Threat and Control in Military Decision Making

Christofer Waldenström
Department of computer and system sciences,
Stockholm University,
Sweden
christofer.waldenstrom@fhs.se

Love Ekenberg
Department of computer and system sciences,
Stockholm University,
Sweden
lovek@dsv.su.se

Mats Danielsson
Department of computer and system sciences,
Stockholm University
Sweden
mad@dsv.su.se

Abstract

This paper presents a model of how military commanders estimate the threat posed by the enemy in a tactical situation and how they use own forces to control that threat. The model is based on interviews with nine commanders from the Swedish navy and the purpose is to find automatic and adequate methods for reasoning about strategic issues based on the long-time experience of highly qualified military officers. The results show that the number of enemy units, the types of enemy units, the behavior of the enemy units, and the uncertainties regarding the number, types, and behavior determines the threat in a tactical situation. The own course of action works as a threat altering function to control that threat. When the commander should decide on a course of action, we suggest that it should be selected so it minimizes the expected threat.

Keywords. Military decision making, threat, worst case, expected value, imprecise probabilities

1 Introduction

Military decision-making means putting peoples life at stake in order to reach military objectives. The military decision makers are not only faced with risk of their own lives, their decisions also means subjecting own personnel and maybe even civilians to grave danger. Furthermore, the decisions often have to be made in highly stressful situations and in almost all cases under conditions of uncertainty and time pressure. When deciding what to do the military commander has to weigh possible gains against possible losses to determine the worth of each alternative. If an alternative where the possible gain outweighs the possible losses can be found, the risk of that alternative is considered worth taking, and it is chosen and implemented.

How military decision makers make such tradeoffs have not been studied to any great extent and empiric data in this field is almost nonexistent [1, 2]. Consequently, research is needed to investigate how military decision makers judge the risk of a certain course of action, and how they decide if that risk is worth taking. The rationale for this is that if we want to devise proper decision support we must first understand how such decisions are made in order to identify possible difficulties and pitfalls. This study is based on the assumption that determining acceptable risk means making a decision that strikes a balance between the factors that increase risk, the factors that decrease risk and the factors that justify risk. If such balance can be found, the risks following from the decision are acceptable and are worth taking. This paper focuses on how a commander estimates the threat posed by an enemy in a tactical situation and what he or she does to controls that threat. The results will be used as the groundwork aiming at devising a military decision support system.

2 Background

How a rational human being should make choices under conditions of uncertainty have been extensively studied in the field of normative decision-making, and a widespread opinion is that utility theory captures the concept of rationality [3-6]. Nevertheless, people seem to make decision in other ways but those stated by expected utility theory as has been demonstrated in a vast of psychological experiments [7, 8]. To accommodate deviations between the normative theories and the experimental results descriptive theories have been proposed [9, 10].

Luce and Raiffa's [5] distinction between certainty, risk or uncertainty has been further developed by Einhorn & Hogarth [11]. They distinguish between ignorance, ambiguity and risk according to the degree to which one can rule out alternative distributions. In a state of ignorance no distributions are ruled out, while in a state of risk all but one distribution are ruled out. Ambiguity is an intermediate state between ignorance and risk and results from the uncertainty of specifying which of a set of distributions is appropriate in a given situation. Thus, ambiguity refers to not knowing the structure of the system that produces the outcomes. As showed by Ellsberg [12] people prefer risk to ambiguity).

This observation is of special interest in the military domain. The problem facing a military decision maker is to decide how to solve a mission in a hostile environment, and the decision is made difficult by the uncertainties regarding the enemy [13]. These uncertainties regard both what the enemy looks like (the structure of the system) as well as what the enemy will do (the outcome of the system).

Further, military decision making comprises of more than just selecting the best course of action from a given set. Courses of actions do not present themselves in a ready-made fashion, they must be developed, and this is done according the methods prescribed in military planning manuals [14]. These manuals prescribe the military decision-making process as a process aiming at procedural rationality [15] where course of action are first developed, and then the best is selected according to some criteria. Nevertheless, empirical research show that in many cases the decision maker only develops one 'good enough' course of action that is put to action [16, 17]. Thunholm [16] further showed that under conditions of time pressure rational methods do not produce better courses of action than intuitive methods. Even if this seems to spell bad news for the rational methods, it probably only means that better normative methods are yet to be found[1].

Another distinct feature of tactical decision-making in the navy is the decision-making tempo. The commander may only have a few hours to plan a mission before execution must begin. Once execution begins the focus changes; instead of devoting resources to decide what has to be achieved in the future, resources are redirected to figure out how the current operations are proceeding. Any difference between perceived state and the state predicted by the plan might be a potential problem. The commander must identify the situations that pose threats to the successful accomplishment of the mission. If a potential problem is detected, appropriate action must be devised and implemented in order to prevent derailing of operations. This makes military decision making an ongoing process. New courses of actions have to be developed and implemented as a reaction to the changing events [18].

How people make decisions in such an environment been studied in the fields of dynamic and naturalistic decision-making. In the field of dynamic decision making the focus has been on how people in general control a dynamic system, and the difficulties they face in that task [19]. The results, however, are only on a general level and not immediately applicable to how military decision makers make judgments of threat and control.

Naturalistic decision making (NDM), on the other hand, are interested in how experts make decisions within their own fields and some studies have focused on military personnel [20, 21]. Results from this field indicate that decision makers employ quite stable strategies that, despite the presence of uncertainty, make it possible to make decisions.

