Australian Government
Department of Defence
Defence Science and
Technology Organisation

Moving Forward with Computational Red Teaming

Scott Wheeler

Joint Operations Division
Defence Science and Technology Organisation

DSTO-TN-1104

ABSTRACT

The term *Computational Red Teaming* has recently arisen within the literature to describe the application of new and innovative analytic techniques, tools and methodologies in support of Red Teaming Activities. This report explores Computational Red Teaming as a concept, which is itself undergoing transformation and growth within the practicing community. It describes just what Computational Red Teaming is, how it is applied, and its benefit over traditional Red Teaming practices and techniques. A framework of three key activities: *Information Management*; *Conduct and Execution*; and *Scrutiny and Analysis*; is then developed and decomposed into constituent functions for analysis.

Published by

Joint Operations Division
DSTO Defence Science and Technology Organisation
Fairbairn Business Park Department of Defence
Canberra ACT 2600 Australia

Telephone: (02) 6265 9111
Fax: (02) 6265 2741

AR-015-352
July 2012

APPROVED FOR PUBLIC RELEASE

Moving Forward with Computational Red Teaming

Executive Summary

The term *Computational Red Teaming* has recently arisen within the literature to describe the application of new and innovative analytic techniques, tools and methodologies in support of Red Teaming activities. The approach introduces novelty to Red Teaming, which is yet to be exploited; proposing to reduce risk and increase opportunities through computation.

This report presents Computational Red Teaming as a concept, which is itself undergoing transformation and growth within the practicing community. Perspectives from the literature are presented to explore just what Computational Red Teaming is, how it is applied, and the perceptions of benefit over traditional Red Teaming practices and techniques.

Having explained the concept, and after reviewed the range of competing perspectives within the field; this report defines the term formally and develops a framework to categorise the field of Computational Red Teaming by the three key functions of: *Information Management*; *Conduct and Execution*; and *Scrutiny and Analysis*.

A full taxonomy is developed by means of functional decomposition.[1] This taxonomy can be used to rationalise the application of Computational Red Teaming techniques within a program of work, task or an experimental campaign; by mapping or cross referencing the framework taxonomy elements against analogous manual tasks conducted within the program. This mapping can also be employed to identify where the functions of Computational Red Teaming can be applied, to add value or support program outcomes.

The following recommendation is advised, for forward work planning within the Joint Operations Division's Computational Red Teaming Task.

Recommendation 1.

The JOD Executive should consider initiating a scoping study of one targeted task within the division. This study would apply the taxonomy developed in this report, in

[1] Functional elements are decomposed into their constituent components (Figures 1, 2, and 3 on pp. 22-24). The framework itself is also indexed to the fundamental sciences which underpin the functional elements and a set of critical enablers (Table 2 on p. 16).

order to identify where Computational Red Teaming tools and techniques could add-value (or otherwise contribute) to the task.

This research has been conducted as part of the JOD program of work into the study and development of Computational Red Teaming, following earlier work presented by Gowlett (2011). Gowlett called for the development of a divisional concept demonstrator for Computational Red Teaming. He argued that a niche capability might be developed in a specific targeted area. Should that effort prove successful, a wider program of research could be initiated.

Gowlett's recommendations are still relevant today and development of this proposed prototype can be informed by our functional taxonomy. The greatest benefit is derived if a formal design methodology, such as Systems Engineering, is adopted because of the synergies between the structured approaches. The functional taxonomy is then employed as a cross reference against the design methodology. However, this is only meaningful if the design also employs functional decomposition. Systems Engineering is then a good candidate methodology for the design.

We reinforce the recommendation of Gowlett.

Recommendation 2.

The JOD Executive should consider supporting the development of an executable prototype model for Computational Red Teaming. This prototype should be narrowly focused, as a concept demonstrator, and designed formally through adoption of Software or Systems Engineering practices. This approach will ensure best practice is followed in design and that minimal resources are consumed.

Author

Scott Wheeler
Joint Operations Division

Scott Wheeler joined DSTO as a Research Scientist after completing a PhD in mathematics at the University of Adelaide. Scott previously managed the Complex Adaptive Systems Task in Land Operations Division at the DSTO Edinburgh site before moving to the Defence Systems Analysis Division in Canberra's Russell Offices. In Russell, Scott worked in the domain of Capability Analysis and was the Science Advisor to the Missile Defence Coordination Office. More recently he represented Australia as the National Lead for TTCP AG-14 Complex Adaptive Systems. Scott was previously a Visiting Research Fellow at the University of NSW, Australian Defence Force Academy and now works for the Joint Operations Division DSTO in Fairbairn, Canberra.

This page is intentionally blank

Contents

List of Tables

List of Figures

Acronyms

Acronym	Definition
ADF	Australian Defence Force
ADFA	Australian Defence Force Academy
API	Advanced Programming Interface
ART	Automated Red Teaming
CERP	Corporate Enabling Research Program
CRT	Computational Red Teaming
DGCP	Director General Capability and Plans
DSARC	Defence and Security Applications Research Centre
DSTO	Defence Science and Technology Organisation
JDSC	Joint Decision Support Centre
JOD	Joint Operations Division
OPFOR	Opposing Force
ORBAT	Order of Battle
SME	Subject Matter Expert
UNSW	University of New South Wales

This page is intentionally blank

1. Introduction

1.1 Computational Red Teaming

"The use of red teaming practices and effective capability analysis to assess success on the battlefield is no longer just confined to military campaigns. In today's corporate battlefield decision makers are realising the need to reassess their approach to winning and maintaining their businesses. An innovative, proactive strategy to business management is required where vulnerabilities of systems, practices, processes and structures need to be quickly addressed, and dealt with." (Red Team Consulting, 2011).

The term *Computational Red Teaming* (CRT) has recently arisen within the literature to describe the application of new and innovative analytic techniques, tools and methodologies in support of Red Teaming Activities. This approach introduces a novel element to Red Teaming which is yet to be exploited; proposing to reduce risk and increase opportunities through computation.

