The Paradoxes of Military Risk Assessment:

Will the Enterprise Risk Assessment Model, Composite Risk Management and Associated Techniques Provide the Predicted Benefits?

Chris. W. Johnson,

Glasgow Accident Analysis Group,
Department of Computing Science, University of Glasgow, Scotland, UK.

Email: Johnson@dcs.gla.ac.uk; http://www.dcs.gla.ac.uk/~johnson

Keywords: Safety; Composite Risk Management, ERAM, Risk Assessment; Military Systems Engineering.

Abstract

Risk management provides the most important single framework for strategic, tactical and operational decision making across the US Military. Composite Risk Management (CRM) has been introduced to guide decision making across the US Army in training, combat and peacekeeping operations as well as off-duty activities. The Department of Defence's Enterprise Risk Assessment Model (ERAM) provides a framework for acquisition and procurement policy. Rather than considering the hazards associated with particular operations, planners evaluate project risks in terms of the likelihood and consequences of failing to meet service requirements on time and to cost. The annual statement of the Chairman of the Joint Chiefs of Staff to Congress now also uses notions of likelihood and consequence to assess the nation's military preparedness. However, risk management is not a panacea for the problems that affect military operations. It is unclear whether the Department of Defense can achieve the culture shift that is necessary before risk analysis might 'revolutionize' their business strategy. At a tactical level, there is also a danger that enemy forces could learn to exploit systematic biases in decisions that are informed by particular risk assessment techniques. At an operational level, it is unclear whether leaders in the field can accurately collate and then communicate the products of a hazard analysis on the battlefield. The following pages, therefore, identify some of the paradoxes that complicate the application of risk management to guide military decision making.

Introduction

Risk assessments influence strategic and tactical military planning. At the highest level, the language of hazards, of consequences and likelihood has begun to dominate the allocation of both technical and managerial resources. US military policy is strongly influenced by the risk assessments that the Chairman of the Joint Chiefs of Staff present to Congress each year. In 2007, General Peter Pace reported that the strains imposed on the US military forces had increased the risks it faces in defending the nation from 'moderate' to 'significant' as a result of the ongoing wars in Iraq and Afghanistan. The important of these high-level risk assessments does not stem from any underlying quantitative calculation but from their impact on public opinion and on political decision making. Following Pace's upgrade in the level of military risk, Defense Secretary Robert Gates was required to provide Congress with a mitigation assessment explaining how the Pentagon would respond to potential contingencies in the light of the CJCS statement. Recent Senate debates over the Emergency Supplemental Spending Bill reveal an important paradox in the presentation and response to these statements. **Paradox 1: The link between perceived levels of risk and increased expenditure has left the military vulnerable to claims that threats have been over estimated.** It is important to stress that the aim of this paper is not to make a series of political points or to criticize the underlying techniques of risk assessment. Instead, the intention is to identify some of the paradoxes that complicate the application of risk management to guide military strategic, tactical and operational decision making.

From Political Risk Mitigation to Military Enterprise Risk Management

The General Accounting Office have argued that the Department of Defense (DoD) must exploit risk-based approaches to strategic investment given increasing financial pressures in an uncertain security environment [1]. The DoD's Business Transformation Agency has responded by developing the Enterprise Risk Assessment Model

(ERAM) to identify and mitigate risks during acquisitions [2]. A 'risk assessment team' spends two weeks reviewing existing project documentation. This analysis then informs a series of more focused interviews with program stakeholders that last from 2-3 days. A further two weeks are then spent reviewing material, formulating additional questions and devising a risk mitigation proposal. The program manager helps to review the initial findings before a final mitigation strategy is disseminated to program participants. ERAM outputs identify vulnerabilities, propose solutions, and provide an action plan to reduce program risks. The intention is to ensure that Department of Defense projects deliver *capabilities* rather than focusing on particular technologies. For example, several different approaches may be trialed in order to spreads the risks associated with the failure of any particular technological 'solution'. This creates a further paradox. **Paradox 2: In military acquisitions there is a tension between accepting sufficient risk to create innovative systems that exceed enemy capabilities and yet rejecting those projects that are so innovative that they are unlikely to yield operational benefits within a fixed timescale and to a specified budget.**

