Proceedings of the 2007 IEEE Symposium on Computational
Intelligence in Security and Defense Applications (CISDA 2007)

A Temporal Risk Assessment Framework for Planning A Future Force Structure

Michael Barlow, Ang Yang, and Hussein A. Abbass
Defence and Security Applications Research Centre,
UNSW at Australian Defence Force Academy,
Canberra, 2600, Australia.
{m.barlow,a.yang,h.abbass}@adfa.edu.au

Abstract— **Planning future force structures is usually associated with a high, but difficult to quantify, risk factor. Among many other reasons for the importance of this planning process, the defence industry requires the military establishment to communicate their decisions on the capabilities needed in the future. This communication enables the industry to shape their R&D programs and tailor their production plans. Overall, the decision maker needs to anticipate the state(s) of the environment across a relatively long time frame. The process of anticipation is surrounded with many risk factors. Moreover, transforming a force structure is not a single-step process. Intermediate force structures need also to take into account threats in the medium future.**

This paper presents a temporal risk assessment methodology for planning future force structure. The methodology relies on constructing a topological structure of intermediate force structures with transitions based on the proximity of these structures to each other and budget constraints. The path with minimal maximum risk is then identified using a dynamic programming min-max path finder algorithm. The methodology is demonstrated with two simple examples.

I. Introduction

The question of the most suitable future force structure for a defence organisation to pursue is a difficult one. Plagued with difficulties such as uncertainties about future operations the organisation may be asked to undertake; changes in technology and the nature of warfare; constrained budgets and timeframes; and a shifting international political, economic and military environment; decision-makers not only face an extremely difficult challenge, they currently have few tools to help them in the process.

What few tools exist for the analysis of capability development choices are predominantly qualitative in nature. Most of these tools rely on traditional decision analysis and planning methodologies such as the field anomaly relaxation (FAR) technique which is often used for strategic planning by the Defence Science and Technology Organisation (DSTO) in Australia. Those that are quantitative are primarily simulation based - with the approach known as Agent Based Simulations (ABDs) showing considerable promise due to the lightweight, abstracted, and versatile nature [1], [6], [3], [12], [8], [11], [13] of the ABD approach. Typically ABDs are used to simultaneously explore a number of possible force improvements (e.g., sensor range, communication infrastructure, firepower, "hardening", mass, etc.), selecting the best force composition (mixture of capabilities) from that search space [9], [10], [13]. Due to the potentially enormous size of the parameter space, innovations such as employing evolutionary computation techniques to search for the best solution have recently been introduced [10], [8], [14]. However, to date, no substantive approach has considered the temporal dimension of force transformation - that is that there is no such thing as an ideal final force structure, but rather a slowly metamorphing structure governed by a process of step-wise changes in force composition from some starting state in a response to the risks (that is challenges and potential deleterious outcomes) that the organisation faces.

In the literature, there is no unifying definition of the term 'risk' (see the differences in [4], [7]). Ortwin Renn [7] states "All risk concepts have one element in common, however: the distinction between reality and possibility". This statement of Ortwin forms the basis for this paper: how can we generate and search efficiently the space of possibilities? Once the space of possibilities is explored efficiently, probabilities can be estimated and risk can be quantified. Risk assessment identifies points of vulnerability, the likelihood of a potential problem, the possible frequency of the risk, and the extent of the potential damage.

In the defence and security context, these possibilities translate into threats. Decision analysts are usually faced with a large number of potential threats and ultimately try to make decisions in such a way that vulnerabilities are mitigated before the implementation and execution of these decisions. Vulnerabilities are holes in a security system, tactic, operation or plan. Red teaming [5] is a connotation for playing the devil; trying to penetrate the mind of the enemy or competitor to imitate their behaviors; understanding risk in the eyes of the opponent and mitigating vulnerabilities before it is too late. Recently, defence organizations [5] have identified red teaming as a valuable activity to mitigate risk and challenge plans and tactics. Red teaming is a risk assessment activity which answers questions such as: what are the type of risks that may arise in an operation and what are their natures? How do these risks come to existence in the first instance? Who can create them so that we are able to understand and avoid them? How can we defend ourselves against these risks? What are

their consequences? etc.

In this paper we introduce a new quantifiable methodology for risk assessment through time, of direct applicability to future force structure planning, as well as many other domains. The methodology quantifies the risk to a force, starting at the force's current state and moving forward through time, considering and quantifying the risk as various capability development options are considered. The methodology delivers not only a quantification of risk through time, but a path of capability development that minimises risk to the organisation, while still being constrained by temporal, budgetary and any other considerations.