Following its original use by Yang *et al* (2006), there have been many competing descriptors including *Automated Red Teaming*, *Auto Red Teaming*, *Assisted Red Teaming* and *Computerised Red Teaming*. As with any new field of research, there is debate as to the precise understanding of the term. As a result, there is some uncertainty and confusion as to when CRT can be applied and its suitability for use within specific research programs, in both the civilian and military domains.

1.2 Background

The program for CRT within the Joint Operations Division (JOD) of DSTO has been running since 2009; originally proposed as an application of *Asymmetric Business Modelling*. The client, Counter Improvised Explosive Device Task Force, provided the application area for the research.

JOD engaged academia to determine potential directions for further work, leading into the report *Moving Forward with Computational Red Teaming* by Gowlett (2011). This report presented a number of options to progress the program. One of its key findings was that the field of research was comparatively new and was beset by problems of understanding. Gowlett recommended further scoping of the field, noting that an approach based on first principles was merited.

1.3 Scope

This report implements the recommendation of Gowlett (2011). It will provide a scoping study of CRT to advance the science in this field.

1.4 Outline

This report is structured in three sections:

a. initial definition of terms and scoping of the field;

b. a framework which categorises the domain of CRT by function; and

c. delivery of recommendations for the JOD program.

Section 2 begins from first principles to define the terms Red Teaming and CRT. These definitions provide a foundation for this study from which concepts for the implementation of CRT are be developed. A summary literature review is also presented at the end of the Section. The review introduces some of the many and varied applications for CRT for Defence.

Having established a working definition for CRT, Section 3 builds a framework which identifies a core set of three root functions. Using this framework, the principle techniques and approaches within each function are identified. Finally, spanning all of the functions, a set of capability is developed which underpins those functions. This perspective is provided in contrast with the description provided in Section 2, which explains the purpose of CRT. Given both perspectives, a practitioner will be better informed in identifying potential applications for CRT and the techniques within the field which would be useful to that application.

2. Background

2.1 Alternative Analysis

"Whether you run a corporation or a country, the stakes are high, and business as usual is no longer good enough. More than ever, you need to know what your competitors and opponents are thinking. You need to overcome your organization's biases and generate creative, resourceful strategies that work. You need to anticipate the next crisis, prevent it if possible, and respond swiftly and effectively if not." (Mateski, 2008).

Mateski (2008) presents a compelling case, expanded upon in his paper. The global strategic environment is complex, uncertain and of a faster tempo than every before. It is also comprised of a greater range of government, non-government and non-conventional protagonists (both friendly and adversarial) with diverse mandates, objectives and goals and each in possession of different levels of capability with varying capacities to fulfil those goals. To comprehend an adversary's actions in such an environment is a noble aspiration. However, no adversary will ever knowingly provide such insight to their opposition (Malone & Schaupp, 2002).

The term *Alternative Analysis* has been coined to encompass the class of techniques which seek to study decision-making processes, with the aim to improve them (Red Team Journal, 2009). In essence, Alternative Analysis seeks to both progress a rigorous framework for critical self-review and to establish a scientific basis for the study of Adversarial Reasoning. Applications

within the field inform policy makers and analysts through formal techniques. To that extent, Alternative Analysis also encompasses practical branches of research with the direct intention of generating actionable outcomes through structured argument (Fishbein & Treverton, 2004).

Alternative Analysis offers many benefits. Through formal process, intuitive understanding can be elicited, structured and tacit knowledge explicitly recorded in explicit form. The field helps to overcome bias in thinking and to define working assumptions. Techniques can also help to identify uncertainty, knowledge gaps and explore associated risks.

2.2 Red Teaming

Red Teaming is perhaps the principle domain of application for Alternative Analysis; to the extent that the two are often considered synonymous. This term originates from American military war gaming in the era of the Cold War.[1] The *blue team* was traditionally the United States and the *red team* the Soviet Union. In this context, Red Teaming was the term used to describe structured activities or exercises wherein participating personnel played the opposing side to understand the competitive context between both sides and their possible action spaces in potential future states (Beck, 2000).

There are many definitions of Red Teaming (refer to Appendix A). Different definitions emphasise one or more perspectives or components of Red Teaming. However, throughout the community or practice, there also exists a root understanding, which is accepted as being a core. The Red Team Journal (2009) defines this loosely, "Red Teaming is the practice of viewing a problem from an adversary or competitor's perspective." In this fashion, "Red Teaming is seeking to get inside the heads of adversaries, not asking what we would do if we were them but creatively trying to ask what they might do given their own goals, culture, organization, and the like." (Treverton, 2001).

However, it is important to understand that Red Teaming does not necessarily require the existence of a traditional adversary, defined in the military context as the Opposing Force (OPFOR). Red Teaming techniques are also applied to critique ones own planning, strategy and execution. When applying Red Teaming, the Red Team may notionally represent:

- neutral or unaligned agencies;
- 'mindless' organisms (such as viral contamination or disease);
- physical or environmental effects (such as arctic frost or radiation);
- natural disasters and events (such as wild fires or floods); and
- situational concepts (such as the strategic environment or political context).

[1] The concept is considerably older. Lauder (2009) explains that from a war-gaming perspective, "games in various forms date back to the second and third millennium BC". Contemporary war-gaming can perhaps be credited to George Heinrich Rudolf Johann von Reisswitz, who used the practice to train Prussian military officers in the early 1800s.

In this sense, the term Red Teaming is not the focus of the activity. It is the element of *challenge* that is the critical defining element of Red Teaming techniques and that challenge does not have to come from role play of a sentient opposition.[2] The definition proposed above is then insufficient because it fails to capture this aspect. The distinction is also noteworthy because it distinguishes Red Teaming from the related field of *Adversarial Reasoning* (Kott & McEneaney, 2007). Adversarial Reasoning specifically studies decision making against a sentient opponent. While there is significant overlap between the two, they are nonetheless distinct.

