military risk analysis are studied. The two areas, military intelligence and legal assessment, are chosen to serve as examples of how the work is performed today in international joint operations.

Initially, in Section 2, this article discusses risk based approaches in general and their application within military organisations. In this study, based on research in risk philosophy, the five generic quality requirements of risk analysis from above will be presented in more detail with reference to their implementation. Thereafter, in Section 3, the article presents two military application areas for risk analysis: military intelligence, and risk management in legal assessments. In Section 4 the two areas are analysed in relation to the presented quality requirements of risk analysis. The result of the analysis is discussed in Section 5 and the conclusions are summarised in Section 6.

2 Risk based approaches

2.1 Risk management

Risk management is a decision support process and the risk analysis itself is a form of policy tool, as well as a vital tool for military planning and decision-making (NATO, 2010). According to Johnson (2007) "Risk management provides the most important single framework for strategic, tactical and operational decision-making across the US military". Risk management and its components, such as risk assessment and risk analysis, have been employed since the 1950s for the control of hazards in areas such as industrial plants and space travel (Andrews & Moss, 2002). Sometimes risk management, in military or civilian organisations, is discussed under terms such as Operational Risk Management (ORM) or Composite Risk Management (CRM), see for example Marine Corps Institute (2002) and

Department of the Army (2006). However, there is no substantial difference between these methods and risk management in general.

Risk management is defined here as the systematic application of management policies, procedures and practices to the task of analysing, evaluating and controlling risk. Risk management is often defined by concluding the following activities:

1. A risk analysis including scope or scenario definition, hazard identification and risk estimation.
2. A risk evaluation including risk tolerability decisions and analysis of options.
3. A risk reduction and control including decision-making, implementation and monitoring. (Bakx & Richardson, 2013; DCDC, 2010; Department of the Army, 2006; Kuo, 2007; NATO, 2010).

Risk assessment is defined here as consisting of steps 1 and 2 from the list above. See also Figure 1 for an illustration of risk management and its components and sub-components. Risk or risk level is defined as a function of the probability of the occurrence of an unexpected/unwanted event and the consequence of it happening.

Figure 1. The security risk management process and its components developed from Department of the Army (2006) and Marine Corps Institute (2002).

The results of a risk analysis must always be weighed against both risk tolerability levels and other operational parameters, such as financial considerations, requested reliability and possible operational gain. Generally, higher risks are tolerable if the

possible operational gain is high (Department of the Army, 2006; Marine Corps Institute, 2002; NATO, 2007, 2010).

In general probabilistic risk assessments offer a sound and systematic basis for evaluating potential hazardous activity. However, the methods used are specialised and often complex, and auditing the assessment is vital to ensure a logical and consistent approach and that relevant data has been adopted (Andrews & Moss, 2002).

2.2 Military risk based approaches

In military planning risk analysis has a role in creating a situation awareness with the aim to support the analysis of options (NATO, 2010). According to the NATO Force protection doctrine (NATO, 2007) casualties, deliberate or accidental, are a reality of military operations, and the desire to avoid them totally may impact adversely on the achievement of the mission. Consequently a balance of risk is required. Therefore, for example force protection requires risk management and prioritisation, including an integrated threat, vulnerability and risk analysis, and a comprehensive risk assessment process is essential to guide risk management decision-making and prioritisation (NATO, 2007, 2010).

This study uses the military risk based approaches described in a selection of doctrines from NATO, United States, United Kingdom, and Sweden (DCDC, 2010; Department of the Army, 2006; Marine Corps Institute, 2002; NATO, 2007, 2010; RTO/NATO, 2008; Swedish Armed Forces, 2009a, 2009b) to formulate a generic description of military risk based approaches. To some extent civilian practice is also used to further define some of the central steps and tools. There are studies of the occupational risks in military organisations such as Lehtomäki, Pääkkönen, and Rantanen (2005). There are, however, a limited number of studies on military risk management and how it is implemented in military organisations, one example is Bakx and Richardson (2013).

Worth noting is that the military applications of risk management have great similarities with their civilian predecessors, even though the civilian approach mainly is developed for safety, while military applications often are about security. According to Liwång (2012), risk approaches for security can be consistent with safety approaches but the methods proposed for security events must also be

specifically tested for security cases. This is because hazards (without intent) and threats (with intent) evolve in different ways into risk; therefore, they must be analysed differently in order to capture the causal relationship. If the focus is security rather than safety, particular attention must be given to:

- the lack of objective data, because each intent has its own set of probabilities,
- the antagonistic threat, i.e. the probability of an attack is dependent on intent and protection methods (Liwång, 2012).

2.2.1 Identify hazards

The first step of the risk analysis is the identification of hazards which will lead up to the scope and scenario definition. In the identification of threats, both creative and analytical techniques are used. Threat analysis is described as a tool to support risk management decisions, and it must describe the causality and process of an attack. The analysis determines the capabilities and intentions of an identified group or organisation and how likely they are to carry out the defined threat and actions (NATO, 2007):

1. Threat capability: The ability of potential threats to cause harm to assets. Analysis of threat capability considers threat structure, leadership, professionalism, tactics, weaponry, targeting and logistics.
2. Threat intent: The willingness of potential threats to target assets. Analysis of intent considers threat ideology, objectives, strategy, likely intentions and previous history.
3. The threat's likelihood of exploiting vulnerability: Analysis of likelihood includes threat history under similar circumstances, the threat's overall campaign plan, currently implemented security controls and measures and the most probable threat course(s) of action.