In one NDM study Lipshitz and Strauss [22] studied how Israeli Army officers coped with uncertainty and concluded that the participants distinguished between three types of uncertainty: uncertainty caused by inadequate understanding, uncertainty caused by incomplete information and uncertainty caused by undifferentiated alternatives. They coped with these by applying five different strategies: i) reducing uncertainty (by collecting more information), ii) assumption-based reasoning, iii) weighing pros and cons of competing alternatives, iv) suppressing uncertainty, and v) forestalling. Similar strategies have been obtained by others, although the context in their studies was not military [10, 23]. Hutton [24] has made an extensive review of strategies with focus on the military context. But as in the case of dynamic decision-making no studies have explicitly focused on threat or control judgments.

Even if some effort has been made to describe how military decision makers cope with uncertainty, very few attempts have been made at investigating how they judge risk. What increases or decreases military risk, how uncertainty affects military risk and what makes military risks worth taking have neither been investigated to any great extent. This paper presents a model of how military decision maker judge the threat posed by the enemy and what he or she does to control that threat, and will be used to establish the requirements for a military decision support system. It should be noted that what people do is not necessary a good guide to what they should do. Nevertheless, a practical approach when designing support systems is to start with the problems people have in a task, helping people with things they find easy will probably leave that support unused. Thus, to identify these potential problems you need a descriptive account the task.

3 Method

The participants were nine officers who either were or had been in active duty in the Swedish navy. One of the participants had served as Chief of Navy, the highest commander of the Navy and a direct subordinate com-

[1] It should be noted that in some situations 'good enough' solutions, i.e., statisficing solutions, can be considered normative or even the only possible solution [26].

mander to the Supreme Commander. One had served as Chief of Fleet, the highest commander of the Fleet. Two participants had served as Commander of a Surface Warfare Flotilla (the highest tactical commander of a naval mission consisting of 15-20 navy ships often coupled with support units such as helicopters, attack, fighter, or surveillance aircrafts). Three participants had served as Commanders of Surface Warfare Divisions (subordinate to a Flotilla Commander and in charge of approximately four to six navy ships). Two participants had served as Commanding Officers of a ship. Eight of the participants were specialized in anti surface warfare and/or anti submarine warfare and one officer in mine warfare. The participants had led between 10 to 100+ military planning processes on the tactical level or above, and they had led between 10 and 100 naval missions (exercise and/or live)[2]. All respondents were men.

The study was conducted using semi-structured interviews, duration ranging between 0.5-1.5 hours. The questions were based on the steps and tasks prescribed by the Swedish Navy's decision-making process (SNDMP), which like other military decision making processes is highly proceduralized process where of a number of distinct steps should be completed in sequence [25]. However, none of the steps or tasks in SNDMP explicitly states that the decision maker should carry out risk estimates, so asking how the respondents made such estimates would probably yield little or no data. Instead it was assumed that risk estimates would be embedded in the decision-making process and consequently all respondents had to describe how they carried out each of the steps.

The interviews were transcribed verbatim, leaving out pauses, humming etcetera and analyzed using content analysis. As no stage of the SNDMP explicitly calls for risk estimates it was suspected that the participants would use other phrases together with 'risk' when they accounted for how they made such considerations. Consequently, all statements containing the words "risk", "threat" and "danger" were excerpted. To determine if a statement related to judgments of threat or control, each were analyzed by the author. The data were reduced by amalgamation of similar statements and the result was checked for internal consistency (no contradictions within the statements) and integrated to form a coherent model of threat and control in military decision making.

4 Results

The results show that two things determine the level of threat in a tactical situation: i) the enemy and ii) the level of uncertainty regarding the enemy. All respondents expressed that the enemy is the major threat determinant (9 of 9). When considering the enemy, two questions occupy the participants: what forces does the enemy have and what can the enemy do? As expected, the more forces the enemy have and the more capable the forces, the higher the threat. Further, the forces can be employed differently leading to more or less threatening actions.

The other threat driver is uncertainty. The results indicate that the respondents (6 of 9) regard uncertainty almost synonymously with threat, risk or danger[3]. An uncertain situation is a threatening situation. As one of the lower experienced respondents put it "You often regarded different aspects of risk taking, what risks were acceptable, what uncertainties". When faced with uncertainty, as understood by some of the participants in this study (4 of 9), they deal with it by worst-case reasoning. This, however, gives a different bounding of risk than probability would give.

Consider the uncertainty about the enemy forces. Given no uncertainty at all, all enemy units that pose a threat, are known. Thus, the risk is equivalent to the threat posed by those units. As uncertainty increases, the more the decision maker tends towards worst-case reasoning. Consequently, risk is bound on the lower end by the threat posed by the known forces, and on the upper end by the threat posed by the worst plausible combination of enemy forces. The same reasoning goes for what the enemy can do. When uncertainty is zero then the risk is equal to what the decision maker knows the enemy is going to do. As uncertainty increases the risk approaches the threat posed by the worst plausible enemy course of action. The following statements from two of the higher-ranking respondents serve as examples:

> Let us say that you can get a decent understanding of what resources the enemy got, but what his possibilities are, how he thinks and ponders, that is not as easy. If you start to sort out, what are his resources? What kinds of ships are there, what kind of aircrafts, what other forces does he have?
>
> And then you lay low and wait. You know that he can approach this area, and your mission is to prevent him from entering and doing something in this area. […] Then you must keep track of where he is and what the most dangerous thing he can do is, and decide how you can counter that. And yes, the difficult part is to know how big they are, how many they are, and how strong they are. That is what you are going to think about.