A number of caveats can be raised about the ERAM approach. A capability-based program that spreads development risk between alternate technologies can also lead to resource starvation and under-investment in key areas. It can increase the uncertainty for companies deciding whether or not to invest in innovative approaches. It also remains to be seen whether or not individual initiatives can have the 'root and branch' impact advocated by the GAO. One reason for this is that ERAM is being introduced in a piecemeal fashion. In April 2006, the Under-Secretary for Defense (Acquisition, Technology, and Logistics) approved a trial of ERAM focusing initially on the Defense Integrated Military Human Resources System, General Fund Enterprise Business System, and Integrated Data Environment/Global Transportation Network Convergence projects. These initiatives were chosen because they are typical of the business critical ICT applications that often pose particular problems for public agencies acquisition. The validation bodies, the Investment Review Boards and the Defense Business Systems Management Committee have still to publish their analysis of the risk-based approaches within ERAM. A number of further concerns center on the piecemeal introduction of such initiatives. For example, previous Department of Defense initiatives to introduce risk management into the security of ICT applications have failed to achieve 'critical mass': "…there is no specific Defense-wide policy requiring vulnerability assessments or criteria for prioritizing who should be targeted first. This has led to uneven application of this valuable risk assessment mechanism." [3] **Paradox 3: It is difficult to identify appropriate metrics for measuring the success of any risk-based approach to military planning and acquisitions, too stringent control might eliminate program novelty while too lax control may lead to program failure.**

ERAM is one part of a more general response to the principles encapsulated in Department of Defence Directive 5000.1 and Instruction 5000.2. These advocate the use of risk-based approaches across all procurement activities, including weapon systems and automated information systems. Instruction 5000.2 is intended to establish a management framework to translate 'mission needs and technology opportunities' into 'stable, affordable and well managed' acquisitions programs. Again, risk assessment is advocated as a key tool in achieving these objectives. The gradually development of 'evolutionary' prototypes or demonstrators will help end-users, testers and developers flush out any risks that were not identified during the inception stage. This was intended to satisfy address GAO concerns that pilot programs should be limited to low-cost, low-risk prototypes [4]. The evolutionary approach advocated in 5000.1 and 5000.2 helps to explain the piecemeal application of ERAM, described in previous paragraphs. It is unclear how the bureaucratic structures that support these initiatives will help with the higher-levels of strategic decision making that are required to address the paradoxes of military risk assessment, cited above.

Operational Risk Management

Risk assessment techniques also guide the planning and execution of tactical military operations. For example, US Army Field Manual 3-04.513 deals with battlefield recovery and evacuation of aircraft: "Risk management is a commonsense tool that leaders can use to make smart risk decisions in tactical and everyday operations. It is a method of getting the job done by identifying the areas that present the highest risk and taking action to eliminate, reduce, or control the risk. It is not complex, technical, or difficult" [5]. FM3-04.513 places responsibilities on all soldiers who must: understand, accept, and implement risk reduction guidance and the concept of risk management and assessment; maintain a constant awareness of the changing risks associated with the operation; make leaders

immediately aware of any unrealistic risk reduction procedure and report risks beyond their control or authority to their superiors for resolution.

Table 1 illustrates the risk assessment tools that have been proposed to support rotary wing operations. The box labeled '1. Supervision CMD/CONTROL' provides a means of assessing the risks associated with operations involving personnel from the same unit or from an attached unit. Particular hazards stem from devolved lines of command hence a higher risk value is associated with operations involving crews from attached units than those for which all staff are drawn from the same command. This section of the form also associates a higher level of command and control risk with operations after dark. A mission involving attached units at night would be assigned an initial risk value of 4. In contrast, a mission that was conducted by an integrated unit in daylight would only score a risk value of 1. A companion paper explains the high-levels of risk associated with nighttime operations [6]. For now it is sufficient to observe that the US Army has identified 'human-error accelerator profiles' from its accident data. An example of a high-risk mission profile would be an NOE ('nap of the earth') flight using night vision goggles with less than 23% and 30 degrees of illumination. The accelerator in this case would be lack of illumination and limited visual field making crew scanning errors more likely to occur. Hence, these factors may be given a high risk-value weighting within the matrix.