The structure of the paper is as follows. The next section provides a brief background to WISDOM-II, the ABD simulation tool employed to quantify the risk to a particular force structure. This is followed by a description of the methodology - both of the temporal risk assessment framework, and how it is applied to several examples of force development. This is followed by the results section in which the quantifications achieved with the new framework - risk assessment and path of best development (minimal maximum risk) through time are illustrated. The paper concludes with a discussion of the implications and potential of the new methodology, together with indications of the authors' future directions of research.

II. WISDOM-II: THE LAND COMBAT SIMULATION SYSTEM

WISDOM [9], a 3rd generation ABD, was first proposed in 2004 and re-developed based on the Network Centric Multi-Agent Architecture (NCMAA) [12] in 2005. Version II of WISDOM (WISDOM II) has been used in many experiments for capability planning.

Generally speaking, there are five components in WISDOM-II. The first three components form the core simulation engine, and are used to model the internal behaviors of warfare. The last two components are analysis tools.

1) the C3 component – including both command and control (C2), and communication.
2) the sensor component – retrieving information from the environment
3) the engagement component – including firing and movement activities
4) the visualization component – presenting various information with graphs
5) the reasoning component – interpreting the results in natural language during the simulation process

Five types of networks (relationships between agents) are defined in WISDOM–II (Figure 1) which is the basis of the reasoning engine in WISDOM-II and makes up the top layer of the NCMAA. These 5 concept networks are:

- **The C2 network** This network defines the command and control hierarchy within one force. Figure 2 depicts the C2 hierarchy in WISDOM-II. Since commands can only be sent from the agents at the higher level to the agents at the lower level, the C2 network is a directed graph.

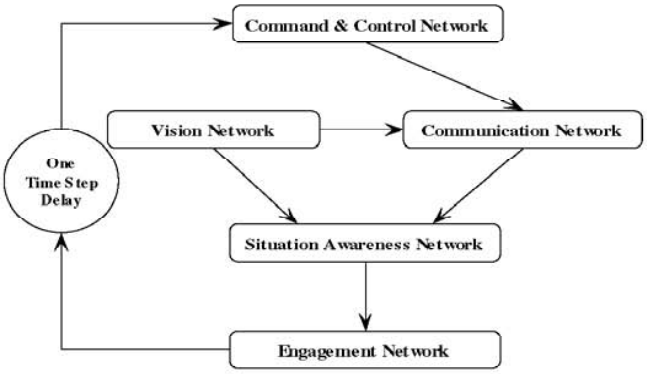

Fig. 1. The causal network in WISDOM-II

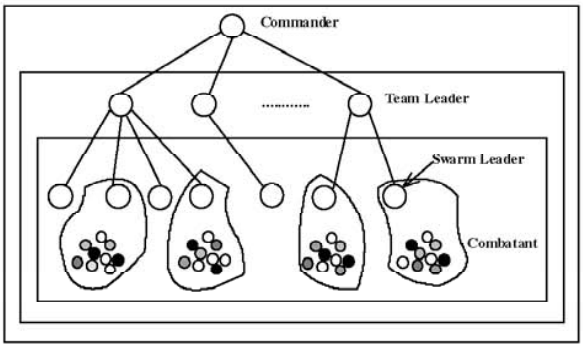

Fig. 2. Command and Control Hierarchy in WISDOM-II

- **The vision network** If agent A can see agent B, then there is a link from Agent A to Agent B. The vision network is also a directed graph.
- **The communication network** These communication networks are capable of carrying two types of information: situation information and commands. Since the network is employed to model communication, it is easy for WISDOM II to support various types of communication: Point to Point directly (P2Pdirect), Point to Point indirectly (P2Pindirect) and Broadcast (BC). Because the information flows from source to sink, the communication network is obviously a directed graph.
- **The situation awareness network** This network defines current knowledge about the friends and enemies (of an agent) through vision and communication. The information collected by vision and communication is fused and then this network is developed. Since both vision and communication are direction dependent, the situation awareness network is a directed graph also.
- **The engagement network** This network defines the agents being fired at based on the firing agent's current knowledge about its enemies and friends. This network is also a directed graph. Agents may be destroyed as the result of being engaged, therefore the engagement network can cause changes in the C2 network in the next

time step.

Four types of agents are supported in WISDOM-II: combatant agents, swarm leaders, team leaders and commanders. Both team leaders and commanders are virtual agents which exist in the force headquarters. They only have one capability: communication. Basically each combatant agent and swarm leader has five characteristic groups: health, vision, communication, movement and engagement.

