Australian Government

Department of Defence
Science and Technology

A Simple Handbook for Non-Traditional Red Teaming

Monique Kardos and Patricia Dexter*

Joint and Operations Analysis Division
***National Security and ISR Division**

Defence Science and Technology Group

DST-Group-TR-3335

ABSTRACT

This report represents a guide for those wishing to apply red teaming methods in a structured manner, and provides lessons developed in both the military and national security environments. It describes the practice of red teaming in the context of biases and heuristics followed by techniques and activity designs allowing others to design and apply red teaming activities across a range of domains.

Produced by

Joint & Operations Analysis Division
DST Group Edinburgh
PO BOX 1500, Edinburgh, SA, 5111

Telephone: 1300 333 362

January 2017
AR-016-782

Conditions of Release and Disposal

A Simple Handbook for Non-Traditional Red Teaming

Executive Summary

This report describes the application of red teaming as a methodology in a broader, less traditional sense. It is designed to enable people to employ a more analytical approach to their problem analysis or evaluations, and to tailor the scale and complexity of red teaming activities to meet their specific needs.

It provides a cognitive bias and heuristics context to further the reader's understanding of how red teaming is intended to mitigate these issues, as well as how structured analytical techniques can help manage these issues within red teaming itself. While the methodologies discussed are drawn from a variety of disciplines (e.g. operations analysis, operations research, human sciences, and systems engineering to name just a few), they are often complementary in terms of the outcomes they support when applied to the appropriate problems.

Four critical aspects of successful red teaming are identified, and include: providing clarity about what is being tested, defining appropriate objectives for the test activity, carefully deciding how to best conduct the activity to obtain meaningful outcomes, and working within the resources available to achieve the optimal outcome. By keeping these four aspects in mind during the planning and decision processes, the appropriate method(s) for the activity can be selected. As with any exercise that aims to evaluate or analyse performance, validity or other aspects of plans, processes, actions, other analyses or reports (particularly those looking to be predictive in nature), the quality of the outcomes are determined by the quality of the decision making and preparation that went into planning the activity.

This report provides simple initial guidance regarding the development and conduct of red teaming activities by enabling an understanding of the broader utility of red teaming: what it is useful for, and how it can be applied in a variety of contexts (both within and outside of Defence). With the outline of various cognitive biases (the effects of which red teaming is designed to help combat) and a variety of bias mitigation strategies provided, it enables activity planning with a base knowledge of the underlying value of a red teaming approach. Further, with the outline of the various activity types that fall under the red teaming umbrella, as well as the additional activity and method descriptions, readers can then identify the necessity for a red teaming approach and the type of methods that would best suit the purpose of their activity.

Once red teaming has been selected as the required basis for the activity, some guidance and lessons based on learning from previously conducted red teaming activities in both the military and civilian domains has been provided, and should assist with the design of the activity itself, particularly in terms of personnel selection.

Finishing with a brief examination of training issues, and several links to a variety of red team training providers, this report will serves as a simple enabler for individuals wishing to explore the applicability of red teaming approaches to address their challenges.

Authors

Monique Kardos
National Security and ISR Division

Monique has a background in both general science and a PhD (Psychology) in the field of Learning and Behaviour. She has taught Psychology to undergraduates at both Adelaide University and University of South Australia, and has undertaken research field trips with both the Department of Environment and Natural Resources, and the Adelaide Zoo. She joined the DST Group as a research scientist in 2000, beginning with the Human Systems Integration discipline and tender evaluation for the Air87 project. She has worked on the Force Operations Analysis task, focusing on the analysis of deployed Army use of the Military Geographic Information and information management capabilities during deployment to East Timor and since then, her work focus has broadened to include counter terrorism exercise and operational evaluations, the social and psychological aspects of information collection, development and application of a new evaluation framework and methodology (including red teaming) for the ANZCTC National Security exercise program and the Army as well as her current focus, which is the evaluation and application of biometrics for both military and non-military intelligence.

Patricia Dexter
Joint and Operations Analysis Division

Patricia has a background in Physical Chemistry with a specialty in Spectroscopy from Flinders University and has taught at both Flinders University and TAFE SA. Following a period in pharmaceuticals she commenced at DST Group in 1999 and has worked in various areas of Land Operations Research covering simulation for training and skill degradation, combat entropy, historical analysis for population reactions to stimuli, emerging technologies, scenario and dimensional analysis and land futures research. With a keen interest in Judgement Based Operations Research her recent expertise has developed in structured and environment analysis specialising in Red Teaming in the Land Operations Domain.

This page is intentionally blank

Contents

Glossary

AAR	After Action Review
ANZCTC	Australia-New Zealand Counter Terrorism Committee
Bde	Brigade
BoAI	Building on Army Initiatives
C3ISR	Command, Control, Communication, Intelligence, Surveillance and Reconnaissance
CIA	Central Intelligence Agency
COA	Course of Action
CPX	Command Post Exercise
CRT	Computational Red Teaming
CT	Counter Terrorism
DIV	Division
DST	Defence Science and Technology
FAE	Fundamental Attribution Error
FLWR	Future Land Warfare Report
ICBM	Inventory of Cognitive Biases in Medicine
LADS	Land Analytical Decision Support Studies
MJEX	Multi-Jurisdictional Exercise
MOE	Measure of Effectiveness
MOP	Measure of Performance
NS	National Security
OIC	Officer in Command
RT	Red team
SME	Subject Matter Expert
SOP	Standard Operating Procedure
TOPOFF	Top Officials (national level domestic exercise)
US	United States
USA	United States of America

This page is intentionally blank

1. Introduction

This report is intended to form a simple guide to aid the development and conduct of activities that either wholly or partially apply some form of red teaming to achieve their goals. While red teaming is applied across a broad range of fields such as business, finance and manufacturing as well as the military and national security, this work is aimed primarily at the national security and military contexts, and the examples used within will be based on these two arenas.

1.1 Structure of the report

This report will walk the reader through a process beginning with the underlying reasons for using red teaming methods, and will introduce relevant concepts along the way including cognitive bias and heuristics, the broad array of methods being applied to the red teaming arena, how to apply red teaming in various contexts (including guidance for various aspects to help ensure success), and several examples of successful red teaming activities conducted at various scales / levels of complexity.

More specifically, the report will begin by discussing the issue of cognitive bias and heuristics and their impact on human decision making and analysis, and introduce the use of red teaming as a means of mitigating these issues. The next section will explore the broadening of red teaming beyond the initial Cold War application (i.e. 'taking the red perspective'), and introduce the concept of red teaming as an umbrella term for a larger variety of activities that now includes a variety of scales and levels of complexity. This will also include a review of the methods suitable for use with red teaming activities, and a table summarising their utility.

Subsequently, the report will discuss the application of red teaming methods in different contexts, and how the aims or goals of the activity drive the design of the activity: that is, the questions to be answered, the scale of the activity required, and the suitable types of methods. This includes the combination of different methods and activity types to achieve the aim. This section will also include learnings from past red teaming activities and some essential ground rules for participants. Examples will be discussed, and the requirement for some form of training (including an example course already in use) is also examined.

Many of the issues underlying the creation of plans or making of decisions can be identified as related to human cognitive processes. These are very common, and quite individual in terms of their origins for each person, and can (both consciously but more commonly *sub*consciously) affect how humans reason about issues and make decisions. In the contexts covered in this report, such flawed reasoning can lead to problematic decisions with serious consequences, so an examination of these underlying causes is necessary to gain insight into the need for - and utility of - red teaming.

2. Cognitive biases and heuristics

This section presents a brief summary of cognitive biases and heuristics, and how they may impact on decisions and plans. It is brief because there are estimated to be in excess of 200 identified types of bias and/or heuristic, and it is not within the scope of this paper to discuss all of them in detail. The concepts will therefore be covered in broad terms initially, and then narrow to focus on the relevant biases and heuristics for the national security and military contexts.

2.1 Biases and heuristics: a general introduction

Cognitive heuristics are defined in the Cambridge Dictionary of Psychology (2009, p. 234) as "a rule of thumb for making decisions of a particular kind which usually works but does not guarantee a correct solution." Cognitive biases, however, refer to a systematic pattern of deviation from the norm or rationality in human judgment, whereby inferences about people and situations may be drawn in an illogical fashion. In other words, individuals create their own "subjective reality" from their perception of the input, which is driven by (for example) previous experience or other pieces of information.

Traditionally, cognitive biases have been studied by comparing the way individuals actually make decisions with the normative rationality standard of decision making (Chapman & Elstein, 2000). Humans tend not to use the rational choice model when making decisions, however, as we do not function in the way that machine programs do (by weighting all the options appropriately and making a completely objective choice based on the outcome of complex comparisons and equations). Tversky and Kahneman (1986: 68) state that "... the deviations of actual behaviour from the normative model [i.e., rational choice theory] are too widespread to be ignored, too systematic to be dismissed as random error, and too fundamental to be accommodated by relaxing the normative system." (Kardos, 2006)

This indicates that there is a set of rules of thumb or systematic 'shortcuts' that humans employ in order to process information efficiently. Tversky and Kahneman (1974) explain this as follows: "This is so, it is suggested, because people do not follow a process of subconsciously multiplying potential gains or losses by their respective probabilities in reaching a decision. Instead, they rely on a limited number of heuristic principles which reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations." (pp. 1124)

It is also clear (through observing the way people make their way through life) that, in spite of their relative simplicity and lack of sophistication, these heuristics are usually quite effective (Harvey, 1998) and can often result in a decision making performance similar to that expected from optimal rational performance (Gigerenzer & Hug, 1992). Even so, they tend to create bias and error more often than the decisions arrived at via the use of the more precise expected-utility theory (Harvey, 1998; Nisbett, 1993; Plous, 1993). This may be due to the fact that while the judgement process is adapted to suit the

requirements of many everyday decisions, the processes may not be particularly adaptable to changing needs (Klayman & Brown, 1993; Mitchell, 2003).

Humans employ a range of heuristics for two key reasons:

1. Because they represent efficient use of our limited cognitive abilities. That is, rules of thumb are not perfect, but perfection is generally an unrealistic goal and the most that can be hoped for is a "best solution under the circumstances".
2. Our understanding of the world tends to encourage the use of such heuristics. We rely on our subjective, culturally-specific understanding of the world around us rather than having access to some objective reality from which we can gather the necessary unbiased data for our decision processes. (Harvey, 1998)

Some heuristics can lead to relatively predictable biases and inconsistencies in terms of judgement and decision making; the example here relates to the representativeness heuristic. The *Representativeness Heuristic* is possibly the best-known and most studied heuristic (Nisbett, 1993). It is used to label peoples' tendency to judge the probability of an event by finding a 'comparable known' event and assuming that the probabilities will be similar. Humans tend to want to classify things, and if they can't find an exact match in a known category, they will often approximate to the nearest similar class available. The primary fallacy in operation here, then, is the assumption that similarity in one aspect will lead to similarity in others. This is a common problem with applying heuristics – overgeneralisation.

2.2 Biases and heuristics relevant to military and national security contexts

A list of relevant heuristics is shown below Table 1, with biases listed in Table 2. It should be noted that these lists are not all-inclusive: that is, there may be additional relevant biases or heuristics that have not been included here. This list has been chosen based on the characteristics of (and activities conducted in) the military and national security contexts. The descriptions shown here are simplified for brevity, and more expansive explanations of the heuristics and biases (and examples of their impact on human decision making and plans) can be found in Appendix A.

Table 1: List of relevant cognitive heuristics

Cognitive Heuristics	**Brief description**
Anchoring & Adjustment Heuristic	Adjusting evaluation (usually inadequately) according to an existing reference point
Availability Heuristic	Ease of actual recall / perceived ease of recall
Elimination by aspects Heuristic	Using one characteristics at a time to narrow options
Recognition Heuristic	Viewing recognised events/options as more meaningful
Representativeness Heuristic	Classifying events / options based on similarity to

	existing categories
Satisficing	Selecting options that meet minimum acceptable criteria
Similarity Heuristic	Choosing options similar to past positive outcome options
Simulation Heuristic	Viewing easily imaginable options as more likely
Take-The-Best Heuristic	Choosing options based on a single differentiating criterion

When cognitive heuristics fail to produce a correct judgement, the result may be cognitive biases (the tendency to draw incorrect conclusions based on cognitive factors). There are several cognitive biases that individuals may apply when decision-making and choosing responses or options in military or national security activities, and these are outlined in Table 2 below.

Table 2: List of relevant cognitive biases

Cognitive Biases (falling into four categories)	**Brief description**
Category 1: Behavioural and Decision Making Biases	
Attentional Bias	Using a narrow focus and ignoring other options
Bandwagon Effect	Conforming to the group consensus view
Bias Blind Spot	Assuming bias in others and not in oneself
Choice-Supportive Bias	Retroactively viewing choices as having only positive attributes
Confirmation Bias	Favour confirmatory information or interpret all information as confirmatory
Congruence Bias	Testing only the hypothesis one wants to accept
Curse of Knowledge Bias	Inability to take a naïve perspective
Defensive Decision Making	Making the defensible instead of the best decision
Distinction Bias	Viewing two options as more dissimilar if judging them in isolation of each other
Escalation of Commitment	Continuing to invest in a sub-optimal decision based on the investment already made
Expectation Bias	Choices influenced by expectations / mindset
Exposure-Suspicion Bias	Narrowing of perspective to only view choices through the lens of own profession
Framing Effect	Impact of the formulation of the problem/decision on the choice made
Focusing Effect	Overemphasis of one aspect unduly influencing choice
Functional Fixedness	Preferring only the traditional application of options
Irrational Escalation (related to "escalation of commitment")	Continuing to invest in a bad choice based on an initial good choice or to justify past actions
Mere Exposure Effect	Preference for familiar options
Normalcy Bias	Underestimation of the possibility of or effects of a disaster occurring
Omission bias	Judging harmful actions as worse than harmful inaction

Outcome Bias	Judging choices by the quality of the outcome instead of the quality of information on which the choice was based
Persuasion Bias	Perceiving all new information as independent of any previous information
Seer-Sucker Illusion	Over-reliance on expert advice
Selective Perception	Effect of peoples' beliefs/attitudes/etc. on their perceptions
Semmelweis Reflex	Rejection of new contradictory information
Status Quo Bias	Preference for things to remain the same
Turkey Illusion	Extrapolating the past to predict the future without factoring in changes
Category 2: Probability and Belief Biases	
Ambiguity Effect	Tendency to choose options for which the probability of a positive outcome is known in the face of ambiguous information
Authority Bias	Influence of an expert on the judged value of an option
Belief Bias	Believability of the conclusion influences the evaluation of the logical strength of the option
Clustering Illusion	Overestimating the importance of small runs or clusters of in large amounts of information
Forward Bias	Using old data to validate models built using that data
Illusory Correlation	Seeing events, attributes or categories as belonging together (can create stereotypes)
Illusion of Validity	Belief that added information generates additional data for predictions even when it clearly does not
Overconfidence Effect	Occurs when peoples' subjective confidence in their ability is higher than their objective accuracy
Primacy Effect	Stronger influence of early options on final choice
Recency Effect	Stronger influence of later/last options on final choice
Subadditivity Effect	Judging the probability of the whole as less than the sum of the parts
Subjective Validation	People placing more meaning or value on a statement or option that is personally significant or meaningful to them
Category 3: Social Biases	
Group Think (Herd instinct)	Agreeing with the group consensus regardless of own opinion
Ingroup Bias	Preferring the opinions of people perceived to be a member of one's own group
Status Quo Bias	Preferring things to remain the same
Shared Information Bias	Over-focusing on information familiar to the group
System Justification	Defending the status quo except in the face of compelling evidence
Category 4: Memory Biases	
Illusion of Truth Effect	Familiar statements being perceived as more truthful
Misinformation Effect	Increasing inaccuracy of memory due to interference from post event information
Von Restorff Effect	Tendency to recall distinctive items/events

As previously stated, there may be other biases that individuals subconsciously apply to their analysis, planning and decision making, all of which impact on the quality and effectiveness of the outcome.
Appendix A presents the explanations in a more simplified way than standard psychology texts, as this is intended to be a useful guide for practitioners in the military and national security fields looking to broaden their application of red teaming. For this purpose, the minute details of probability based reasoning and subsequent mathematical and statistical reasoning flaws relating to these biases are not required, merely the impact they have on reasoners.

While research has identified many biases and heuristics applicable across a variety of human activities, it is more difficult to identify consistent means of overcoming many of these biases. Red teaming – in its original inception – was devised during the Cold War as a means of analysing opposition tactics and strategies, with the term "Red" symbolising the communist adversary. Since then, the method has also been suggested as a means to inject more rigour into analyses and testing activities in order to identify deeper issues, with the application of e.g. structured analytical techniques (Heuer & Pherson, 2015; Pherson & Pherson, 2013). The current broader application of red teaming - as shown by the series of activities depicted in Figure 1 [section 3] - has added scope to address biases and the problematic applications of heuristics. That is, not only can these be mitigated during the practical red teaming activities, there are other ways to pre-emptively address bias and heuristic issues before an activity begins. Some of the available methods will be discussed in section 2.3.

2.3 Bias mitigation strategies

Each bias and heuristic an individual experiences (or applies) will have distinct origins and triggers, and these can differ widely between individuals. That is, the combination of life experiences contributing to the formation of both biases and heuristics are peculiar to each person. While some biases such as cultural, racial and religious stereotypes may be 'programmed' into children from a young age through the actions and words of their parents and other authority figures (or even peers), some are produced by the types of training people receive for their work tasks, and some form independently and are based on the experiences of the individual throughout their lifespan.

Researchers have explored several ways to approach the mitigation of cognitive biases and problematic heuristics, some of which are outlined below.

2.3.1 Training-based video games

Dunbar et al. (2014) proposed and tested a serious training video game named *MACBETH (Mitigating Analyst Cognitive Bias by Eliminating Task Heuristics)* , which was designed to address and mitigate cognitive biases. Specifically, they focused on two biases: the fundamental attribution error (FAE), and confirmation bias. Testing the efficacy of the game against the use of an instructional video regarding these biases, the researchers found that the game was more effective at mitigating these cognitive biases when explicit

training methods were combined with repetitive game play. In addition, the explicit instruction in the game provided greater familiarity with and knowledge about the biases than did implicit instructions.

The MACBETH game involves individuals playing the role of analysts being presented with a fictional scenario of an impending terrorist attack. The task is to identify who the suspect is, where the attack will occur, and what will be the mode of attack. Part of the gameplay involves taking turns with two other computer generated characters, and being able to gather two pieces of information per turn from a combination of intelligence sources. Using these, the human player can generate hypotheses of their own and aid the other analysts with their hypotheses. Players receive information about the cognitive biases and receive implicit or explicit feedback (depending on the test condition) encouraging them to do such things as seek disconfirmatory evidence, delay hypothesis formation, and offer alternative hypotheses in order to mitigate confirmation bias. For the fundamental attribution error mitigation, players are trained to use an Archive mini-game to review case files and make threat assessments on past real life individuals. Here players are encouraged to use situational rather than dispositional cues to mitigate FAE, and are rewarded with additional resources that can be used to unlock extra intelligence.

The instructional video followed a more traditional format, informing viewers about the biases and mitigating strategies using entertaining vignettes.

The results here mirror what tends to be found in much of the training and education research, which is that experiential learning is an effective model for teaching skills to adults in particular. Experiential learning requires that people both intend to learn, and undergo an active learning phase (Moon, 2004). That is, experiential learning is most effective when it involves the provision of a theoretical basis combined with a reasonable amount of hands-on practice to allow for reflection and feedback on performance (Kolb, 1984).

2.3.2 Teaching awareness of cognitive bias and contributing factors

Greitzer and Andrews (2010) in their work on combat identification and bias explore various ideas for training mitigations that can be used to address stress-induced cognitive and emotional factors which may introduce bias into combat identification decisions. Combat identification is a combination of situational awareness and target identification, and is designed to enhance unit effectiveness by reducing fratricide and collateral damage. So while it is critical that this is performed as close to optimally as possible, this is clearly a challenge given the stressors in the battle context.

Greitzer and Andrews recommend two key additional training characteristics to enhance planning and warfighting:

- Training for combat identification "must be designed to address cognitive biases" (p.183)
    - Biases such as confirmation bias and irrational escalation can lead to experienced personnel relying solely on past experience and potentially ignore relevant indicators in each environment

    - Such training may include the use of After Action Reviews (AARs).
- Training must also address the effects of stress on cognitive biases and performance
    - Enhanced awareness of the impact of stress (e.g. the potential for eliciting flawed decision making strategies) and coping strategies to mitigate these effects should form part of training
    - Emphasis on the testing of assumptions forms an important part of the training
    - Actually eliciting stress as part of the training activity/scenario is an important part of the training, as it provides the real-world validity that will help to cement learning for personnel.

The red team training described in this report may be useful as an initial introduction to the issues of bias, demonstrating how and why biases occur and what can be done to manage them. Further development of this training package could delve further into the underlying causes and contributors to stress and cognitive biases in order to provide personnel with a basic understanding of the mechanisms through which such issues occur.