Table 1: Example of a suggested format for a rotary-wing risk assessment matrix (US Army TC 1-210 [7])

ROTARY-WING RISK ASSESSMENT MATRIX

1. SUPERVISION CMD/CONTROL (Risk Value/Mission)

VALUE	TACTICAL DAY/NIGHT	
Parent Unit	1	2
Attached	3	4

2. PLANNING GUIDANCE (Risk Value/Time)

	IN-DEPTH	ADEQUATE	MINIMAL
Vague	3	4	5
Implied	2	3	4
Specific	1	2	3

3. CREW SEL/PC (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

4. CREW SEL/PI (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

5. CREW SEL/ADD (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
50	2	3	4	5
>50	1	2	3	4

6. ALL CREW MEMBERS ARE CREW COORDINATION TRAINED

No	+2
Yes	0

7. ALL TASKS REQUIRED ON THIS MISSION ARE SUPPORTED BY THE UNIT MISSION ESSENTIAL TASK LIST (METL)

Yes	0
No	5#

#Requires bn cdr approval.

8. CREW ENDURANCE (Risk Value/Flt Hrs)

QUALITY OF REST	>8 HRS	6-8 HRS	<6 HRS
Field	2	6	10
Garrison	1	4	10

Add 2 for missions flown during the last half of the duty day.

9. COMPLEXITY TYPE OF MISSION (Value/Condition)

	VMC D	VMC N	NVG	IMC HOOD
Multiship	2	6	4	NA
Sling load	2	3	5	NA
Stabo/Rappel	1	2	4	NA
Terrain Flt	1	3	2	NA
Paradrop	2	2	NA	NA
Routine	1	2	2	3
NOE	2	8	4	NA
MTP	3	5	NA	NA
Maint Recovery	3	5	NA	NA

10. WEATHER** (Risk Value/Ceiling/Visibility)

	<1000/3	<700/2	<500/1	>1000/3
D	3	4	6	1
N	4	6	10	2
NVG	3	4	8	1

11. ADDITIONAL RISK FACTORS (D, N)

Single Pilot	+4

ADDITIONAL COMMENTS

* Area of operations.
** Visibility values are given in miles.

ROTARY-WING RISK ASSESSMENT MATRIX

12. NVG CREW SEL/PC (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

13. NVG CREW SEL/PI (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

14. NVG CREW SEL/ADD (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

15. PERCENT OF ILLUMINATION (NVG)

100-80	79-60	59-40	30-23	<23
1	2	3	4	5

16. MOON ANGLE (NVG)

90-70	69-50	49-30	<30
0	1	2	3

17. ADDITIONAL RISK FACTORS (NVG)

RISK VALUES: DAY/NIGHT MISSIONS

1. Supervision _____
2. Planning _____
3. Crew Selection/PC _____
4. Crew Selection/PI _____
5. Crew Selection/Add _____
6. Crew Coordination Trained _____
7. METL Task _____
8. Crew Endurance _____
9. Complexity _____
10. Weather _____
11. Additional Risk Factors _____

TOTAL _____

RISK VALUES: DAY/NIGHT MISSIONS

12. NVG Crew Selection/PC _____
13. NVG Crew Selection/PI _____
14. NVG Crew Selection/Add _____
15. Illumination _____
16. Moon Angle (NVG) _____
17. Additional Risk Factors _____

TOTAL NVG MISSIONS _____
TOTAL DAY/NIGHT MISSIONS _____

TOTAL RISK VALUE NVG _____

COMPUTATIONS DAY/NIGHT MISSIONS

Low Risk	<16
Medium Risk	16-28*
High Risk	>29**

COMPUTATIONS NVG MISSIONS

Low Risk	<25
Medium Risk	25-40*
High Risk	41-50**
Extremely High	>50***

* Medium-risk missions require approval of the company commander.
** High-risk missions require approval of the battalion commander.
*** Extremely high-risk missions require approval of the brigade commander.

ADDITIONAL COMMENTS

Complex missions can be broken down into a number of activities using Mission Essential Task Lists. By summing the risk values for the hazards associated with each mission component, it is possible to form a partial ordering of those tasks that contribute most to overall risk. It is these high-risk sub-tasks that become the focus for risk reduction and mitigation. This relatively simple approach provides considerable flexibility. For example, an otherwise low risk mission might have a significant increase in the overall risk value if, for instance, one of the crews had less than 25 hours in the area of operation. Leaders might then intervene by introducing highly experienced crews into the operation. The overall mission risk is obtained by summing the hazards for each stage of the mission. The total can then be assigned to a particular risk level. For example, Table 1 associates 'Low Risk' with risk values less than 16. Medium risk operations range between 16 and 28. High risk operations are associated with scores of 29 and above. In each case, commanders must seek additional levels of authorization before embarking on a mission. Company level approval must be provided for medium risk operations, while battalion commanders must support high risk plans. In this example, extremely high-risk operations associated with the use of night vision equipment must be approved at brigade level.