The description above shows that the threat analysis focuses not only on the threat but also the threat in relation to the vulnerability of the assets in question. The importance of analysing the interaction between the threat and the asset has also been stressed by Kunreuther when describing security risk analysis (Kunreuther, 2002).

A threat analysis should address the full range of threats and attack possibilities and the analysis is used as a basis for risk assessment and a tool for countermeasure planning (NATO, 2007). To facilitate this the vulnerability analysis should include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up and response capability. A vulnerability assessment is used to determine the susceptibility of assets to attack from threats identified in the threat analysis, so the analysis must describe the interaction between a threat's intent, capability, and likelihood to perform an attack and the asset's vulnerabilities (NATO, 2007).

The scenario definition will always affect the validity and outcome of the analysis, but a clear and sound definition is also a requirement for effective analysis. Therefore, the definition of the scenario must be thoroughly documented and presented with the results of the analysis (Liwång, 2012).

Risk scenarios must be based on the threats identified and should collectively quantify the risk throughout the system's lifecycle. This should be done to ensure that identified threats relate to event categories with major hazard potential. When generic scenarios are available, they must be adapted and customised to the specific operation in question (Liwång, 2012).

2.2.2 Assess hazards to determine risk

After threat identification and scenario definition, the scenarios must be analysed in detail in order to estimate the risk. The purpose of this analysis is to investigate the consequences of the identified threats and to estimate or calculate their probabilities.

In traditional civilian risk analysis the analysis of low-level factors, such as engineering specifications, system schematics and measured or assessed probabilities are linked to the probability of the identified consequences. For this process there are several tools documented in risk analysis literature. However, each tool has specific limitations and benefits and the analysis process has to be chosen carefully. The analysis can, for example, be carried out using a combination of event trees, influence diagrams and Monte Carlo simulations.

In military doctrines there is little guidance to the risk estimation process and how the choice of tool affects the robustness of the output. See Bakx and Richardson

(2013) as well as Liwång, Ringsberg, and Norsell (2013) and Yang, Wang, and Li (2013) for examples of a more specific discussion on tools for security risk analysis.

A risk analysis cannot be performed without a definition of the consequences under study. Also, difficulties in defining consequences must be documented, especially in relation to the perception of security, and these difficulties must be thoroughly weighed in risk tolerability decisions, analysis of options and risk reduction (Liwång et al., 2013).

The estimation of the probability for each consequence is central and in order to enable the results of an analysis to reflect the uncertainties and the possibility of surprises occurring, there is a need for a risk informed approach that is more than calculated probabilities and expected values (Aven, 2009). Including uncertainties in phenomena and processes will enable a broader context where the uncertainties and possible surprises are considered to be an important part of the risk picture. This would then provide for a rational input to decision-making (Aven, 2009) and increase the credibility of the study (Kunreuther, 2002).

2.3 Limitations with risk based approaches

The traditional engineering approach to risk analysis is based on objectivist expected utility, which combines objectivist probabilities with objectivist utilities (Hansson, 1993). The assumptions for military risk analysis are not explicitly stated in the doctrines, but from the definition of the risk and the process described it must be assumed that military risk based approaches are also based on objectivist expected utility. This means that the concept of probability used is interpreted as an objective representation of the frequency of the studied event and that there is a linear relationship between the consequences studied and their utility assignments (Hansson, 1993). According to Hansson, in his research on the philosophy of risk, this can only be the case if the following criteria are satisfied:

1. The decision's options, as well as the system/scenarios studied, must be finite and defined.
2. The analysis must be able to identify the negative outcomes of the studied hazard.
3. From the analysis it must be possible to objectively describe the consequences of the hazard.

4. It must be possible to obtain/assess the probabilities with reasonable accuracy.
5. It must be rational to keep the expected outcome (the risk i.e. the probability times the consequence) as low as possible. (Hansson, 1993) and further developed in Hansson (2012)

These criteria are seldom fully fulfilled (Hansson, 1993) and the result of the risk analysis should therefore only be seen as a simplified description of the risk. In Section 4 criteria 2 and 3 will be discussed together as they both deal with analysing the consequences.

3 Areas for risk-based approaches in military operations

The two areas, military intelligence and legal assessment, are chosen to serve as an example of how the work is performed today in international joint operations.

3.1 Area 1: Military intelligence

Within the NATO Force Protection Process, the intelligence section is assigned to deliver the threat assessment which is one part of the risk analysis. The threat assessment in the military context is primarily an intelligence assessment of possible threats towards one's own forces in a given geographical area (NATO, 2007). A threat assessment is the product of one, or several, entities' capability, intent and the likelihood of a threat exploiting a vulnerability (NATO, 2007).

If the risk analysis claims to have a quantitative approach, the base rate of the event is central, and will affect the three components mentioned above. Within NATO's Force Protection Process the threat likelihood of exploiting a vulnerability includes the history i.e. the frequency of the event under similar circumstances. In the Swedish example, the component intention is including the entity's previous preformed actions (Swedish Armed Forces, 2009b). Therefore, the accuracy of the estimation of the base rate will have implications throughout the whole analysis.