For the purposes of this report, we use the term Red Teaming broadly; as a synergy of the concepts and themes taken from definitions within the military and civilian domains. We define Red Teaming as follows:

> *Red Teaming is the practice of critical analysis, through means of challenge and contest of argument, as conducted by an independent party, in the study of reasoning, and for the purposes of improving decision-making processes.*

This definition captures all of the key criteria for Red Teaming and avoids over-specification. Other themes which have been rejected focus on particular areas of application, client space or owner (for example, informing policy development, national security, or intelligence respectively). Some definitions specify the composition of the Red Team and their qualifications (for example, being adaptable or multi-disciplinary). Others highlight a perception of benefit in the technique (for example, creating collaborative learning relationships).[3]

2.3 Context of Application

Lauder (2009) notes that applications of Red Teaming are based upon "client needs, available resources, and the context of the operating environment." However, these do not guarantee definitive outcomes. Within the limits of what is known or can be deduced, Red Teaming can only develop theories and models of ones own decision processes and the reasoning of an adversary. It can be used to explore a range of possible future contexts but will not generate a definitive end state.

However, this alone is particularly useful in military planning because it can be used to cue commanders' information requirements. Malone & Schaupp (2002) provide a critique of Red Teaming as applied to military planning and course-of-action development.[4] They explain that Red Teaming can help synchronise plans, identify shortfalls, exploit overlooked

[2] Although historically this has been the case.
[3] This definition does not specifically mention vulnerability and penetration testing (ethical hacking for example). However, it is implied that such activities also fall under the broad concept of critical analysis (of a system) by means of challenge. The reasoning then applies to reasoning about the system. This reasoning is still conducted for a purpose; that being, informing an outcome by supplying experimental based evidence to decision makers.
[4] Those unfamiliar with military planning may refer to Australian Army (2001) for an explanation of the Australian Military Appreciation Process.

opportunities and extrapolate unanticipated implications. In this sense, by its very nature, Red Teaming ideally leads staff to develop robust, adaptive and flexible planning products.

In general, Red Teaming is used across both public and private sectors and is not the sole domain of the military. Red Team Consulting (2011) notes that "the use of red teaming practices and effective capability analysis to assess success on the battlefield is no longer just confined to military campaigns. In today's corporate battlefield decision makers are realising the need to reassess their approach to winning and maintaining their businesses. An innovative, proactive strategy to business management is required where vulnerabilities of systems, practices, processes and structures need to be quickly addressed, and dealt with."

The particular benefits gained from Red Teaming depend on the context of application. Within any sufficiently complex competitive environment, there are benefits to be gained from the robust planning processing enforced when Red Teaming techniques are applied and advantages to be leveraged from considered analysis of opponents. Mateski (2009) identifies a framework in which Red Teaming is applied in one or more of four possible contexts:

- *understand* (yourself, the adversary, and the conflict environment);
- *anticipate* (opponents actions, the resultant consequences, and possible outcomes);
- *test* (your strategy or plan, the force structure, operational concepts, and doctrine);
- *train* (your force and develop professional expertise).

Decision making (one's own and adversaries) is traditionally heavily dependent on experience and instinct. This experience is essential in understanding how factors in an operational environment influence one another. Although Red Teaming today is also critically dependent on subject matter expertise, it is structured to compensate for individual bias. As an application domain of Alternative Analysis, Red Teaming shares all of the benefits (and weaknesses) inherent to the field. Through directed process, assumptions are challenged and tested in accordance with the scientific principle of Critical Rationalism (Chalmers, 1999).[5] This presents an epistemological basis for the application of Red Teaming techniques within a structure of conjecture, critical review and refinement. In this way, Red Teaming can be applied to better understand your own force, adversary (and friends), and the conflict environment.

As noted by Craig (2007), anticipating an opponent's actions, the resultant consequences of those actions, and the range of possible future outcomes is no trivial matter. Red Teaming assists stakeholders to identify outliers, exceptions, special cases and external factors that are not otherwise addressed through other traditional *blue-centric* methods. Identification of uncertainty in judgement, gaps in knowledge and risks in outcomes are specifically targeted. No technique can provide certainty. Red Teaming does, however, produce an auditable trail of logic, together with reasoned analysis. With this record of rational, logical argument and analysis, it supports development of actionable outcomes.

[5] Also popularly known as the science of Critical Thinking Theory.

Red Teaming can also be used as a means to perform audits (Malone & Schaupp, 2002). Decision makers are often interested in knowing the breaking points of strategies or plans, the critical vulnerabilities and capability gaps in force structures, flaws in operational concepts, and weaknesses in doctrine. Testing, audit and evaluation then support the development of contingency plans and also underpin the process of refinement of existing plans. As further point of note, this testing function can be conducted against proposed (virtual) systems and established systems in-being. Peer review is an important part of the function of test and evaluation. However, other techniques such as *directed attack* are also common (for example, within the *ethical hacking* community).

When used to train personnel, Red Teaming is a facilitated mechanism which presents opportunities for participants to learn (US Army, 2008). Red Teaming can be used to sharpen existing skills or develop new ones. It can also be used as a form of knowledge transfer, to brief participants of advancements in the capability of the adversary or ones own. For example, the application of new technology and practices, and their impact on operations, is likely to be both explicitly absorbed during Red Teaming background briefs and also to be implicitly absorbed over the course of the activity. Techniques which are applied during Red Teaming for training purposes include use of case studies, coaching and mentoring, reflective supervision and consultation, amongst others. In all cases, the objective is to enhance the capability of personnel, in their chosen profession or role, by means of inquiry. This process of inquiry encourages statement of the rational for their beliefs and practices.

Mateski's (2009) framework has since been reinterpreted by Lauder (2009). Lauder takes a complementary approach which presents an alternative perspective to the original work. This is useful because it provides clarity on the context of application for Red Teaming. Lauder also proposes a framework of four contexts for the application of Red Teaming:

- *innovation*
  (policy, concept, program or product development leading to transformation)
- *planning and analysis*
  (planning, design and development, and predictive intelligence analysis)
- *operations*
  (assessment of live / operational activities, systems or networks)
- *training and professional development*
  (individual and collective training; typically in an exercise environment)

The matching between Lauder's framework and Mateski's is presented in Table 1. This matching is not identical and the two authors do not entirely overlap. However, it is still useful to contrast the two authors to aid comprehension.