It is essential to validate the risk values that are embedded within risk matrices. There is a danger that risk assessments are unnecessarily conservative – in other words mission success might require an unnecessary level of resources in order to mitigate low levels of risk. These resources might have been better deployed on other operations. Alternatively, incorrect risk values might persuade commanders to accept hazards that threaten both mission success and the resources that are deployed to perform a particular operation. The US Army is, therefore, concerned to compare the risk values in tools, such as Table 1, with outcome data from accident investigations and from training exercises. The Army Safety Risk Management Information System and the Army Safety Management Information System-2 have both been used in this way. However, this raises further concerns. **Paradox 4: Military risk assessments are usually validated by reference to the hazards that were realized in previous missions, this makes them overly conservative given that few records are maintained of successful operations where hazards were avoided.**

Once leaders have identified critical tasks and hazards, such as crew inexperience, it is important to develop controls that reduce overall mission risks. FM3-04.513 argues that commanders should be presented with a series of options for risk control. Before presenting such a list, it is necessary for staff to consider any negative side-effects. For example, allocating experienced personnel to reduce the risks associated with a hazardous operation can increase the risks associated with other missions that might otherwise benefit from their participation. Similarly, deploying experienced personnel may reduce the opportunities to increase the skill set of other staff while increasing the levels of stress and fatigue on the crews who are allocated to the mission. US Army TC 1-210 urges commanders to think through the consequences of each potential risk control and then 'visualize what will happen once the option has been implemented'. **Paradox 5: Most risk assessment techniques focus on hazard identification and prioritization with relatively little support provided for the analysis and planning of risks associated with the implementation of particular controls.**

The implementation of risk controls can involve changes to operations orders (OPORDs), standing operating procedures (SOPs), and drills or rehearsals. As might be expected, considerable emphasis is placed on communicating information about the purpose of controls, 'from the commander down to the individual soldier' so that any attempts to mitigate a risk is not inadvertently undermined. Similarly, commanders must take steps to supervise the application of risk controls. As with previous stages in the risk management processes advocated by the US Army, the superficial simplicity of the approach hides numerous detailed problems. For example, too close a monitoring may alienate staff, if they feel that their actions are under close supervision. Time may be wasted in providing evidence of controls to the point where supervision begins to undermine core mission objectives. **Paradox 6: The success of any mitigation may only be measured by monitoring that creates additional risks, especially when delays can undermine mission objectives.**

Further concerns affect the risk management techniques embodied in FM3-04.513 and TC 1-210. There are few guarantees that different personnel will identify similar hazards for the same mission elements. The instantiated forms in Table 1 take little account of risk exposure either in terms of the length of mission elements or the number of personnel involved. Finally, the existing provision does not easily enable leaders to offset the risk exposure against mission benefits – where for instance, the costs to an opposing force may be so great as to justify limited exposure of friendly forces to elevated levels of risk. In other words, this straightforward approach ignores the complexity of many military operations. **Paradox 7: Operational risk assessments must be simple enough that they can be conducted by personnel in the field yet military operations are often exposed to dynamic factors, including enemy actions, which cannot easily be captured using conventional risk assessment techniques.**

Training Related Risks

In order to prepare staff to make tactical decisions and execute complex plans under a wide range of environmental pressure, military organizations rely upon training and simulation tasks that carry their own degree of risk: "Tough, realistic training conducted to standard is the cornerstone of Army war-fighting skills. An intense training environment stresses both soldiers and equipment, creating a high potential for accidents. The potential for an accident increases as training realism increases, just as it does in combat. The end result is the same; the soldier or asset is lost"[5]. In other words, there is a need to simulate risk. This creates tensions because it can be difficult to justify the use of hazardous training exercises that result in military fatalities each year, for example from heat stress, accidental discharge of weapons, or from military vehicles turning over during night exercises. **Paradox 8:**

Operational effectiveness is perceived to depend upon the simulation of risk in training exercises that often result in accidents, this involves techniques that would not be acceptable in other safety-critical industries and which are often rejected as unethical by the general public.