In the medical world, cognitive bias can play a significant role in the success or failure of the diagnosis and treatment of patients. Some researchers have attempted to address the issues of bias and misused heuristics with a variety of interventions. For instance, Hershberger, Part, Markert, Cohen & Finger (1995) outline a seminar they conduct with medical students and internal medicine residents at Wright State University to address these very problems. Their stated focus is on the "predictable tendencies in information processing that can have adverse effects on decisions made in the clinical setting"(p. 661), with emphasis on the more uncertain situations which require probability estimates to be made. They deal with three types of issue: the representativeness heuristic, the availability heuristic, and the most commonly known of the three - confirmation bias. From each of the two heuristics, they chose a set of the most critical characteristics (e.g. insensitivity to prior probabilities, illusory correlation) on which to focus attention. The effectiveness of their seminars have been tested using 265 participants divided into an experimental and a control group, and applying the Inventory of Cognitive Biases in Medicine (ICBM) which is composed of 22 medical scenarios with known psychometrics. They found that the group who received the instruction seminar on biases scored between 9 – 10% better than the group who received no instructions regarding biases, with the control group scoring below chance level on the ICBM. Hershberger et al. conclude that there is some merit in the use of seminars such as theirs to assist in controlling the effects of bias on medical decision making, and helping to develop skills in this area for both students and residents. The authors of this report would argue that there is also merit in applying these seminars to established medical practitioners, who will – over time – feel the effect of cognitive biases and misplaced heuristics on their medical decision making, as experience alone is not a mitigating factor for bias.

2.3.3 Managed release of information for decision makers

Dror (2012) recommends a method of sequential unmasking (i.e. release) of information when forensic scientists are performing analyses that has also been supported by 13 other authors in this field as an alternative to a suggested 'working blind' bias management method (i.e. without contextual information)[1]. The 'working blind' method assumes that meaningful analysis can be conducted without context – and this is incorrect, particularly in a complex analytical framework such as forensics. This is where sequential unmasking provides an effective alternative; it allows the context to be factored into the analysis, yet in a controlled manner. Items of information which may have a biasing effect on the forensic scientist's analysis can be weighed in terms of the pros and cons of having each item, in terms of the value added to the analysis versus the likelihood of bias if the information is provided at a given time. For example, knowledge of whether the suspect admitted to the crime or not is generally irrelevant information to a forensic examiner, and so can be safely withheld to prevent the introduction of bias. If information *is* relevant, however, its value to the work of the examiner needs to be assessed first to determine when it should be provided. The potential drawbacks of this method are that it requires pre-analysis of the information to weigh the costs and benefits of introducing it, and a means (personnel charged with the role?) of managing this information release to the examiner.

2.3.4 Other alternatives for managing bias

Techniques such as the Delphi process (Heuer, 2015) were designed to collect group data while minimising hierarchical bias in extremely stove-piped military organisations such as Strategic Command. However for many years, this technique was used blindly with the assumption that it minimised hierarchical bias, while paying little attention to other types of bias. Many practitioners often implemented individual elements of the Delphi technique which have since been identified as methods for reducing cognitive biases even within this technique itself. Winkler and Moser (Winkler, 2016) identified six design features which are easily implemented within the technique (many features similar to these were already in use by the Defence Science & Technology (DST) Group) in order to minimise the effects of Framing & Anchoring, Desirability, the Bandwagon Effect, and Belief perseverance. Their work highlights a key factor in using bias minimisation techniques; i.e. that practitioners of red teaming methods need to be aware of the pitfalls of their chosen techniques, as well as the benefits of their use in minimising biases. This is where multi methods can provide overlapping techniques which minimise bias in different areas. While these overlapping techniques are highly effective in achieving bias minimisation, the application of the techniques themselves must be appropriate to ensure additional biases are not introduced.

While it is difficult to manage such issues due to natural human tendencies as well as the subconscious nature of mental shortcuts, there are potential mitigating strategies available. These strategies may lessen some of the effects of biases (and heuristics, where they are inappropriately applied) to help ensure that objectivity, unbiased analysis, and the

[1] For further information, refer to Thompson et al (2011), Thornton (2010) and Krane et al. (2008).

contextually appropriate decision making are maintained, through reducing the occurrence of such issues as groupthink and other decision making biases. Ideally, these methods should be applied in conjunction with (or supplemental to) the red teaming activities outlined below to ensure the most objective approach to decisions and planning in the national security and military contexts.

3. Red teaming: more than just a single methodology or perspective

In the early days of the red teaming, it was viewed as a single methodology that was most commonly used in the military domain. For example, it was used during the Cold War to allow US officers to take a Soviet perspective and identify ways that Soviets could potentially defeat US plans or systems (Heuer & Pherson, 2015). This involved the wargaming of plans and courses of action, and then pitting those against a red team who would take the adversary's perspective and identify counter actions / Course of Action (COAs) and gaps in the blue plans/COAs.

More recently, red teaming has enjoyed a broader definition, including application in the intelligence analysis, cyber, business, and finance fields (for example) as well as the national security domain. The key difference between this broader definition and the original use of red teaming appears to be the emphasis on critical thinking and analysis *from a general adversarial perspective*, rather than solely from a *specific* adversary's point of view. That is, while the original form of red teaming tended to involve critical thinking in terms of examining the blue's material for weaknesses and planning counters to exploit these, the broader version identifies gaps, risks and issues in general – which encompasses things that may be exploited by an adversary, things that may be problematic even before an adversary is engaged, and problems with the decision making process that lead to a less-than-optimal product or decision. One of the definitions of red teaming used for recent work with the national security arena is as follows:

> Any activity that analyses plans, processes, systems or equipment by using an alternate perspective, typically of an adversary (Malec et al, 2012).

This definition has recently been broadened to encompass the potential for multiple perspectives.

> Any activity that analyses plans, processes, systems or equipment by using one or more alternate - and generally adversarial - perspectives.

Here, red teaming – (in its broadest form) - is a methodology that enables organisations to view their own vulnerabilities and challenge assumptions. It involves any activity—implicit or explicit—in which one actor attempts to understand, challenge, or test a system, plan, or perspective through the eyes of an adversary or competitor. The expected

outcome of red teaming is the development of more robust plans, policies and procedures in any domain.

In this way, red teaming has become something of an umbrella term for a variety of methods and activities. Various consultants have identified several approaches to red teaming other than simply wargaming; Noetic's approaches, for example, include the following:

- *Design assurance red teaming* (will a system achieve its mission in hostile environments)
- *Red team hypothesis testing* (confirm or reject a conjecture, understand competing alternatives)
- *Red team gaming* (interactive, exploratory development of adversarial scenarios, with focus on the goals of the adversary)
- *Behavioural red teaming* (record how adversary may act in various situations, helps analysts to identify preventative actions and attack indicators)
- *Red team benchmarking* (establish a baseline for comparing system responses to adversary actions and help measure progress)
- *Operational red teaming* (field deployment where adversary tries to defeat Blue mission)
- *Analytical red teaming* (use of formal and mathematical models to identify and evaluate adversary's possible COAs)
- *Penetration testing* (help determine if and how a particular adversary may defeat security controls).

These approaches are a good representation of the broader scope for red teaming developed in recent years, yet the definitions (except for hypothesis testing) share a common characteristic: the perspective of the red team/adversary. While this is important and has a well-cemented place in the worlds of military and national security activities, there is value in broadening the view of the adversary to be more generic in some instances. That is, the focus can feasibly be on analysing the veracity and robustness of plans or COAs to identify *any* gaps or weaknesses that could either be exploited or lead to a breakdown in the system functions, not just what the red team could be expected to think or do to undermine the blue team. So for design assurance red teaming, for example, the "hostile environments" for which the system is being tested needs to include the actual terrain, weather, the culture of the intended users, and any other contextual information relevant to its intended deployment.

What emerges here, then, is the importance of the **context** during both framing of the problem and activity design. Three important questions must be considered when red teaming:

- What is being tested?
- What knowledge needs to be gained from the testing?

- How should it be tested to produce the most appropriate and meaningful outcomes?

These three questions combined can provide guidance to the design of the activity. They help to ensure that the system (or 'test item') is challenged with the most appropriate environment and actions to provide information that will identify problems or gaps. This then enables mitigation of identified issues so that adversaries cannot exploit them to cause system dysfunction/failure.

The diagram in Figure 1 below was developed to represent the broader scope of red teaming, where it primarily consists of challenging assumptions that may limit the effectiveness of the item being tested. It is an initial, simplified representation of the span of activities that are common to the national security and/or military contexts, as well as the commonly used perspectives and modes of conduct of the activities.

While there are other red teaming activities listed in the literature, those shown in Figure 1 are most relevant to the national security and military contexts addressed in this report. The activities in the diagram generally increase in either scale or complexity (or both) from right to left, beginning with the smallest, *critical analysis* (which can involve one or more people, and can be used to create meaningful input to all the other activities). The field deployments or exercises tend to be larger scale activities involving many players, a large amount of resources, and substantial planning prior to the event.

It should also be noted that the methods shown on the right hand side of the umbrella are the human-focussed, often face-to-face interactive activity types (although the field/deployment exercises activity also fits this description), while the cyber and computational/modelling/simulation activity types rely more on technology as their basis. A set of simplified descriptors of each of the activity types is included in Table 3 (see page 14).

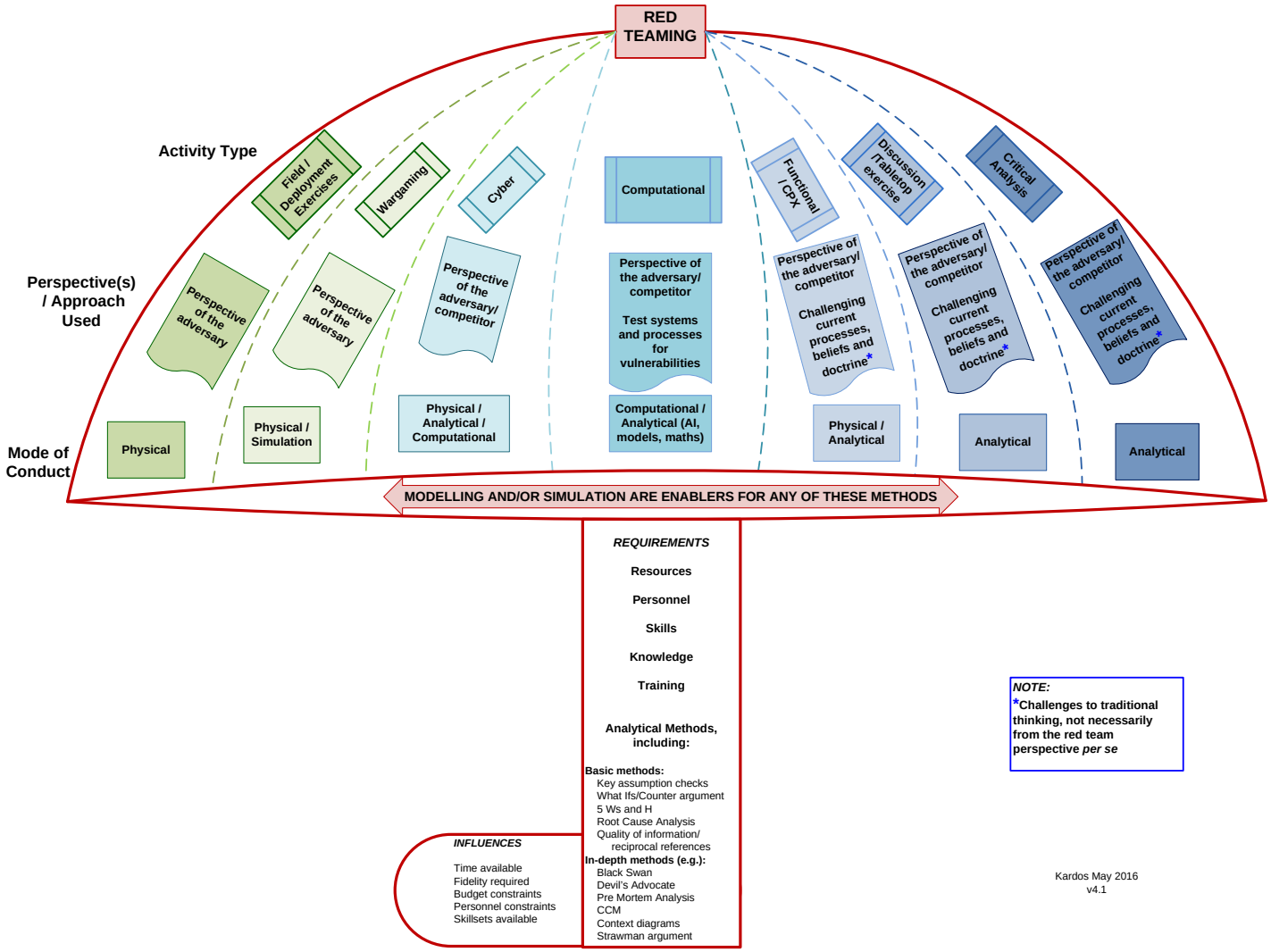

Figure 1: The Red Teaming Umbrella

Table 3: Simple definitions of the activity types shown in Figure 1.

Field / Deployment Exercises	Active deployment of troops / agencies into the field to physically put into practice the Standard Operating Procedures (SOPs) needed to manage an incident, conduct an operation, etc. Red teaming aspect involves challenges to the deployed troops/personnel by a designated red team.
Wargaming	Is a context-based, iterative, competitive model of war or disaster that is independently adjudicated to resolve the outcomes of the interaction between the competing participants (or participants and the environment). The red teaming impact comes from the competitive actions of a group of participants challenging another.
Cyber	Cyber red teaming is a common activity performed within large organisations to assess how susceptible their infrastructure, business processes and staff are to attacks from cyber-enabled adversaries. It is sometimes termed 'penetration testing', and can be complex to conduct due to the highly complex nature of the cyber domain.
Computational	Computational red teaming (CRT): is a framework for assessing system-level vulnerabilities by applying computational intelligence techniques and models.
Functional Exercises / Command Post Exercise (CPX)	Use of a select number of knowledgeable personnel to simulate deployed activities on a smaller scale than full field deployment exercises. Often used to test command and control functions, and requires knowledge of response and action times, as well as resource and personnel availability to meet the requirements of the scenario.
Discussion / Tabletop exercises	Generally paper- or table- based activities run using a relatively small group of personnel discussing the scenario and the requirements (personnel, vehicles, and other resources) associated with conducting an operation. Red teaming discussion exercises involves the use of a red team to challenge answers and assumptions during the discussion.
Critical Analysis	The use of various combinations of established analytical methods to identify key insights about selected issues for both the military and national security domains. The challenges to assumptions and deeper critical insights into relevant aspects including (but not limited to) war/disaster scenarios, SOPs, policies, doctrine, operations, resources, force structures, deployment, and responses to incidents provide the red teaming aspect here, by not accepting the status quo without carefully reviewing the evidence.
Modelling / Simulation ***(ENABLER)***	Modelling / Simulation: tools used to support decision making and assessment of capability, often used as a tool to support or drive other types of activity, such as wargaming or functional exercises.

The next section outlines some of the characteristics of the activity types. What quickly becomes apparent is that many of the characteristics cannot be written in stone, as they are dependent on the aim and objectives of the activity, the budget and resources available, or the availability of skilled personnel who meet the knowledge and experience criteria to be suitable for the activities. In a later section, we will examine a flowchart for deciding whether to conduct red teaming, and if so, what types of red teaming may be suitable. Many of the uncertain aspects noted in the following section can be clarified during the activity planning process once the broad parameters are known.

3.1.1 Characteristics of various activity types

While computational red teaming methods, modelling and simulation can be used to enhance any of the activities in this table that do not already incorporate these elements, most of the other types of activities can also be combined to produce a deeper examination of performance or processes. This enables the identification of strengths as well as gaps for remediation. Previous activities that have applied some of these methods will be used in section 6.1 of this report to illustrate their application.

Tables 3A to 3G: Essential characteristics of the various activity types

Table 3A: Field Deployments / Exercises	
Number of personnel	Varies (dependent on the aim and scale of the activity)
Perspective / Approach	Traditionally takes the adversary's perspective; can be used to field-test equipment prior to deployment in theatre, which does not require the adversary perspective (simply the ability to think beyond the stated use of the item(s)).
Relevant Analytical Methods	Collect information to address Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) relevant to the agency(ies) / organisation(s)
Resources Required	Appropriate location to achieve aim, equipment and transport, all kit required for the unit to carry out the necessary activities
Time Required	*Preparation:* Varies. Upwards of one month, depending on staff and time available *Conduct:* ≥ ½ day (may span weeks, depending on the aim)
Budget Required	Funded through organisation, is dependent on the scale of the activity
Skilled personnel Required	Staff familiar with the design and conduct of exercises, including the evaluation component; personnel from the units being tested should be familiar with the SOPs and processes being tested
Training Required	Dependent on whether staff and personnel meet the requirements in the previous column
Comments	Can be conducted in conjunction with most other types of exercise / activity to enhance the value of the outcomes; these activities are effort-intensive in the lead-up due to the design and logistics requirements.

Table 3B: Wargaming	
Number of personnel	Varies: will require experienced simulation personnel if this is being used; red and blue teams can be any size.
Perspective / Approach	Usually addresses the interaction of the red and blue team to help blue identify counters.
Relevant Analytical Methods	Collect information to address MOEs and MOPs relevant to the agency(ies) /organisation(s)
Resources Required	Physical space; computing facilities if simulation being used;
Time Required	*Preparation:* Varies. Upwards of one month, depending on staff and time available *Conduct:* 1 – 2 days (can be longer, depending on aim of activity and amount of testing required)
Budget Required	Funded through organisation 'in kind' effort

Skilled personnel Required	Staff familiar with wargaming methods; Staff with specific simulation skills (if using this)
Training Required	Some training to ensure that staff are familiar with wargaming methods.
Comments	Wargaming can be both simulation based and tabletop/discussion based exercises.

Table 3C: Cyber	
Number of personnel	Varies: Computing personnel required to design and conduct these activities, SMEs with domain specific knowledge required to aid the activity design and identify key variables.
Perspective / Approach	Red team exploiting blue team and system vulnerabilities
Relevant Analytical Methods	Collect information to address MOEs and MOPs relevant to the agency(ies) /organisation(s)
Resources Required	Physical space; computing facilities; software, hardware
Time Required	*Preparation and Conduct:* Varies. Dependent on what is being tested.
Budget Required	Varies dependent on the aim of the activity and the number of organisations involved (particularly if international organisations are involved)
Skilled personnel Required	Skilled computing staff; Staff familiar with red team modes of action; my require coders to modify software
Training Required	(should be covered if skilled computing staff are being used)
Comments	Can be conducted in conjunction with Field / Deployment exercises

Table 3D: Computational	
Number of personnel	Varies according to the type and complexity of the computational activity.
Perspective / Approach	Red challenging Blue to identify systemic weaknesses
Relevant Analytical Methods	Computational algorithms to analyse the problem space of interest.
Resources Required	Physical space; computing facilities, software, hardware;
Time Required	*Preparation and Conduct:* Varies. Dependent on what is being tested.
Budget Required	Varies – but much of the cost maybe already be covered through the development or purchase of the software and hardware.
Skilled personnel Required	Skilled computing and modelling staff with a particular skill in mathematics and computational red teaming analysis.
Training Required	(should be covered if skilled computing and mathematics staff are being used)
Comments	Can be conducted in conjunction with all other activities (except Cyber) to produce required outcomes

Table 3E: Functional / CPX	
Number of personnel	Varies according to the extent of testing required. Is intended to reflect the real life context in terms of staff and resourcing, but this can be done by selecting adequately knowledgeable staff at a higher level.
Perspective / Approach	Identifying vulnerabilities in current systems / processes. Can assign red team status to select staff to insert specific challenges to the activity.
Relevant Analytical Methods	Collect information to address MOEs, MOPs and issues relevant to the agency(ies) /organisation(s)
Resources Required	Physical space; computing, phone and printing facilities; agency/ organisation specific equipment for the Headquarters/command centre
Time Required	*Preparation time:* Varies according to the complexity of the activity and underlying scenario and inputs. *Conduct*: Usually not more than 1 - 2 days.
Budget Required	Varies – dependent on how much in-house expertise is used, and whether expensive tools are required to facilitate the activity.
Skilled personnel Required	SMEs to act as the red team, as well as usual operational staff. In addition, staff for facilitation and data collection and analysis are required.
Training Required	Participants in the activity will require a level of red teaming induction to familiarise them with the activity. The red teaming facilitators and analytical staff should already be familiar with the techniques and analysis they are applying.
Comments	Can be conducted in conjunction with Field / Deployment exercises; are heavily front-loaded activities due to the preparation and design needs of the activity

Table 3F: Discussions / Tabletop exercises	
Number of personnel	Varies. Depends on whether a separate red and blue team are being used, and the number of agencies or functional areas within / across organisations are taking part. Requires staff to design the activity and write the scenario / background for the activity, as well as the guidance for the participants. The participant group should be as diverse as possible.
Perspective / Approach	Identifying vulnerabilities in current systems / processes. Can assign the red team to play both the adversary and perform the 'reality check' function for the blue team.
Relevant Analytical Methods	Collect information to address issues and contexts relevant to the agency(ies) /organisation(s). The full range of techniques can be used as long as they are tailored to suit the context and the aspects being investigated.
Resources Required	Physical space and the capability to collect and project the relevant information.
Time Required	*Preparation time:* Varies according to the complexity of the activity and underlying scenario and inputs. *Conduct*: Usually not more than 1 - 2 days.
Budget Required	Varies but should be minimal or only cover costs of bringing the participants together with the facilitation team.
Skilled personnel Required	Facilitator able to guide the red team in their activities and data collection staff able to capture information as it flows.
Training Required	Training (even brief) to ensure that staff are versed in the methods they

	can use, how to apply them correctly, and ways to ensure they have identified and addressed potential biases.
Comments	Can be conducted in conjunction with Field / Deployment exercises, Wargaming and individual critical analysis.