In the military context, threat is controlled by employing own units and by devising an appropriate own course of action. On this point all respondents agree (9 of 9). The number of own units and the types of own units deter-

[2] About half of the respondents have participated in countering the repeated violations of Swedish territorial waters by submarines during 1980-1995, where several targets were engaged. If, and to what extent these violations took place are still causing controversy but this will not be further discussed here.

[3] This may be in part linguistic. The word 'uncertainty' has two meanings in Swedish, which can be translated to 'uncertain' and 'insecure'. However, when military personnel talk about 'uncertainties' regarding an operation they generally refer to the former meaning.

mines the control created by own units. The more own units, the higher the perceived control. The more capable the own types, the higher the perceived control. Following statements from two of the highly experienced respondents serve as examples:

> What is it that has to be done? What does the threat look like? What enemy forces are in the area? What forces will I have at my disposal? In that situation the first thought is: Do I have enough own forces or do I need support from other units? Do I need recognizance aircrafts, attack aircrafts, surveillance helicopters, or support from other surface attack forces? A first feeling; do I have enough forces, enough capability to solve this mission?

> I mean, what is level of risk you must be prepared to take? Of course there is a connection to the resources as I as tactical commander can use. And the difficulty is of course what resources I can get. What support can my mission [as tactical commander] get from the mission commander [the higher command]? There is a discussion about the supporting functions that I can get related to the level of risk. As an example: Can I get air support, costal missile batteries or something else as an additional strength. Or can I get submarine missions as support?

Control is also achieved by devising/selecting an own course of action that subjects own forces to more or less risk. The control achieved by own course of action is consequently transitive. Consider following statement from one of the high experienced respondents:

> It is embedded in this, the comparison of forces. How can I, so to say, protect my own forces and when can I strike, that is what it is all about. And if this comparison is to my advantage, which it seldom has through the years, it has always been an advantage to the enemy, both in numbers, size, resources, ranges, additional aircrafts and everything […] well yes, then I must, to protect my own forces as much as possible, utilize the protection I can get from maybe the terrain or similar, that is the archipelago, in another way than if we had an advantage of some sort in ranges. If that were the case, then you had been able to go out [on the open sea] in another way.

The results indicate that the threat posed by an enemy force is a function of how large the enemy force is (how many units it contain), how capable it is (what kind of types of units it contains), what the enemy is doing (behavior), and the uncertainties regarding the number, types and behavior of the enemy. Beginning with the properties of a unit, the threat posed by a unit is determined by its ability to destroy other units. To destroy another unit it must first be able to detect the other unit, and second, have a weapon that can be used to engage the detected unit. Thus, the threat or control posed by a unit is determined by the unit's ability to detect other units, together with the weapons carried by that unit.

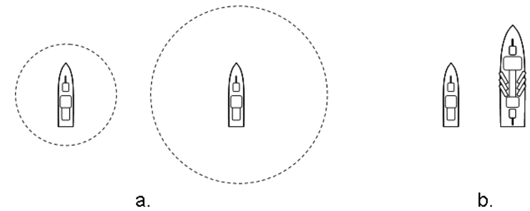

Figure 1

Looking at Figure 1a, two identical ships with regard to armament and maneuverability are depicted. In this example the right ship will be considered as more of a threat since it can detect units (and consequently fire a weapon against them) at a further distance than the left ship.

If we continue to the weapons, a unit is perceived as more of a threat if it carries more powerful weapons. Figure 1b depicts two ships: a patrol boat (to the left) and a destroyer (to the right). The patrol boat carries a single gun while the destroyer carries two guns and six surface-to-surface missiles. In this case, the destroyer will be perceived as the higher threat due to its heavier armament. Furthermore, the range of the weapons carried by a unit also determines its level of threat. A unit with long ranged weapons will be considered more of a threat than the same unit with shorter ranged weapons. The reason for this is that a unit with long ranged weapons may fire that weapon outside the detection range of friendly units.

Yet another property that increases threat or control is a unit's ability to avoid detection, its ability to stealth. If a unit has a high ability to stealth, the unit has the advantage of coming into range with its own weapons and sensors without being detected by the opposing unit.

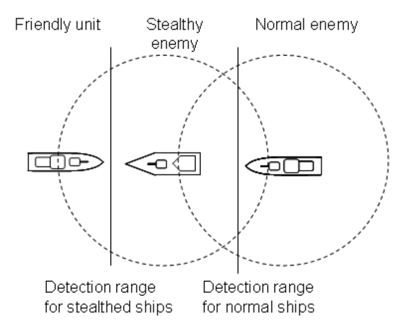

Figure 2

Looking at Figure 2, three ships are illustrated: a friendly unit (left) a stealthy enemy (middle) and a normal enemy (right). Even though the stealthy and the normal enemy have the same weapons and sensors, the stealthy enemy will be perceived as more of a threat since it can detect and fire a weapon on the friendly unit without being detected. Consequently, a unit with high ability to stealth may pose a higher threat than a normal unit, even if the normal unit is equipped with better sensors and armament.

As said earlier, the behavior of an enemy unit also affects the perceived threat. In Figure 3 an enemy ship is moving north, its weapon and sensor ranges illustrated by the dashed circle. Now suppose that the enemy unit suddenly changes course. If the course change will bring the enemy closer to the friendly unit, the perceived threat will increase since the friendly unit runs risk of coming within range of the weapons carried by the enemy. On the other hand, if the course change will bring the enemy further away from the friendly unit, the perceived threat will decrease for the opposite reasons.