TC 1-210 emphasizes the need to minimize the differences between simulated and operational challenges during US Army training programs [7]. These differences can, however, be due to safety constraints. For example, the hazards of exposing troops to Multiple Launch Rocket System fire during training exercises can outweigh eventual mission benefits. Differences between training and operations may also be due to other practical constraints. For example there was insufficient time for all of the troops that were issued with Night Vision Devices during Desert Shield to train with those devices before deployment [6]. Each safety or functional constraint that creates differences between training and operations should be challenged. If possible, they should be removed to increase the veracity of the training program; 'With proper controls in place, these restrictions can be reduced or eliminated' [7]. If the constraints cannot be removed then they should be subject to risk assessment.

It is extremely difficult to ensure that risk assessments address the hazards that arise during training exercises. For example, heat stress continues to affect many soldiers as armed forces recreate operational demands. 13 US Army personnel died from heat related injuries during 2005; there were more than 500 cases of heat stroke and 2,200 of heat exhaustion. Commanders can, and have been, relieved of duty within the US Army when soldiers suffer from avoidable heat-related injuries. Even so, it can be difficult for individuals to raise concerns when they believe that undue risks are being taken during training exercises. **Paradox 9: Military training often fosters a form of mutual support and a focus on mission success that often dissuades individuals who are best place to recognize the risks of training activities from raising their concerns.**

A number of accidents involving improvised explosive devices (IEDs) also illustrate the difficulty of using risk management to maintain safety while at the same time reducing the differences between operational and training exercises. IEDs are one of the biggest threats currently facing many armed forces around the globe. In an effort to prepare personnel, US Army units have constructed 'makeshift' devices in pre-deployment training. In particular, several variants have been developed using ad hoc extensions to the M21 (Hoffman) Artillery Flash Simulator. This device is responsible for more explosives accidents and personnel injuries than any other simulator. These improvised IEDs often include flour mixtures with military grade munitions that can have extremely unpredictable results. The US Army Combat Readiness Center [8] observes that 'although their intentions are good, the risks associated with using homemade IEDs might be worse than the potential training benefits'. These devices contravene both Federal laws and Army regulations (eg AR385-63, Range Safety, paragraph 2-2).

Composite Risk Management

The attacks of 2001 revealed that existing army doctrine, including FM3-04.513 and TC 1-201, did not adequately consider the terrorist threat to military personnel both on and off duty. It was argued that these documents created arbitrary distinctions between the methods used to identify hazards in tactical and non-tactical operations. Such concerns led to the introduction of Army Field Manual 5-19 [9]. A primary motivation behind this document was to coordinate the military response to a changing operational context. FM5-19 advocates a 'holistic approach'. It rejects the traditional military distinctions between accidental and tactical hazards embodied in the divide between training and operations. This integrated policy led to the new term 'Composite Risk Management' (CRM). The motivation stemmed, in part, from initiatives at a strategic level to introduce risk assessment as a key tool to inform decision making throughout the military. It also stemmed from dissatisfaction with previous methods reflected in the change of name from the US Army's Safety Center to the new US Army Combat Readiness Center. This field operating agency located at Ft. Rucker, Alabama is the main agency for promoting operational risk management throughout the US Army. Senior staff leading this transformation summarized the need for change to CRM: "…the Army was still operating under a 1970's paradigm for safety, relying on lagging indicators, consequence management, and a compliance orientation… Mishaps behind the wheel accounted for nearly ¾ of the deaths in the past 2 years, the same proportion as reflected in the Army Safety Center's 1984 review… Thus, the (new) offensive on loss prevention has elements for the close fight and the deep fight. The plans consider the main effort (CRM in Army operations) and the flanks (CRM in off duty activities)" [10]. As might be expected, the move from a separation of concerns between accidental and tactical risks towards a holistic Composite Risk Management approach required a significant cultural change.