Each combatant agent has its own sensor which is defined by the sensor range and detection rating. The detection rating defines what kind of agents can be detected by using this sensor. If the detection rating of agent A is equal to or larger than the concealment rating of agent B and Agent B is within Agent A's sensor range, then agent A may detect agent B.

Combatant agents can communicate with other agents linked directly to them through the communication network. This communication occurs through a communication channel, which is modeled by the noise level, reliability, latency and communication range. The agent may only communicate with agents within the range of that communication channel. A probabilistic model is adopted to implement the noise level and reliability of a communication channel. Each communication channel has two probabilities corresponding to the noise level and reliability. At each time step the message can only be transferred from one agent to another agent. The message will permanently be lost if it is older than a number of time steps predefined by the user.

The movement of an agent is determined by its speed, situation awareness and personality vector. WISDOM-II supports four kinds of speeds: still, low speed, medium speed and high speed. Agents with high speed can move one cell per time step. The low speed is one third of the high speed while the medium speed is half of the high speed. The movement algorithm is based on a tactical decision making and strategic decision making mechanism. The strategic decision making mechanism provides guidance to each group at the macro level, while the tactical decision making mechanism is based on the agent's personality attributes, and determines which location the agent should move to. An agent's personality in WISDOM-II is defined by sets of two values: a magnitude and a direction vector representing the attraction-repulsion direction and weight for each agent for each factor (e.g., towards or away from friendlies or enemies). In each time step, the agent can only move to its neighbour cells based on the overall influence of all perceived agents (the resolution of all vector forces "acting on" the agent).

Engagement in WISDOM-II is determined by what kind of weapon the agent uses. The weapon is defined by the following attributes: weapon power, fire range and damage radius. Based on the damage radius, two types of weapons are supported in WISDOM: a point weapon, the damage radius of which is zero, and explosive weapon, the damage radius of which is larger than zero. WISDOM-II also supports direct and indirect fire. The projectile from an indirect fire weapon can fly over obstacles.

The status of each combatant agent and swarm leader is defined by their health level and position. There are four actions available to each combatant and swarm leader.

1) scanning the environment, which may change the status of vision, communication and situation awareness networks;
2) communicating, which may change the status of the communication and situation awareness networks;
3) movement, which may change the status of the vision network, the communication network, the situation awareness network, and the position status of agents;
4) firing, which may change the status of the engagement network, the C2 network, and the health status of agents.

WISDOM–II collects information for each entity as well as for the interaction between entities. By this mechanism a large volume of data is available for subsequent analysis, as well as the simulation's own reasoning. Thus this data forms the input to WISDOM's real-time reasoning engine, with inferences output in natural language for the user's convenience. WISDOM–II also provides capabilities such as interactive simulation. For more details of WISDOM-II, please refer to Yang *et al.*[12].

III. METHODOLOGY

This section both introduces the temporal risk assessment methodology as a general framework, as well as describing the experimental setup for two capability development cases used to elucidate the features of said framework.

A. Temporal Risk Assessment Framework

The temporal risk assessment framework proposed here comprises three major components. First, a central simulation system, employed to quantify the risk facing a particular force structure in one or a set of scenarios. Secondly, a set of constraints which govern the possible transformations of the force from some beginning composition to other possible compositions. Thirdly, the composition of a graph structure in which each vertex represents a possible force structure, and each edge represents a possible transition (transformation) from one force structure to another under the given time and other resource constraints.

The process for risk assessment is as follows. A simulation system - for the purposes of this paper the WISDOM-II ABD, but within the framework any appropriate simulation or indeed quantification tool may be used - is selected and a set of scenarios constructed representing possible current and future tasks and challenges. A current (starting) force composition is then modelled within the simulation. Next, the temporal and resource (e.g., budget) constraints governing force transformation that will apply across the period of analysis are discretised into a fixed number of changes per time period. For instance, risk analysis may be required for a period of fifteen years, which has been divided into 30 intervals of six months each. Within each interval there may be four possible, mutually exclusive, changes that can be made. These might be replacing communication equipment for 10% of the force, better arming 15% of the force, providing better sensors for

10% of the force, or improving the mobility of 5% of the force.

Once all possible discrete transformations are known, all potential future force structures - across the period of the analysis - are then enumerated. This can be constructed as a graph, where each graph vertex represents a potential future force structure - reachable from the starting structure - and each (directed) edge indicates that the connected target vertex (force structure) can be derived from the originating vertex (force structure) in one discrete time-step (Figure 3).