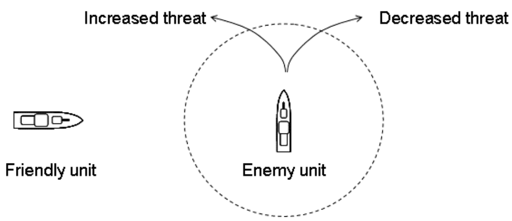

Figure 3

The capability of a force is determined in the same way as the capability of a single unit, by its ability to detect and destroy targets. But on a force level a procedure of target sharing can enhance those abilities. Once a naval operation is underway all units use their sensors to survey their immediate surroundings. All contacts are reported to designated units in the force, which compile the reports into a single, coherent view of the operation's area. This view is then distributed to the whole force. This procedure allows all units to become aware of all contacts held by the force, including contacts out of range by their own sensors.

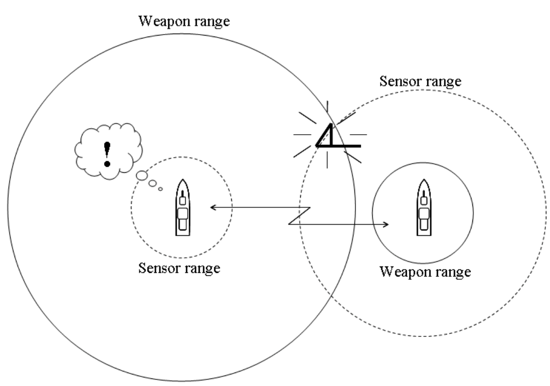

Figure 4

How this procedure can enhance the combined effect of the force is illustrated in Figure 4. The right ship with the greater sensor range detects a target with its radar. As the target is outside the range of its own weapons the right ship cannot itself destroy it. However, by sending the target to the partner to the left, the partner also becomes aware of the target. The left ship has much greater weapon range and as the target is within that range, the left ship can engage the target.

This simple scenario illustrates that the more capable a force is to detect targets, the more threatening will it appear. However, a force with superior surveillance capability is no threat at all if it does not have the capability to destroy the targets it has detected. Thus, the weapons it can employ also determine threat. The more powerful and the longer ranged they are, the more threatening the force will be perceived. On the other hand, the force is of no threat at all if it cannot detect any targets. Thus, to be a superior force it must have the upper hand both when it comes to sensor capability and weapons capability.

Figure 5 further illustrates the situation. To the left we see a force consisting of two ships of the same type. The inner zone, denoted by a dashed line, depicts the total area covered by the force's sensors. The outer zone shows the area covered by the force's weapons. The gray zone shows the area, in which this force can both detect and destroy targets; in this case it is the same as the area covered by sensors. If we now look at the right force we see that it consist of one ship and one helicopter. If we assume that this ship is of same type as the ships in the left force, we see that the area in which the right force has control is much larger that the left force's. This is due to the superior sensor range provided by the helicopter. If we now compare the threat perceived by the commanders in each force, the commander of the left force will probably perceive a higher degree of threat, despite the fact that he or she has twice as many weapons. This is quite evident since the right force can close in on the left force, use the helicopter to find the left force, fire its missiles at max range, without risking detection of the left force. Thus, the threat or control provided by a force is determined by its composition of the own force, in the same way as the threat posed by the enemy is determined by the composition of the enemy force.

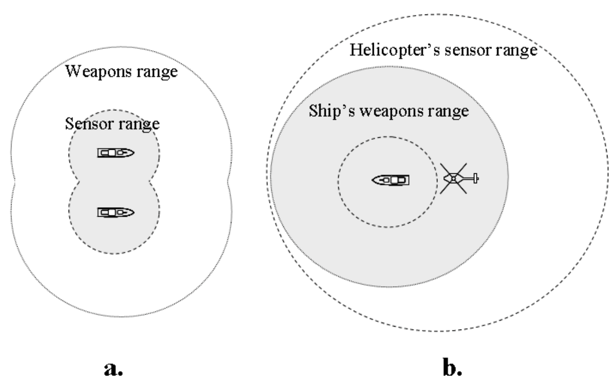

Figure 5

As have been illustrated above, the control provided by own units was determined in the same way as the threat posed by the enemy. The second way to handle the threat was to devise an appropriate own course of action. How this can be accomplished is illustrated in Figure 6. The mission is to move the ship from Port A on the mainland to Port B on the island. Intelligence has reported that during the initial phases of the operation no enemy is in the area, but as the operation is underway the enemy will most likely try to prevent the transport. The commander concludes that if we move quickly we might get the transport to Port B without giving the enemy a chance to interfere. The plan is to move the transport ship at high speed across the open water, thus minimizing exposure time to the enemy threat. The friendly units will establish a protective screen.

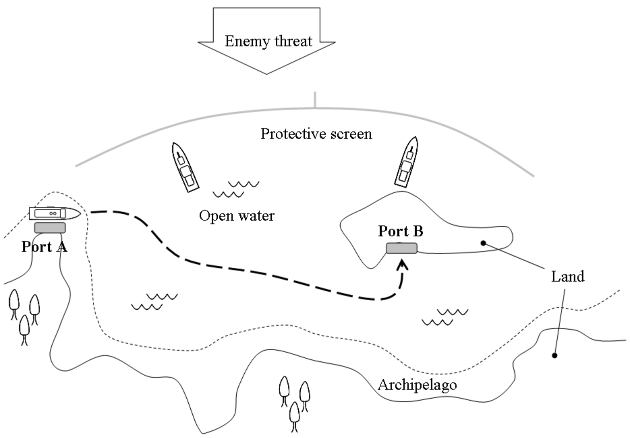

Figure 6

Now assume the operation is underway and the transport ship has reached a point on the open water between Port A and Port B. Suddenly, an enemy ship is detected and identified. Since the open sea does not provide any protection it is assumed that the enemy also has detected the transport ship. Figure 7 illustrates the situation. The enemy has a weapon range denoted by r_1 and the friendly ship a weapon's range of r_2. This means that the enemy ship cannot be allowed to get any closer than r_1 to the transport ship, or else the transport ship runs risk of being sunk.