Under FM5-19 a hazard is interpreted to be any "condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation". They include "a situation or event that can result in degradation of capabilities or mission failure" [9]. However, the holistic nature of Composite Risk Management introduces important differences that reflect the US military concern to look after personnel on and off-duty. Hazards are defined to exist in all environments, including but not limited to "combat operations, stability operations, base support operations, training, garrison activities, and off-duty activities". The revised field manual also advocated the METT-TC mnemonic (Mission, Enemy, Terrain and weather, Troops and support available, Time available, and Civil considerations). METT-TC can be used to identify hazards irrespective of whether units are on or off-duty. It can, therefore, be argued that the new Field Manual has been specifically developed to address two further paradoxes of military risk assessment. **Paradox 10: Risk assessment has been most widely applied to operational decisions in civilian industries, yet off-duty accidents and Privately Owned Vehicles continue to rank amongst the highest causes of military losses.** In addition, here has been a realization that risk assessments must be used to address hazards created by new forces threatening military personnel. **Paradox 11: Those operational risk assessments that have been developed within military organizations tend to focus on conventional enemies and do not consider the risks associated with terrorist attacks on off-duty personnel.** FM5-19 extended the scope of previous guidance by arguing that all Army personnel should be trained in the principles of risk management. In consequence, Composite Risk Management doctrine has been institutionalized in the Risk Management Chain Teaching program created by the Chief of Staff of the Army [11].

The CRM doctrine emphasizes that commanders must identify those enemy capabilities that pose hazards to an operation or mission. Key to this hazard analysis of enemy capacity is the Intelligence Preparation of the Battlefield (IPB). The IPB is intended to support 'threat based risk assessments by identifying opportunities and any constraints the battlefield environment offers to both enemy and friendly forces' and hence must explicitly capture 'enemy capabilities and vulnerabilities' [9]. However, FM5-19 also recognizes the temporal constraints that create considerable pressures for the field commanders who must make key tactical decisions. The more considered quantitative approaches to likelihood and consequence assessment are ill suited to the rapidly changing context that many commanders must address: "In these situations, they perform hasty risk assessments. A hasty risk assessment may be performed mentally. It may be transmitted verbally or in writing via a FRAGO (Fragmentary Order)…Only the essential information necessary to complement the FRAGO and forward the risk guidance received from the battalion commander are included. As in the example, an overlay may be included with the risk assessment to clearly portray the location of hazards. The hasty risk assessment (can be) a separate document. However, it may be included within the FRAGO issued by the company to the platoon" [9]. The time limited nature of these situations and the critical nature of their decisions makes it essential that FRAGOs are successfully communicated to their intended recipients. FM5-19, therefore, provides detailed guidance on how hazard assessments can be passed in annotated form within these orders. The integration of 'ad hoc' risk assessments in fragmentary orders again illustrates the holistic approach advocated in the new Field Manual. Even where time is strictly limited, commanders should explicitly take the opportunity to consider potential hazards as part of the Military Decision Making Process.

It is too soon to judge whether CRM will provide the anticipated benefits. Some caution is necessary because there is only limited evidence to suggest that training personnel in the principles of risk management will have any longitudinal impact on accident rates [12]. There is a concern that attribution bias will impair the critical and unbiased assessment of risk assessment initiatives across the US military. Attribution bias refers to inferences that are made by observers often with the benefit of information or resources that were not available to the individuals involved in an incident. This can be illustrated by a recent accident report that describes how two M1A2 Abrams tanks were assigned to escort an explosive ordnance disposal (EOD) team to an enemy weapons cache site. Neither the tank crews nor the EOD team was familiar with the location of the weapons cache. Maps and imagery provided insufficient detail to plan the mission. A process of trial and error led them the cache and the EOD team completed their task after dark, around 18:45. The leaders decided to return using the route over a sandy, clay road that ran alongside a canal. The trail tank crossed a bridge over the canal and turned right over a berm. It's rear began to shake violently and the track commander (TC) told the driver to go left as the right edge of the road collapsed under the tank's weight. The crew heard the TC announce "rollover, rollover, rollover" as the tank overturned into the water-filled canal. The TC's death was attributed to blunt-force trauma suffered during the rollover and a lack of oxygen after the tank settled in the water. The subsequent investigation identified two primary causes: a failure to

adequately plan the mission and a failure to execute proper rollover procedures because the TC did not immediately drop inside the turret. Attribution bias can be seen in the commentary that accompanies the account of this accident: "Had the tank crews used CRM when they were trying to identify alternate routes, they might've realized the hazards they faced on the unimproved roads they ultimately selected. This instance wasn't the first time a canal road collapsed under a tactical vehicle in theater; similar roads have caved in under vehicles weighing far less than an M1 tank, including HMMWVs. The bottom line is every Soldier must take into account all the hazards, both tactical and accidental, that can hurt or kill them or their buddies. We need each one of you, so use CRM to stay ready and Own the Edge!" [13]. The key term here is 'might' – without significant additional operational experience in the application of CRM, considerable questions must remain as to whether the ad hoc risk assessments recommended in FM5-19 could really have helped the leaders and their crews to identify the hazards at the end of a long day, filled with other earlier missions as they made their way back to base through a potentially hostile environment. **Paradox 12: The enthusiasm for techniques, such as CRM, in some sections of the military may create a hostility and cynicism amongst those personnel who are faced with the application of simple risk assessment techniques under complex, time limited constraints with incomplete information.**