Table 1: Frameworks for Red Teaming - Mateski (2009) and Lauder (2009)

Element	Mateski	Lauder
1	Understand	Innovation
2	Anticipate	Planning and Analysis
3	Test	Operations
4	Train	Training & Professional Development

2.4 Computational Red Teaming

CRT is a comparatively new research science, within the wider field of computational modelling and the boundaries of the field are less well defined than that of Red Teaming. Central to the field is an objective to enhance the quality of decision making by "increasing the degree of rigor that can be brought to bear on complex problems." Gowlett (2011).

One of the core concepts in Red Teaming is incorporating alternative perspectives into decision-making. Often, decision makers fail to account for the range of opposing (yet equally valid) viewpoints and base their decisions solely on their own. Longbine (2008) remarks, "by understanding these tendencies and accounting for these alternative perspectives" better decisions can be made.[6] Both Alternative Analysis and Red Teaming seek to improve the robustness of decision making processes; to provide both better outcomes and also to provide a greater range of options. The question then remains as to how internal bias can be addressed when it is an instrumental part of the cognitive processes of every human being and how options can be developed, assessed and analysed with finite resources. CRT is a subset of the field of Red Teaming which specialises in providing such support.

Abbass and Barlow (2010) attribute the seminal work in the field to Yang *et al* (2006). "Collaboration between the Defence Science and Technology Organisation (DSTO) and the University of New South Wales (UNSW) campus at the Australian Defence force Academy (UNSW@ADFA) ... established the first use of Red Teaming within the computational sciences." Shortly after, Choo *et al* (2007) adopted the use of the term *Automated Red Teaming*. In a more recent publication, Skroch (2009) debates the use of modelling and simulation in support to Red Teaming activities. Since then there have been a number of other publications in the area. Notably, Gowlet (2011) provides a comprehensive literature review of the field.

Campbell (2010) defines CRT as "the use of computer models and/or other mathematical techniques, using a variety of modelling approaches, that provide support to the red team in exploring and understanding the complex interactions… and the local population within which the actions are taking place in order to provide useful information to blue force." This description is representative within the literature (see Appendix B). As with the definition of Red Teaming, there is some variation and leeway in nuances of the phrasing. However, it is apparent that the root definition of the term is comprised of two key concepts:

[6] Longbine proceeds to discuss the psychological tendances of Mirror Imaging (applying ones own sociological mores, ethical codes, moral standards, and philosophical techniques to others) and Ethnocentrism (the inherent belief in ones own superiority over others and/or the superiority inferred through membership in a particular group, culture, organisation or entity, over another).

1. to support the application of Red Teaming; and
2. by means of modelling and simulation.

Campbell's definition is also notable in that it specifically draws attention to the fact that computational techniques do not necessarily have to be provided in the form of a model executed on a computer but also include all forms of applicable mathematical approaches. For the purposes of this report, we define the term as follows:

> *Computational Red Teaming is the science concerned with the provision of analytic tools, in support to Red Teaming, for the purposes of improving the outcome of its application.*

We also acknowledge that the provision of support to Red Teaming activities do not necessarily have to be through the use of computers. We use the term *analytic tools* to mean any form of applicable technique. In essence, CRT does indeed include any technique, model, approach and method which improve the outcome of a Red Teaming activity. More generally, this also includes models and frameworks which do not execute an explicit numerical function (for example; software whose sole purpose is the visualisation of information, or the storage of data).

2.5 Context of Application

CRT is also a constructive and efficient complement to traditional Red Teaming activities because it offers many advantages:

- computational techniques are not (directly) subject to limitations in human thought process, bias, experience, or capability;
- executable models can be used to explore and evaluate large numbers of possible states of interest, far more that a human could in the same period;
- those models operate, without loss of objectivity, in contexts where complexity would degrade human performance;
- simulations can be used to identify emergent behaviour, which might otherwise be unpredicted or unanticipated; and
- outcomes can be automatically recorded, visualised, and re-played for post-analysis.

To understand the advantages in applying CRT, first consider the limits to human decision making processes. *Bounded Rationality* is the idea that in decision making, rationality of individuals is bounded by: the information they possess; personal cognitive capabilities; and limiting timeframe. Established by Simon (1955), the theory attempts to explain how decision making is constrained by the available options, the perception of their value, and preference to outcomes and their likelihood. Simon draws attention to some of the observed limits in human decision making. People have difficulty when presented with too many or two few choices. This is sometimes called the *Paradox of Choice* or *Analysis Paralysis* (Schwartz, 2004).

Difficulties are also observed when presented with choices which are similar or options across an infinite space (for example, selection of an optimum on the real number line where the required level of precision is uncertain). Computational techniques do not suffer from these symptoms. Humans are also inclined to assign value to options based on subjective judgment; biased by their personal experiences and past history. A computer is entirely objective, within the scope of its original programming.

Next consider the aims of Red Teaming and extend them into the realm of computational techniques. Red Teaming seeks to provide decision makers with a greater range of options. Within the context of computer simulation, CRT can be used to explore a vast number of possible states of interest. In this way, it can be applied for the purposes of *Data Mining*. Additionally, those states of interest can be evaluated objectively against defined sets of measures. The logic of such evaluations is transparent and the rules and mechanisms are open for review.

Consider also the context of application. Oh (2009) explains how globalisation, the rise of emerging powers, environmental impacts and competition for resources, non-state actors, and advances in technology are all adding to the complexity of the future strategic environment. Military personnel are highly trained to manage such complexity. However, there are limits to human ability to understand complex relationships between the multitude of interacting entities and in identifying causes and effects (especially when confounded by effects offset in time). In such situations, it becomes difficult to make *good* decisions. Computational techniques operate, without loss of objectivity, in contexts where complexity would otherwise degrade human decision making abilities.[7]

CRT can be used to support Red Teaming activities by identifying emergent behaviour, which might otherwise be unpredicted or unanticipated. Emergence describes the way systems produce complex outcomes as a result of comparatively simple interactions. This is defined by Corning (2002) as "the arising of novel and coherent structures, patterns and properties during the process of self-organization in complex systems". CRT can be used to identify outliers and unexplained results, for further analysis, or generate a greater range of options for consideration by decision makers.