This problem can be exemplified with the case of Improvised Explosive Devices (IED) and the Swedish intelligence section's production of threat assessments. IEDs have become the normative threat for troops stationed in Afghanistan. Threat assessments for IED attacks are conducted routinely in the intelligence section of

the battalion headquarters. An example of this is the attachment that is included in the daily intelligence summary produced by all the provincial reconstruction teams. The annex includes a threat assessment for the area in general, but also specifically for Ring Road 5, which is the main road in the country. Within the Regional Command North, to which the Swedish units belong, the road is assessed on a three-point scale, green, yellow and red. This assessment gives direct impact on the operation in the area. For example if a part of the road is assessed to be red or green it leads to different restrictions regarding minimum sizes of units moving in the area. However, there has been a lack of structure for how this classification should be conducted. As a result the quality of the assessments is questioned by Swedish analysts, primarily because of too low data quality. It is not only the opponents' deception that has implications on assessments (Bang, 2014). In 2013 ISAF was forced to redraw information stating that the insurgent attacks had declined by 7 %, due to inaccurate numbers. The reason was an incorrect coding by an analyst (Burns, 2013).

The reasons for the uncertainty in the assessment can be connected to a diversity of factors: e.g. the number of incidents and co-linearity in the data, the quality of the data as well as lack of routines for processing data. If we focus only on the quality of the base rate (i.e. the historical frequency of an incident) the uncertainty in reported incidents can be seen as high. There are incidents reported that have not existed/did not happen, and some incidents never get reported at all. This is combined with a lack of routines for how to process data and one's own operational pattern also affects the probability of receiving information. The consequence is that the accuracy of available statistics is biased, also due to the units reporting on IED findings in the areas they operate in. In cases where there is no base rate or where it is of low accuracy as well as in low frequency events (events that are unique or happening so seldom that any statistical analysis of previous incidents is irrelevant) the importance of the accuracy on indicators is increasing. The consequence is that the accuracy in the available statistics for incident frequency can be questioned. This is increased by deception and denial which is also an affecting factor within all intelligence (Clark, 2013). An opponent will try to deliberately affect our view through denial of information or by making our information inaccurate in different ways.

What effect low data quality might have can be exemplified with a *non-military* case: the swine flu outbreak in 2009. Although it appears seemingly to be quite

separate from military *intelligence*, there are major similarities. The risk assessment is as mentioned a product of the probability and the consequence. The consequences of an epidemic similar to the Spanish flu 1918 in a globally connected world as ours are catastrophic (Osterholm, 2005). The probability (one of the results of the threat assessment) on the other hand, is harder to assess. The low number of events during the last century makes a prediction problematic. For a given time/year, the base probability of a handful of incidents during a century is low from a statistical perspective, approximately 10 cases the last 300 years (Osterholm, 2005). To be able to conduct any analysis more data needs to be collected in the same way as within intelligence, including a search for indicators. One such indicator epidemiologists are looking for is the fatality rate, which is how many of the infected individuals die as a consequence of the flu. However, the fatality rate cannot be accurately predicted until after the flu has passed and therefore has an unknown level of uncertainty. In a country such as Sweden or the United States, the uncertainty in the data regarding cause of death is low; however in developing countries the situation might be completely different. During the 2009 swine flu, Mexico started to show an alarming level of deaths (Silver, 2012). In April 2009 the World Health Organisation declared a phase five pandemic alert which is the next highest level below g*lobal pandemic* (Doshi, 2009). The case fatality is the ratio between total numbers of death caused by the flu divided with the total number of infected individuals. The population, and in this case the sample population, has a *systematic* bias towards overestimating fatality and underestimating the total number of cases, a form of *collecting bias.* The result is a risk assessment that is incorrect and in the swine flu case led to decisions that in retrospective did more harm than good. In the same way an overestimation or underestimation of the probability of the event might lead to inappropriate decisions that in the worst case can lead to own casualties.

How does this then connect to the military context? Leaving out the uncertainty from risk assessment may result in insufficient decision support in the same way as with the swine-flu case. For the IED case leaving out the uncertainty will give a false sense of reliability and might lead to misguided decisions. But here one must also remember that acquiring a correct base rate (historic frequency) is only the beginning of the threat analysis, which is a combined estimation including the intention, capability and opportunity.

The intelligence process as well as the risk assessment is multi-dimensional, a lower risk for an individual soldier might lead to a higher risk for the mission. A decision that is assessed to give a high risk in a short time frame might give a lower risk assessment when it is studied in a longer time perspective. The multi-dimensional can be exemplified with the IED attacks in Afghanistan, where one countermeasure is to drive a vehicle on the side of the road. This is one way to "easily" lower the risks in the short time frame. However, there might be long term consequences on the security situation as a result of the farmer's seeing their crops being destroyed by foreign troops. There might also be consequences at an operational level if the insurgents see a systematic change and start digging down IEDs on the side of the road as well.

The base rate may also be a very coarse way of describing the security situation that cannot capture all the nuances of the threat. Therefore, it is important to decide if the estimation should be valid for an ordinary car or the General's car and how this difference affects the probability of an attack (see Shearer (2011) for an example of probability of attack on different types of targets).