Table 3G: Critical Analysis	
Number of personnel	Individuals to small groups of up to 15 individuals
Perspective / Approach	Not dissimilar from Discussions/Tabletop exercises, these activities are on a smaller scale again. Often used for quick turnaround, rapid issue identification, and background preparation for larger or more resource intensive activities. The individual or small group acts as the alternative perspective to undertake the challenge role using a range of analytical techniques to provide structure and focus.
Relevant Analytical Methods	Any or all of the methods listed in the red team umbrella figure can be used for this activity, depending on the need. Should also use some form of checklist to identify whether biases and heuristics have been identified and addressed (or at least noted for subsequent use), and that analysis has been sufficiently critical.
Resources Required	Minimal – staff and the necessary information.
Time Required	*Preparation:* Minimal, other than gathering the necessary information for analysis. *Conduct*: Varies dependent on need and time available.
Budget Required	Minimal, primarily staff time
Skilled personnel Required	Dependent on the types of analytical methods being used; some are relatively simple to apply while others can be quite complex and require guidance or training to be applied correctly
Training Required	Training (even brief) to ensure that staff are versed in the methods they can use, how to apply them correctly, and ways to ensure they have identified and addressed potential biases.
Comments	Can be conducted in conjunction with Field / Deployment exercises

It can be seen in the tables above that there are many items listed as dependent on or varying according to the aim and scale of the activity. This, then, is one of the issues that those seeking to conduct red teaming need to be aware of. Identifying the aim of the activity should be a priority, followed by an analysis of what is required to achieve the aim. If the red teaming approach is then identified as appropriate to your needs, you should identify your resources, constraints and limitations in order to ascertain whether you can conduct an activity appropriate to your needs. This means that you can begin to manage expectations from senior personnel regarding the outcomes, or potentially justify a request for increased investment in the activity in order to enhance the value of the outcomes.

3.1.2 Scale and complexity

Two important aspects of red teaming are the *scale* and *complexity* of the activities themselves. While these are largely influenced by the aim (and the resulting questions that

need to be answered), personnel designing these activities need to manage both aspects carefully in order to ensure maximum return on investment. These two aspects are often closely related, since as an activity increases in size or scale, it frequently becomes more complex due to the sheer number of moving parts. There are many examples of small activities that are also complex, however, due to the nature of the issue(s) being addressed.

The red teaming umbrella in Figure 1 shows activities ranging from the most simple (individual analytical activities, potentially involving a single method) through to large scale, complex field deployment exercises, which can be a logistical nightmare when they involve (for example) hundreds of personnel, a large amount of equipment, and many interacting units/agencies/organisations in order to appropriately achieve the aim.[2] An example of a large scale, highly complex activity in the Australian national security arena is the Multi-Jurisdictional Exercises (MJEXs), four of which were conducted in Australia under the auspices of the Australia – New Zealand Counter Terrorism Committee (ANZCTC) exercise program between 2004 and 2010. These activities involved up to two years of planning, up to six of the eight Australian States and Territories, hundreds of agencies, thousands of personnel, and all the relevant equipment that these personnel require to perform their functions. For these activities, each State and Territory provided their aims and objectives to a coordinating body within the Attorney General's Department[3], who then assisted with the fine tuning of the objectives as well as the measures required to speak to those as part of an overarching evaluation strategy. Subordinate to these higher level ('strategic') jurisdictional objectives were the capability and agency objectives. These fed into the jurisdictional objectives, but could be measured independently and provided performance and process feedback to the capabilities and agencies to feed into their own capability development cycles. Due to the complexity of the scenarios such activities required in order to test the large number of objectives and different agencies, and the issues associated with large distances and time zone differences between the various jurisdictions, coordination of the various activities within these scenarios was complicated.

Conducting the activities was an important part of an overall strategy, however; testing individual components of a larger system serves a purpose, but there comes a time when the whole system must be put into play to test the spaces between the components – that is, their interoperability. It is often in the interoperability space where problems occur during multi-jurisdictional or multi-agency responses to incidents. It is critical to identify – preferably *prior* to a real-world incident and response requirement – whether there are any weaknesses in the ability of agencies to coordinate and cooperate effectively. This is where such large and unwieldly activities are targeted (in addition to being an opportunity to exercise the skills of individual capabilities).

---

[2] It should be noted that the umbrella is an overly simplistic means of representing the types of red teaming activities in that it does not show the potential for most of them to become large scale and complex. A decision was made to maintain the clean simplicity of this diagram for ease of use, and to discuss the issues of scale and complexity separately to allow red team practitioners to piece this information together themselves.

[3] The National Security Evaluation and Exercises Section of the Crisis Coordination Branch within the Attorney General's Department.

These types of activities - in which the performance of single capability or agency may be at least partially reliant on the performance of others with which they interact – become complex in terms of collecting performance data, and separating and analysing the effects of different variables or factors on the performance of each of the capabilities and their overall performance in managing an incident.

Red teaming such complex issues as these prior to the conduct of an activity can provide important information regarding the targeting of evaluations, and identify gaps or weaknesses that can be analysed to identify causes and potential remediation strategies. In an example activity conducted during 2014 (further details in section 6.1), a similar approach to this was used and found to be effective in helping response planners to determine remedial actions for performance issues during the conduct of the field deployment component. This was then followed by a subsequent red team discussion regarding performance, and the brainstorming of solutions led to changes to the approach of the participants to the problem for future activities. These changes were tested in a subsequent activity to ensure that they were effective in closing the identified gaps – and in not creating new ones as a side effect of their implementation.

It should also be noted that even simple single question analysis activities may become complex as a function of performing the analysis. The analytical process in itself tends to identify a broader range of related issues (particularly where the original issue represents a symptom and not an underlying problem or root cause). That is, when attempting to identify the root cause of a problem in order to design a solution, a series of contributing issues may be identified in the process. Each of these contributing issues may also require attention to ensure that the end solution truly remedies the problem.

Because the critical thinking involved in this broader application of red teaming does not limit red teamers to the perspective of an adversary alone, it is possible to identify a wider range of potential issues, gaps, weaknesses and threats – and mitigation strategies for these. This is an important aspect, as people not indigenous to a given culture or subset of the population may not be best placed to act as red team Subject Matter Experts (SMEs) in those domains. A more objective view of the threats and weaknesses is therefore a valuable means of ensuring that nothing relevant is excluded from consideration. This also means, however, that the number of individual (and combined) methods that can be applied to red teaming has increased substantially, and these methods originate from a variety of disciplines, including (but not limited to) psychology, systems dynamics, soft systems analysis, operations research, critical thinking and more. The red teaming methodology has become more akin to the intelligence analysis domain[4], and in fact (as shown in the Central Intelligence Agency (CIA) Tradecraft Primer) includes two varieties of red teaming subsets of the overarching set of techniques available for use.

[4] Intelligence analysis is a domain that also applies structured analysis techniques to help reduce bias.

3.2 Methods and activities suitable for red teaming

The two most valuable aspects of applying red teaming methods to exercises and other activities are that (1) they help to reduce bias for those involved, and (2) they bring analysis *into the activity itself*. This enables the development of immediate insights, and allows action to be taken much more quickly than relying solely on post-activity evaluation and analysis. This can be achieved via a number of different techniques (or combinations of techniques) and some of these are discussed below.

There are some fundamental techniques (or core methods) which underpin most of the detailed or resource intensive techniques used in red teaming. Appendix B shows a comparison of these, and where these core techniques form part of the broader methods. These core methods (depending on how they are applied) are all able to manage elements of bias to certain degrees. They are:

- Key assumptions check
- What if & counter arguments
- Quality of Information
- Brainstorming
- Visualisation

On their own, they provide a simple yet powerful set of tools which provide a red teaming questioning framework to any problem space. Coupled together, they allow a solid foundation to be built and – when used in a variety of combinations - can provide a tailored range of techniques for different types of scenarios and contexts. These techniques also form the backbone of the more in-depth, formal techniques, a selection of which is presented below. These all vary in scope, resource intensity, depth, and application which results in a useful range of options when tailoring techniques for detailed study spaces. These techniques are all from a range of related analytical domains, such as structured and intelligence analysis, judgment based Operations Research, and management science.

A range of available techniques which may be used in addition to the five core methods shown above are presented in Section Five ('Methods review').

4. Red teaming in a variety of contexts

This section addresses a series of issues, including the contexts for red teaming: those that are suitable, and those that are not. It also explores the purpose of the red teaming – what it is supposed to achieve will have a bearing on the scale and design of the activity. Key learnings from past non-traditional red teaming activities will be outlined, and issues around the design of tailored red teaming activities will be discussed.

4.1 Contexts for red teaming

There are a multitude of contexts in which red teaming may usefully be applied, but some of these require different methodologies to the previously understood "standard" mode of red teaming. This is why non-traditional red teaming methods have been developed and documented. Most of the Army's activities – particularly in terms of planning and analysis – are amenable to red teaming. In fact, red teaming (even in its simplest form, with two or more individuals challenging each other's perspectives) provides valuable clarity and assumption checking during any part of the decision making cycle.

The types of questions that may be addressed include (but are not limited to) the following examples:

- Understanding the factors underlying critical aspects of organisation, team or individual performance, and how these are impacted by changes in context or environment
- Anticipating developments in adversary capability and strategies, and the requirements for own plan changes or adaptations
- Training individuals or teams in specific activities, particularly those that are more effectively learned through deeper understanding
- Testing of established SOPs, arrangements, plans, strategies for organisations in response to particular incidents/events
    - The example used in this report will be the testing of the counter terrorism (CT) arrangements between two Australian states in response to information indicating a likely / imminent attack.
- Testing of new plans, procedures and tactics to identify gaps and issues, and implement immediate remedial actions.
    - An example here is the drafting of procedures for teams, units or departments within an organisation who wish to test the soundness of these documents prior to physical implementation of the procedures themselves.
- The test and retest of team, unit or organisation activities with a red teaming component to provide immediate analysis and feedback.
    - An example here is a combined field and discussion exercise, which allowed the provision of immediate expert feedback on activities. This could then be used to identify modifications to procedures to be integrated into procedures prior to subsequent activities.
- Testing the assumptions and information underlying reports and other documents
    - The relevant example here is the critical analysis of existing documents, particularly those dealing with future expectations.
- Comparison and testing of new organisational structures and COAs.

- An example is the change in unit structures of the military forces to enable better resource allocation for a broader range of missions and to meet Government directives.

There are many situations in which a full sized red teaming activity is not required, and presents too much of an impost in terms of the resources and effort needed to implement the activity. In these instances, there are alternative means to achieve these ends, such as exercising capabilities or skillsets or - in the case of smaller tasks that require unbiased analysis yet are too small to warrant a resource-intensive group effort – individual application of critical thinking and structured analytical techniques.

4.2 Purposes of red teaming

The purpose of each red teaming activity will vary. Using a broad taxonomy that was developed by Mateski (2004), the main purposes of Red Teaming could be listed in four main categories: (1) understanding, (2) anticipating, (3) testing or (4) training. These are described below.

1. **Understand**: In these activities the blue team attempts to understand the red team and how the red team perceives them. By understanding the red team, any existing biases or flaws can be exposed. One application of this type of activity is as part of the military intelligence gathering process.
2. **Anticipate**: Many Red Teaming activities, particularly military ones, are aimed at anticipating what the red team will do. Again, these activities involve viewing the scenario from the enemy's perspective and predicting what they would most likely do considering their motives, resources, and abilities. These activities, if done effectively, are able to reduce the likelihood of unanticipated actions, and contribute to the development of plans to reduce the impact should the red team act as anticipated. One application of this type of activity is as part of threat, risk or vulnerability assessment.
3. **Test**: Activities that involve testing systems usually build on previous understanding and anticipate activities. By testing a system with the Red Teaming method, the flaws or weaknesses are clearly exposed. In many cases it is not possible to expose weaknesses using any other method. By identifying weaknesses, it is possible to alter the systems (or procedures) in order to mitigate threats from adversaries. Common examples are war-gaming and security penetration tests. War-gaming involves testing strategies or tactics against an independent Red Team in order refine them prior to use on the battlefield. In the case of security penetration, weaknesses in security systems are exploited and exposed in a non-threatening environment so they can be mitigated before becoming a real-life issue.
4. **Train**: A Red Teaming training activity is designed to educate participants about how the Red team thinks or could potentially act. This may also involve training in response procedures for the red team's anticipated actions. An example of this type of activity is the TOPOFF (Top Officials) series of exercises in the US.

Mateski views these purposes as cumulative in that each process builds on the previous ones. For example, it is not possible to anticipate how the red team will act if one does not understand the red team. Furthermore, a firm understanding of the red team as well as being able to anticipate what they might do is essential to performing a test of current capabilities or systems.

In addition to the *purpose*, each activity can be classified as either *passive* or *active*. *Passive* activities do not actively play out situations in an experimental or operational environment, but instead involve understanding and anticipating the red team's actions. *Active* activities, on the other hand, are generally deployment based, and involve acting out situations as well as training. This passive (analytical/computational/simulation) versus active (physical) aspect has been included in Figure 1 (the red teaming umbrella), although it is not a clean continuum from passive to active: many of the activities involved in red teaming encompass both types of activity, although the degree to which they do so varies.

A conceptual framework was developed by Lauder (2009), who disapproved of using the building block approach of Mateski (2004). Within his conceptual framework, Red Teaming methods and techniques are based around the organisational processes of Innovation, Planning and Analysis, Training and Professional Development, and Operations, where each of those organisational processes can be conducted independently of each other. This framework is provided in Table 3, and examination of this shows that it in fact compliments that of Mateski (2004).

Table 4: The Red Teaming Framework of Lauder (2009) with Mateski's Taxonomy labels (2004)

Organisational Process	Description	Method Examples	*Mateski*
Innovation	For transformation of concepts, products, tactics, procedures or policies	- Peer review/critical analysis - Experimentation	*Understand*
Planning and Analysis	Plan design and development and predictive intelligence analysis	- Peer review/critical analysis - Alternative analysis (what ifs) - Team B approach - Devil's advocate - Advisory Role	*Anticipate*
Training and Professional Development	Individual and collective training, typically in an exercise environment	- Adversary role playing - Peer review/critical analysis of After Action review (AAR) - Advisory Role	*Train*

Operations	Assessment of live / operations activities in a cyber of physical setting	- Tiger teams - Ethical hacking - Peer review/critical analysis, attack the whiteboard	*Test*

While this provides some good initial guidance, the passive – active aspect of the red teaming still needs to be included, as this impacts the cost of activities in terms of time, resource and staff requirements.

4.3 Learning from past activities

Several lessons have been identified from recent red teaming activities conducted in both the military and national security domains, and these need to be shared to help prevent others repeating them wherever possible. The lessons are divided into key areas, as well as a general set of lessons that are applicable to most exercises or activities.

4.3.1 Preparation

The preparation phase is where much of the effort is spent for red teaming activities: ensuring that the right information, scenario, participants and support mechanisms are in place is key to ensuring the outcomes of these activities.

4.3.1.1 Begin planning with enough lead time

One of the commonly identified issues with activities or exercises is the amount of lead time required to properly design and plan one. While short or inadequate lead times are sometimes forced on planners due to circumstances beyond their control, adequate time for the preparation of the detailed red teaming plans must be allowed if the activity is to achieve its aim and objectives. Because red teaming is often a 'front-loaded' activity (where there is a degree of forecasting of participant responses occurring in order to ensure that adequate triggers are incorporated into the activity before it begins), personnel must have enough time to fully consider the depth and breadth of the issues being investigated during the activity. Having this degree of planning in place also provides a level of redundancy should the red team not perform according to expectations.

4.3.1.2 Participants: *The selection of an appropriately targeted and willing set of participants to act as the red team is important.*

The personnel required for a given activity will vary depending on the desired outcome and the concepts or systems being examined. Whatever the objective of the activity, however, the participants must be open to the red teaming concept and take part with the right frame of mind (open and curious rather than closed and defensive or aggressive). As

red teaming is a deeper examination of issues, often from a variety of perspectives, diversity of the red team members will foster the mitigation of biases and allow broad and potentially competing insights to be elicited. For activities such as a military or national security exercise testing existing SOPs or inter-State / agency arrangements, SMEs from each of the functional areas taking part in the activity should be selected based on seniority, as well as knowledge of and experience with the relevant SOPs and arrangements and how they work in a variety of contexts. Ideally, they will contribute to the design of the activity by (at least) reading through the planned activity and identifying where there may be scope for better triggers in the questioning or scenario injects (or both, if these are being used).

For red teaming of equipment prior to deployment, for example, it would be preferable to engage a selection of SMEs (in both the equipment and the deployed context), experts in design and construction of the equipment, as well as intelligent non-experts who may bring a fresh and unexpected perspective to the analysis as they do not have the biases that experts in the field tend to develop over time.

4.3.1.3 Selection of appropriate staff for all roles

There are many roles involved in preparing for and conducting activities and exercises, and each of these requires the right combination of personnel. Facilitators for discussion exercises (and any other activity requiring facilitation) will be discussed in the next subsection; however there are other equally important roles to be assigned. Exercise control personnel, activity/exercise writers and planners, those organising logistics, Workplace Health & Safety managers, blue team participants (if they are required), all need to be selected with the purpose of the activity in mind. As with the red team participants, they must also be willing to take part in order to have the best chance of fully engaging with the activity to ensure a quality product.

Staff – particularly those involved with writing and planning the activity – must be engaged early enough to provide time to fully understand the problem space and design the activity accordingly. The availability of staff can be a major issue, and requires support from senior management – which often relies on presenting the activity and its intended outcomes to them in a way that makes the benefits very clear.

4.3.1.4 Stakeholder buy-in

Another key aspect of successful red teaming is buy-in from stakeholder(s) - regardless of the actual outcome of the activity. This means that stakeholders are committed to truly investigating the potential issues as part of the activity, and are prepared to accept the findings rather than expecting findings to match a preconceived and preferred result. It is another prerequisite for the success of red teaming activities.

4.3.1.5 Planning for a reasonable intensity and duration of activity

One of the learnings from previous red teaming activities (including the facilitated discussion activities conducted as part of the Southern Intellection counter terrorism

exercise series, as well as a document and process analysis activity with Army) is that these activities are intense and require a large amount of energy. An intense day-long activity is very draining, and can leave the topics dealt with towards the end of the day somewhat lacking in depth as participants are too fatigued (both physically and mentally) to sustain the effort.

Similarly, underestimating the time required to adequately explore and discuss a topic is problematic, as it leaves participants feeling dissatisfied and may mean that critical aspects of the analysis are overlooked. For both of these issues, the scope of the activity needs to be carefully managed; a run-through of the activity (almost a dress rehearsal with the red team and writers / planners) can provide insight into the likely run time of the activity in its current state, allowing refinement and alterations to be made prior to formal conduct.

4.3.1.6 Selection of appropriate locations.

Locations must be selected to suit the requirements of the activity (the decision will need to be made once the activity has been designed in order to cater for the differing physical layouts of various activities). The availability of supporting resources such as communications tools and live audio/video feed links should also be considered when conducting a facilitated red teaming discussion activity with separated red and blue teams.

4.3.2 Facilitators

Some red teaming activities do not require facilitators – for example, the small scale activities which involve critical thinking or analytical techniques being applied by one or two people. However, once a group is involved, and there is a requirement to exchange views and probe issues, a facilitator is an excellent addition to the team. In fact, a good facilitator can make a red teaming activity produce meaningful outcomes, while less able facilitators can stifle discussions and result in a distinct lack of insight or outcomes of any utility. The role should enable a facilitated engagement approach, where participants are encouraged to engage with the problem at hand and drill into the critical details of issues identified and means of solving those issues.