One final note is that outcomes of computational techniques, simulated on modern computers, can be automatically recorded, visualised, and re-played for post-analysis. When implemented appropriately, CRT can support all modern advances in computation including data farming approaches with parallel computation and database management. This is useful in analysis and search over large state spaces.[8]

[7] Abbass et al (2011) make similar observations; in terms of exploring a space of possibilities, in a world of "increasing connectivity, interconnectedness, interdependency and competition."
[8] See Project Albert (US Marine Corps Warfighting Laboratory, 2011) for more on data farming / mining and its use in supporting computational analysis.

2.6 Applications within Defence

Within the literature there are many papers which discuss Red Teaming and CRT. For our purposes, we limit the scope of review to those relevant to defence. Review of these papers will prepare the reader for Section 3, which develops a coherent framework for understanding CRT. Also, due to the large number of relevant publications, we focus on sources which review the field.

2.6.1 Agent Techniques

Berryman (2008) provides an overview of agent modelling environments, with demonstrated application for military use. These included BactWars, EINSTein, MANA, MASON, NetLogo, Repast, Swarm and WISDOM-II. This is important because Agent-based modelling is one of the more commonly applied methodologies in CRT.

The tools listed above largely fulfil the same functions. Each features, to varying degrees, support for discrete and real-time event scheduling, with a library of templates for custom implementation of agents through scripting, and visualisation and information management functions. Repast claims to "move beyond the representation of agents as discrete, self-contained entities in favour of a view of social actors as permeable, interleaved, and mutually defining; with cascading and recombinant motives" (SourceForge, 2011). However, this is also likely to be the aspiration of all of the toolsets above. This list of agent models specifically targets only agent-based distillations[9] and largely disregards other forms of agent modelling environments.

Carley (2004) documents the development of the large scale agent model, BioWar. The software offers a "scalable city-wide simulation, capable of simultaneously simulating the impact of background diseases, natural outbreaks and bioterrorism attacks on the population's behaviour within a city" (CASOS, 2011). BioWars has been applied to study infection, contagion, and outbreaks of disease. Within the scope of other large scale agent models, other potential applications include the study of preparedness in response to disasters (e.g. emergency response) (Wu *et al*, 2008), proliferation of Chemical, Biological, Radiological, and Nuclear contaminants (Ligt, 2010), behavioural studies of riot and crowd dynamics (Henein & White, 2005) and others. Since 2004, even larger simulations have been developed; Parker (2007) proposes a model of 100 million agents which is capable of modelling the dynamics within clusters of cities.

[9] "Agent-based distillations trade sophistication for speed and lower simulation costs. As a result simulations tend to be less scripted with less user input than high–fidelity high–cost combat simulation software or seminar wargames. In such models, the emergent behaviour of the system as a whole is considered more important than the behaviour of any single constituent part of the system. This emergent behaviour is a characteristic of complex adaptive systems resulting from combined low-level interactions between numerous low-level entities in the system. These entities act according to comparatively simple rules but their behaviours combine in synergy to exhibit complex dynamic behaviour." (Wheeler, 2005).

2.6.2 Decision Support

In 2008, DSTO was tasked by the Director General Capability and Plans (DGCP) to review the software available to support the then Force Options Testing program; which has since developed into the Force Structure Review. In reply, Lowe *et al* (2008) delivered an unpublished briefing which contained a review of almost 60 different tools.[10] The review was broad in scope but could be described as focusing on products which assist in decision support.

In support to DSTO, the Defence and Security Applications Research Centre (2008) reviewed almost 40 tools[11] in support of capability planning and decision making. The review is complimentary to Lowe *et al*, in that it specifically focuses on capability engineering, design and requirements. Tools such as this are essential to CRT in structuring, capturing and recording critical argument and logic.

More recently, the DSTO facility at Fairbairn in Canberra has been established to provide a flagship capability in decision support for defence. It was constructed in collaborative arrangement between DSTO and Capability Development Group and now offers services to Defence and wider national security services. The facility is called the Joint Decision Support Centre (JDSC).[12] The JDSC offer around fifteen tools to clients.[13]

---

[10] These included:
a) Tools from the UK for operational assessment: CLARION, DIAMOND, COMAND.
b) Force Allocation models: JOWST, TT, CHIMERA, JICM.
c) Strategic Lift models: MobSim, BRIDGE.
d) Performance Models for ORBATS against Military Tasks: H-Frame, CATACM, CapDIM, CRAM.
e) Campaign Level Models: ITEM, JSAF, GCAM, JSWAT.
f) Network Analysis: DARNOS.
g) Portfolio Investment: Equity.
h) Normative Group Techniques: FOT1999.
i) Decision Support Tools: DynaRank, Expert Choice, HIVIEW, On-Balance, VISA, HIPRE, Force Value Model, Project Viewer, FIDO, Monsarrat, Hi-Priority.
j) Miscellaneous Applications: EADSIM, WISE, JTLS, CAEN, FleetSIM, SOCRAM, Janus, CASTFOREM, Harpoon 3, JICM, TEMPO, FOX-Ga, JADE, DART, CAPS, TEM, STORM, NSS, EAGLE, BRAWLER, COSMOS, VIC, JIMM, SIMDIS, CATCAM, CapDim, iCAPT, FSAT.

[11] These included:
a) Planning and Management: Microsoft Project, InventX, Planisware OPX2, Vertabase, Artemis, CA Clarity.
b) Capability Engineering: Simunicator, iRise, METIS, Profesy, Statemate MAGNUM, Statestep, CORE, Scenario Plus.
c) Requirements Engineering: OpenOME, TIGER, ACE, ET, CARP, RAT, ARCWAY Cockpit, Cradle, DOORS, Enterprise Architect, FastTask, DataModeler, FreeFlow, GMARC, IBM Rational Suite (RequisitePro, Rose, ClearCase, ClearQuest), MooD Transformation Toolset, RDD.COM, CaseComplete, Contour.

[12] The JDSC Homepage is accessible online through the DSTO Restricted Intranet at: http://community.dsto.defence.gov.au/SiteDirectory/division/jod/JDSC/default.aspx

[13] These include: Engle Matrix Game, JSAF, BattleModel, JSAF Reports, Extend CP, STK, CNR-Sim, VBS2, OPNET Modeller, Grouputer, DARNOS, VR-Forces, SIMDIS and Falcon View.