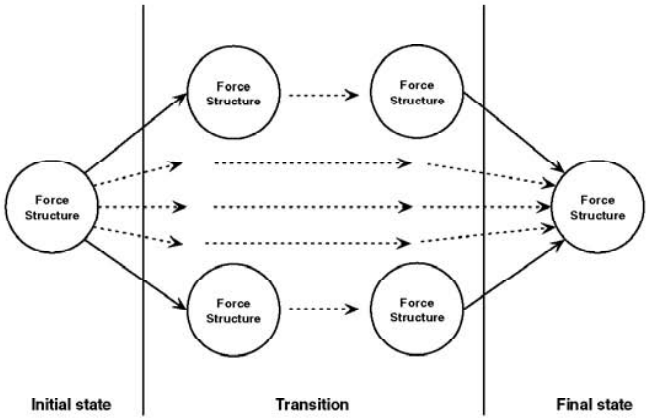

Fig. 3. Force transformation discretised as a number of steps and mapped into a directed graph structure.

The risk to each of these individual, potential future force structures (the vertices in the graph) is then quantified through the simulation engine. Dependent on the simulation engine, particular force and scenarios envisaged, risk may be quantified as losses suffered by the force, economic impact of the outcome, or changes in public opinion or international standing as a result of the outcome.

The final step in the process is then a traversal of the graph (shortest-path, min-max or other algorithms dependent on independency assumptions) in which risk is sought to be minimised. In this paper, the path with minimax risk [2] is defined as the path of minimal risk. Each edge on the path represents a step forward in time and the corresponding transformation in the force. The path itself encodes both the risk through time, and the best possible force transformational strategy to mitigate risk to the organisation and its mission. Numerous analyses based on the graph structure are also possible.

To illustrate the framework, two examples motivated by previous studies will be employed. In the first study [11], to be known as Systematic, a force's mass (size), weapon range, and communicator reliability were systematically varied to find the most suitable force operating in a network-centric mode. The temporal risk assessment framework was then applied to this base problem by, rather than searching the entire parameter space for the optimal structure, starting from an initial force structure; defining possible transformations in terms of force size increase, improvement in firing range, and improvement in communicator reliability; evaluating risk as losses suffered by the force using WISDOM-II; and traversing the resulting graph in order to find not only the most suitable force structure after a fixed time interval, but the best path (minimax risk) through time in order to minimise risk.

The second example [8], to be known as Evolutionary, used a combination of evolutionary computation and multi-objective optimisation to derive a suitable force structures to meet a set of scenarios under cost, casualty (suffered), and impact (on enemy) constraints. For the study a number of different weapons and communication options were available - varying in capability and hence cost. The extension of the study carried out here sees the selection of the most effective casualty/defence force and the most effective impact/attacking force. These two forces then represent two applications of the temporal risk assessment framework: Starting from a common initial force structure, and constrained by a fixed budget that could be "spent" each time-step, the possible transformations at each time-step were determined by the actual costings (as used in the original paper) of the equipment. This then allowed the search for a path with minimax risk in order to (best) transform a force from the initial configuration to the final target as originally found by the combined evolutionary and multi-objective techniques. Risk for each force structure was quantified by the Loss Exchange Ratio (LER) - the number of casualties suffered by the force for every enemy casualty.

B. Systematic Example

The systematic force structure example concentrated on a MOUT (Military Operations in Urban Environments) scenario, where the urban density was varied. Three typical environments are defined in Figure 4. Environment a (on left) represents an open environment without any obstacles, environment b (middle figure) represents an environment with random obstacles while environment c (right figure) represents an environment with organized obstacles. Each environment is a 30x30 grid.

Fig. 4. The three different environmental densities used in the Systematic experiments and as represented in WISDOM-II.

For each environment, the red force with fixed capabilities plays against the blue force with different capabilities. The red force is platform centric with a force size of 50 agents. Each red agent can communicate with any other red agents within 2 cells. Both the blue and red force use direct fire weapons. The blue force is network centric. In this paper, a platform centric force means that each agent may communicate with any other agents if they are within each other's communication

range, while a network centric force means that each agent can only send information to the force headquarter and then the common operating picture (COP) developed by the force headquarter is sent back to each agent in the battlefield.

The capability of both forces is defined in Table I. The loss probability is the probability that messages are lost in a communication channel. For both blue and red agents, they will lose mobility after 5 hits and be destroyed after 6 hits.