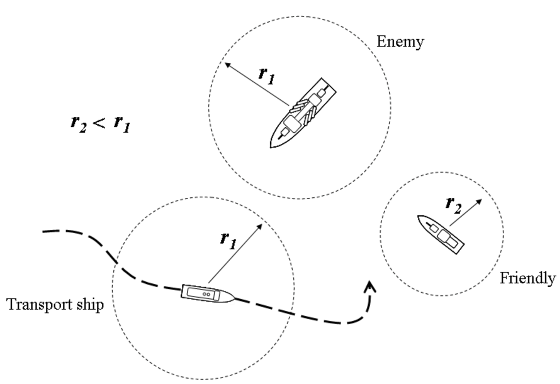

Figure 7

The commander can handle the threat in two ways. One alternative is to order the transport ship to head south and hide in the archipelago. This makes the transport ship difficult to detect and consequently difficult to destroy. The other option is try to sink the enemy ship, removing the threat altogether. However, attacking the enemy is dangerous since the own ship is inferior when it comes to weapon ranges ($r_2 < r_1$). On the other hand, it may be worth the risk since a successful attack will lower the overall threat for the rest of the operation.

In this case the commander orders the transport ship to head south and seek cover in the archipelago. The idea is to let the transport ship move in the archipelago to the point on the mainland where the distance to the island is minimal. Once there, it will lay low and wait until the friendly units have cleared the route to Port B, as shown in Figure 8. Using same reasoning as before, the area that must be cleared is obtained by measuring the range of the enemy's longest ranged weapon and apply that distance perpendicular to the planned route. When the area is cleared the transport ship will rush out at maximum speed, giving the enemy minimum amount of time to act before the transport ship reaches Port B.

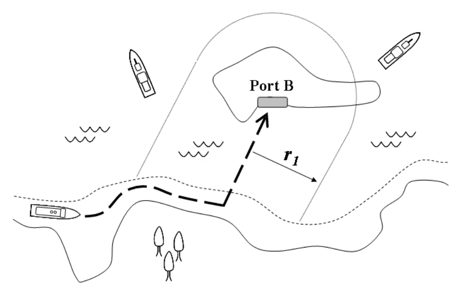

Figure 8

As pointed out, one of the most difficult aspects of military decision-making is the analysis of the enemy. Such analysis is made difficult because all information regarding the enemy is afflicted with uncertainty. The uncertainty regards three aspects of the enemy forces: (i) the number of units, (ii) the types of units and (iii) the behavior of the units. All these aspects affect the perceived threat.

This can be modeled in a tree structure (see Figure 9). The root node (S) represents the current scenario, i.e., the context in which the naval operation should be conducted. The intermediate nodes consist of the three aspects describing the enemy, where the first level represents the number of enemy units (n), the second level the types of enemy units (t), and the third level the behavior of the enemy units (b). The value nodes (v) quantify the perceived threat of each branch in the tree.

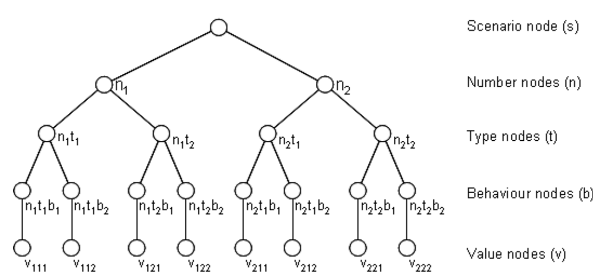

Figure 9

But as we saw above, the threat posed by a naval force could not be obtained by just adding the threat values of the single units. It was the composition of the force that created the actual threat value. The tree structure accommodates this situation. Earlier it was illustrated that a force consisting of one surface ship and one helicopter posed a different threat than a force consisting of two surface ships (all surface ships are of the same type). A tree representation of this situation is presented in Figure 10. The two forces consists of the same number of units, hence the number node is n=2. The types are however different giving two type-nodes: t_1=2 surface ships; t_2=1 helicopter and one surface ship. If we assume the same behavior of each force, b_1=Attacking, then different threat values are assigned to the value nodes, $v_{n_1 t_1 b_1}=4$ and $v_{n_1 t_2 b_1}=8$.

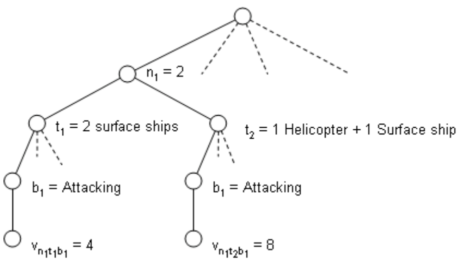

Figure 10

When analyzing the own forces, the commander considers the same aspects as those of the enemy, the number of units, the types of units, and the behavior of the units. It is consequently tempting to model the own forces in a tree structure, similar to the enemy. There is, however, a difference. There is hardly any uncertainty at all regarding the own forces. When an operation is initiated the commander receives a mission statement from higher command. This statement contains the task to be solved, a roster of the forces assigned to the commander, and information about the enemy. When planning begins all these pieces are fixed. The commander can neither influence the mission assigned, nor the forces, nor the intelligence about the enemy. Representing the own force could be quite straight forward, as illustrated in Figure 11:

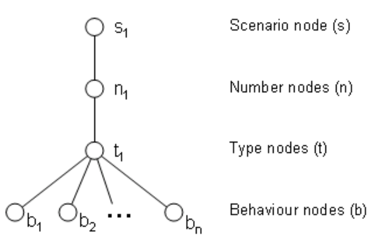

Figure 11

Nevertheless, using a tree structure in the case presented here brings along two problems: (i) it is hard to determine the value nodes since the control provided by the own force depend on a comparison between the own force and the enemy, (ii) the probability assignments of the own behavior has no meaning because the commander decides on a course of action given the own force and the threat. So, how should the own force be represented taking these constraints in mind?