Discussion and Conclusions

Does the dominance of risk assessment create any concerns? The paradoxes identified in this paper capture problems that complicate the application of these techniques to inform strategic, tactical and operational decision making in military organizations. Many approaches, including the Enterprise Risk Assessment Model and Composite Risk Management, are relatively novel. Their impact on operational effectiveness has yet to be studied; many units are still being trained in the doctrines embodied in FM5-19. Significant questions remain to be answered. For example, it is unclear whether there will be systematic biases in the risk assessments conducted by units with different operational backgrounds, including both full time and National Guard units.

Experience at other levels within the military has shown the difficulty of using risk assessment techniques to reliably inform decision making. For example, the US General Accounting Office surveyed risk assessment practices and argued that: "DOD faces four challenges that have affected the implementation of the framework. First, DOD's organizational culture resists department-level approaches to priority setting and investment decisions. Second, sustained leadership, adequate transparency, and appropriate accountability are lacking. Further, no one individual or office has been assigned overall responsibility or sufficient authority for the framework's implementation. DOD also has not developed implementation goals or timelines with which to establish accountability, or measure progress. Finally, integrating the risk management framework with decision support processes and related reform initiatives into a coherent, unified management approach for the department is a challenge that DOD plans to address during the 2005 QDR" [15].

There are further concerns. In particular, there is a miss-match between the simplified forms of risk assessment that are being taught at most levels of the US Army command structure and the complexity of the decisions that they are being called to make. The concept of exposure is often poorly dealt with. Although this might seem to be an abstract concern, it has critical practical consequences. For example, consider a leader who must decide between two plans in which a unit either has to cross a river using a bridge or must make a significant detour to cross at a fording point. In the former case, there may be a relatively short exposure to an extremely high risk while in the latter case there would be prolonged exposure to a lower level of risk. Simply decomposing mission plans into a Mission Essential Task List will not help much to balance the relative risks here. Research in prospect theory has developed a series of techniques to help decision makers evaluate different outcomes with relative risks in the form described above. However, it remains to be seen whether these approaches could be translated into the Army doctrine in field manuals. Until more sophisticated methods are developed, leaders continue to face considerable problems in mapping between the simple techniques that they have been trained to use and the complex, dynamic decisions that they must make every day.

Previous sections have described how lightweight risk assessments are to be integrated into FRAGOs (Fragmentary Orders) when leaders must make complex decisions against hard deadlines. The Composite Risk Management proposals are also intended to ensure that these assessments are communicated to the units involved in particular mission components. The precise format for both the FRAGOs and the communication of risk based decisions must be tailored to the particular situations facing individual units. Only time will tell if this emphasis results in the

development of appropriate tools and techniques that can be used in the field. One concern is that many military staff are pre-selected and then trained for decision-making characteristics that are very different from those in the civilian population. There seems to be very little direct evidence today that CRM techniques will be able to compensate for the risk preference biases that are often seen in military personnel. This concern can be illustrated by a recent edition of the US Army's Countermeasure where the author describes the risk seeking nature of many soldiers and then raises an, as yet, unsubstantiated hope that Composite Risk Management will address some of the consequences in military activities: "Have you ever deliberately put yourself in a situation you didn't think you'd get out of alive, only to survive and vow never to do the same thing again? … Playing football on a semi-thawed lake, passing traffic uphill in a no-passing zone, driving drunk and boating in a lightning storm—none of these are sound decisions, but I've done them all. When you're young, it's hard to distinguish risk from what we perceive as adventure… We can step back and make smart decisions, which is the beauty of Composite Risk Management. Even in combat, Soldiers of all ranks have the authority to stop unsafe acts and implement controls to ensure everyone makes it home from the fight. Please take advantage of this great tool and apply it to everything you do, especially if you see some idiot pulling charges out of a powder pit!" [16]. Such assertions arguably underestimate the problems of 'groupthink' and 'risky shift' that are well known to affect team-based decision making in combat operations [12]. The term 'group think' refers to the way in which co-workers will reinforce mutual beliefs and discount lateral thinking if it contradicts accepted norms within the group. 'Risky shift' refers to a process by which team members will gradually adopt the position of more risk seeking individuals even if they would normally reject those positions if they were not in that team. More work is urgently required to determine whether the implementation of CRM across diverse units will have the envisaged benefits.