3.2 Area 2: Risk and risk management in legal assessments

A central aspect of the legal assessment in military operations is the proportionality of a specific attack. Although it might appear to be comparing apples and oranges, this assessment in part touches upon the same issues as force protection assessments, and they are both important parts of the planning process for military operations. Where one is internally focused (force protection) the other is externally focused (avoiding/minimising collateral damage to civilians and civilian objects through military operations). And, how do we combine a high level of force protection with the legal requirement to avoid, or at least minimise, collateral damage as a result of military operations? The perspectives clash in legal assessments, where maintaining a high level of force protection leads to using a mode of operation that makes it more difficult to live up to the principle of proportionality and minimise collateral damage.

For force protection purposes, risk management does not mean eliminating all risks, but rather to balance the risk and continuously re-evaluate perceived risks in order to achieve decision-making on risk management and also to achieve prioritisation (NATO, 2007).

For a military legal adviser, legal assessments on proportionality will focus on the risks posed by the military operation to protected people/civilians. The assessment is weighing the military advantage or value of hitting a specific military target, with the estimated risks of collateral damage to civilians or civilian objects. But, how does force protection influence the assessment of proportionality, can it be a factor or not?

Proportionality is one of the basic principles of international humanitarian law (IHL), both as a matter of customary and treaty law (Henckerts & Doswald-Beck, 2010 and Dinstein, 2011). In one of several references in treaty law, it is codified in Article 57 (2) (iii) of Additional Protocol I to the Geneva Conventions which states: "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated". The principle is based on two parts: first, there is a military objective and second, attacking the military target can be expected to cause the effects listed in Article 57. This is a very rudimentary description of the principle, based on what we need for the example in this text. For a more in-depth analysis and discussion about the different features and facets of the principle of proportionality see, for instance, *Customary International Humanitarian Law* (Henckerts & Doswald-Beck, 2010).

Applying this principle may sound straightforward enough, but it carries with it several difficult issues that need to be taken into consideration. One of the main issues of interest here is the difference in how a legal analysis of risks is carried out in comparison to the force protection risk assessment mentioned above.

A legal adviser who receives a plan for attack in order to review it with regard to IHL, and specifically the principle of proportionality, will do this in most if not all cases without performing objective calculations of risk. The starting point is that the intended target is a military objective in line with the principle of distinction (for a definition of military objectives see: Art. 52(2) Additional protocol I to the Geneva Conventions), that analysis will not be discussed here. Once the intended target is established as a military objective the legal adviser will focus on the proportionality of the attack. This comprises three questions: What is the expected collateral damage? What is the concrete and direct military advantage of attacking the intended target? Is the expected collateral damage excessive in relation to that

advantage? The end result should in this sense be weighing the expected collateral damage and the military advantage of the attack, and provide an answer as to whether or not the planned attack can be carried out in accordance with IHL. An attack which is expected to cause excessive damage to civilians or civilian objects must then be cancelled.

This analysis opens up many other questions – for example, how do we define expected collateral damage? Another question that is often debated in legal forums is what the term 'excessive' means. For some it is clear that it means that the disproportion of the attack is clear, see for instance Dinstein (2011). An example would be the extremely heavy use of artillery against villages inhabited mostly by civilians in order to seize those villages, as discussed in the *Blaskic case*. There it was deemed to be "out of all proportion" to military necessity due to the civilian deaths and the destruction that was bound to occur as a result of the action (ICTY Trial Chamber, 2004).

It should also be remembered that the analysis is conducted before an operation, so it is the expectation of collateral damages that is assessed. What are "expectations" built on, that is, what factors are considered? There are many possible factors: prior attacks against similar targets, intelligence regarding the intended target and the area where the target is located, the density of the civilian population in the target's vicinity, whether the defender is deliberately exposing civilians to risk (human shields), the timing of attack, types of weapons available to the attacker and their accuracy, and so on. Although it is possible to objectively assess the accuracy and destructive capacity of specific weapons, the common denominator for most of the factors mentioned is that they to a large degree build on subjective elements. It is not possible to objectively quantify most factors of the equation.

There are of course ways to calculate the projected civilian deaths and also to make an estimation of damage caused to civilian objects or installations. But, how do you measure the military advantage and how do we weigh the military advantage and the projected civilian deaths against each other?

This will also be the diverging point between many legal advisers and military planners. Lawyers are used to conducting analyses and balancing factors based on words and are used to the fact that estimates will not be an exact science based on formulas, calculations or statistics. For a military planner the lawyer's estimates and assessment will seem unclear at best and unquantifiable and arbitrary at worst.

For a practical example we can turn to NATO's Bombing Campaign against the Federal Republic of Yugoslavia (FRY) in 1999. NATO has stated that as a matter of protecting their own forces from the FRY air defence systems, for the first part of the campaign the pilots flew at a minimum altitude of 15 000 feet (Amnesty International, 2000). One of the incidents investigated both by a Committee reporting to the International Criminal Tribunal for the former Yugoslavia (ICTY) and by Amnesty International is the bombing of a railway bridge at Grdelica Gorge on 12 April 1999 (Amnesty International, 2000; Committee report to ICTY, 2000) (Nobody has been prosecuted for attacks during the campaign and in its investigation the Committee did not suggest any further action or investigations).