2.6.3 Fundamental Sciences

Moving Forward with Computational Red Teaming (Gowlett, 2011) explored potential requirements for implementing a CRT program for CIED.

A total of four research papers were commissioned from each of:

- the University of South Australia (Campbell, 2010);
- the University of New South Wales at the Australian Defence Force Academy (Abbass & Barlow, 2010);
- the University of Western Australia (MacNish, 2010); and
- Edith Cowan University (Hingston, 2010).

These papers provide an overview of the literature, each from the perspective of their internal research programs.

An additional workshop was also held to bring together stakeholders in the field. The workshop was held in Canberra at the JDSC on the 7th of June 2010. A mix of seventeen academics and DSTO personnel presented their work and discussed future research directions.

The outcomes of this workshop were directed towards informing two key initiatives in the field; namely, the sciences of CRT, and their applications to CIED. Gowlett concluded that the science of social and cognitive modelling underpinned the successful development of models for CIED, particularly agent-based models. He further concluded that search algorithms and methodologies for the conduct of data mining and exploration activities over complex problem domains and scenario spaces were essential for successful application and analysis of those models.

3. Understanding Computational Red Teaming

3.1 Towards a Coherent Understanding

To further the understanding of CRT and the scope of its application, it is necessary to develop a method by which this vast array of information can be managed. A simple framework has been developed to identify and bound the space. Such a framework acts to aid comprehension and can be used to broadly categorise the techniques, fields of study, methods and practices employed.

3.2 A Framework for Computational Red Teaming

In Section 2, two context-based frameworks (Lauder, 2009; Mateski, 2009) have already been proposed. These are helpful in explaining how CRT is used. By their nature, they do not provide a decomposition of the field by function. The difference between a context-based and function-based framework is that the first informs you where to apply CRT and the second directs you in choosing an appropriate approach.

The framework is presented over-page. It is divided into three layers, a set of corresponding disciplines and a set of critical enablers. Only the first two layers are displayed in Table 2. The third layer is presented in Figures 1, 2, and 3.

1. *Functions*: Provides the top-level functions. Three functions are presented including Information Management, Conduct and Execution, and Scrutiny and Analysis.
2. *Sub-functions*: The layer which provides a decomposition of the corresponding top-level function into its second-level sub-functions.
3. *Third-level functions:* The layer which provides a decomposition of the corresponding second-level into their third-level functions.
4. *Discipline*: A list of fields of research from which the base skills, techniques, and methodologies in each category are derived.
5. *Critical Enablers*: These items span all categories. They can be considered to be universal in supporting the entire range of functions performed in CRT.

The third level functions are explained in more detail in Appendix C. The critical enablers are explained in the following section.

Table 2: CRT framework

Functions	1. Information Management	2. Conduct and Execution	3. Scrutiny and Analysis
Sub-Functions	Collection, Capture, Storage & Retrieval of Information Data Design, Architectures & Structured Representations Visualisation & Replay	Adjudication Knowledge Discovery Problem Scoping & Structuring Quality Control & Management	Adversarial Reasoning Assumption Testing Data Mining
Discipline	Computer & Information Sciences Information Engineering Software Engineering Systems Engineering	All Branches of Science for Experimental Practice Military Service Softer Systems Sciences Systems Engineering	Cognitive Psychology Mathematics & Operations Research Psychometrics Sociology Social Psychology Statistical Practice

Critical Enablers	*Corporate Knowledge*	*Capacity to learn, incorporate lessons learnt, new practices & techniques*
	Expertise & Capability	*Experienced Red Teaming capability, a developed & mature support base*
	Planning & Guidance	*Focus & cohesion, outcomes are actionable & inform stakeholders*
	Professional Mastery (Military)	*Brings in the Military knowledge*
	Understanding & Comprehension	*Ability to understand the problem space and communicate this understanding*
	Verification & Validation	*Is conducted, against all components, the process and its outcomes*