TABLE I
RANGE OF VARIABILITY IN CAPABILITY OF BLUE FORCE FOR SYSTEMATIC EXPERIMENT

	Blue Force	Red Force
Force type	Network centric	Platform centric
Force size	10 - 55	50
Firing range	1 - 10	2
Loss probability	0 - 100%	0

The initial blue force structure selected was 10 agents, possessing weapons with a firing range of 1, and communicators with 100% loss probability. At each time-step the following transformations were possible:

1) increase the force mass by 10 agents; or
2) increase the weapon range by 2 units; or
3) reduce the communicator loss probability by 20%; or
4) increase force mass by 5 agents and weapon range by 1 unit; or
5) increase force mass by 5 agents and reduce communicator loss probability by 10%; or
6) increase weapon range by 1 unit and reduce communicator loss probability by 10%.

For each possible force structure (a total of 1100), WISDOM-II simulated 100 conflicts on each of the three environments. For each run a Loss Exchange Ratio figure (number of enemy losses per friendly loss) was calculated, and these values (across 100 repetitions by 3 environments) were averaged to provide a quantification of the risk facing the given force. A dynamic programming min-max path finder algorithm was then used to find the path of least risk starting from the initial force structure and extending ten time-steps (10 transformations) into the future.

C. Evolutionary Example

In this example, the red force is a platform centric force which has fixed capability resources. There are 30 combatants and 2 surveillance agents in the red force. The 30 combatant agents are divided into three groups of eight agents each and one group of 6 agents. All red agents use type-1 communicator and type-1 weapon except that one agent in the 6-agent group uses a type-6 weapon.

The blue force is network centric with 15 agents in total. The blue force may have at most four groups, each of which consists of homogeneous agents.

The simulation environment is 30x30 cells and the destination flag (each force has a goal to occupy this area) is located at the mid of the left of the environment. Initially the blue force is located at the upper-right corner while the red force is located at the bottom-right corner. Figure 5 presents an example of the initial position of both blue and red forces.

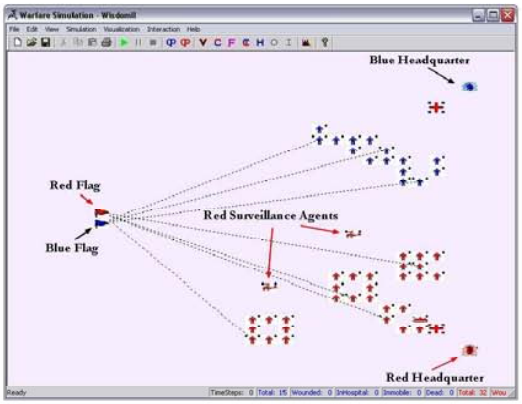

Fig. 5. Screen capture of the WISDOM-II simulation showing an early state of one of the Evolutionary scenarios.

The cost of a force is based on the infrastructure cost and operational cost [8]. The set of weapons and communicators - together with their costs - available for the evolutionary process was as defined in Table II [8].

TABLE II
COMMUNICATOR AND WEAPON CONFIGURATIONS SELECTABLE THROUGH THE EVOLUTIONARY PROCESS. A UNIQUE ID (TYPE), SET OF CAPABILITIES, AND COST IS LISTED FOR EACH.

Communicator								
ID	0	1	2	3	4	5	6	7
Range	8	2	4	6	2	4	6	8
Loss Prob.	0.1	0	0	0	0.1	0.1	0.1	0
Latency	2	0	0	0	2	2	2	0
Cost	260	200	400	600	60	120	240	800

Weapon								
ID	0	1	2	3	4	5	6	7
Range	3-8	0-4	3-8	0-4	3-8	0-4	3-8	6-12
Strength	3	3	3	3	6	6	6	6
Radius	2	0	1	2	0	1	2	3
Cost	159.5	6	104.5	70	33	92	605	1638

As stated above, two evolved force structures - the "most destructive", and the "most defensive" were selected to be target force structures needing to be achieved through a systematic transformational process. Table III shows the two force structures in terms of numbers of agents possessing which combinations of communicators and weapons, together with the mutually exclusive transformations available at each time-step in order to (ultimately) achieve the desired end-state structure. Table III also defines the possible transformations at each time step. The positive number means the number of agents increases in this group while the negative number means the number of agents decreases in this group. For both cases a common initial force structure was selected of fifteen agents in a single group, each possessing type-1 weapon and type-1 communicator.