A NATO aircraft launched two laser-guided bombs at the railway bridge and hit a 5-carriage passenger train with both missiles. At least 10 people were killed and 15 injured in the incident (Committee report to ICTY, 2000). The designated target was the railway bridge which under IHL can be seen as a legitimate military target as one of the main lines of communication with a strategic importance (Dinstein, 2011). According to NATO's official explanation, the pilot saw movement on the bridge after the missile was already launched. As it was a remotely directed attack where the pilot was unable to physically view the bridge, he could no longer abort the operation when he saw movement on the bridge. According to NATO, the pilot realised that he had not hit the bridge but the train and as "he believed he still had to accomplish his mission, the pilot circled back around" (Committee report to ICTY, 2000). The pilot then tried to strike a different point on the bridge, however the force of the first missile's impact had caused the damaged train to slide forward and the second missile also hit parts of the train. NATO explained the events as a regretful and sad incident. On the other hand, Amnesty International in its report also states that the account given of the pilot's rationale for continuing the attack after he hit the train suggests that "the pilot had understood the mission was to destroy the bridge regardless of the cost in terms of civilian casualties" (Amnesty International, 2000).

The initial restriction of flights to be carried out above 15 000 feet allegedly is also part of the problem in this case. An aircrew flying at that altitude will only be able to identify whether the objective was the intended one according to the planning (Amnesty International, 2000: 16). It is, however, not possible to tell if civilians moved closer to the intended target, or as in this case if a train approached the bridge, or if any other changes occurred between the planning and the conducting

of the attack. Any changes of that kind would lead to an obligation to suspend the attack as the target would no longer be legitimate, or an attack could be expected to cause collateral damage not in line with the principle of proportionality. Can we then accept a way of action that efficiently makes it impossible to live up to obligations in international law? As breaches against the law of armed conflict lead to criminal responsibility the answer would be no. But, where lies the responsibility – with those ordering attacks or the ones carrying them out?

Looking at this from the perspective of a legal adviser, what do we expect in terms of analysis material during the planning phase of an attack like this? The force protection issue is important here as in all other cases, there is no denying that. Is it acceptable to put a requirement for altitude so high that the likelihood of collateral damage increases due to inability to note changes in the target in comparison to the planning phase? From a legal advisers perspective it would also be expected that there is clear guidance regarding the effects of a hit, if a target is hit and it is evident it has caused excessive collateral damage the operation should be aborted. But, that also means that we need to be clear on what excessive collateral damage for a certain attack would be. Hitting a target a second time, after realising that the first missile caused collateral damage has been labelled as negligence by some, especially since the real target, the bridge, was obscured from vision, due to smoke from the burning train. There was simply no way to know what the pilot was actually hitting the second time and so, the second missile should not have been launched.

In the end we end up with the same questions here as in other cases where the principle of proportionality has been the subject of debate. These are also quite in line with the questions that the Committee reporting to the ICTY prosecutor is asking in its report about Operation Allied Force:

- What relative value can be assigned to the military advantage gained and the death of civilians and damage to civilian objects?
- What factors do we include or exclude in the weighing of expected collateral damage and military necessity?
- How much danger is a military commander obligated to expose his own forces to in order to limit civilian casualties? (Committee report to ICTY, 2000).

4 Analysis

The two examples of application areas presented involve assessments of risk. For the intelligence analysts supplying the risk management process with estimates and assessments is a central activity. For the legal proportionality analysis the risk management aspects are not as clearly expressed, but the assessment of possible future consequences is nevertheless central. However, it is also important to note that in both the presented areas the negative consequences and their probability (which combines to risk) as well as positive outcomes and their probability (which combines to expected gain) have to be estimated and assessed. Risk is therefore only half of the decision input and has to be weighed against the expected gain. It is thus clear that the risk analysis is an integral part of the decision analysis process and will be analysed as such in this section.

1. The decision options, as well as the system/scenarios studied, must be finite and defined

The real system and options are never finite and therefore the system and scenarios must be a well-defined and documented simplification of the reality and the definition must be easily understood throughout the risk management process. The scenario definition will always affect the validity and outcome of the analysis, but a clear and sound definition is also a requirement for effective analysis.

Looking at the description of Area 2 it can be concluded that different focuses exist side by side, where force protection is internally focused on one's own troops and the legal process is externally focused on collateral damage to civilians and civilian objects through military operations. It is unlikely that these two focuses can be combined in one scenario because the questions studied differ. The choice of scenario definition will also affect which factors will be included or excluded in the totalling of sums for both the consequences and successes from the studied operation or activity.

One of the most challenging aspects to define is the finite time span to study in order to include how short term effects of an incident will affect the threat's future intent and the future morale of one's own troops. A small-scale local incident can over time have large strategic, positive as well as negative, effects. This challenge

has no real counterpart in civilian risk analysis but research on safety culture has some similarities with the effects on one's own troops.

The COPD discusses the time span to be studied in general terms and states that approaches has to consider "near, mid and longer term" risks (NATO, 2010). However, this kind of statement does not aid the analyst, nor does it positively affect the results. There must be different scenario definitions for different types of decision-making situations, otherwise the scenario cannot be finite. This will mean that the scenarios studied have to be dependent on the decision at hand, but choosing the right scenario definition beforehand is not a trivial task.