As we saw earlier, the roster of the own forces made both the numbers of ships (n) and the types of ships (t) fixed. The only thing the commander can influence is the behavior of the own forces. As a consequence, the own force can represented similar to the enemy, as a single type-node that is then used as an argument when deciding how to solve the mission. Thus, the own behavior can be seen as a threat-altering function that given the own force influence the enemy's opportunity to pose threat to the own operation. Consider the situation described in Figure 7. When the transport ship heads south to take cover in the archipelago the negative value of being sunk is the same, however the probability that the enemy will sink the ship has been reduced. The alternative behavior, attacking the enemy ship and trying to sink it, will lead to that the probabilities of the number of enemy ships are altered.

To this point we have looked at how the commander analyses the threat and how the commander's own course of action alters that threat. However, the problem facing the commander is of course how to devise a proper course of action, taking in to account all uncertainties inherent in the information about the enemy. As the results indicated, the commander copes with this situation by employing worst-case reasoning. Even if this strategy might reduce the cognitive load it brings along at least two problems. First, the commander may have to design a very specific course of action to deal with the worst possible threat. The risk of that is of course that the commander may stretch the own resources towards the specific case so much that the solution might be fragile to other cases: by optimizing to solve a single case the robustness of the solution is lost. A second problem is that given limited resources the commander may end up in a situation where no solution can be found. In any case, if we want to analyze the situation beyond what is done intuitively a more systematic approach is required.

5 Representation and Evaluation

The commander's decision consists of selecting one of several scenarios. In such a scenario tree, the decision is represented in tree form as a sequence of probabilities leading to some final outcomes described by the end nodes. All decision trees consists of a root node, representing the decision, a set of intermediary nodes, representing the scenarios and uncertainty regarding the scenarios, and the outcome nodes describing the consequences of the scenarios. For each intermediate node, there is a probability associated with the node (number node, type node, or behavior node). In real planning situations, there is uncertainty inherent in the input data to the planning process. In the model, this is represented by probabilities and outcome values being in the form of interval variables, i.e. the variables having a lower and an upper bound. For example, the decision-maker statement that probability p_i is between a_1 and a_2 is denoted $p_i \in [a_1, a_2]$ and translated into $p_i > a_1$ and $p_i < a_2$ in the model. Similarly, the value of the outcome i (v_i) is between a_1 and a_2 is denoted $v_i \in [a_1, a_2]$ and translated into $v_i > a_1$ and $v_i < a_2$. In this way, sets of statements (inequalities) are formed.

The collection of probability statements in a decision situation is called the node constraint set. A constraint set is said to be consistent if it can be assigned at least one real number to each variable so that all inequalities are simultaneously satisfied. The probability and value constraint sets are collections of linear inequalities. A minimal requirement for such a system of inequalities to be meaningful is that it is consistent, i.e., there must exist some vector of variable assignments that simultaneously satisfies each inequality in the system. In other words, a consistent constraint set is a set where the constraints are not contradictory.

> **Definition:** Given a tree T, let N be a constraint set in the variables $\{ n_{...i...j...} \}$. Substitute the intermediary node labels $x_{...i...j...}$ with $n_{...i...j...}$. N is a *node constraint set* for T if for all sets $\{n_{...i1},\ldots,n_{...im}\}$ of all sub-nodes of nodes $n_{...i}$ that are not leaves, the statements $n_{...ij} \in [0,1]$ and $\sum_j n_{...ij} = 1$, $j \in [1,\ldots,m]$ are in N.

Thus, a node constraint set relative to a tree can be seen as characterizing a set of discrete probability distributions after a certain level (the *probability constraint set*). The core of these can be thought of as an attempt to estimate a class of mass functions by estimating the individual discrete function values. The normalization constraints ($\sum_j x_{ij} = 1$) require the probabilities of sets of exhaustive and mutually exclusive nodes to sum to one.

Requirements similar to those for node variables can be found for value variables. However, no dimension reducing normalization constraints (variables summing to one) exist for the value variables.

> **Definition:** Given a tree T, let L be a constraint set in $\{t_{...1}\}$. Substitute the leaf labels $x_{...1}$ with $c_{...1}$. Then L is a *value constraint set* for T.

Similar to probability constraint sets, a value constraint set can be seen as characterizing a set of value functions. The elements above constitute a command frame, which constitutes a complete description of the probabilistic threat situation.

> **Definition:** A *command frame* is a structure $\langle T,N,V \rangle$, where T is a scenario tree, N is a node constraint set for T and V is a threat constraint set for T.

While an evaluation of a consequence set may result in an acceptable expected value, the consequences of selecting it might be so dire that it should nevertheless be avoided. The commander may want to exclude particular alternative courses of action that are, in some sense, too risky. It might, for example, endanger the entire purpose of the operation, and in that case even a consequence with a low probability is too risky to neglect.