TABLE III

FINAL FORCE STRUCTURE, AND POSSIBLE CHANGES IN FORCE STRUCTURE PER TIME-STEP FOR THE OFFENSIVE AND DEFENSIVE FORCE STRUCTURES FOUND THROUGH EVOLUTION.

Destructive Force				
	Grp 1	Grp 2	Grp 3	Grp 4
# Agents	1	10	4	0
Comm Type	1	3	2	1
Wpn Type	1	1	1	4
Possible transformations	-1	+1	0	0
	-2	0	+2	0
	-10	0	0	+10
	-6	0	+1	+5

Defensive Force				
	Grp 1	Grp 2	Grp 3	Grp 4
# Agents	7	4	3	1
Comm Type	1	2	1	1
Wpn Type	1	1	4	5
Possible transformations	-2	+2	0	0
	-7	0	+7	0
	-2	0	0	+2
	-4	+1	+3	0
	-2	+1	0	+1
	-4	0	+3	+1

For each possible force structure (a number which varied for each of the different final forces in question), WISDOM-II simulated 30 conflicts. Like the Systematic study, for each run a Loss Exchange Ratio figure (number of enemy losses per friendly loss) was calculated, and these values were averaged to provide a quantification of the risk facing the given force. A dynamic programming min-max path finder algorithm was then used to find the path of least risk starting from the initial force structure and extending through to the final, desired force structure.

IV. RESULTS

This section presents the results of applying the temporal risk assessment framework to the two classes of problems - the Systematic and Evolutionary examples. In both cases a path of minimal risk - a sequence of force transformations that minimise overall risk to the organisation - is found by the methodology and examined in terms of total risk and the sequencing of transformations.

A. Systematic Results

Figure 6 shows the average (across the three terrain types) LER - our quantification of risk for the purposes of this paper - landscape as a function of the three force capabilities - mass, weapon range, and communicator falability - that were varied. It is this landscape of risk, under the temporal and budgetary constraints listed above, that the temporal risk assessment framework traversed.

Figure 7 shows the path of minimum risk - both the force structure change and resulting risk for that configuration - when ten force transformation time-steps were allowed. It is worth noting that the methodology supports either a final desired force structure (such as in the evolutionary example) or the best possible (minimal overall risk) after a certain time-period as in this example.

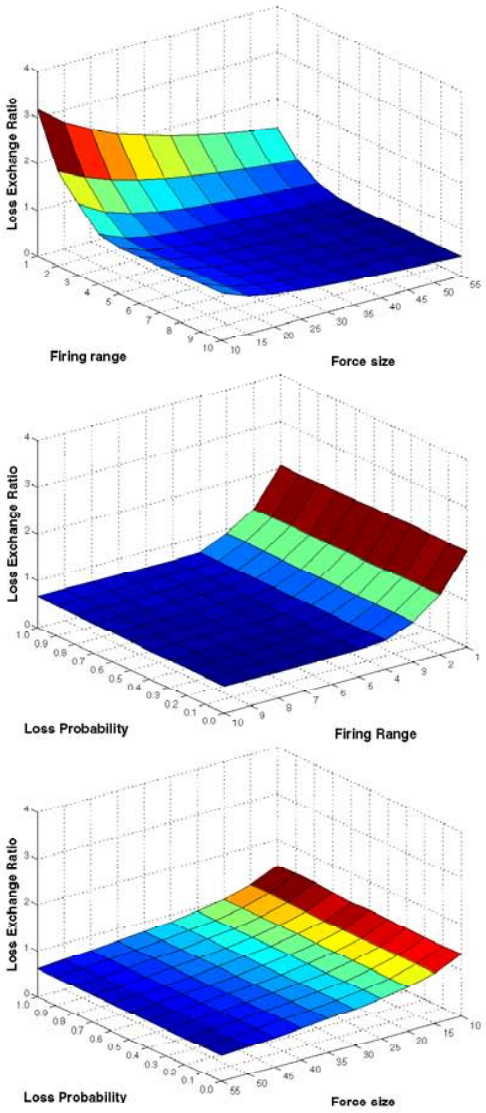

Fig. 6. Average LER for the Systematic experiments. All pairings of capabilities being shown, with averaging occuring across the three environment types and all values of the third capability.