Facilitators of group activities in general have several common characteristics, such as: the ability to stimulate interaction and the free sharing of ideas through honest dialogue; excellent listening, observation and speaking skills; the ability to remain impartial during discussions; and sensitivity to culture, gender issues and any power dynamics in the group (Omni, 2000). Facilitation for red teaming activities must be frank and fearless, and willing to encourage participants to critically discuss aspects they may be reluctant to address regardless of rank or position within the organisation. Facilitators for this type of activity should be prepared to ask 'what if' questions and inject prompts where required to draw out the depth of participants' knowledge about the subject matter. In addition to these skills, they must be able to keep the discussion to time, and keep the participants engaged even when they are not directly involved in the discussion.

For some red teaming activities conducted previously in the national security space (see Kardos et al., 2014; Kardos and Hanly, 2012), the workload for a single facilitator was found to be too high due to the context and structure of the activity. For these activities, co-facilitation was found to be an excellent arrangement. This was particularly true for cases where incoming external information was being fed into discussions (e.g. activities with both a blue team and a physically separate red team in play), or where a facilitator is highly skilled in the facilitation aspect but is not a domain expert (or vice versa). It allows the primary facilitator to focus on the discussions and where injects from the red team may be required, while the co-facilitator acts as the conduit between the red team and the primary facilitator, as well as keeping track of participants' discussions, feeding red team injects to the primary facilitator, and noting key outcomes /items that occur during discussions for follow-up. The co-facilitator may simply play the role of asking the deeper probe questions to follow up a line of questioning initiated by a non-domain-expert facilitator.

The facilitators' goal is to maintain a relatively smooth flow of discussions so that participants work through the material in a sensible order, while exploring the issues identified in reasonable depth. This helps to keep participants focused and aids their ability to think clearly about the topic at hand.

4.3.3 Blue team

The blue team must be prepared for the type of activity being conducted, and full knowledge of what to expect (and the guidelines for such activities) will assist with this. That is, it is *intended* to be an activity that challenges assumptions, and may cause discomfort when discussions become focused on specific areas and probe answers already provided. As in the red teaming ground rules in section 4.3.5 below, participants need to avoid taking challenges as personal attacks in order for red teaming to proceed effectively. The entire aim is to step outside the realm of the assumed and identify real life conditions, problems and outcomes.

Selection of appropriate personnel for the blue team is driven by the type of activity and the questions being answered. For example, to test existing SOPs or arrangements, blue team personnel need to have enough knowledge and experience to reflect the way business is currently conducted (remembering that red teaming is not a test of the individual, it is probing the concepts and processes). Red teaming equipment prior to field deployment would place more emphasis on the red team (which might be made up of technical experts, the client purchasing the equipment, experts in contributing fields [e.g. electronics, mechanical engineering, etc.], and potentially an educated/trained individual who is naïve of the equipment itself to provide a completely objective view), while the blue team would likely be designers/manufacturers of the equipment. Some activities may not require a blue team at all, for example when individual critical analysis or a small number of people are red teaming a concept or document.

Because the questions to be answered drive the design of the activity, it is critical to identify these prior to selecting the blue (and red) team members.

4.3.4 Red team

As previously mentioned, the composition depends on questions need to be answered, and what the activity needs to achieve.

A red team can be defined as any team that has been designed to anticipate, understand, or test processes or products – whether or not this involves a blue team. This red team can take a variety of forms, which will be largely driven by processes or products being analysed. The composition of a red team will be influenced by both the aim of the activity and the type of red teaming method used. Additionally, the recruitment of the right people for the role will have a significant influence on the success of this type of activity (Malec et al., 2012).

The actual red teaming process used depends on the risks associated with the system or product being tested. For example in some cyber exercise activities, it would be acceptable to hack a security system, while in others a simulated system is preferable due to potential consequences of an actual security breach.

The level of interaction with blue during an activity or exercise will also be determined by the type of activity being conducted: that is, there may be a direct interaction with a blue team, or interaction via an exercise facilitator. Some activities, such as peer review or document reviews, do not require a blue team *per se*.

The roles played by experts in discussion-based exercises are another example of a red team. Here, SMEs can critically analyse plans or procedures to find existing faults or weaknesses, and provide challenges to blue team responses to questions. This analysis can be used to provoke discussion between the client and SMEs to identify different ways to view plans/procedures, and to allow the identification of gaps or issues that may otherwise have gone overlooked.

4.3.5 Red teaming ground rules for all participants

In order for the larger scale red teaming activities to function correctly and produce meaningful outcomes, the basic ground rules outlined here must be applied to both red and blue team participants wherever possible. That is, they should be applied regardless of the level of challenge presented during red teaming (from critical analysis type activities through to the more formally adversarial-style activities involving both a red and blue team). In the adversarial context, the ground rules relating to interpersonal interactions and the attitudes of participants are crucial to success.

The participants should be asked to observe the following ground rules as a means to effectively achieve the aim of the activity.

General conduct. The activity and methods are intended to elicit challenges and innovation in terms of processes; to achieve this, participants need to apply the

appropriate behaviours to the activity. Success is best achieved during red teaming activities such as this when participants do the following:

- Avoid taking comments, questions and challenges as personal attacks: remember, this is a challenge of the processes/plans/SOPs, not individual performance
- Question everything
- Avoid framing comments, questions and challenges in the form of personal attacks

Inappropriate Phrases. There are several phrases that should not be used during red teaming activities, as they do not support effective critical analysis of materials (e.g. processes, plans, etc.) or ideas. These include:

- "That will never happen"
- "That's not how we do things"
- "We've always done it this way"
- Any variant of 'because I said so'

These are phrases that will stall the critical analysis process because they do not allow the red team to freely consider all the alternatives and - in the worst case - lock the red team into supporting the viewpoint of a single individual with no recourse to in-depth discussion.

Subject Matter Experts. Past learning and experience should not be ignored; but experiential knowledge *should* be examined at a basic level so that it's applicability to other contexts can be understood. That is, successful past actions may be successful again – in the right context. Additionally, as previously noted, expertise is not a guarantee against cognitive bias – thus contextualised understanding of the implications of an expert red team member response is important.

Deference to Authority/Rank. To gain maximum benefit from activities such as this, individual rank should not impact on the process. That is, personnel of all ranks need to be free to put forward and challenge ideas, choices, and reasoning without fear of retribution. Mutual respect is key, as is an understanding that during this activity the emphasis is on the use of evidence and sound reasoning in critically analysing processes and options.

Recording Information. Participants need to remember that not every heuristic or assumption is necessarily bad, however each one should be identified and recorded (where possible) to allow an audit trail of reasoning underlying decisions, and analysis of the validity of the assumption(s).

4.3.6 Cultural issues

It should be noted here that, while red teaming encourages free discussion and expression of questions and ideas – which relies on a conducive atmosphere that supports free speech

and encourages commanders and higher ranking officers in military and policing arenas to discuss issues with their subordinates – this may also be somewhat problematic. The cultures in hierarchical organisations (particularly the military and para-military) often dictate that the commander does not discuss problems with or ask the opinions of his subordinates. Where this is a firmly entrenched belief, to do so may foster a perception of indecisiveness or weakness from subordinates about their higher ranked officers. Currently, this is an issue which has been observed anecdotally, but further research is warranted in this area to ensure that the benefits of red teaming can be gained without sacrificing other important aspects of team/organisational functioning.

Non face-to-face methods such as Delphi have been used in DST Group and other organisations as a method through which to potentially mitigate some of these hierarchical issues (Pincombe et. al., 2013 & Winkler & Moser, 2016). The benefit of this technique is that the anonymity allows all participants to openly and freely express their contributions without fear of reprisal or social status effects. The added benefit is that all valid ideas are captured and equally weighted, valued, and considered rather than just those ideas from individuals with the loudest voices or greatest rank / status in the room.

5. Methods review

This section examines the available and useful methods that can be applied to achieve red teaming aims. There are five core analytical methods that provide robustness, validity and rigour to red teaming processes and these will be discussed briefly here. Additional, more detailed methods will then be listed, along with a brief description and useful references, so that personnel interested in using these can explore them further.

5.1 Key assumptions check

- Helps explain the logic of an argument and expose faulty logic/data. Forms the cornerstone of the other analyses.
- Understand the key factors of an issue
- Stimulate thinking
- Identify developments that challenge assumptions
- Prepare for changes which could surprise.

Three key definitions:

Key assumption is any hypothesis or statement that is accepted to be true. Assumptions guide an interpretation of evidence and reasoning about a problem and are usually taken for granted.

Judgements highlight the most significant analytic points. They include facts and analysis and convey meaning or purpose. They often use the word *because*. They are still an interpretation.

Assessments are judgements about unknowns.

Method:
List the key working assumptions on which arguments rest. Include all assumptions, judgements and assessments. Assess any diagrams for assumptions. Do not include facts and statements. Articulate them all in writing.

Then question each assumption in turn:

- Why am I confident that this assumption is correct? What is the research, references, evidence? What are the trends and why are they valid?
- What circumstances or information may undermine this assumption? When might it be untrue? What is the impact of this?
- Is a key assumption more likely a key uncertainty or key factor?
- Is it time-sensitive? Could it have been true in the past, and not now or in the future?
- If the assumption proves to be wrong, how would it impact the argument?
- Has this process identified new factors that need further analysis?

Refine the assumptions to three categories:

- Those that are solid and well supported to sustain the argument.
- Correct with caveats – make corrections.
- Unsupported/questionable – key uncertainties: Remove those that are faulty and assess if the argument requires new evidence or development. Acknowledge and manage key uncertainties.

Take any new factors and undertake analysis to build them into the argument or work the new argument into the concept. If necessary, change the concept given the new arguments.

5.2 What if & counter arguments

What if? Scenarios often follow on from the Key Assumption Checks but can also be used independently to test scenarios or arguments.

This assumes that an event has occurred with potential (negative or positive) impact and explains how it might come about. This is a technique for challenging that an event will not happen or that a forecast may not be entirely justified.

By changing the perspective from whether an event could occur to how it may actually happen, the analysis focuses on what events (however unlikely) might allow such outcomes.

Method:

- With the list of assumptions, judgements and assessments use brainstorming and creative thinking to generate a list of what if questions and counter arguments.
- Identify one or more plausible pathways or scenarios to an unlikely event; very often more than one will appear possible.
- Assess each new possibility and document how the original assumption / judgement /assessment and argument holds up under the new conditions.

5.3 Quality of information

The quality of information used in any study is a fundamental factor in the quality of its outcomes. Hence the commonly used saying "Garbage in – Garbage out".

Quality of information is critical to the confidence in the product

- All information needs to be checked for veracity and validity
- Sources need to be checked that multiple references are not all using the one source of information
- Argument judgements need to be checked against competing sources which might provide contrary judgements. Competing views should be articulated or at least noted and explained why they are not used.
- This all needs to be kept in a database/ tracking system and revisited regularly.

Trend information and markers of change to those trends need to be identified – especially if they form key assumptions.

5.4 Brainstorming

There are many techniques which can be used for brainstorming. At its simplest it involves the analysts or participants free reign in both creative and critical thinking to produce a "dump" of all possible related ideas. There are several structured techniques which can be used to facilitate and guide various brainstorming methods. These structured techniques can help manage bias within the study. These include:

- Structured Brainstorming
- Virtual Brainstorming
- Nominal Group Technique
- Critical thinking

- the Delphi method.

Some common key characteristics to all methods of brainstorming include:

- specific goals and focus of the brainstorming
- providing the goals and focus and context to the participants beforehand
- all ideas have merit and should not be criticised
- if face to face methods are used, only allow one speaker at a time (else remote contributions using Delphi or group computer input sessions are valuable)
- if face to face methods are used, allow participants silent time to digest and individually generate more input (multi round Delphi's provide this function remotely)
- allow sufficient time to undertake brainstorming. It can take hours for a session to start to generate and capture creative ideas. Do not underestimate the time and resource intensiveness of this process.
- Prepare for data capture methods if face to face (this is where the Delphi and group computer capture processes are invaluable). Sticky notes and note takers are a good way to do this.
- Two phases (depending on the outcomes required) can be used : *creative thinking phase* to capture all ideas and an *analytic phase* to assess and evaluate the ideas. Clustering of ideas tends to occur in the second phase and can lead to other red teaming techniques for deeper analysis.
- Ensure the participant group is as broad as possible. The inclusion of those from outside an area are valuable in providing different perspectives and also help avoid "group think".
- Summarise all the key findings and outcomes and circulate these to the group at a later time to ensure that interpretations and information is not missing. Any last ideas can also be captured at this time.

5.5 Visualisation

Like brainstorming above, there are many varied techniques for visualising problem spaces. These vary from being as simple as a basic diagram of the key aspects of a context space through to full analytical concept and argument maps or social network analysis representations. The level of visualisation for each context space will vary and may not be appropriate in some areas. However, in most cases, some level of visualisation may assist in organising complex knowledge/information and identifying previously unforeseen information which is not readily sourced from a text based analysis. The main techniques of use in visualisation are

- basic diagrams or mind maps
- context or concept maps

- relationship diagrams
- influence diagrams
- argument maps
- network analysis including social network analysis
- chronologies and timelines
- process maps and Gantt charts.

Indeed there are also techniques such as **matrices** and **Venn diagrams** which can be used for visualising a problem or context space. Specific details on each technique can be easily sourced for further detail.

Some common key characteristics to all methods of visualisation include:

- specific focus and context of the visualisation
- source of input data identified and rated for quality
- identification of the key concepts or items (depending on the context and which kind of visualisation is being applied)
- linking or representation of the concepts and their connectedness

5.6 More detailed techniques

The techniques presented below in Figure 2 are all additional methods to those in the basic toolbox above which can be applied to different problem spaces in order to both understand and challenge the concepts and contexts. Some are repeated from the previous section due to their applicability in a broad range of areas. For example, Delphi is mentioned above as a technique to help with brainstorming, but its application is much broader and can be applied to data capture and challenge analysis across the entire Red teaming space.

Note that several can overlap into several of these groupings provided below. The groupings are purely for clarity and to give a focus of different techniques and where they have been applied analytically.

Some of these techniques are specifically for determining a certain kind of information and others are methods which enable a range of information to be gathered. They all are able to manage some elements of bias to certain degrees. They all have differing ranges of intensity and resource usage which would be required depending on the problem space. The range of techniques applied to a range of red team participants will determine the degree of success in bias management.

Figure 2 represents the detailed methods in a visual structured representation of where they are likely to be best focussed when designing an activity for a new problem space. That is not to say that they aren't useful or couldn't be applied in the other areas, this is

purely where they are likely to have the greatest impact and have been applied analytically. This also provides a starting point for deciding which techniques might be of use initially in design of an activity requiring more than the basic toolbox. It is important to note that the critical thinking aspect (listed in Figure 2 below as an enabling technique) involved in this broader use of red teaming means that, by not limiting themselves to the viewpoint of a single adversary (whose perspective may not be well represented by persons not indigenous to that culture), participants can identify a much wider range of potential issues, gaps and weaknesses and mitigation strategies for these. Ideally, critical thinking is coupled with other techniques to sample broader perspectives; alternatively, choosing a broad participant base (in terms of knowledge, skills and backgrounds) provides robust insights from multiple lenses and viewpoints.

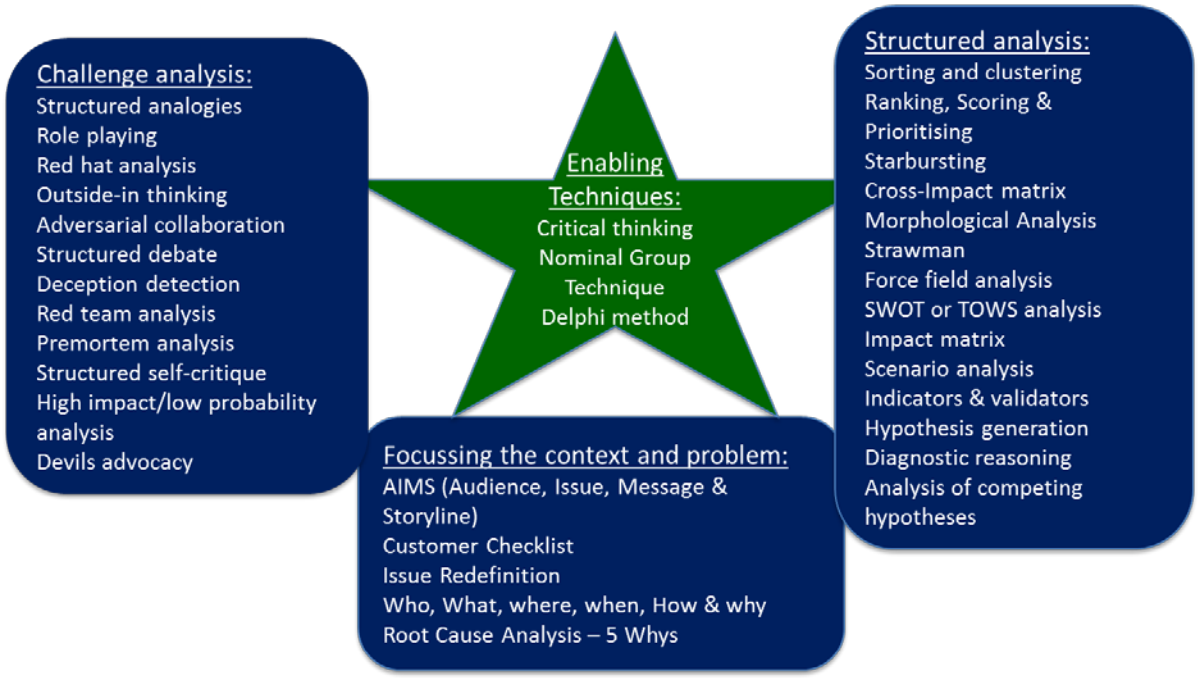

Figure 2: This figure represents where some of the more structured analytical techniques of use in red teaming are best focussed to provide quick selection of useful techniques beyond the basic toolbox.

There are many other techniques from a variety of domains which may have application to red teaming. A review of techniques and a mapping of several of the detailed and core techniques above (as well as some techniques from other domains) can be found in Appendices B and C; it shows their overlapping and often resource intensive nature compared with the core methods. Additionally, the need to tailor methods to the problem space and manage bias, along with the use of the challenge approach, means that many techniques are not amenable to certain problem contexts.

5.7 Validity of techniques and outcomes

The various techniques used in many red teaming activities are well established methods from a variety of domains. As such, all have well established applications and external application validity in the literature (Heuer and Pherson, 2015). However, when undertaking any activity, it is important to ensure that the methods employed will indeed generate the required output from that activity. For example, when undertaking a survey based data collection activity (such as a Delphi process) it is important to run a face validity test first to ensure that the questioning mechanism both delivers the required output and can be understood clearly by the participants. In face to face or small group workshop contexts, a similar process can be followed by having a third party check over and question your facilitation plans. In large multi scale events the plans and processes can and should be checked by someone who is not directly involved to ensure the validity of the process is upheld.

In this section, a variety of methods and techniques suitable for different contexts of red teaming have been outlined and discussed. In order to keep the size of this document manageable, the level of detail provided is relatively basic – however, there are resources freely available to readers who wish to follow up any of the listed techniques. The resource-intensiveness of the various techniques differs, and the utility of each technique for different red teaming contexts varies. It is therefore important to understand what is required of the activity (the key question to be answered), and which of the techniques can provide this outcome based on the resources and time available, and the level of detail needed. These issues will be discussed in more detail in the next section.

6. Designing a tailored red teaming activity

This section examines the design of red teaming activities, beginning with the identification of whether a question in fact requires the red teaming approach. The design of activities driven by the requirements (what is the desired outcome, what needs to be achieved) and taking into consideration any limiting factors (such as resources) is critical for the conduct of a successful activity. Several examples of successful red teaming activities are provided to assist with individuals' understanding of these concepts and how flexible (or 'tailorable') the red teaming arrangements can be.

Activity design is often complicated by several factors, with the four most common being the availability of the required personnel, facilities, equipment, and funding. For this reason, one of the most important issues to address prior to beginning is the top level (management/high-ranking officer) support for the activity and its outcomes. This helps to ensure that those four key elements will be available for the activity (within the limits of feasibility, of course; operational requirements will always be the priority).

As part of the planning process, then, the type and scale of the activity must be considered in relation to both the questions to be answered and the outcomes required. While red teaming methods are extremely effective, they can also be time and resource intensive in

terms of planning (and sometimes conduct, depending on the type of activity chosen). Red teaming often sees front loading of effort, with the preparation being more complex and effortful than the conduct in many cases.

It is therefore important to identify whether red teaming methods are fit for the current purpose, or whether alternative methods are preferable. Section 6.1 is designed to assist with the decision process regarding the need for red teaming, and the selection of the appropriate red teaming method(s).

6.1 Planning for best effect

This section contains a diagram which maps out the considerations required to effectively choose an exercise or activity, particularly when a choice is to be made between red teaming and non-red teaming types of activities.