The intuition behind security levels is that they express when a scenario is undesirable. Thus, a decision-maker might regard a scenario as undesirable if it has consequences with too low a value, and with too high a probability to occur. This means that if several consequences of a strategy are too dire (w.r.t. a certain value parameter), their total probability should be considered even if their individual probability is too low to render the scenario undesirable. Such exclusions can be dealt with by specifying a security level for the probability and a threshold for the value. Then a consequence set would be undesirable if it violates both of these settings. The security level has the following basic form

$$S(C_i, r, s) = (\sum_{v_{ij} \le r} p_{ij} \le s)$$

where r is the minimally tolerable value threshold and s is the maximally acceptable probability for events below the threshold to occur. This is a boolean function sorting out unwanted consequence sets.

The remaining scenarios are selected according to a decision rule, usually by maximizing the expected value of an alternative. Looking at Figure 9 the expected threat in the situation s, T(s), is calculated using the following formula:

$$T(s) = \sum_{i=1}^{2} n_i \sum_{j=1}^{2} t_j \sum_{k=1}^{2} b_k v_{ijk}$$

This structure is generalized into the following formula for calculating the generalized expected threat:

> **Definition**: Given a scenario S_i for $i=1,\ldots,r$ the expected threat of that scenario is given by the expression

$$T(S_i) = \sum_{i=1}^{n_i} n_i \sum_{j=1}^{n_j} t_j \sum_{k=1}^{n_k} b_k v_{ijk}$$

where n_i denotes the probability that the enemy has n_i number of ships, t_j denotes the probability that the enemy has t_j types of ships, b_k denotes the probability that the enemy will use behavior b_k, and v_{ijk} denotes value of the perceived threat of the combination $n_i\, t_j\, b_k$.

Given the threat in a scenario, the own course of action was regarded as a threat-altering function, taking the own force and the threat as arguments:

> **Definition**: Given a scenario S_i with the expected threat $T(S_i)$ and the own forces F(n,t) where n=number of ships and t=types of ships. Behavior B_j is a function such as:

$$B : B\big(F(n,t), T(S_i)\big) \rightarrow T(S_i)'$$

Faced with many possible own course of action the question arises of which one to choose. What rule the commander uses have not been established but we suggest that the commander should *devise and select a behavior that given the own force solves the mission and minimizes the expected threat.*

Definition: Given a scenario S_i with the expected threat $T(S_i)$ and a set of own behaviors B_j, j=1...r such that $B_j : B_j(T(S_i)) \rightarrow T_j(S_i)$ giving the set of expected threats $T'(S_i) = \{T_1(S_i), \ldots, T_r(S_i)\}$. Minimizing the expected threat means selecting B_j such that $T_j(S_i) = \min T'(S_i)$

Here we use expected utility, but the framework allows for other methods to be used. As an example, quantiles can be implemented using security levels. It seems however somewhat reasonable to use the mean as an initial assumption because this will distribute the own forces according to the 'center of gravity' of the threat. Nevertheless, if the commander uses such an approach has to be established empirically.

Often, however, the expected value by itself is unable to discriminate between the scenarios. In such cases, a further analysis is called for in the form of an automated analysis called contraction. Contraction is a generalized sensitivity analysis that can be carried out in any number of dimensions. In complex decision situations, when an information frame contains numerically imprecise information, the different principles suggested above are often too weak to yield a conclusive result and will often yield a far too crowded set of candidates. One way to handle this could be to determine the stability of the relation between the considered consequence sets. As interval statements are deliberately imprecise, a natural way to investigate this is to consider values near the boundaries of the intervals as being less reliable than more central values. Using contractions we take this into account by indirectly measuring the dominated regions.

The principle of contraction is justified by the difficulties of performing simultaneous sensitivity analysis in several dimensions at the same time. If one uses only one-dimensional analyses, it can be hard to gain real understanding of the solutions to large decision problems because different combinations of dimensions can be critical to the evaluation results. Exploring all possible such combinations would lead to a highly complex procedure regarding the number of cases to investigate. Using contractions circumvents this difficulty. By co-varying the contractions of a set of intervals, it is possible to gain a much better insight into the influence of the structure of the information frame on the solutions. Both the set of intervals under investigation and the scale of individual contractions can be controlled. Further, contractions are measures of the strength of statements when original solutions sets are modified in controlled ways, rather than measures of the solution sets as given by volume estimates. Consequently, a contraction can be regarded as a focus parameter that zooms in on central sub-intervals of the full statement intervals.

Definition: X is a base with the variables $x_1, \ldots, x_n$, $\pi \in [0,1]$ is a real number, and $\{\pi_i \in [0,1] : i = 1, \ldots, n\}$ is a set of real numbers. $[a_i, b_i]$ is the interval corresponding to the variable x_i in the solution set of the base, and $\bar{k} = (k_1, \ldots, k_n)$ is a consistent point in X. A *π-contraction* of X is to add the interval statements $\{x_i \in [a_i + \pi \cdot \pi_i \cdot (k_i - a_i), b_i - \pi \cdot \pi_i \cdot (b_i - k_i)] : i = 1, \ldots, n\}$ to the base X. $\bar{k}$ is called the *contraction point*.

By varying π from 0 to 1, the intervals are decreased proportionally using the gain factors in the π_i-set, thereby facilitating the study of co-variation among the variables.

6 Discussion and further work

We have presented a model of how a commander estimates the threat in a tactical situation and how an own course of action is selected to control that threat. In a tactical situation the information about the enemy is almost always afflicted with uncertainty and the results indicated that the commander coped with this situation by worst-case reasoning. This work is part of the groundwork for further study of how a decision support system for tactical decision-making could look like. If such system should be realized as automatic quantitative support or as verbal heuristics remains to be determined.