2. The analysis must be able to identify the negative outcomes of the studied hazard and
3. From the analysis it must be possible to objectively describe the consequences of the hazard

The Committee report to ICTY raises several questions related to identifying negative outcomes and if they can be objectively described. These questions discuss the assignment of an objective value to the military advantage gained and the death of civilians, and which factors should be included in such values (Committee report to ICTY, 2000). The report also discusses the relation between different consequences, such as danger to the military personnel versus the probability of civilian casualties (Committee report to ICTY, 2000).

In his article on civilian risk analysis Frosdick (1997) discusses the too narrow perspective of many analysts when it comes to identifying hazards and consequences, especially in regard to risk perception and cultural bias. This also an issue in military risk analysis (George & Bruce, 2008; Rebugio, 2013). Therefore, it is important to make sure that a non-physical consequence such as the perception of security is included. The human factor aspects of risk perception should therefore never be overlooked in any organisation both as an aspect under study in the risk analysis but also as an aspect that can introduce bias into the analysis process.

Based on the discussion above it can also be concluded that the definition of the scenario studied will affect which consequences can be included in the analysis. The scenario definition can therefore not be done without also looking at which limited number of consequences that should be included in the risk analysis. At the

same time the doctrine texts, such as Department of the Army (2006) and NATO (2010), make a long list of types of consequences that should be studied including armed attacks, criminal acts to civilians and environmental aspects without guide on how this should be adapted to the specific need of the analysis at hand.

The decision maker has the responsibility to weigh different consequences against each other, not the analyst, therefore the decision maker has to be involved in the scenario definition and the definition of the consequences under study. The analyst must be responsible for documenting and describing all consequences studied and the limitations as a result of the scenario definition.

4. It must be possible to obtain/assess the probabilities with reasonable accuracy

How the probabilities have been obtained must be documented and highlighted in the process together with uncertainties. The uncertainties must then be taken into account in the decision process. Both Aven (2009) and Kunreuther (2002) are clear in their opinion that especially for security cases the risk reduction decision cannot be taken based only on consequences and their probability (expected risk), also the uncertainties have to be quantified and presented to the decision maker.

An example where the importance of uncertainties in security assessment is discussed is the US President Policy Directive for critical infrastructure, security and resilience (The White House, 2013). One way to achieve resilience is to focus on robust control options, or generic capabilities, which are less sensitive to uncertainties (Liwång et al., 2013). These aspects can only be studied if the uncertainties are included throughout the risk analysis. However, albeit the doctrines acknowledge the often high uncertainties a clear guide on how to tackle this problem is limited, especially on how the uncertainty should be described, included in the analysis and presented in the results to make sure that the effect is not lost in the analysis.

The lack of specific discussion on the importance of the choice of risk analysis tools and how it affects the output in the doctrines is problematic. This is exemplified in the discussion on base rate bias and how to derive a base rate for an intelligence analysis. In such cases there is a great need for specific recommendations on tools, especially for the estimation of low frequency incidents

which is much more demanding than the assessment of the probability for high frequency incidents.

When analysing low or rare frequency events the uncertainty in the result increases because assumptions for standard statistical methods do not apply. As a result of uncertainties in the estimated probabilities it is important that the uncertainty in the in-data is reflected in the documentation of the analysis, the analysis results and the presentation of the results. Otherwise the risk understanding will differ throughout the organisation which severely affects the organisation's ability to operate close to the limits of acceptable danger, without putting the operation at risk (Reason, 2000).

A shared risk awareness and uncertainty awareness is needed and can only exist if the risk and uncertainty is assessed in a documented, structured and standardised manner. However, a qualitative discussion on the importance of such a process is not included in the doctrines studied.

5. It must be rational to keep the expected outcome (i.e. the probability times the consequence) as low as possible

For frequently occurring cases, it makes sense to keep the expected outcome to a minimum; however, this is not always valid in case-by-case comparisons for hazards with low probability. An alternative use of the risk analysis result is to identify the most robust risk reduction measures or generic capabilities, not necessarily the control options with the lowest expected risk (Liwång, 2012). Therefore, especially for security cases, the risk reduction decision cannot be taken based on only consequences and their probability (expected risk), at least the uncertainties also have to be quantified and presented to the decision maker.

As the risk analysis scenarios studied only represent a part of the operation, there must be interaction between the risk analysis and other activities. There is therefore a need for a more nuanced discussion on how the result and uncertainties of the risk analysis should interact with other decision supporting data.

4.1 Synthesis of analysis

The challenges identified in the analysis for the five analysed quality requirements above all stem from the fact that process oriented risk management models are applied to a reality that is everything but straight forward. The doctrines description of risk management covers in detail the steps to perform (the process) but the guide to how quality is achieved in each step and the analysis as a whole is limited. To meet Hansson's quality requirements the analyst need to be more guided on how to transform the complicated reality to a finite manageable scenario without losing the important information. Therefore, there is a need for describing how the general requirements on the risk management stated in the doctrines can be reduced to specific requirements for a specific situation, especially in relation to time span, definition of scenario, how to introduce necessary assumptions and consequences to study. There is also a need for a more explicit discussion on uncertainties, how they can be reduced and how they should be analysed and presented.

5 Discussion

Risk management is a powerful tool, but it requires an understood and shared definition of risk and the role of the risk management in relation to the decision-making process and the operation in general.