Prior to the beginning the formal planning phase, the key requirements of the activity should be decided. That is:

- What is the aim
- What is the focus (the major area/aspect of interest)
- What are the objectives
- What outcome(s) are required.

Once these are articulated, the suitable range of activities will become narrower. Once key aspects such as what is available in terms of personnel, funding, facilities and equipment have been identified, a final choice of method (or methods, if combining more than one) can be made.

Ideally, the design of every activity is driven by the aim and objectives – this ensures that resources (funds, personnel hours, consumables, etc.) are expended in the way most appropriate for achieving the outcome. This is particularly important in any context where demonstrating value for money is required in order to justify spending ever shrinking budgets on such activities.

Figure 3 outlines a process for choosing the broad methods (illustrated in Figure 1) required to meet the aim and objectives of an activity, and assists with identifying whether red teaming is suitable for the stated purpose. If red teaming has been identified as a suitable tool for the activity, the underlying questions may require the selection of several individual methodologies and the combination of these to provide a deeper analysis of underlying issues.

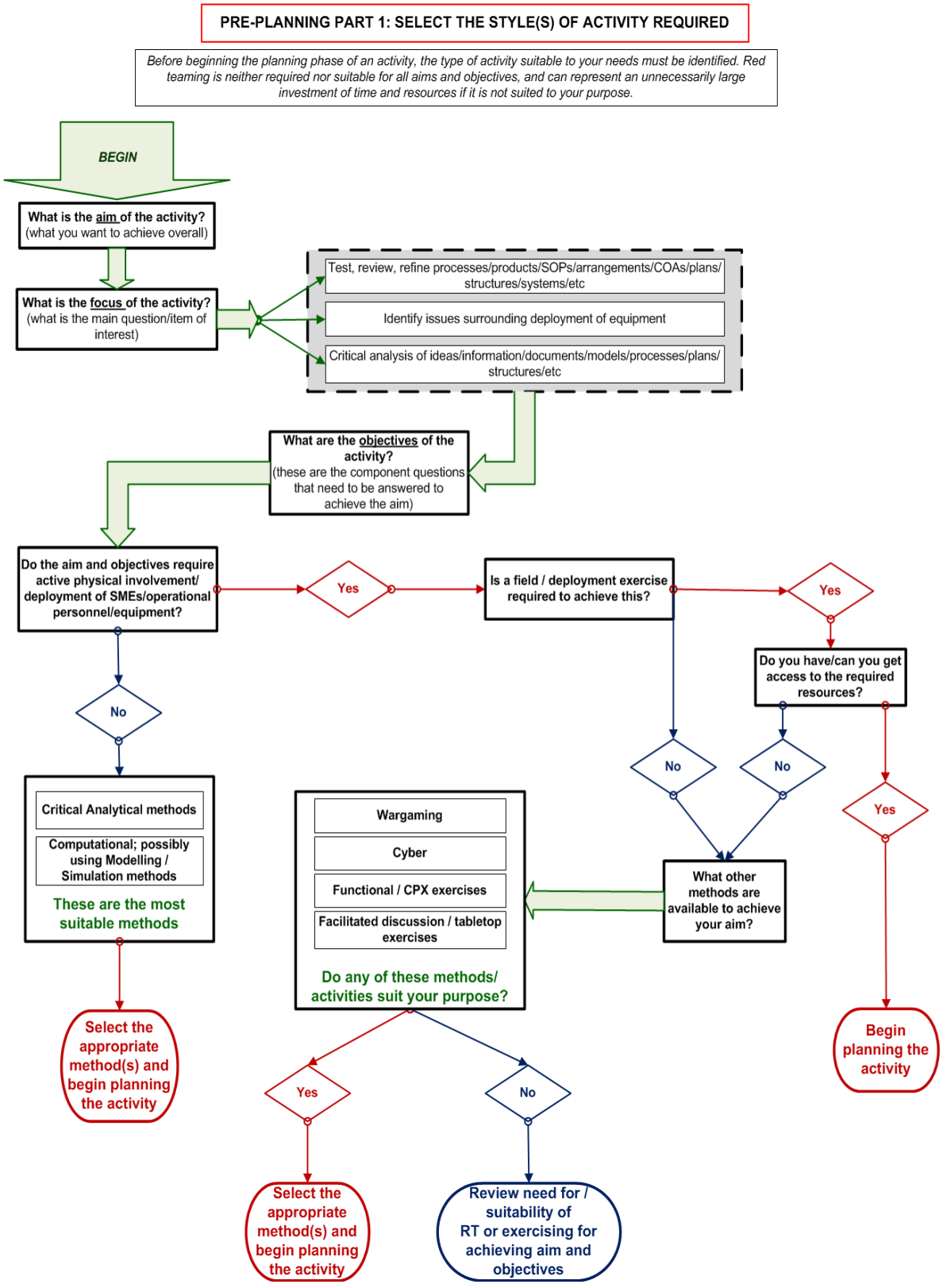

Figure 3: Flowchart of the pre-planning decision processes assisting with choice of activity type

6.2 Example Red Teaming applications

There are various ways that RT activities can be structured, from very simple and short to much longer and more involved. Here we present several examples of both simple and more complex RT activities: your choices of methods will be determined to some extent by both the resources you have available (personnel and time, in particular) and the requirements of your particular issue/question.

6.2.1.1 National Security exercises

Exercise Southern Intellection was an ANZCTC national security exercise program activity designed to test existing counter terrorism arrangements (in the arena of Prevention[5]) between Victoria and Tasmania where a set of potentially terrorism related activities spanned multiple States. It was conducted as a series of three activities, each with a different focus (i.e. #1 - Intelligence, #2 - Investigation and #3 – Disruption). The activity was also intended to field and evaluate the utility of the red teaming methodology in this exercise context, with the method being refined based on the lessons and feedback gained in each activity.

Each activity comprised of a facilitated discussion exercise which ran for one full day, and then a day of follow-up activities involving (a) a debrief from the previous day's activity, (b) listing identified issues from all the evaluators and observers, and allowing all exercise participants to brainstorm potential solutions, and (c) presentations on case studies from prior real world operations.

The Blue team comprised experienced personnel from all of the relevant agencies (policing and intelligence), with the red team comprising more senior individuals from these agencies who also had extensive operational experience. The blue and red teams were located in adjacent rooms, to avoid any imposition of hierarchy issues on blue team functioning. The red team did, however, have a live audio-visual feed of the activities in the blue team room so that they could immediately analyse responses and inject questions where required.

The basic program for the discussion exercise activities were shown below:

0830 – 0900 Welcome and introductory briefing
0900 – 1030 Session One
1030 – 1045 Morning Tea
1045 – 1230 Session Two
1230 – 1300 Lunch
1300 – 1515 Session Three
1515 – 1530 Afternoon Tea
1530 – 1630 Hot Debrief

The first Introductory Briefing involved set the scene for the activity and provided enough background information for the participants to situate their understanding for the coming

[5] Using the PPRR model from the national security arena: Prepare, Prevent, Respond, Recover.

days' discussions. Each of the sessions involved several Special Ideas, each of which was a subsection of the primary overarching topic, and was associated with a series of predetermined facilitator questions along with focus areas for the red team. The blue team were given the special idea to discuss and deliberate on in their agency or functional groupings, and they were then required to brief back to the room regarding their answers. During this time, the red team identified key issues and questions to challenge the blue team, and these were injected at the appropriate point in the discussions by the facilitator.

Example setups for these types of activities include:

Day 1: RT Activity across the entire day
Day 2 AM: Review outcomes and identify gaps and insights for participants to take away
DAY 2 PM: Presentation of case studies

This setup is useful if you're happy to take away identified issues/gaps and develop solutions with management chain or Officer in Command (OIC) of an area, with the added benefit of the operational learnings of others to take away.

Day 1: RT Activity across the entire day
Day 2 AM: Review outcomes and identify gaps and insights
DAY 2 PM: Brainstorm solutions for gaps and RT those

This setup is useful if you want to have solutions developed prior to the end of the activity and have some analysis already done on them to present to management chain/OIC of an area.

Exercise Duplo Alpha was also an ANZCTC national security exercise program activity which incorporated both military and civilian aspects and was designed to examine the extant arrangements for managing active armed offender scenarios on military bases, and the relationships and interactions between the military and civilian responders in these scenarios.

This activity represented a somewhat more immediate usage of the outcomes of red teaming. Here, the red teaming discussion activity was conducted as a review of the field deployment conducted earlier in the day, and became a means of identifying key issues from that performance so that commanders and other participants could modify their responses to the scenario during the second run through of the activity. This provided immediate testing of any new procedures and tactics proposed as solutions to previously identified problems.

6.2.1.2 Military exercises and activities

The *Future Land Warfare Report (FLWR) Red Teaming activity* was designed to identify and evaluate the methodology underlying the development of the Future Land Warfare Report. It did not require a red and blue team, rather the approach was to gather all available information regarding the methodology prior to the activity, include individuals (where possible) who had experience with developing the FLWR in previous years, identify existing and potential new methods for developing the FLWR.

The activity was conducted over two days: the first involved the identification of the key aspects of the FLWR, examine the processes that contributed to its development, and identify potential new systematic means to achieve a high quality FLWR output in future.

Day 1 involved:

1. Introduction to the activity and its objectives
2. FLWR development process: Identification of the intent of the document and the processes used to develop it
3. Examine the processes that identified the meta trends around which the report is based, the intent of the report, and whether it achieved this intent
4. Review and analysis of the meta trends in FLWR 14
5. Systematic examination of the meta trends for key issues and assumptions
6. Brainstorming new FLWR development processes (in two teams)
7. Red Teaming proposed FLWR development processes
8. Wrap up session, participant immediate feedback (positive and negative).

Day 2 involved:

1. Review of the activity process and key outcomes; deployment of participant feedback surveys to gather feedback regarding the activity.

The *Command, Control and Communications/Intelligence, Surveillance and Reconnaissance (C3/ISR) Red Teaming Activity* was focussed on testing future models of C3/ISR and to assess their validity.

Day 1 involved

1. Activity briefing and guidance
2. Content Briefing on the models
3. Key assumption checks using guiding questions with participants and models split into functional groups
4. Development of internal vignettes
5. Structured Brainstorming Activity for each model fragment and group to prioritise key questions and scenario dimensions
6. Group feedback for other groups to discuss and challenge
7. Focused brainstorming regarding the impacts of technology insertions.

Day 2 involved:

1. Review of the updated models based on the Day 1 outcomes

2. "What if?" analysis - Develop scenarios/vignettes in groups to determine where the model breaks.

A Delphi was run following the face to face activities to capture the information which was not captured during the activity due to time constraints.

The *Building On Army Initiatives (BoAI) series of Land Analytical Decision Support Studies (LADS)* were a series of studies testing and exploring issues and structural models in different areas of the Army.

BoAI 1 - 2 Division (DIV) transformation

Day 1 involved briefing on two options (termed Left arc and Right arc), the scope of the transformation, and its terms-of-reference, and undertook a data and mission analysis discussion. This was conducted by the 2DIV transformation team.

Day 2 involved:

Non-traditional red teaming activity

1. Briefing on the red teaming activity
2. Session 1 Left ARC model – Structured Brainstorming for pros, cons, issues & assumption elicitation
3. Session 2 Right ARC model – Structured Brainstorming for pros, cons, issues & assumption elicitation

Day 3 involved:

Non-traditional red teaming activity

1. Exploration of three priority areas using guided brainstorming and facilitation.

The incorporation of the 2DIV Brigades as the red team ensured that they had the opportunity to buy in to the transformation process and be a part of its outcomes and challenges.

BoAI 2 - Raw data to support extension for the 3 Battle Group (BG) problem

A mini Delphi was conducted to source issues and challenge the current model in order to provide the supporting context for a proposal to decision makers

BoAI 3 - Generating Enabler Mass

Activity 1: Day 1 – 6Bde, Day 2 – 17 Bde

1. Briefing on the activity and the pre-identified issues from an earlier major exercise activity

2. Facilitated workshop using structured brainstorming to capture issues and assumptions, identifying missing elements, constraints, hollowness
3. Capture relationships between enablers and combat brigades

Activity 2:

1. ½ day option generation workshop. SMEs and client briefed on the problem and ground rules.
2. Guided structured brainstorming used to collate and capture all participant solutions and ideas.

Activity 3: *Testing options*

Test the generated options using syndicate teams to critically analyse their viability and associated issues. This activity was delivered by survey across three days at the major Army annual experimentation exercise.

7. Training for personnel wanting to undertake red teaming

This section touches on the issue of training for personnel embarking on red teaming activities. It discusses the utility of training in order to provide background for the organisers and participants in these activities, and provides links to several different red team training resources.

A short training activity to give personnel a brief grounding in the concepts of cognitive heuristics and biases, how these impact on decisions, and what can be done to counter/mitigate them (i.e. the methods for red teaming activities) is a very valuable exercise. It enables participants to take on the red teaming activity with at least a basic understanding of the underlying basis for applying the methodology.

Below is one example of a short training workshop provided to Army prior to a red teaming activity focusing on the Future Land Warfare Report (FLWR). The aim of the activity was to analyse the document, the information on which it was based and any analysis used to derive conclusions. Consistent with good practice in learning activities, the theory and background information was presented, along with some guidance on the methodologies available for use. Hands-on practice with selected methodologies was then provided, which cements learning and provides clarity on the application of the methods by the participants. This was then followed (on a separate day) by the actual red teaming of the FLWR document and its underlying foundations.

The training workshop timetable was a follows:

0840 – 0900 Arrival & Coffee
0900 – 0910 Welcome and Introduction
0910 – 0945 Cognitive Biases & Heuristics
0945 – 1045 Red Teaming Methods Part 1 – Introduction to methods
1045 – 1100 *Morning Tea*
1100 – 1230 Red Teaming Methods Part 2 – Application (hands on practice)
1230 – 1315 *Lunch*
1315 – 1415 Red Teaming Methods Part 2 – Application (continued)
1415 – 1430 Workshop wrap-up and Feedback

The three key sessions in this training program are described below.

Cognitive biases and heuristics - This session covers introductory basics of biases and heuristics so that participants gain a better understanding of how they work and why they are a problem. Those most relevant to the focus of the next activity (the red teaming of the 2014 report) were presented in more depth, with some examples and explanation of how they operate to impact on decisions and reasoning. The need to mitigate these is addressed, and the relevance of red teaming as a mitigation strategy is also explained.

Red Teaming Methods Part 1 – Introduction to methods - Again, the focus is on the methods that are useful for the creation of the report in terms of their value in helping individuals overcome particular mindsets and habits in their way of thinking. The methods also enable group exploration and analysis of issues while avoiding the groupthink problem.

Red Teaming Methods Part 2 – Application (hands-on practice) -This session focuses on helping the participants to apply the methods they have just learned to perform analysis on an example report. In two teams, they are given 2.5 hours to identify specific issues, analyse and discuss these amongst themselves, put together a short briefing on their findings, and brief back to the other team. The other team is then tasked with playing devil's advocate and probing the conclusions and identified issues for veracity and to identify any further issues that could have been explored. This provides the participants with both the analytical practice and exposure to the red teaming style of discussion and analysis.

There are many different training courses available for red teaming methods, as shown by the sample in Table 5 below.

Table 5: A sample of the red team training courses available as in-person or online offerings

Name	Provider & Link	Length	Location	Focus
Red Teaming	http://usacac.army.mil/organizations/ufmcs-red-teaming University of Foreign Military	2 days to 18 weeks, dependin	Fort Leavenworth USA	Red teaming for the military including RT

	and Cultural Studies (UFMCS), USA Army http://usacac.army.mil/sites/default/files/documents/ufmcs/UFMCS_Information_Brochure.pdf	g on the course chosen		leaders course, RT members, Critical Thinking, RT hybrid/mobile course
Black Hat USA 2016: Adaptive Red Team Tactics	https://www.blackhat.com/us-16/training/adaptive-red-team-tactics.html Veris Group's Adaptive Threat Division	2 days	Las Vegas, USA	Cyber threats
Black Hat 2015: Advanced Open Source Intelligence Techniques	https://www.blackhat.com/us-16/training/advanced-open-source-intelligence-osint-techniques.html Michael Bazzell	2 days	Las Vegas, USA	Cyber threats
Black Hat 2013: Red Teaming Training	https://www.blackhat.com/us-13/training/red-team-training.html Iftach Ian Amit & Chris Nickerson	2 days	Las Vegas, USA	Physical, social and electronic attacks
Red Team Training	https://chameleonassociates.com/hosted-training/red-team-training/ Chameleon Associates	-	California, Netherlands, NSW Australia, Singapore	Red teaming of security issues for remediation
Red Team Training; The IDART methodology; Red Team Metrics	http://idart.sandia.gov/training/RT4PM.html http://idart.sandia.gov/training/IDART.html http://idart.sandia.gov/training/Metrics.html Sandia National Laboratories	Varies	Various locations in the USA	IDART – analysing system design & implementation from adversary point of view
Red Team: "Train Like You Fight"	https://www.nccgroup.trust/au/about-us/newsroom-and-events/blogs/2015/january/red-team-train-like-you-fight/ NCC Group	Varies	Various locations in the USA, Canada, Europe, UK, Australia	Primarily cyber crime
Red Team Training	http://riskoffensive.com/training/ Risk Offensive	2 days	Australia	Traditional military RT approach
Becoming Odysseus	http://www.watermarkinstitute.com/Becoming_Odysseus.html The Watermark Institute (Dr Mark Mateski)	1, 2 or 3 days	Fairfax, Virginia	Building & framing a red team, and individual red teamer skills

The primary focus of the methods tends to be the devil's advocate or penetration testing, and while there are a few courses aimed at training the types of skills good red teamers require, the overwhelming majority of the training identified online currently appears to

be in the cyber domain. This is not a negative, as there is much to be done in the world of cyber-crime and in terms of cyber security issues – however there are many other areas that would benefit from a red teaming approach without being situated in the cyber world. Even day to day planning activities in both the military and civilian contexts would be enhanced by the application of a level of red teaming (from very simple to large scale and complex, dependent on need).

8. Conclusion

The emphases in this report have been the application of red teaming as a methodology in a broader, less traditional sense. It is provided to enable people desiring a more analytical approach to their problem analysis or evaluations, to tailor the scale and complexity of red teaming activities to meet their specific needs.

While the methodologies discussed throughout this report are drawn from a variety of disciplines (e.g. operations analysis, operations research, human sciences, systems engineering to name just a few), they are often complementary in terms of the outcomes they support when applied to the appropriate problems.

Four critical aspects of successful red teaming include being clear about what is being tested, defining appropriate objectives for the test activity, carefully deciding how to best conduct the activity to obtain meaningful outcomes, and working within the resources available to achieve the optimal outcome. By keeping these four aspects in mind during the planning and decision processes, the appropriate method(s) for the activity can be selected. As with any exercise that aims to evaluate or analyse performance, validity or other aspects of plans, processes, actions, other analyses or reports (particularly those looking to be predictive in nature), the quality of the outcomes are determined by the quality of the decision making and preparation that went into planning the activity.

The aim of this report was to provide simple initial guidance regarding the development and conduct of red teaming activities by enabling an understanding of the utility of red teaming, what it is useful for, and how it can be applied in a variety of contexts (both within and outside of Defence). With the outline of various cognitive biases (the effects of which red teaming is designed to help combat) and a variety of bias mitigation strategies provided, readers should be able to begin their activity planning with a base knowledge of the underlying value of a red teaming approach. Further, with the outline of the various activity types that fall under the red teaming umbrella, as well as the additional activity and method descriptions, readers can then identify (using the flowchart in Figure 3) the necessity for a red teaming approach and the type of methods that would best suit the purpose of their activity.

Once red teaming has been selected as the required basis for the activity, some guidance and lessons based on learning from previously conducted red teaming activities in both

the military and civilian domains has been provided, and should assist with the design of the activity itself, particularly in terms of personnel selection.

Finishing with a brief examination of training issues, and several links to a variety of red team training providers, it is hoped that this report will serve as a simple enabler for individuals wishing to explore the applicability of red teaming approaches to address their challenges. There is a list (by no means exhaustive) of more complex red teaming guidance provided at the end of the reference list in the next section for those wishing to explore further detail of red teaming conduct; however it should be noted that these are primarily for the military context.

9. References

Chapman, G. B. & Elstein, A. S. (2000). Cognitive processes and biases in medical decision making. *In* G. B. Chapman & F. A. Sonnenberg (Eds.), *Decision making in health care: Theory, psychology, and application.* Cambridge series on judgment and decision making (pp.183-210). New York, US: Cambridge University Press.

Dror, I. (2012). Letter to the editor – Combating Bias: The Next Step in Fighting Cognitive and Psychological Contamination. *Journal of Forensic Sciences,* 57 (1), 276 – 277.