One of the most vibrant areas of research within risk management and decision theory has focused on the development of models that explain opponents' behavior in various forms of games. These models assume that competitors make complex decisions with uncertain outcomes in order to maximize their returns while minimizing the rewards for competitors. Considerable benefits are to be gained if one player understands the decision making processes employed by their opponent. These theoretical outcomes have direct applications in the military domain. For example, TC 1-210 and FM5-19 stress that all 'unnecessary risks must be avoided'. This enables opponents to make direct inferences about the risk adverse behavior of the US military. These insights are, arguably, being applied by the insurgents' use of IEDs and snipers in Baghdad. In this case, the opponents are reacting on the basis of direct observations of risk-based decision making in the field. In the future, however, opposing forced could make strategic decisions based directly on the risk averse statements in public documents such as FM5-19. **Paradox 13: If risk assessment techniques, such as Composite Risk Management, offer the benefits that are claimed in terms of encouraging consistent decision making across the US military then they will provide opposing forces with a 'blue print' for US military operational decision making.**

References

1. US General Accounting Office (GAO), High-Risk Series: An Update, Technical Report GAO-05-207, Washington DC, USA, 2005.

2. US Department of Defense, FAQ: Enterprise Risk Assessment Methodology (ERAM), Technical report, Defense Business Transformation Unit, Washington DC, USA, April 2007. http://www.dod.mil/dbt/faq_eram.html

3. US Government Accountability Office (GAO), Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, Technical Report GAO/AIMD-96-84, Washington DC, USA, 2006.

4. US Government Accountability Office (GAO), Business Systems Modernization: DoD Continues to Improve Institutional Approach, but Further Steps Needed, Technical Report Washington DC, USA, 2006.

5. US Department of the Army, FM 3-04.513: Battlefield Recovery and Evacuation of Aircraft, Headquarters, Washington, DC, 27 September 2000. http://www.army.mil/usapa/doctrine/Active_FM.html

6. C.W. Johnson, The Role of Night Vision Equipment in Military Incidents and Accidents. In C.W. Johnson and P. Palanque (eds.) Human Error, Safety and Systems Development, Kluwer Academic Press, Boston, USA, 1-16, 2004.

7. US Department of the Army, TC 1-210: Aircrew Training Program Commander's Guide to Individual And Crew Standardization, Headquarters, Department Of The Army, Washington, DC, 3 October 1995.

8. US Army Combat Readiness Center 2006. Simulated IEDs: Real Problems, Countermeasure, 27:06/06: 10-11, 2006.

9. US Department of the Army, FM 5-19: Composite Risk Management, Headquarters, Washington, DC, August 2006.

10. J.A. Smith and B.R. Yaeger, Tansforming Army Safety: Enhance Combat Readiness through Composite Risk Management, Technical Report, US Army Combat Readiness Center, 2007.

11. US Army Combat Readiness Center 2007, Composite Risk Management Chain Teaching Training Packet. US Army Combat Readiness Center, April 2007.

12. C.W. Johnson, A Handbook of Accident and Incident Reporting, University of Glasgow Press, Glasgow, Scotland, 2003. http://www.dcs.gla.ac.uk/~johnson/book

13. US Army Combat Readiness Center 2006. Loss Investigation: A Map but No Direction, Countemeasure, 27:09/06: 14-15, 2006.

14. US Government Accountability Office (GAO), Chemical and Biological Defense: Improved Risk Assessment and Inventory Management Are Needed, Technical Report GAO-01-667, Washington DC, USA, 2001.

15. US Government Accountability Office (GAO), Additional Actions Needed to Enhance DOD's Risk-Based Approach for Making Resource Decisions, Technical Report GAO-06-13, Washington DC, USA, 2006.

16. R. Andree, Personnel Injury: Great Flying Stoves! US Army Countermeasure, Centre for Combat Readiness, Volume 27:10/06:10-11, October 2006.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail. He has led a number of studies into military incidents and accidents, most recently this involved a study of mishaps involving night vision equipment.