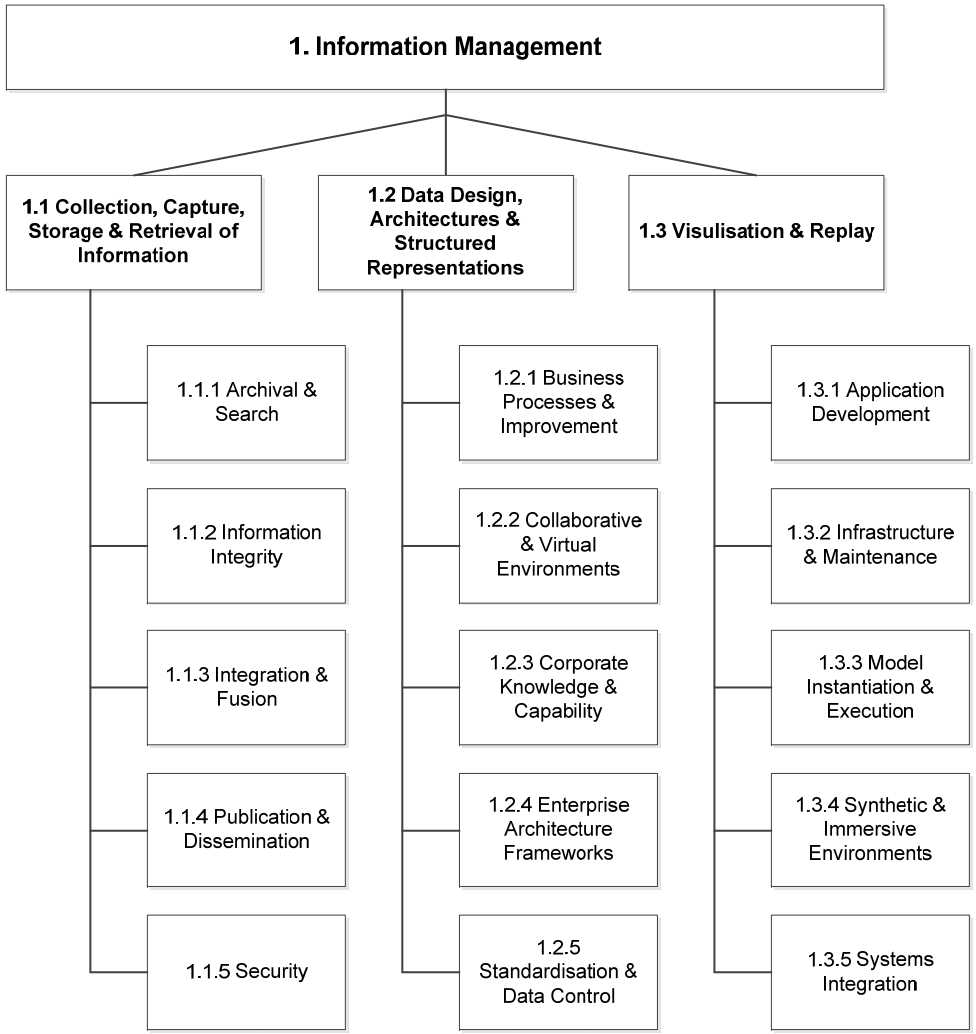

Figure 1: Information Management

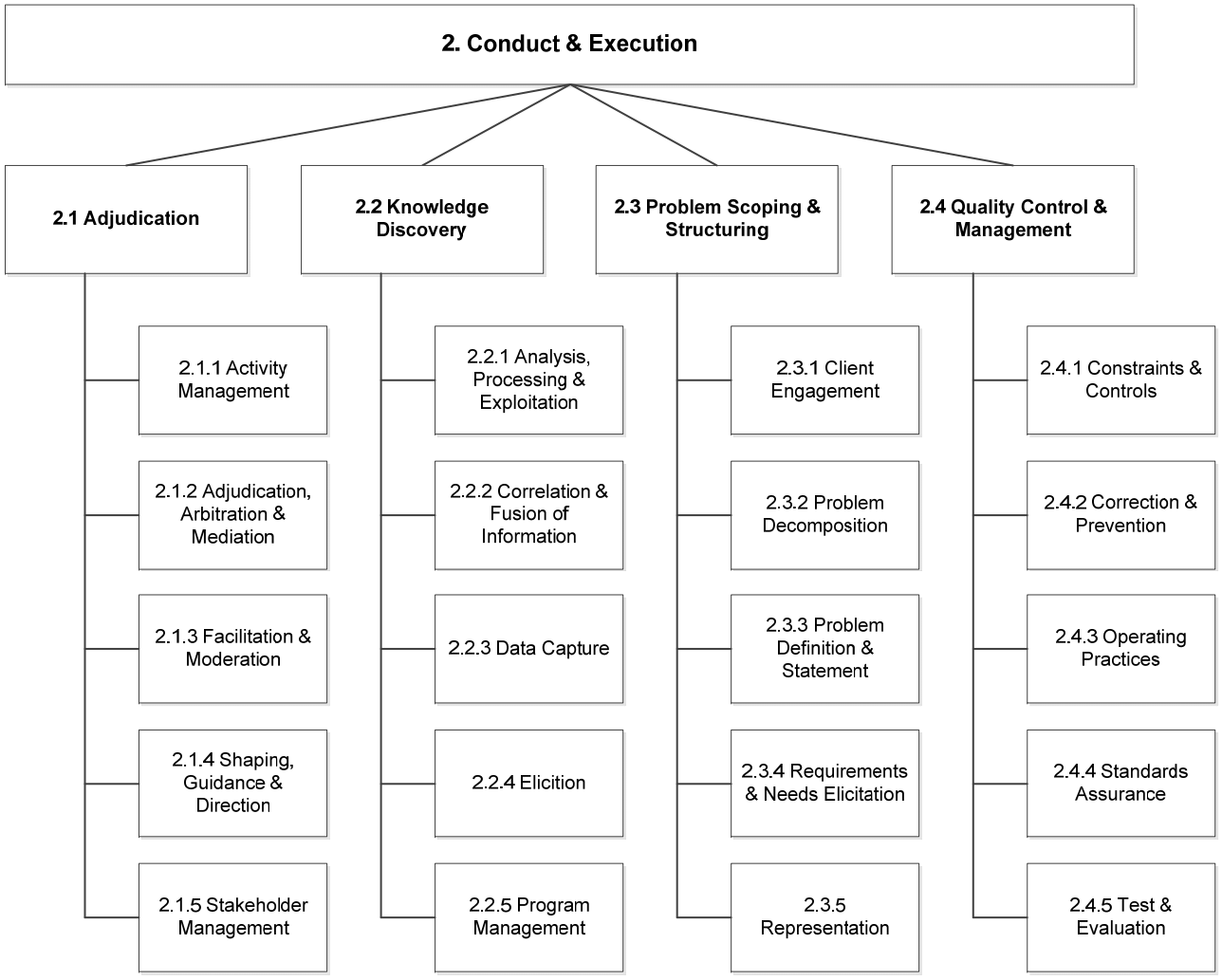

Figure 2: Conduct and Execution

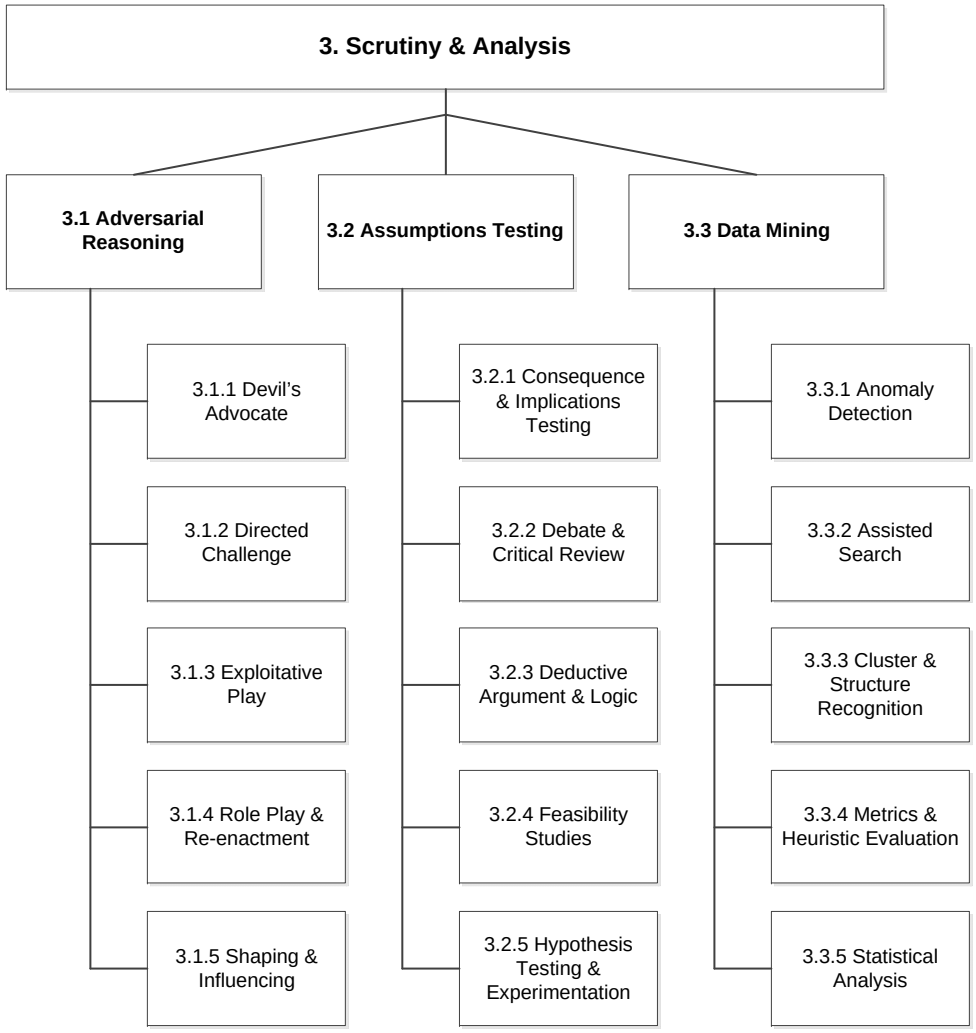

Figure 3: Scrutiny and Analysis

3.2.1 Critical Enablers

Table 2 presented six critical enablers; these being:

- Corporate Knowledge
- Expertise & Capability
- Planning & Guidance
- Professional Mastery
- Understanding & Comprehension
- Verification & Validation.

Corporate Knowledge includes the organisational capacity to evolve its CRT capability at all levels. It is often assumed that this evolution would improve, rather than regress, extant capability. However, in any practical program of work, resources are constrained and will change over time as working priorities change. This enabler encompasses the idea that the capacity to evolve includes evolution to states with lower capacity, should that be required.

Key to any evolution is the capacity to learn, incorporate lessons from experiences (within the organisation and from partner or cooperative activities with others) and to be open to trials of new practices and techniques within the field. New approaches are trialled based on potential benefit adopted into the program of work based on merit.

If Corporate Knowledge focuses on change and development then the enabler *Expertise and Capability* focuses on the maturity and experience of the CRT capability. This category denotes the level of excellence in practice attained by the organisation and the quality of their program. This includes the quality of research and sustainment of core skills.

The concept of a support base is an important consideration when assessing the level of expertise within the organisation. A mature CRT capability takes considerable time and effort to develop. "The role of the Red Team… requires that it be formed from experienced personnel from the functional disciplines applicable to the operations conducted." (Gladman, 2007). In short, participants must individually be experienced but also the collective experience within the Red Team must also be fit for the purpose at hand.

Corporate Knowledge describes the quality of inputs to the Red Teaming process and the development of capability meeting organisational needs. *Planning and Guidance* describes the quality of the outcomes and supported by the Red Team. Planning and Guidance is then output focused. These outputs must inform stakeholders and be actionable, by design. This guarantees that there is a purpose to the application of Red Teaming, in that its outcomes contribute to a client decision. Red Teaming for the sake of the action *per se* is not useful.

The generation of actionable outcomes requires focus and cohesion within the Red Team. Considerable planning should be conducted prior to the execution of any CRT trial. Deviations from original planning may be required, based on the needs at hand. In all