Dunbar, N. E., Miller, C. H., Adame, B. J., Elizondo, J., Wilson, S. N., Lane, B. L., Kauffman, A. A., Bessarabova, E., Jensen, M. L., Straub, S. K., Lee, Y-H., Burgoon, J. K., Valacich, J. J., Jenkins, J. and Zhang, J. (2014). Implicit and explicit training in the mitigation of cognitive bias through the use of a serious game. *Computers in Human Behaviour,* 37, 307 – 318.

Gigerenzer, G., & Hug, K. (1992). Domain specific reasoning: Social contracts, cheating, and perspective change. *Cognition*, 43, 127-171.

Greitzer, F. L. & Andrews, D. H. (2010) Training Strategies to Mitigate Expectancy-Induced Response Bias in Combat Identification: A research agenda. In D. H. Andrews, R. P. Hertz, & M. B. Wolf (Eds) *Human Factors Issues in Combat Identification.* Ashgate Publishing Limited: Surrey, UK.

Harvey, J. T. (1998). Heuristic Judgement Theory. *Journal of Economic Issues,* 32(1), 47 – 60.

Hershberger, P. J., Part, H. M., <arkert, R. J., Cohen, S. M. & Finger, W. W. (1995) Teaching awareness of cognitive bias in medical decision making. *Academic Medicine,* 70 (8), 661.

Heuer, R. J. Jr & Pherson, R. H. (2015) *Structured Analytical Techniques for Intelligence Analysis.* 2nd edition. SAGE press.

Kardos, M. (2006) *The Influence of Critical Human Factors on the Conduct of HUMINT: Cognitive Factors.* DSTO-TR-1894. Defence Science and Technology Group, Edinburgh.

Kardos, M. and Hanly, G. (2012) *The Application of Red Teaming in the National Security Policing Context: An Interim Evaluation of the Concept*. DST Group -CR-2012-0127. Classification: Security in Confidence.

Kardos, M., Hanly, G. and Malec, C. (2014) *Evaluation of a Red Teaming Concept in the Context of National Security Exercises*. DST Group -TN- 1488. Classification: FOUO.

Kardos, M. and Richmond, M. (2015). *A Brief Review of the Red Teaming Concept of Operations for the Directorate of Future Land Warfare.* DST Group -DP-1300. Classification: FOUO.

Klayman, J. & Brown, K. (1993). Debias the environment instead of the judge: An alternative approach to reducing error in diagnostic (and other) judgment. *Cognition*, 49, 97-122.

Kolb, D. (1984). *Experiential Learning as the Science of Learning and Development*. Engelwood Cliffs, NJ: Prentice Hall.

Krane, D. E., Ford, S., Gilder, J. R., Inman, K., Jamieson, A. & Koppl, R., Kornfield, I. L., Risinger, D. M., Rudin, N., Taylor, M. S. & Thompson, W. C. (2008) Sequential unmasking: a means of minimising observer effects in forensic DNA interpretation. *Journal of Forensic Sciences*, 53(4), 1006-7.

Lauder, M., *Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces.* Canadian Army Journal, 2009. **12**(2): p. 25-36.

Malec, C., Hanly, G., Grieger, D. and Kardos, M. (2012) *Red Teaming in Support of National Security*. DST Group -GD-0688. Classification: Restricted.

Mateski, M., *Toward Red Teaming Taxonomy, 2.0.* Red Team Journal, 2004.

Matsumoto, D (Ed). (2009). *Cambridge Dictionary of Psychology*. San Francisco State University: Cambridge University Press.

Mitchell, M. (2003). *Effects of experience and confirmation bias on legal decision making.* Unpublished Honours Thesis, Psychology Department, University of Adelaide.

Moon, J. (2004) *A Handbook of Reflective and Experiential Learning: Theory and Practice.* London: Routledge Falmer.

Nisbett, R. E. (1993) (Ed). *Rules for Reasoning*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Omni (2000) *Information Gathering Toolkit: Basic tools for quantitative and qualitative data collection. Last accessed on 17 February, 2016 at* http://www.omni.org/Media/Default/Documents/Information%20Gathering%20Toolkit.pdf

Pherson, K. H. & Pherson, R. H. (2013) *Critical Thinking for Strategic Intelligence.* SAGE Press.

Pincombe, B., Blunden. S., Pincombe, A. & Dexter. P., (2013) Ascertaining a hierarchy of dimensions from time-poor experts: Linking tactical vignettes to strategic scenarios. *Technological Forecasting & Social Change*, 80, 584-598.

Plous, S. (1993). *The Psychology of Judgement and Decision Making*. Philadelphia: Temple University Press.

Thompson, W. C., Ford, S., Gilder, J. R., Inman, K., Jamieson, A., Koppl, R., Kornfield, I. L., Krane, D. E., Mnookin, J. L., Risinger, D. M., Rudin, N., Saks, M. J., & Zabell, S. L. (2011)

Letter to the Editor: A rejection of "working blind" as a cure for contextual bias. *Journal of Forensic Sciences*, 56(2), 562 - 3.

Thornton, J. I. (2010) Letter to the Editor – A rejection of "working blind" as a cure for contextual bias. *Journal of Forensic Sciences*, 55(6), 1663.

Tversky, A. & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Cognitive Psychology*, 5, 207 – 232.

Tversky, A., & Kahneman, D. (1986). Judgement under uncertainty: Heuristics and biases. *In* Arkes, H. R. & Hammond, K. R. (Eds). *Judgment and decision making: An interdisciplinary reader.* (pp. 38-55). Cambridge: Cambridge University Press.

United States Government. (2009) *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis.* CIA Tradecraft Primer available at https://www.cia.gov/library/publications/publications-rss-updates/tradecraft-primer-may-4-2009.html

Winkler, J. & Moser, R. (2016). Biases in future-oriented Delphi studies: A cognitive perspective. *Technological Forecasting & Social Change*, 105, 63-76

Zenko, M. (2015). *Red Team: How to succeed by thinking like the enemy.* Basic Books: New York.

Red Teaming Handbooks

Australia-New Zealand Counter Terrorism Committee Guide to Red Teaming Exercises. (2014) Classification: FOUO.

Command Red Team. Joint Doctrine Note 1 – 16, Defense Technical Information Center, United States Department of Defense, Fort Belvoir, Virginia.

Brangetto, P., Caliskan, E. & Roigas, H. (2015). *Cyber Red Teaming: Organisational, technical and legal implications in a military context.* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities. (2003) Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Gladman, B. (2007) *The 'Best Practices' of Red Teaming*. DRDC CORA TM 2007-29.

Maritime Commander's Red Team Handbook. (2011) United States Navy.

Red Team Handbook. (2012) University of Foreign Military and Cultural Studies.

Red Teaming Guide, 2nd edition. (2013) Development, Concepts and Doctrine Centre, Ministry of Defence, United Kingdom.

The Applied Critical Thinking Handbook 7.0. (2015) Produced by the TRADOC G2 Operational Environment Enterprise; University of Foreign Military and Cultural Studies.

Appendix A: Descriptive List of Relevant Heuristics and Biases

This table presents basic information about both heuristics and biases to make it easier to apply to any context.

Heuristic or Bias name	Relevant key characteristics	Explanation
Heuristics		
Anchoring & Adjustment Heuristic	A mental shortcut that involves people adjusting their evaluations of things by means of a certain reference point, often one they have generated themselves (Sternberg & Sternberg, 2009). This type of heuristic is related to the human tendency to anchor ratings in a specific starting point and adopt of further information in relation to this. Using this heuristic, people often do not adjust their answer sufficiently in light of new information. That is, people who have to make judgements under uncertainty use this heuristic by starting with a certain reference point (anchor) and then adjust it insufficiently to reach a final conclusion.	Tendency to lock onto certain aspects of the scenario or discussion idea very early in the process and subsequently failing to adjust perceptions and impressions in the light of later information. [*may be compounded by the Confirmation Bias*]
Availability Heuristic	Ease of actual recall or perceived ease of recall	This heuristic judges the probability of events by how quickly and easily examples come to mind (based on having learned that more frequent events are more likely), or how easily we can imagine bringing examples to mind (without actually doing so). So as a time saver, we make decisions based on knowledge that is readily available in our minds instead examining all the alternatives. This happens subconsciously most of the time, and usually this gives us a quick shortcut to the answer we need, which is often an accurate judgement. Sometimes, though, the shortcut can lead us to make mistakes. Some events are easier to recall than others, not because they're more common but

		because they stand out in our minds for various reasons. E.g. sensational headlines related to injury or fatality, deciding whether or not to speed on a given stretch of road based on whether or not you can easily recall seeing speed traps there in the past, etc.
Elimination by aspects Heuristic	Narrowing options using one characteristic at a time	In the elimination by aspects approach, you evaluate each option one characteristic at a time beginning with whatever feature you believe is the most important. When an item fails to meet the criteria you have established, you cross the item off your list of options. Your list of possible choices gets smaller and smaller as you cross items off the list until you eventually arrive at just one alternative.
Recognition Heuristic	Used as a model in the psychology of judgement and decision making, and as a heuristic in artificial intelligence, and states that: If one of two objects is recognized and the other is not, then people tend to infer that the recognized object has the higher value with respect to the criterion. Research by Newell & Fernandez and Richter & Späth tests the non-compensatory prediction of the recognition heuristic, and states that "recognition information is not used in an all-or-none fashion but is integrated with other types of knowledge in judgment and decision making."	Tendency to view a recognised event/outcome (i.e. one that is similar to a previous event/outcome) as more important, meaningful or likely. [*may relate to the Representativeness Heuristic above*]
Representativeness Heuristic	Classify things based on their similarity to our existing category prototypes	When making judgments, we often estimate the likelihood of an event by comparing it to a prototype that already exists in our minds. Our prototype is what we think is the most relevant or typical example of a particular event or object. When we make decisions based on representativeness, we may make more errors by overestimating the likelihood that something will occur. Just because an event or object is representative does not mean that it is more likely. E.g. jury decisions depend partly on the degree to which a defendant's actions are representative of a particular crime category. So someone who abducts a child and asks for ransom is more likely to be convicted of kidnapping than someone who abducts an adult and demands no ransom.

		Both crimes constitute kidnapping, but the first is a more representative example.
Satisficing	Select option that meets minimum acceptability criteria	This is a decision-making strategy that aims for a satisfactory or adequate result, rather than the optimal solution. It's often used because aiming for the optimal solution may mean the expenditure of time, energy and resources (that sometimes you cannot afford). It can also be the case that the optimal solution is not identifiable – i.e. that finding the absolute best of all possible options is so complex that it can't be done – or in some cases, it is a means of maintaining group status quo (i.e. finding a solution that everyone can agree to).
Similarity Heuristic	Choosing things that are similar to positive things from the past	This is an adaptive strategy designed to maximise productivity by repeating favourable actions/experiences/outcomes and not repeating unfavourable ones. This is partly assessed through comparing the similarity of the current situation to the past situation in which the experience occurred i.e. assessing whether the context is the same. Problems arise when judgements of contextual similarity are faulty, and a choice is made to repeat an action that is not appropriate for the current context and results in unfavourable outcomes. E.g. the decision to drive through a partially flooded creek to reach a rendezvous location on the other side may be taken based on the apparent similarity of the situation to one from the past, where you successfully forded the creek. However, *this* creek is much deeper than the previously experienced one, and here your vehicle stalls and is carried away by the strong current.
Simulation Heuristic	(similar to the *Availability Heuristic*) Is a psychological heuristic (simplified mental strategy) according to which people determine the likelihood of an event based on how easy it is to picture the event in their minds. Partially as a result, people have greater regret for missing outcomes that had been easier to imagine, such as "near misses", than when an accomplishment had been much further away.	Tendency to view events/occurrences that can be easily imagined as more likely to occur, leading to biased choices of response (i.e. people want to choose to combat the 'likely' event)

Take-The-Best Heuristic	According to the take-the-best heuristic, when making a judgment based on multiple criteria, the criteria are tried one at a time according to their cue validity, and a decision is made based on the first criterion which discriminates between the alternatives. Gerd Gigerenzer and Daniel Goldstein discovered that the heuristic did surprisingly well at making accurate inferences in real-world environments, such as inferring which of two cities is larger. The heuristic has since been modified and applied to domains from medicine, artificial intelligence, and political forecasting.	Tendency to work through various decision criteria relating to the options or responses that have been suggested until one is reached that shows a significant difference between the options/responses available. There may be a tendency to ignore other decision criteria and rely on this single differentiating one.
Bias Category 1: Decision making and Behavioural Biases		
Attentional Bias	Having a narrow focus and ignoring other options	If recurring thoughts influence you to examine only one or two possibilities and ignore the rest when making judgements, this may be an issue. It is worse than considering alternatives and incorrectly discarding them, because they have never been considered in the first place. This means that there is likely to be no subconscious contingency planning occurring.
Bandwagon Effect	A type of thought within a deeply cohesive in-group whose members try to minimize conflict and reach consensus without critically testing, analysing, and evaluating ideas. During the bandwagon effect, members of the group avoid promoting viewpoints outside the comfort zone of consensus thinking. It is one potential negative consequence of group cohesion.	Tendency for groups of similar people (or those with strong group bonds) to go along with the general consensus in order to keep the peace rather than critically testing the options presented.
Bias Blind Spot	Assuming bias in others and none in oneself	Do you look at others and assume that while *they* might be biased, you're definitely not? This is problematic in that humans accumulate a variety of biases and heuristics during the course of their lives, and they impact on the choices they make every day. While they may always not have detrimental effects, when it comes to decisions that may cost lives, it is worth examining

		the potential for bias and its impact on those decisions.
Choice-Supportive Bias	Retroactive ascription of only positive attributes to past choices	Do you see past choices through rose coloured glasses? Human sometimes view their past choices positively and ignore any negatives associated with them. This makes it difficult to be objective when reviewing your choices.
Confirmation Bias	Favouring confirmatory information/evidence regardless of whether the information is true/accurate	If you aren't looking for contradictory or disconfirmatory evidence when making decisions, you may be suffering from this. Examining the counter evidence provides insight into your choice in terms of the pros and cons, and what you may need to do to manage the cons.
Congruence Bias	Only direct hypothesis testing used, not alternative testing	If you only test ideas or theories you believe are likely, and ignore the alternatives, it is often termed 'trying to prove yourself right'. Again, this can be dangerous because contingencies are not being considered.
Curse of Knowledge Bias	Knowledgeable individuals often have difficulty taking a naïve perspective	As an SME, you may find it difficult to think about problems from a less-informed/non-expert perspective. This makes it more difficult to step back from the issue at hand and look at it through a different, non-interpretive lens.
Defensive Decision Making	Making the defensible decision, while ignoring the decision that would actually be the best	People may tend to make the decision they think they can defend, rather than the one they think is best. This is common in acquisitions, where for whatever reason the decision maker feels they cannot justify spending extra money on important qualities, and so settle for the 'almost good enough' option instead.
Distinction Bias	The tendency to view two options as more dissimilar if viewed and judged in isolation than if evaluated simultaneously.	Tendency for two similar options to be viewed as more dissimilar if they are evaluated sequentially instead of simultaneously. The differences in expected outcomes of two options may therefore be exaggerated if they are not evaluated 'side by side', which may impact on decision making for planning and the development of COAs.
Escalation of Commitment	Continuing to invest in a decision based on the amount of investment already made, even though the future investment will not reap the desired benefit	If you're sticking with a non-ideal choice/COA even though it's clearly not the best option. Often called "throwing good money after bad", and is exemplified by a homeowner who buys a run-down hovel and invests more and more money in fixing it up for resale, even though he will never recoup his spending.
Expectation Bias	Choices influenced by expectations/mindset	This can be seen in different contexts and can manifest as seeing what you expect to see, or hearing what you expect to hear. It is for this reason that it is wise to use an editor when writing reports, since repeated exposure to the document you are working on and the knowledge of what you intended to

		say can influence what your eyes see on the page. Mistakes are easily overlooked this way.
Exposure-Suspicion Bias	Is a narrowing of perspective, where a person can only view decisions/choices with the lens of their own profession	People tend to view things according to the conventions of their own profession, without taking a broader point of view. This is where outside experts – SMEs in areas related to the choices/decisions, but from outside the context or domain in which the choice sits – are very useful for providing fresh perspectives.
Framing Effect	Influence of the framing of options/choices on decisions	A decision frame is the decision maker's conception of the acts, outcomes and contingencies associated with a particular choice. They are controlled in part by the formulation of the problem, as well as by the norms, habits and characteristics of the decision maker (Tversky & Kahneman, 1981: 453). So presenting the same option to people in different formats can alter people's decisions. Specifically, individuals have a tendency to select inconsistent choices, depending on whether the question is framed to concentrate on losses or gains (Plous, 1993). This represents a tendency to be overly influenced by the way options or choices are framed. This may relate to the way the risk of an option is framed against the possible positive outcome of choosing it: e.g. where there are two response options, and option A (has a 100% chance of saving 240 lives) versus option B (a 25% chance of saving 1000 lives and a 75% chance of losing all of them), the majority of people will tend to choose option A where there is a guarantee of saving 240 lives for sure. If a person views an issue from only one perspective, they may be under the influence of this effect. Problem or choice restatements are a useful way to combat this tendency towards tunnel vision. If the original framing of the choice was very positive, trying a neutral way of stating it may bring objectivity back into the choices being made.
Focusing Effect	Overemphasis of one aspect unduly influences choice	When one aspect of a problem/option is overemphasised to the detriment of all others, it can lead to biases decisions. For example, choosing an armoured vehicle because it has the best weaponry even though it is heavy, very slow and has the less effective armour appears to be an effect of focusing too much on the weapons systems rather than the overall combination of characteristics.

Functional Fixedness	Assuming the traditional application of an item is the only way to use it	This is what is happening when you only want to use an object or system the same way it has always been used. This is a problem that can be remedied using red teaming – but it can also be a problem for the red teaming process if it is not identified and addressed. It will tend to constrain the way red team members think about the use of plans/system/objects and other items of interest, and may mean that alternatives and potential weaknesses are not fully explored and mitigated. There must be emphasis on creativity in the red teaming process, and active triggering of creative responses in order to combat this effect.
Irrational Escalation *(related to "escalation of commitment")*	(sometimes referred to as *irrational escalation of commitment* or *commitment bias*) Is a term frequently used in psychology, philosophy, economics, and game theory to refer to a situation in which people can make irrational decisions based upon rational decisions in the past or to justify actions already taken. Examples are frequently seen when parties engage in a bidding war; the bidders can end up paying much more than the object is worth to justify the initial expenses associated with bidding (such as research), as well as part of a competitive instinct.	A tendency to continue to invest in bad/flawed decisions because either they were based on an initial good decision, or because the actions have already been taken and require justification. This may occur with capability development in purchasing decisions, the development of IT (or other) support resources, and in terms of decisions on longer term plans and COAs for example.
Mere Exposure Effect	Preference for familiar things	Humans often have an undue preference for the familiar (especially through repeated exposure), and this can happen without any actual experience of the familiar item – it can occur simply through having seen several times.
Normalcy Bias	A mental state people enter when facing a disaster. It causes people to underestimate both the possibility of a disaster occurring and its possible effects. This often results in situations where people fail to adequately prepare for a disaster, and on a larger scale, the failure of the government to include the populace in its disaster preparations. The assumption made in the case of the normalcy bias is that since a disaster never has occurred	Tendency to underestimate the possibility of, and the potential impacts of, an event/outcome. This can result in people feeling that they should not "overreact" to what they consider the vague possibility of an event/outcome like this occurring, and therefore not being ready (or being under prepared) if/when it does occur. This is likely to be encountered by military and emergency workers when some type of disaster (natural or man-made) occurs, and the public is ill-prepared to respond. It is a problem that is difficult to overcome with public information programs because of the inherent way that humans often interpret possibilities and likelihoods.

	that it never will occur. It also results in the inability of people to cope with a disaster once it occurs. People with a normalcy bias have difficulties reacting to something they have not experienced before. People also tend to interpret warnings in the most optimistic way possible, seizing on any ambiguities to infer a less serious situation.	
Omission Bias	Individuals tend to judge harmful actions as worse than harmful inactions.	This may skew the development of plans and COAs in terms of making personnel more risk averse; rather than risking an action that may have negative consequences, they may tend to err on the side of caution by virtue of the fact that a negative outcome based on a decision not to act is often perceived (by individuals prior to the event) as less harmful. This is not, however, a sound judgement in the current fault-finding and blaming culture, where inaction is seen as equally heinous by those impacted.
Outcome Bias	The tendency to judge a decision by the eventual outcomes instead of the quality of the decision at the time it was made.	This may manifest in a tendency to favour previously 'successful' decisions or plans because the outcome at the time was a success. It is problematic in that, if the basis for the decision is faulty, there is a danger that the same faulty decision making will lead to a negative outcome in the new context.
Persuasion Bias	Perceiving all new information as independent	People often tend to see any new information as independent, and fail to consider possible repetition. This can lead to choices based on badly weighted evidence, simply because more people chose to repeat one source of evidence over others.
Seer-Sucker Illusion	Over-reliance on expert advice	Over-reliance on expert advice comes with the avoidance of responsibility, in that the responsibility falls on the shoulders of the expert. This is not uncommon in high-risk, high-cost scenarios since humans can tend to shy away from decisions or choices they feel they would regret should they be wrong.
Selective Perception	Related to [or the basis of] a series of cognitive biases in which peoples' perceptions of what they see/hear/understand are affected based on their expectations, hopes, beliefs and attitudes.	The tendency for preconceived notions to affect what people see or hear, regardless of the information that is actually placed in front of them.