Just considering alternatives and choosing in accordance with our like or dislike of risk can be considered a quite passive way of treating risk [23]. As we saw in this study, the own course of action was treated as a threat-altering function, which points to a more active stance towards risk: When facing a risky situation the respondents want to take action to influence and modify the risky situation. This is what [23] calls "adjusting the risks" and means gaining time, information or control. Time allows for information to be gathered, and information may resolve the uncertainty that makes the situation appear risky. Gaining control means taking actions to reduce the magnitude or the chance of loss. It would not be too surprising to find similar strategies employed by the participants in this study.

We suggested that a course of action should be selected that minimized the expected threat. It can be argued that a solution that tries to solve all 'possible threats' risk to end up being multi-useless instead of multi-purpose. However, statements like "…have enough width [in your COA]…" indicate a desire to devise a course of action that is easily adaptable so it can handle several developments of events.

To enable automatic reasoning the necessary information must be extracted from the commander or the staff and structured rapidly. Populating the threat constraint set could be time consuming but a solution would be to find a formula that given the enemy forces and the own forces automatically can calculate the threat posed by any combination of own and enemy forces.

This study was based on the assumption that determining acceptable risk means making a decision that strikes a balance between the factors that increase risk, the factors that decrease risk and the factors that justify risk. Having dealt with the former two, our next work will focus on how a military decision maker judge if a risk is worth taking.

7 References

[1] Z. Lanir, B. Fischhoff and S. Johnson, "Military risk-taking: C^3I and the cognitive functions of boldness in war," *Journal of Strategic Studies,* vol. 11, pp. 96-114, 1988.

[2] Y. Vertzberger, *Risk Taking and Decisionmaking: Foreign Military Intervention Decisions.* Stanford, California: Stanford University Press, 1998,

[3] L. J. Savage, *The Foundations of Statistics.* ,2nd ed.New York: Dover Publications, 1972,

[4] J. von Neumann and O. Morgenstern, "Theory of Games and Economic Behavior," 1944.

[5] D. R. Luce and H. Raiffa, *Games and Decisions.* New York: Dover Publications, 1957,

[6] F. Knight, *Risk, Uncertainty, and Profit.* ,Reprint ed.Washington, D.C.: Beard Books, 2002,

[7] D. Kahneman, P. Slovic and A. Tversky, *Judgement Under Uncertainty: Heuristics and Biases.* US: Cambridge University Press, 1982,

[8] T. Gilovich, D. Griffin and D. Kahneman, *Heuristics and Biases.* New York, US: Cambridge University Press, 2002,

[9] D. Kahneman and A. Tversky, "Prospect theory: an analysis of decision under risk," *Econometrica,* vol. 47, pp. 263-291, 1979.

[10] Z. Shapira, *Risk Taking a Managerial Perspective.* New York, US: Russel Sage Foundation, 1995,

[11] H. Einhorn and R. Hogarth, "Ambiguity and uncertainty in probabilistic intference," *Psychological Review,* vol. 92, pp. 433-461, 1985.

[12] D. Ellsberg, "Risk, ambiguity and the Savage axioms," *Quarterly Journal of Economics,* vol. 75, pp. 643-669, 1962.

[13] C. Waldenström, "What is difficult in naval sensemaking," in *Proceedings of the 13Th International Command and Control Research and Technology Symposium,* 2008,

[14] US Army, "Field Manual 5-0 Army Planning and Orders Production." 2005.

[15] H. Simon, "Rationality as process and product of thought," *The American Economic Review,* vol. 68, pp. 1-16, 1978.

[16] P. Thunholm, "Military decision making and planning: towards a new prescriptive model," 2003.

[17] J. Schmitt and G. Klein, "A recognitional planning model," in *Proceedings of the 4Th ICCRTS,* 1999,

[18] M. van Creveld, *Command in War.* US: Harvard University Press, 1985,

[19] D. Dörner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations (Originally Published in Germany 1989 Under the Title Die Logik Des Misslingens by Rowholt Verlag).* ,3rd ed.NY: Metropolitan Books, 1996,

[20] G. Klein, J. Orasanu, R. Calderwood and C. E. Zsambok, *Decision Making in Action: Models and Methods.* Norwood, NJ: Ablex Publishing Corporation, 1993,

[21] R. Flin, E. Salas, M. Strub and L. Martin, *Decision Making Under Stress: Emerging Themes and Applications.* Ashgate, 1997,

[22] R. Lipshitz and O. Strauss, "Coping with Uncertainty: A Naturalistic Decision Making Analysis," *Organizational Behavior and Human Decision Processes,* vol. 69, pp. 149-163, 1997.

[23] K. R. MacCrimmon and D. A. Wehrung, *Taking Risks.* New York, US: The Free Press, 1986,

[24] R. J. Hutton, "Types of "uncertainty about" and strategies for uncertainty management: An integrative approach," Klein Associates Inc., Fairborn, OH, Tech. Rep. #04TA2-SP1-RT2, 2004.

[25] Swedish Armed Forces, *Taktikreglemente För Flottan (Tactical Regulations for the Navy).* Stockholm: Chefen för Marinen (Head of Navy), 1987,

[26] R. Selten, "What is bounded rationality?" in *Bounded Rationality: The Adaptive Toolbox* G. Gigerenzer and R. Selten, Eds. US: First MIT Press, 2002, pp. 13-36.