It is important to note that the negative outcomes and their probability (risk) as well as positive outcomes and their probability (expected gain) have to be estimated and assessed. Risk can therefore only provide half of the knowledge needed for taking a decision, and it has to also be weighed against the expected gain with a certain action or operation (Bakx & Richardson, 2013). It is thus clear that the risk analysis is an integral part of the decision analysis and cannot be separated, in time, space or organisationally, from the decision-making process in general. Therefore, the tendency to separate risk management from other decision support activities, described by Tomes (2012), is problematic. Specifically, if the results of the risk management should have an effect on the security and hence the freedom of action in a conflict.

From the analysis it is clear that the scenario definition is a central task and will affect every aspect of the risk estimation. One of the most challenging aspects of the definition is the time span to study and there is no discussion on that aspect in

the doctrines studied here. There must be different scenario definitions for different decision-making situations otherwise the scenario cannot be finite. This understanding must be implemented throughout the organisation and the principles for scenario definition must be communicated and continuously updated. If there are different principles for scenario definition existing side by side within an organisation the basis for decision-making will be unbalanced which may lead to decisions not making use of the actual knowledge at hand. This is not supported by the general statements on time span and consequences to be studied in for example COPD (NATO, 2010).

The choice of indicators is important and the indicators must be representative for the consequences under study or the estimated probability will be wrong. The aspects of only studying direct consequences, and ignoring indirect consequences, are extra troublesome for security risks analysis. This because the consequences, for one's own troops and the threat, in one incident often must assume to affect the future intent of the threat and therefore change the scenario.

Identification of social issues such as risk perception and cultural bias has shown to be weak (Frosdick, 1997) and the reasoning in respect to risk rationality differs at different hierarchy levels (Bakx & Richardson, 2013). Therefore, an effective application of risk analysis places non trivial responsibilities on the analyst as well as on the decision maker. The analyst must also be responsible for documenting and describing all consequences separately and the limitations resulting from the chosen scenario definition and introduced assumptions. The decision maker then has the responsibility to weigh different consequences against each other. This also leads to a need for the decision maker to be involved in the scenario definition and the definition of the consequences under study.

Shared risk awareness is needed throughout the organisation and it can only exist if the risk and uncertainty are assessed in a documented, structured and standardised manner. To develop shared risk awareness is especially difficult as the risk analysis scenarios studied only represents separate parts of the operation. Therefore, there must be an interaction between the risk analysis and other decision support activities and the decision-making.

An important aspect not included in the doctrines, but studied here that will affect all parts of the analysis are false positives and false negatives and how systematic errors, or biases, in the analysis affect the decisions taken, the safety culture and the

perception of security. It is, however, clear that this aspect has to be thoroughly thought through and communicated throughout the organisation.

In order to develop resilient systems and generic capabilities there is a need for input from a thorough risk analysis that includes uncertainties throughout the analysis process. There is no guidance for such an analysis in the doctrines studied here and very limited research in the area.

In the analysed doctrines there is an ambiguity regarding to what extent the risk analysis should be fully quantified or just be dressed in quantitative terms. This ambiguity is troublesome but the full effects are not analysed in this work, it is, however, clear that there is a need for a more nuanced discussion of how the result and uncertainties of the risk analysis should interact with other decision supporting data.

This study has only studied military risk analysis in two of many important areas and in the light of the five criteria presented in Section 2.3. Therefore, there is a need for further research in many areas in relation to military risk analysis. We recommend that further research also include other areas for military risk management and include scenario definition, time span analysis, methods for including uncertainty, resilient military systems and how to find generic capabilities that have low sensibility to the actual uncertainties. Also the conditions and process for risk decisions deserve further research.

6 Conclusions

In relation to quality requirements on risk analysis this study has analysed two military application areas for risk analysis: military intelligence and risk and risk management in legal assessments.

From the analysis it is clear that risk analysis is an integral part of decision analysis and cannot be separated, in time, space or organisationally, from the decision process in general. The scenario definition is a central task in the risk analysis and will affect every aspect of the risk estimation. Therefore, the principles for scenario definition must be communicated and continuously updated throughout the organisation. To define the time span studied is especially challenging.

The decision maker also has the responsibility to weigh different consequences against each other which implies that the decision maker has to be involved in the scenario definition and the definition of the consequences under study.

The drive for resilient systems and generic capabilities set new requirements on military risk analysis, especially in relation to how to include uncertainties. These requirements will call for a more thorough analysis and will also improve the reliability of the results.

From the study it therefore can be concluded that risk analysis is a non-trivial task that has to be fine-tuned with other decision support processes. This is today not always the case and the doctrines studied give limited direction on how this can be done.

References

Amnesty International. (2000). NATO/Federal Republic of Yugoslavia "Collateral damage" or unlawful killings? Violations of the Laws of War by NATO during Operation Allied Force: Amnesty International.

Andrews, J. D., & Moss, T. R. (2002). Risk assessment *Reliability and risk assessment* (Second ed., pp. 411-448). London: Professional Engineering Publishing Limited.

Aven, T. (2009). Identification of safety and security critical systems and activities. *Reliability Engineering & System Safety*, *94*(2), 404-411.