Semmelweis Reflex	Rejection of new contradictory information	Humans can tend to become invested in their ideas and assumptions, and this can manifest as a tendency to ignore or dismiss any new information that doesn't confirm to what they already believe.
Status Quo Bias	The tendency to like things to stay relatively the same *(related to Loss Aversion, Endowment Effect, System Justification)*	Humans sometimes display a tendency to prefer unchanging, predictable environments. This can be influenced in a variety of ways, but in the military and national security contexts it may translate to a preference for particular types of choices or COAs in response to the actions of adversaries or nature.
Turkey Illusion	The tendency to extrapolate the past to predict the future. e.g. A turkey sees the farmer as a source of food, and never anticipates Thanksgiving.	Humans tend towards extrapolating from past experience to determine the path of the future, or outcome of future events/plans/actions. In many instances, this is appropriate and saves time in the process of planning strategies and more immediate actions. It can, however, lead to biases and assumptions when considering the projected outcomes of COAs, decisions and plans.
Bias Category 2: Probability and Belief Biases		
Ambiguity Effect	A cognitive bias first identified by Daniel Ellsberg where decision making is affected by a lack of information, or "ambiguity". The effect implies that people tend to select options for which the probability of a favourable outcome is known, over an option for which the probability of a favourable outcome is unknown. Relates to the issue of choice under uncertainty.	When making decisions under conditions of uncertainty, people tend to favour any option for which a good outcome has at least some known likelihood over one for which the outcome probability is completely unknown.
Authority Bias	Judged value of option influenced by opinion of 'expert'	Humans can tend to be overly influenced in their judgements by perceived experts, and this applies even when the option or likely outcome is ambiguous. That is, when there is little information available to make an informed judgement and the option itself is confusing or unclear, the opinion of an expert in the area will be enough to influence the person's choice.
Belief Bias	The effect where a person's evaluation of the logical strength of an argument is biased by the believability of the conclusion.	This can be problematic when analysing the relative effectiveness of a COA or a decision; if the projected outcomes are believable, people tend to be drawn to assess the argument leading up to it as sound when this is in fact *not* a good way to make that judgement.

Clustering Illusion	The tendency to overestimate the importance of small runs, streaks or clusters in large samples of random data (i.e. seeing phantom patterns)	When applied to the context of military or national security judgements/decision making, this can translate to viewing clusters of similar outcomes as meaningful patterns and using this as a basis for judgement of future plans and COAs. This may not be an effective means of judging true patterns in events and outcomes.
Forward Bias	Use only old data to validate models built based on that data	When models and assumptions are built on old information (for example, the outcomes of an operation in a desert environment ten years ago) and then are only assessed using the original information rather than testing them against the new relevant information or context, this is problematic. It can lead to faulty decisions based on inappropriate application of models and options to the wrong context.
Illusory Correlation	The tendency to see particular events, attributes or categories as belonging together. This can result in stereotypes when in reference to attributes and people, and false cause-effect relationships can result when applied to events (Sternberg & Sternberg, 2009).	Simple examples include - coming across an uncooperative person in an agency with which you are supposed to be working may lead people to assume the agency as a whole is uncooperative; - superstitious behaviour (e.g. a football fan believes that his team wins when he wears a specific jersey, so each time his team plays he will only wear that jersey); -a worker is treated poorly by a person of a specific ethnicity, and he then chooses to never work for a person of that ethnicity again because he has related the person's behavior to his ethnicity.
Illusion of Validity	This is the fallacious belief that additional information generates additional relevant data for predictions, even when it clearly does not. E.g. If SACE scores correlate highly with IQ test scores, then using both in judging a job candidate's suitability would be unnecessary, since it would add very little extra information and would not increase decision confidence by much. This may be partially caused by confirmation bias and the representativeness heuristic, and may in turn result in the overconfidence effect.	This can be problematic when information or intelligence are being analysed to make decisions on COAs or plans: building increasing quantities of information may not be adding anything more than repeated incidences of the same information to what is currently being analysed. This then is not additional objective outside confirmation of the current information and its interpretation, it is simply revisiting the same information again (often from the same originating sources). It may then skew the decision process due to the illusion of confirmatory evidence (hence the impact of confirmation bias on the process).

Overconfidence Effect	A bias in which someone's subjective confidence in their judgments is reliably greater than their objective accuracy, especially when confidence is relatively high.	Tendency to have more confidence in one's own judgement than is warranted by one's past performance record. It often occurs when people do not realise how little they know, or that the information they do have come from unreliable sources.
Primacy Effect	A bias wherein the characteristics of a thing that appear early in the list influence impressions/decisions more strongly than those appearing later in the list. Also consider as evidence/information discovered early tending to impact decisions more strongly than that discovered later. Relates to the strength of first impressions, for example.	Tendency to weight evidence/arguments presented earlier as more important or influential for choices than that presented later, regardless of their relative quality/actual impact. i.e. first impressions can last throughout the decision making process
Recency Effect	A bias where the last piece of information/evidence heard affects the decision/impression more strongly than those heard first/earlier. This can be related to individuals' memory for items, as the more clearly recalled items are often the most recently gained.	Tendency for the last evidence/arguments presented to impact on choices more strongly than those presented early on. This may be a stronger effect if peoples' memories are not very good or the evidence/arguments are more distinctive.
Subadditivity Effect	The tendency to judge the probability of the whole as less than the sum of the probabilities of the parts.	The best illustration of this is from research using a medical example: one group of participants were asked to rate the probability of dying from cancer (18%), heart attack (22%), and "other natural causes" (33%). A second group were asked to rate the probability of dying from natural causes (the definition of which included cancer, heart attack, and 'other natural causes') and the result was 58% (clearly far less than the total of 73% the initial group would have had).
Subjective Validation	Sometimes called *personal validation effect*, is a cognitive bias by which a person will consider a statement or another piece of information to be correct if it has any personal meaning or significance to them. Relates to the *Confirmation Bias* and *Selective Perception.*	Tendency to buy into choices or options selected as being the right ones if they have more personal meaning or significance to the individuals.

Bias Category 3: Social Biases		
Group Think (Herd instinct)	Agreeing with the group consensus regardless of own opinion	If you agree with the majority opinion even though you believe there is a better alternative, you could have a case of this. It is often driven by the need to maintain the status quo in a group.
Ingroup Bias	The tendency to give preference to people perceived to be a member of one's own group.	For example, a person may lend greater weight to an opinion voiced by someone they perceive as part of their ingroup than by someone external, which they may justify to themselves by reason of level of the knowledge or experience the external (outgroup) person is assumed to have.
Status Quo Bias	Preference for things to stay the same	This relates to Group Think, where people prefer to have things remain as they are than change them.
Shared Information Bias	Over-focus on information familiar to the group	This is a common tendency in groups; decisions/items/options about which people have more shared information are more readily discussed (which contributes to group cohesion), and so groups may spend more time on these shared items than on new, less well-known items.
System Justification (related to *Status Quo Bias)*	Defence of the status quo except when evidence is compelling	Related to Status Quo Bias, it is the tendency to want to keep established behaviours and arrangements unless there is a very good reason to do otherwise.
Bias Category 4: Memory Biases		
Illusion of Truth Effect	People tend to find more familiar statements more truthful, even if they can't recall where or when they heard them previously.	A similar effect to the Mere Exposure Effect, where there is an undue preference for the familiar. That is, greater positive affect (in this case, the characteristic of truthfulness) is ascribed to familiar items.
Misinformation Effect	Memory becomes less accurate due to interference from post event information. This can include random information being incorporated into memory, as well as the effects of leading questions.	Long term memory is affected by information absorbed after an event, and leading questions can cause the effect to increase. (similar to the *Framing effect*) An example from Loftus is asking witnesses of a car accident the same question in two different ways: "how fast were the cars going when they bumped into each other?" versus "how fast were the cars going when they smashed into each other?" In the majority of cases, the speed was estimated to be greater for those with the word 'smashed' in the question. A week later, those with the word 'smashed' in the question were twice as likely to "recall" broken glass at the scene compared with those with the word 'bumped' in the question.
Von Restorff Effect	Distinctive items are more likely to be remembered than others	When you try to recall past experiences, there may be some that come very easily to mind because they are quite distinctive. These are more likely to be

		remembered than most others, and are the items that tend to influence people's decisions. If, for example, a faulty grenade detonated too early and caused unintended damage to a vehicle, this incident is much more likely to be remembered than the other 50 times when this did not happen.

Appendix B: Detailed Review of Methods

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
Basic Techniques	*Methods 1, 2, 3 & 4 can be framed for both process and content questioning. They can be used by the individual, teams or pushed by an external "reviewer". They are all very simple but powerful techniques and provide a basic toolkit which together with some of the above methods such as the concept map/influence diagram and devil's advocate can allow thorough questioning and challenging to ensure robustness is maintained.*			
1. Key Assumption Check: This is a means of listing and reviewing the key working assumptions that affect judgements.	Yes. This can and should be applied to all content being added or contributing to the content. Can be undertaken by the team/individuals or an external person.	Yes. Participants can identify and challenge both process and content assumptions.	1 and 4 are similar and related and should be done together. This overlaps somewhat with devil's advocate.	Fundamental questioning technique should be applied to any process/development or concept problem.
2. Root Cause Analysis (the 5 Whys): Is a means of identifying the causes of potential problems, and the mitigating strategies or alternatives that can be used to avoid the problem occurring.	Yes. These questions can be applied to all content and processes and concepts being developed or questioned.	Yes, these can be used to push the key assumption check as well as pulling apart elements of the concept. The iterative nature allows a true cause to be identified.	2 and 3 are related and could also be done together.	Fundamental questioning technique should be applied to any process/development. The iterative identification of causes can lead to a fishbone or cause and effect diagram to be drawn which can be linked to a concept map or influence diagram. This method can allow a cause to be identified and either acted upon or a strategy developed. e.g. if an underlying assumption is found it can be challenged for veracity.
3. Who, what, where, when, how & why questioning.	Yes. Can be applied all along the development process.	Yes. Can be used as a prompt or guide to	2 and 3 are related and could also be done	Fundamental questioning technique should be applied to any

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
		questioning why content was included or decisions were made.	together.	process/development. This can used to support key assumption checks.
4. What if scenarios and counter arguments /assumptions.	Yes.	Yes. These can be applied to the participants or inserted as prompts when assumptions have not been identified easily.	Black swan. Devil's advocate. 1 and 4 are similar and related and should be done together.	These questions allow the "void" in the scenario space which is not "in trend" to be identified and captured. Trends are only valid until a change happens. These disruptive events are where those that are unprepared are usually caught out.
5. Quality of information and reciprocal reference check.	Yes.	Maybe – if it hasn't been undertaken previously. Though this is more of a "bookkeeping" issue and would be wasting time in a workshop setting – unless it were used to raise questions about the quality of information and references.		This is really important especially with trend data. The sources of many of these references tend to reference each other. It is really important to search for and check for other independent analysis sources which either correlate with or provide another view. This will provide the most robust product. This will also allow capturing of alternate worldviews and help to challenge assumptions. This will also expose voids in the trends and provide counter arguments. Additionally the applicability of trend data and where it came from can be checked.
Contrarian techniques/views				
Team A/Team B: Using two (or more) separate analytic teams	No.	No.	The simpler techniques would provide similar	Not feasible. The number of scenarios/options to "play" would

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
to contrast two or more views or competing hypotheses.			outcomes.	become unmanageable very quickly. This is really for challenging one or two strongly held mindsets.
Devil's Advocate: Challenging a single strongly held view/consensus by building the best case for an alternative explanation.	Yes.	Maybe. Best if an external person plays the devil's advocate. Is this any different to the other simpler techniques already identified?	Key assumption check Who, what, where, when, how, why? What if? And counter arguments	A devil's advocate would run through the process and play off the questions from the overlap techniques anyway.
Strawman argument: In this context, is a first draft proposal based on limited information designed as a temporary solution to a problem: it is intended to be pulled apart when a better quality solution is developed.	Maybe if a new problem space/concept space is being developed from scratch.	No. the FLWR is quite developed and there is plenty of information available.	Most of them. The idea of RT techniques and other problem structuring techniques is that you are pulling apart and questioning your problem as you do along. So at each stage you should be doing the top 5 simple things below.	This really is an iterative development process which should happen anyway with the simpler techniques.
Black swan: An analytic method that highlights seemingly unlikely events/outcomes with major consequences.	Maybe. If it is used in a way to ensure that trends and assumptions are not ignoring the low probability high impact "black swan" events.	Yes – if it is used purely as a way to identify and recognise where these events sit in the concept space and to ensure they are not ignored.	These can be coupled with what if? And counter argument scenarios to make sure that black swans are not missed. This can be done in a simple quick extension to these techniques by having a 20 min extreme event or	At the end of the day all futures are plausible. Trends only remain trends until something different or disruptive occurs. You need to make sure that scenarios are robust enough to cover the broadest range of scenarios and that low probability high impact scenarios are not ignored as they will be the biggest tests. Low probability is still plausible. Until

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
			disruptive event brainstorming session as a group – or by getting external people to think some up.	something has occurred you cannot rule it out. However this technique is more of an additional one to ensure all scenarios are scoped and is easily coupled with simpler techniques. It ideally would be considered by a team in the scenario scoping phases.
Pre mortem analysis: A plan evaluation technique that identifies potential areas of weakness/gaps that may lead to failure prior to the implementation of the plan, allowing the plan to be modified appropriately.	Maybe. This could be used at key development points to assess gaps and holes in the content.	It could be done as a workshop on its own using something like a gap analysis or TOWS method. However, this is more easily undertaken in an anonymous online distributed fashion where there is no hierarchical bias possible and everyone can air their views. Strategies and gaps and problems can then be identified early on. This would need to be done very early on in a development process.	Gap analysis, TOWS method – not expanded on here. The 1-5 questions identified below would probably give very similar results for a document like the FLWR.	Failures can be identified easily through the root cause analysis and counter arguments.
Hypothesis analysis methods				
Collaborative conceptual modelling: The main aim of CCM is to help personnel improve their understanding of how a system/plan will likely respond to factors that affect it. It provides coherent support	Can be used to capture the concept space elements early on. Doesn't need to be formalised into a process. An influence diagram or concept map could be easily generated by an individual	If one (influence diagram or concept map) is developed early on it can be used to prompt or pull apart and question elements during a group activity.	Influence diagrams or concept maps from soft systems analysis or judgement based soft OR.	This is good for presenting a visual representation of the problem space and the interactions between elements in that space. He ability to link this to an impact analysis is useful.

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
to the growth of shared understanding and the development of robust, adaptive plans.	or group as they go along. The elements of the concept space can be related and both the elements and relationships can be questioned using the 5 simpler techniques.	This could also be used and extended to an impact analysis where the visual representation of relationships can allow flow on effects of what ifs to enable better prompts and questioning of assumptions in a workshop setting.		
CATWOE/RD: The Soft Systems Methodology CATWOE (Customer, Actors, Transformation, Worldview, Owner, Environment) uses the named categories of information to identify the critical components of a system of interest. This information is then used to produce a Root Definition (RD).	See comments.	Not unless you are presenting it to frame a context and concept space people are not familiar with. Ideally all SMEs / participants should be across this before pulling a concept apart.		This technique may have some value at the very beginning of a new concept development phase. However beyond that it's value rests with anchoring a description of the problem space which can then be (in theory) developed into a visual representation of factors of interest to the problem space.
Problem Restatement: Intended to broaden peoples' perspective on a problem by helping them to identify central issues and alternative solutions.	Maybe.	Not really.	The 5 simple techniques should address the similar issues as they aim to cut across bias issues. This overlaps quite largely with devil's advocate outcomes.	Problem restatement can be useful if the original problem statement is not generating useful progress. Really best used at the very beginning of a problem space. This would border also on devil's advocate roles as well.
Analysis of Competing Hypotheses: Intended to identify alternative explanations and evaluate all	No.	No.	The 5 simple techniques should address the similar issues and allow	The brainstorming to capture all alternatives is something that should be done at the beginning and also would be picked up in

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
available disconfirmatory evidence.			identification of preferred courses of action. If these are a major issue then a proper future scenario analysis should probably be conducted independently. There are many judgement based OR/scenario analysis techniques designed to help in these situations.	scenario scoping and with the 5 simple techniques. You can prove a hypothesis anyway – only disprove one. When considering future scenarios you can never know what it will be until you get there or you hit "trend" "markers" – such as Faustian tree tipping points as conducted in a Field Anomaly Relaxation process. Your competing hypotheses at the end of the day are likely both plausible future scenarios.
Logical traceability				
Context Diagram: Is a component of functional modelling that produces a high- level model of a system (real or planned) that outlines its boundaries and interactions the critical elements of the environment.	Yes if developed and maintained early on. Could be an influence diagram, concept map or even a rich picture.	Yes if one is used as a context framing point which can be used to identify relationships and elements which can both be questioned using the 5 simple techniques. This can also be used to prompt questioning and what ifs.	All the diagramming techniques overlap.	Simple and easy to do easy on and build on. Used as a reference not as an actual method in itself.
Functional Flow Block Diagrams (FFBDs) : Are a multi-tiered, time-sequenced, step-by-step flow diagram of a system's	Not unless you are mapping the process.	No.		Good for rigid and process driven exploration spaces. Not relevant to this kind of system concept.

Technique	Ongoing / development use?	Workshop use	Overlap with other techniques	Comments
functional flow, commonly used in systems engineering. It shows the sequence of all the functions performed by a system.				
Logic Modelling: Is a tool used to describe the effectiveness of programs. The model describes resource linkages, inputs, outputs, activities, audiences, and short/medium/long term outcomes for a problem or context. This then allows the development of performance measures.	This might help with the process itself but not with a future space concept like the FLWR.	No.		Might help identify if statements contradict – but not really useful in concept documents.
Program Theory: It is used to explain why a program is expected to work based on the why, the how, and the conditions in place; it predicts the outcomes of the program and the requirements for the desired effect to occur (and this is illustrated using the logic model above).	Maybe.	No.	Field Anomaly relaxation – morphological analysis	There would be so many If/then combinations in the plausible future scenario space that this would become untenable very quickly. However, the If/then possibilities might help structure an exploration or development space early on.
Requirements Breakdown Structure: Is a means of organising and structuring the resources required for a program in a hierarchical manner, and can be represented in a tree diagram.	No.	No.		Really only useful for the process of concept delivery. This would not add value to the development of the FLWR or to the questioning and challenging of it.

Appendix C: Cross-matching of core techniques with detailed techniques

This table compares the basic toolkit methods (key assumptions, what ifs and counter arguments, quality of information and references, visualisation and brainstorming) with the more detailed ones in order to identify where there are linkages and redundancies. This shows that the basic methods can be used on their own, and subsequently supported by more detailed methods where required. This would enable a tailored activity design for each problem. The overlaps (indicated by "Y" in the table below) also demonstrate where the common elements lie, and that the five basic methods do indeed provide the underpinnings of most of the techniques used in the red teaming and structured intelligence areas. Based on this, we propose that it is possible to construct a basic toolbox using these five fundamental techniques to apply to most problems, before requiring a detailed process using one or more of the detailed techniques in a more resource intensive manner.