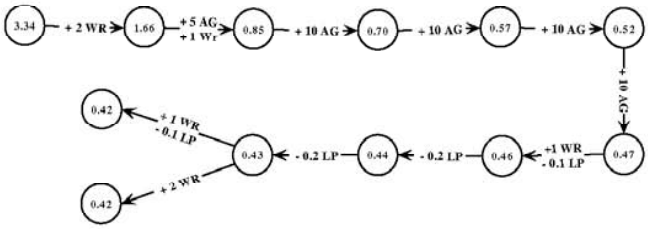

Fig. 7. Path of minimum risk for the Systematic scenario. Vertices show the risk to that particular force structure, while edges show the transformation to the force that should occur at the next time-step to reduce overall risk.

The force structure changes along the path include improvements to all three capabilities but in a particular order. That is that weapon range is first partially increased (from

1 units to 4 units), before force mass is increased to its maximum (55 agents) across several time-steps after which communicator reliability, and to a lesser extent further weapon range improvements are made - to little change in the risk to the force structure.

This sequencing is particularly important in reducing the overall risk profile. An analysis of the same total set of alterations but performed in alternate orders (e.g., communicator improvements first) always yielded a greater - often significantly so - overall risk.

B. Evolutionary Results

For the example in which the temporal risk assessment framework was applied to the evolutionary examples, two force structures were examined - the best offensive (destructive - maximise enemy casualties) force evolved, and the best defensive (minimise own casualty) force structures.

Table IV and graph 8 apply to the destructive force structure. As can be seen by analysing the sequence of changes, the number of agents equipped with the type-2 configuration was rapidly increased to 70% of its final necessary size, before any agents equipped with the type-3 configuration were seen.

TABLE IV

CAPABILITY PAIRINGS (COMMUNICATOR AND WEAPON TYPE) FOR THE DIFFERENT AGENT GROUPS IN THE DESTRUCTIVE FORCE RISK ANALYSIS.

	Communicator	Weapon
Group 1	type-I	type-I
Group 2	type-III	type-I
Group 3	type-II	type-I
Group 4	type-I	type-IV

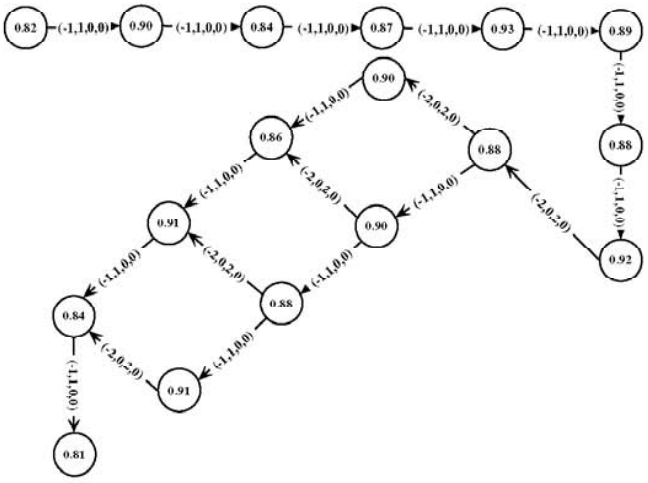

Fig. 8. Path of minimum risk for the destructive force of the Evolutionary scenario. Vertices show the risk to that particular force structure, while edges show the transformation (changes in number of agents in each group) to the force that should occur at the next time-step to reduce overall risk.

Table V and graph 9 show the far simpler case of the defensive force structure. Simpler because far less transformational steps were required in order to reach the final configuration. In this and the above destructive force structure cases, as for the systematic example, analysis of alternate paths to the final goal vertex in the graph structure showed that the sequencing of transformations found by the methodology were the best possible in terms of minimising overall risk.

TABLE V

CAPABILITY PAIRINGS (COMMUNICATOR AND WEAPON TYPE) FOR THE DIFFERENT AGENT GROUPS IN THE DEFENSIVE FORCE RISK ANALYSIS.

	Communicator	Weapon
Group 1	type-1	type-1
Group 2	type-2	type-2
Group 3	type-1	type-4
Group 4	type-1	type-5

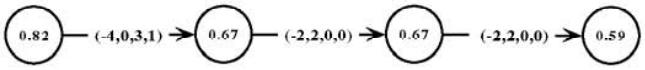

Fig. 9. Path of minimum risk for the defensive force of the Evolutionary scenario. Vertices show the risk to that particular force structure, while edges show the transformation (changes in number of agents in each group) to the force that should occur at the next time-step to reduce overall risk.