Bakx, G. C. H., & Richardson, R. A. L. (2013). Risk assessments at the Royal Netherlands Air Force: An explorative study. *Journal of Risk Research*, *16*(5), 595-611.

Bang, M. (2014). Pitfalls in Military Quantitative Intelligence Analysis: Incident Reporting in a Low Intensity Conflict. *Intelligence and National Security*.

Burns, R. (2013, Feb 26 2013). APNEWSBREAK: Taliban attacks not down after all, *The Associated Press*.

Clark, R. M. (2013). *Intelligence analysis* (4th ed.). London: Sage.

Committee report to ICTY. (2000). Final Report to the Prosecutor by the Committee established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. The Hague: International Criminal Tribunal for the former Yugoslavia.

DCDC. (2010). Joint doctrine for joint force protection, Publication 3-64. Shrivenham: The Development, Concepts and Doctrine Centre, Ministry of Defence, United Kingdom.

Department of the Army. (2006). Composite Risk Management, FM 5-19 (FM 100-14). Washington DC: Headquarters Department of the Army.

Dinstein, Y. (2011). *The Conduct of Hostilities under the law of International Armed Conflict* (second ed.). United Kingdom: Cambridge University Press.

Doshi, P. (2009). Calibrated response to emerging infections. *BMJ, 339*.

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management, 6*(3), 165-177.

George, R. Z., & Bruce, J. B. (2008). The age of analysis. In R. Z. George & J. B. Bruce (Eds.), Analyzing intelligence (pp. 295-308). Washington D.C.: Georgetown University Press.

Hansson, S. O. (1993). The false promise of risk analysis. *Ratio-New Series, 6*(1), 16-26.

Hansson, S. O. (2012). *Riskfilosofi, En introduktion [In swedish]*. Stockholm: Liber.

Henckerts, J.-M., & Doswald-Beck, L. (2010). *Customary International Humanitarian Law* (Vol. Volume I: Rules). United Kingdom: Cambridge University Press.

Hubbard, D. W. (2009). Worse than useless: The most popular risk assessment method and why it doesn't work *The failure of risk management: Why it's broken and how to fix it*. Hoboken: John Wiley & Sons Inc.

ICTY Trial Chamber. (2004). Prosecutor vs. Blaskic, Blaskic case IT-95-14-T, 122 ILR 1. The Hague: the International Criminal Tribunal for the former Yugoslavia.

Johnson, C. W. (2007). *The Paradoxes of Military Risk Assessment*. Paper presented at the the 25th International Systems Safety Conference, Baltimore, USA.

Kunreuther, H. (2002). Risk analysis and risk management in an uncertain world. [Editorial Material]. *Risk Analysis, 22*(4), 655-664.

Kuo, C. (2007). *Safety management and its maritime application*. London: The Nautical Institute.

Lehtomäki, K., Pääkkönen, R. J., & Rantanen, J. (2005). Risk Analysis of Finnish Peacekeeping in Kosovo. *Risk Analysis, 25*(2), 389-396.

Liwång, H. (2012). *Risk-based ship security analysis – an approach based on civilian and military methods.* (Licentiate in Engineering), Chalmers Univeristy of Technology, Gothenburg.

Liwång, H., Ringsberg, J. W., & Norsell, M. (2013). Quantitative risk analysis – Ship security analysis for effective risk control options. *Safety Science, 58*(0), 98-112.

Marine Corps Institute. (2002). Operational Risk Management, ORM 1-0. Washington DC: Headquarters Marine Corps.

NATO. (2007). Allied joint doctrine for force protection, AJP-3.14. Brussels: NATO Standardisation Agency.

NATO. (2010). Comprehensive operations planning directive, V1.0. Brussels: NATO Supreme Headquarters Allied Power Europe.

Osterholm, M. T. (2005). Preparing for the Next Pandemic. *New England Journal of Medicine, 352*(18), 1839-1842.

Reason, J. (2000). Safety paradoxes and safety culture. *International Journal of Injury Control and Safety Promotion, 7*(1), 3-14.

Rebugio, A. B. (2013). Bias and Perception: How it Affects Our Judgment in Decision Making and Analysis. *Small Wars Journal*.

RTO/NATO. (2008). Improving Common Security Risk Analysis, RTO-TR-IST-049. Brussels: The Research and Technology Organisation (RTO) of NATO.

Shearer, R. (2011). Operational analysis in Iraq: Sifting through the fog of war. *Military Operations Research, 16*(2), 63-71.

Silver, N. (2012). *The signal and the noise, Why so many predictions fail - but some don't*. New York: the Penguin Press.

Swedish Armed Forces. (2009a). *Försvarsmaktens gemensamma riskhanteringsmodell [In swedish]*. Stockholm: Swedish Armed Forces.

Swedish Armed Forces. (2009b). *Handbok bedömning antagonistiska hot [In swedish]*. Stockholm: Swedish Armed Forces.

The White House. (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience. Washington DC: The White House, Office of the Press Secretary.

Tomes, S. (2012). Risk: misunderstanding or military misnomer. *The British Army Review, 153,* 32-40.

University of Cincinnati. (2004). Introduction to the principles of war and operations. Cincinnati: University of Cincinnati.

Yang, Z. L., Wang, J., & Li, K. X. (2013). Maritime safety analysis in retrospect. *Maritime Policy & Management, 40*(3), 261-277.