Core elements/ common techniques Detailed techniques	1. Key assumptions	2. What ifs and counter arguments	3. Quality of info and references	4. Visualisation	5. Brainstorming
AIMS (Audience, Issue, Message & Storyline)	y		Y	Y	
Customer Checklist	Y		Y	y	
Issue Redefinition	y				
Chronologies & Timelines	Y		Y	y	
Sorting / Clustering/Categorising			Y	Y	
Ranking, Scoring & Prioritising	y		Y	Y	
Matrices			Y	Y	
Venn Analysis				Y	
Process Maps / Gantt Charts			Y	Y	
Network Analysis	y		Y	y	
Mind Maps /Concept Maps	y		y	Y	Y
Who, What, where, when, How & why	y		y		

Core elements/ common techniques Detailed techniques	1. Key assumptions	2. What ifs and counter arguments	3. Quality of info and references	4. Visualisation	5. Brainstorming
Root Cause Analysis – 5Ws	y				
Structured Brainstorming	y	y	y		Y
Virtual Brainstorming	y	y	y		Y
Nominal Group Technique	y	y	y		Y
Starbursting	Y		y	y	y
Cross-Impact matrix	Y		y	y	
Morphological Analysis including Field Anomaly Relaxation	Y	y	y	y	y
Strawman	y		y	Y	y
Delphi Technique	y	y	y		y
Hypothesis generation	y	y	y		Y
Scenario analysis	y	y		y	y
Indicators & validators	y			y	
Hypothesis generation	y		y		y
Diagnostic reasoning	y	y	y		
Analysis of competing hypotheses (alternative analysis)	y	Y	y		Y
Argument mapping	y	y	Y	y	Y
Deception detection	y	y	y		
Key assumptions check	y	y	y		Y
Structured analogies	y	y	y	Y	Y
Role playing	y	y			
Red hat analysis	y	y	Y		
Outside-in thinking	y	y	Y		Y

Core elements/ common techniques Detailed techniques	1. Key assumptions	2. What ifs and counter arguments	3. Quality of info and references	4. Visualisation	5. Brainstorming
Reference checks – quality of information	y	Y	y		
Critical thinking	y	y	y	Y	y
Premortem analysis	y	y	y	Y	Y
Structured self-critique	y	y	y	Y	y
What- if? Analysis	Y	Y	Y		Y
Counter argument/counter assumptions	y	Y	Y		Y
High impact / low probability analysis	y	y	y		Y
Devils advocacy	y	y	y	Y	y
Red team analysis	y	y	y		y
Adversarial collaboration	y	y	Y		
Structured debate	y	y	Y		
Decision trees & matrix	y	y	y	Y	
Pros-cons-faults & fixes	y	y	y		Y
Force field analysis	y	y		Y	
SWOT or TOWS analysis	y	y	y		Y
Impact matrix	y	y		y	Y
Trends	y	y	y	y	y

Appendix D: Sample Handout Booklet for Military Non-Traditional Red Teaming Activity

Directorate of Future Land Warfare
Red Teaming Activity Guide
March 2015

This is a brief guide to the red teaming training workshop and first pilot activity for the Future Land Warfare Directorate in 2015. This guide will be updated once the details of the FLOC red teaming activity have been refined.

1. RED TEAMING WORKSHOP

This workshop is a brief introduction to the concepts relevant to red teaming for the Future Land Warfare Directorate pilot activities.

1.1 Aim of workshop

To introduce the working definition of red teaming for the activity, the underlying cognitive issues red teaming techniques are intended to address, and a set of methods suitable for this purpose.

1.2 Workshop Format

The workshop will involve two lecture style sessions to provide participants with the required information, followed by a practical session applying the methods in order to cement learning. The final session will request feedback from participants and introduce the basics of the FLWR 14 red teaming activity.

1.3 Red Team Training Workshop Schedule

Wednesday 25th March 2015

0840 – 0900	Arrival & Coffee
0900 – 0910	Welcome and Introduction
0910 – 0945	Cognitive Biases & Heuristics
0945 – 1045	Red Teaming Methods Part 1 – Introduction to methods
1045 – 1100	***Morning Tea***
1100 – 1145	Red Teaming Methods Part 2 – Application

1145 – 1200 Workshop wrap-up and Feedback

1.4 Following this workshop, personnel participating in the FLWR 14 red teaming activity to be held 8 – 9 April, 2015 are requested to ensure they are familiar with the following:

- The guidance for Red Team participants in this handbook (p. 3 - 5)
- The FLWR 14 document
- The methods to be used during the FLWR 14 red teaming activity

This will help to ensure that the pilot activity provides meaningful outcomes in the time available, for both personnel and the directorate as a whole.

2. FUTURE LAND WARFARE REPORT 2014 RED TEAMING ACTIVITY

The first pilot activity for this style of red teaming is focused on a critical analysis of the FLWR 14. This will enable the identification of focus areas for future reports and a way forward with the report development process, as well as identifying the strengths and gaps in the red teaming method itself.

2.1 Aim of activity

To identify strengths and gaps in the current Future Land Warfare Report development process, and provide guidance regarding the focus and processes for future FLWR development.

2.2 Objectives of activity

Objective 1: Identify the strengths, gaps, and processes used in the development of FLWR 14.

Objective 2: Devise and analyse (using a red teaming approach) a set of valid and feasible processes for the development of future FLWRs.

Objective 3: Identify the intent of FLWRs, and focus areas for future reports.

Objective 4: Verify the utility of the red teaming methods used for the activity.

2.3 FLWR 14 Red Teaming Activity Schedule

Wednesday 8th April 2015

0840 – 0900 Arrival & Coffee

0900 – 0920 Welcome and introduction to activity

0920 – 1020 Identification and analysis of FLWR 14 development processes

1020 – 1030 ***Morning Tea***

1030 – 1200	Review and analysis of meta-trends in FLWR 14 (process and content)
1200 – 1300	***Lunch***
1300 – 1430	Group Activity Brainstorming new FLWR 14 processes
1430 – 1440	***Coffee break***
1440 – 1600	Red Teaming proposed FLWR development processes
1600 - 1630	Hot Debrief and Participant Feedback

Thursday 9th April 2015

0845 – 0900	Arrival and coffee
0900 – 1030	Activity outcome review and participant survey

2.4 Conduct of the activity

The activity will be facilitated to ensure that the objectives are met. It will begin with the identification and review of previously applied processes, followed by the examination of the meta-trends in terms of the processes and content. Analysis of these aspects will form a basis on which to consider existing strengths and gaps, and use these as inputs to the process brainstorming activity. The participants will form two or three groups (depending on the number of participants) and identify new processes for developing the FLWR. Once alternative means of developing the report have been identified by each group, the proposals from each group will be critically analysed by the remaining group(s). Once each of the groups has undergone the critical analysis, a set of viable options and their conditions of use will remain that can inform the Future Land Warfare Report Development Handbook.

There are non-traditional aspects to the current red teaming activity, as outlined in the next two sub-sections.

2.4.1 Red Team

This activity is structured differently to a standard red versus blue exercise. For this activity, there will only be a red team. That is, a single team comprising selected personnel who are experts in various critical aspects of land warfare and futures. No formal blue team will be used, as the red team will be critically analysing an existing product (FLWR 14).
As the Red Team, the SMEs will challenge traditional thinking, routine behaviours, and both implicit and explicit assumptions. They will also critically examine plans and processes in order to identify areas where oversights, assumptions and flaws in reasoning may impact the outcome of the FLWR development process.

2.4.2 Brainstorming and critical red teaming analysis

When participants engage in the process brainstorming activity, they should note the reasoning underpinning their decisions to select or discard process options, and any potential negative aspects of the options they have selected. This will provide information for the subsequent red teaming of the options proposed by each group, as well as consideration of the mitigating strategies available to minimise the impact of any negative characteristics on the end product.

2.4.3 Facilitation

This activity will be facilitated by a combination of DSTO and DFLW staff. This is intended to ensure that the objectives of the activity are met, that a frank and fearless approach is taken to guiding the activity and discussions, and will also serve as a mechanism to develop local facilitation skills in the red teaming context.

3. RED TEAM GROUND RULES

These ground rules apply to red teaming activities conducted in the current context, as well as to the more adversarial-style activities involving both a red and blue team. In the adversarial context, the ground rules relating to interactions and the attitudes of participants are crucial to success.
The red team members are asked to observe the following ground rules as a means to achieve the aim of the activity.

The activity and methods are intended to elicit challenges and innovation in terms of processes; to achieve this, participants need to apply the appropriate behaviours to the activity. Success is best achieved during red teaming activities such as this when participants:

- Avoid taking comments, questions and challenges as personal attacks: remember, this is a challenge of the processes, not individual performance
- Question everything
- Avoid framing comments, questions and challenges in the form of personal attacks

Participants should remember that not every heuristic or assumption is necessarily bad, however each one should be identified and recorded (where possible) to allow an audit trail of reasoning underlying decisions, and analysis of the validity of the assumption. Additionally, it provides an evidence base for readers (and potential future writers) of the report to understand how and why conclusions were reached.

There are several phrases that should not be used during red teaming activities, as they do not support effective critical analysis of material (e.g. processes, plans). These include:

- "That will never happen"
- "That's not how we do things"
- "We've always done it this way"
- Any variant of 'because I said so'

These are phrases that will stall the critical analysis process because they do not allow the red team to freely consider all the alternatives.

Past learning and experience should not be ignored; but experiential knowledge *should* be examined at a basic level so that it's applicability to other contexts can be understood. That is, successful actions in the past may be successful again – in the right context.

To gain maximum benefit from activities such as this, individual rank should not impact on the process. That is, personnel of all ranks need to be free to put forward and challenge ideas, choices, and reasoning without fear of retribution. Mutual respect is key, as is an understanding that during this activity, emphasis is on the use of evidence and sound reasoning in critically analysing processes and options.

3.1 Facilitation

Facilitation for red teaming activities must be frank and fearless, potentially encouraging participants to critically discuss aspects they may be reluctant to address. Facilitators for this type of activity should be prepared to ask 'what if' questions and inject prompts where required to draw out the depth of participants' knowledge about the subject matter.

Co-facilitation is a good arrangement to employ for red teaming, particularly in the case where incoming external information is being fed into discussions (e.g. where there is both a red and a blue team in play). It allows the primary facilitator to focus on the discussions and where injects may be required, while the co-facilitator can be the conduit between the red team and the primary facilitator, as well as keeping a rough track of participants' discussions, feeding red team injects to the primary facilitator, and noting key outcomes /items that occur during discussions for follow-up.

The goal is to maintain a relatively smooth flow of discussions so that participants work through the material in a sensible order. This helps to keep participants focused and aids their ability to think clearly about the topic at hand.

Appendix E: Sample Booklets for Red Team SMEs

The skeleton of the handbook for the second exercise – the Investigation phase – is provided here; some of the details have been removed to maintain the unclassified nature of this document. The headings of the relevant sections however, remain.

ADMINISTRATION AND LOGISTICS

Exercise Date

Tuesday 28 February 2012 & Wednesday 29 February 2012

Timings

The exercise will officially commence at 0830 hours and conclude at 1630 hours.

Registration will run from 08:00 – 08:30 hours.

The workshop will run from 08:30 – 15:00 Hours.

Location

The exercise will be conducted at the *(enter appropriate address(es))*

Venue Address

Map provided

Entry and Security Procedures

As the exercise is located with a secure perimeter, upon arrival you will need to approach reception where you will be provided with a visitors pass. Reception will then guide you to the Registration Desk where you will receive a Southern Intellection name badge. Only those with a name badge and visitors pass will be able to move freely in and out of the centre.

Travel Arrangements

In accordance with the ANZCTC Financial Guidelines, the attendance of interstate participants and Subject Matter Experts (SMEs) will be funded from the ANZCTC Administrative Fund allocated to *Southern Intellection*.

Flights

Unless otherwise arranged, flights to and from Capital City for participants and SMEs will be booked by the *(relevant agency)*. Flight itineraries will be emailed to participants.

Cab Charge Vouchers

Cab charge vouchers will be sent to interstate participants prior to the exercise to cover transport to and from airports.

Accommodation

Accommodation has been reserved for participants and SMEs at *(hotel name)* located at *(address)*

Accommodation costs will be invoiced directly to Tasmania Police and the Attorney-General's Department; guests are asked to settle accounts in relation to any additional expenses on check out.

Catering
Full catering will be provided for the duration of the exercise. *Please forward any special dietary requirements to administration personnel as soon as possible.*

Points of Contact

(Exercise directors, coordinators, and administrative staff)

EXERCISE SCHEDULE

Tuesday 28 February 2012

08.00 - 08.30	Registration & Coffee
0830 – 0845	Welcome and Introduction
0845 – 0900	Exercise Briefing and Q&A
0900 - 1030	Session 1 – Special Idea 1 & 2
1030 -1045	Morning Tea
1045 - 1230	Session 2 – Special Idea 3
1230 - 1300	Lunch
1300 - 1515	Session 3 – Special Idea 4 & 5
1515 - 1530	Afternoon Tea
1530 - 1630	Hot Debrief and Survey

BACKGROUND

Traditionally, ANZCTC exercises have focussed on response and recovery mostly using deployment style of exercises. However, in recent times the benefit of conducting deployment style exercises is being reviewed and other styles are being considered.

At present, ANZCTC has identified XXXX as one of their key priorities. In order to progress this priority and consider other styles of exercising, the ANZCTC agreed as part of the 2010-11 exercise program for a working group, in conjunction with the Exercise Management Capability, to be established to examine this issue and to commence to plan a XXXX related exercise to be conducted in Tasmania in 2011-12.

(Names of participating agencies and organisations) is planning to conduct three discussion/hybrid style exercises and developmental workshops in respect to prevention during 2011-12. These exercises and workshops will focus respectively on the XXXX1, XXXX2 and XXXX3 phase of a national security incident.

The exercises will be based on the *Red Teaming* concept where a group of Subject Matter Experts (SMEs) will act as a *Red Team* that will act as a devil's advocate to identify gaps in existing organisational plans and to challenge traditional thinking, routine behaviours and anticipated responses

As this style of exercise has never been conducted under the ANZCTC banner, the working group will explore the relevance and future applicability of the *Red Teaming* type concepts to the ANZCTC exercise program.

Aim

The aim of *Southern Intellection* is to explore the preventative arrangements designed to detect and prevent X within the contemporary threat environment and determine opportunities for improvement.

Objectives

There are three strategic objectives, followed by seven sub-objectives focused on specific areas to be addressed by participating agencies in achieving the overarching objectives.

Strategic Objectives

(overarching objectives for the activity)

Sub-Objectives:

(More specific objectives related to particular outcomes of the activity)

Exercise Format

Southern Intellection will take the form of scenario-driven facilitated discussions between participants and will contain an element of the military *Red Teaming* Concept.

The Red Team (SMEs) will be located in a different room and will provide their response through the facilitator.

This aim of this format is to challenge participant's responses in order to highlight gaps and areas for improvement.

Exercise Context

Exercise participants will use real-world data and/or their professional judgement in the absence of information provided by the scenario.

Control documents or a response from the Red Team will be provided where applicable.

Exercise Assumptions

The following assumptions underpin the planning for the exercise:

- The scenario is designed to explore the issues within the exercise.
- Exercise participants are well-versed in their own organisation's prevention, preparedness, response and recovery plans and procedures, and
- Implementation of specific organisational response plans and procedures indicate actions that are expected to occur under actual response conditions and, therefore, provide a sound basis for analysis.

The scenario for *Southern Intellection* incorporates a number of fictitious entities, including people, addresses, businesses and phone numbers. It is important to note however that they are based on real life equivalents.

The exercise is premised on the current security environment (security alert level of Medium).

As a result when considering a question it should be in conjunction with your actual knowledge of local, international and security environment and your agencies current practices and procedures.

Exercise Materials

Participants will only receive the Participant Handbook prior to the exercises, which contains pre-reading material on page 16. In addition to this, participants should be well across their own organisations procedures and processes.

Exercise Security Classification

All participants and any observers are required to have a minimum security clearance of **(nominate appropriate level)**.

PARTICIPATING AGENCIES

(list agencies involved)

EXERCISE CONTROL STRUCTURE

Role	Name(s)
Chief Controller and Workshop Facilitator	
Deputy Controller / Exercise Management Capability	
ANZCTC Exercise Coordinator	
Scenario Tracker Team Leader/ SME Liaison	
Scenario Tracker	
Scenario Tracker	
Scenario Tracker	
Facilitator	

Assistant Facilitator	
Administration	
Administration / Chief Safety Officer	
Issues Monitor	
Subject Matter Experts – agency 1	
Subject Matter Experts – agency 2	
Subject Matter Expert – agency 3	
Subject Matter Expert – agency 4	

PARTICIPANTS

Agencies	Names

SUBJECT MATTER EXPERT (SME) GROUND RULES

Subject Matter Experts (SMS) will essentially be the Red Team for this exercise. As the Red Team they will challenge traditional thinking, challenge both implicit and explicit assumptions, look at alternative perspectives and take a critical look at plans, processes and procedures to identify areas where such plans, processes and procedures could go wrong, oversights, flaws in reasoning etc.

This process is designed to identify gaps in existing organisational plans and to challenge traditional thinking, routine behaviours and anticipated responses.

Ground Rules

SMEs are asked to use the following exercise ground rules as a guide in order to best achieve the aim of the exercise. SMEs should:

- Assess participant's response and consider all aspects that are effected in the scenario,
- Develop red team response to expose gaps in the current process and planning procedures displayed by participants,
- Consider real resources on hand in day to day business when developing a response,
- Consider all parties affected when developing a response (see below considerations), and
- Provide all injects/responses through the Facilitator.

Considerations

The Red Team are constantly acting as all parties involved in the scenario. The will need to always consider who would be affected by the scenario and the participant's responses, and act as the opposing side. Some groups and roles they will consider are:

- Daily Resources and Conditions, including:
  - Personnel
  - Equipment
  - Intelligence and Information
  - Weather
  - Regular Events

- Characters from exercise scenario may include but are not limited to:

  - S Council
  - F Community
  - Other Communities
  - Universities
  - Businesses
  - Xs
  - Witnesses
  - Police
  - Emergency Services
  - Government
  - Senior Decision Makers – State and Federal
  - Legal Advisers (Legislation)
  - International and local events
  - Councils
  - Funding Organisation/authority

INVESTIGATION WORKSHOP

The Workshop will be conducted the day following the exercise to examine and discuss findings and issues raised during the exercise and consider possible treatments.

The workshop will be facilitated by *(name)*.

Aim

The aim of the workshop is to discuss key vulnerabilities identified during the exercise relating to the current X investigative arrangements and identify treatment options.

Schedule

Wednesday 29 February 2012

0830 - 0900 Welcome and Introduction

0900 – 0930 Recap from previous day

0930 – 1015	Each agency is expected to list the issues they identified that need improvement and suggest possible solutions (resources, money, other investigations, political/social affects etc.). Will include feedback from the Issues Monitoring Team (IMT)
1015 – 1045	Morning Tea, including an opportunity for informal discussion between participants
1045 – 1130	Continue Issues identified, including Red Team Input
1130 – 1230	Presentation 1 & 2
1230 – 1300	Lunch
1300 – 1330	Presentation 3
1330 – 1500	Summary and Survey

GENERAL IDEA

(a one and a half page description of the relevant individuals and their general activities, the overarching context, scenario elements of importance, relevant events here and overseas, etc.)

EXERCISE BACKGROUND – In Exercise

Outcomes of Phase 1

(outline the outcomes of the previous related activity, particularly as they are relevant to the current activity)

Part 1 - Today is Tuesday 27 September 2011 *(topic area and exercise objectives addressed)*	
(brief description of the current situation, the relevant factors and events coming into play, and any new information that should be considered) **Aim *(of the special idea)*: To identify issues related to the management of items during a X Investigation.**	
Outcomes:	**Primary Questions**
(What are the issues or questions that should be answered during this discussion)	1. What are the key issues relating to this situation and why? *(who are these questions primarily aimed at)* ***Closing question:*** 2. How will you address the issues you have identified? *(who are these questions primarily aimed at)* 3. *If required* - What ongoing advice and direction would you give to the staff member on how to deal with this source? *(who are these questions primarily aimed at)*
Red Team Scope	**Red Team Considerations**
(what role do they play and what requirements should they be addressing)	*(what important things might impact on the way the red team conducts itself)*

Control Documents	Order of Events
(List the relevant documents required for this special idea in order)	*(List the events in the order required for this special idea in order)*

Note: The Facilitator Handbook

The facilitator handbook is structurally similar to the red (and blue) team handbooks, however it contains more depth of information regarding the scenario, the special ideas, the supporting documents and the intended outcomes. It also contains: the text of the exercise briefing that the facilitator will need to provide to the participants (red and blue teams); the biographic information of the red team members so they can be introduced to the blue team; and the description of the exercise setup and how it will be conducted so that the facilitator can introduce these concepts to the participants (particularly any new participants who did not take part in the previous activity).

DEFENCE SCIENCE AND TECHNOLOGY GROUP DOCUMENT CONTROL DATA	1. DLM/CAVEAT (OF DOCUMENT)

2. TITLE	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (U/L) NEXT TO DOCUMENT CLASSIFICATION)
A Simple Handbook for Non-Traditional Red Teaming	Document (U) Title (U) Abstract (U)
4. AUTHOR(S)	5. CORPORATE AUTHOR
Monique Kardos and Patricia Dexter	Defence Science and Technology Group PO BOX 1500 Edinburgh, SA,5111

6a. DST Group NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DST-Group-TR-3335	AR-016-782	Technical Report	January 2017

8. Objective ID	9. TASK NUMBER	10. TASK SPONSOR
AV14666724		

13. DOWNGRADING/DELIMITING INSTRUCTIONS	14. RELEASE AUTHORITY
	Chief, Joint and Operations Analysis Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No limitations

17. CITATION IN OTHER DOCUMENTS Yes YES

18. RESEARCH LIBRARY THESAURUS

Red Teaming, critical analysis, contestability, bias, heuristic

19. ABSTRACT

This report represents a guide for those wishing to apply red teaming methods in a structured manner, and provides lessons developed in both the military and national security environments. It describes the practice of red teaming in the context of biases and heuristics followed by techniques and activity designs allowing others to design and apply red teaming activities across a range of domains.