V. DISCUSSION

This paper has introduced a novel new risk assessment methodology that employs a core simulation engine, while capturing and minimising risk through time via a graph based technique. The methodology has been exercised on three force transformation problems by way of example. In each case temporal and budgetry constraints were imposed to force a step-wise transformation from an initial force structure to the desired end-state. The methodology constructs a graph in which vertices represent potential future force structures, and edges indicate the possibility of changing between the two force configurations. At each vertex a risk value - to the organisation of that particular force structure - is placed. In our case this was calculated as a Loss Exchange Ratio using the WISDOM-II simulation. A dynamic programming min-max path finder algorithm was then employed to find the path of minimal risk from the starting vertex (force configuration) to the desired vertex (final force configuration).

The three examples of final force structure, found herein, were selected due to their ability to illustrate different features of the methodology. They show that the methodology can be applied both in situations when a final, desired force structure is known, together with when a fixed time period alone is being modelled. Despite being relatively simplistic examples, these show the potential of the technique and there is no reason that it could not, and should not, be applied to more realistic problems.

Beyond finding application in more complex and realistic problems, there is considerable scope for expansion - both theoretically and in an application sense - for the methodology. Other quantifications of threat (than the Loss Exchange Ratio used here) are possible and could seamlessly be integrated into the framework, and alternate simulation or threat quantification

tools are all possible. One significant improvement would be a change from the discrete, sequential temporal model currently being employed to a continuous time model, as well as one in which the threat environment (scenario set currently) changes over time, and earlier events (threats) have a "flow on" effect.

VI. Acknowledgement

We would like to acknowledge the financial assistance of the Australian Research Council discovery grant number DP0667123.

References

[1] M. Barlow and A. Easton, "CROCADILE - an open, extensible agent-based distillation engine," *Information & Security*, vol. 8, no. 1, pp. 17–51, 2002.

[2] J. O. Berger, *Statistical Decision Theory and Bayesian Analysis*. Springer, 1985.

[3] D. P. Galligan, "Modelling shared situational awareness using the MANA model," *Journal of Battlefield Technology*, vol. 7, no. 3, pp. 35–40, 2004.

[4] B. S. Fischhoff and S. R. S. Watson and C. S. Hope, "Defining risk," *Policy Sciences*, vol. 17, no. 2, pp. 123–139, 1984.

[5] DOD, "Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities," *Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, D.C.*, Unclassified Report 20301-3140, 2003.

[6] M. K. Lauren and R. T. Stephen, "MANA: Map-aware non-uniform automata, a new zealand approach to scenario modelling," *Journal of Battlefield Technology*, vol. 5, no. 1, pp. 27–31, 2002.

[7] O. Renn, "Three decades of risk research: accomplishments and new challenges," *Journal of Risk Research*, vol. 1, no. 1, pp. 49–71, 1998.

[8] A. Yang, H. A. Abbass, M. Barlow, R. Sarker, and N. J. Curtis, "Evolving capability requirements in WISDOM-II," in *Advances in Artificial Life, Proceeding of The Second Australian Conference on Artificial Life (ACAL05)*, H. A. Abbass, T. Bossamier, and J. Wiles, Eds. Sydney, Australia: World Scientific Publisher, 2005, pp. 335–348.

[9] A. Yang, H. A. Abbass, and R. Sarker, "Landscape dynamics in multi-agent simulation combat systems," in *Proceedings of 17th Joint Australian Conference on Artificial Intelligence, LNAI 3339*. Cairns, Australia: Springer-Verlag, 2004.

[10] ——, "Evolving agents for network centric warfare," in *GECCO '05: Proceedings of the 2005 workshops on Genetic and evolutionary computation: Second Workshop on Military and Security Applications of Evolutionary Computation*. New York, NY, USA: ACM Press, 2005, pp. 193–195.

[11] ——, "Risk assessment of capability requirements using WISDOM-II," in *The International Society for Optical Engineering (SPIE), International Symposium of Microelectronics, MEMS, and Nanotechnology: Complex Systems Conference, Proceeding of SPIE Vol 6039*, A. Bender, Ed., Brisbane, Australia, 2005.

[12] ——, "WISDOM-II: A network centric model for warfare," in *Ninth International Conference on Knowledge-Based Intelligent Information & Engineering Systems (KES 2005), LNCS 3683*, Melbourne, Australia, 2005.

[13] ——, "Characterizing warfare in red teaming," *IEEE Transactions on Systems, Man, Cybernetics, Part B: Cybernetics*, vol. 36, no. 2, pp. 268–285, 2006.

[14] ——, "Land combat scenario planning: A multiobjective approach," in *The Sixth International Conference on Simulated Evolution And Learning (SEAL'06), LNCS*, Hefei, China, 2006.