situations, maintaining focus on obtaining the required results for the activity is the principal consideration. All participants should be oriented to this end, although each participant might play their own part. In this way, individuals contribute to the group goal while maintaining individual speciality.

Understanding and Comprehension presents the opposing side of planning and guidance. This item denotes participants' abilities to understand the problem space. As outlined in Section 2.5, there are many concerns regarding limitations on humans' abilities to comprehend and manage complex problems or decisions. Throughout the entirety of the Red Teaming process, the single largest point of weakness is the individual. CRT has been promoted as being more robust but it is still fundamentally limited by the reasoning and ability of those designing, executing and analysing the computational support (Ryan, 2006).

Communication is essential in building mutually shared understanding. From conception, arrangements for the Red Teaming activity and associated computational support must be negotiated between stakeholders. During the activity, communication provides a means for knowledge transfer. Post-activity, any analysis, outcomes, results and recommendations must be briefed to decision makers.

Understanding and comprehension is also underpinned by the *Professional Mastery* brought by the military participants. Of all the contributing parties, in defence applications, the military are most valuable. Military knowledge is accumulated over years of training and honed through live exercises and deployment in the field. Lack of military participants cannot otherwise be easily compensated for because that specialist knowledge (and associated experience) does not reside elsewhere.

This military knowledge might otherwise be analogous in non-defence related applications to domain knowledge. Specifically, this is the idea that subject-matter expertise is held by participants; independent and separate from the expertise and capability relating to the process, conduct and science of Red Teaming.

Finally, *Verification and Validation* must be conducted against all components of the Red Teaming activity and computational support. "Verification and validation are independent procedures that are used together for checking that a product, service, or system meets requirements and specifications and that it fulfils its intended purpose." (Wikipedia, 2011). Verification describes the action of testing that a system complies with an internal set of requirements or specifications. Validation is a test process to make sure that the system or outcome conforms to the expectation (and original intent) of the consumer.

4. Summary and Recommendations

4.1 Applications to Programs of Work and Experimental Campaigns

In the introduction to Section 3, we built the CRT framework to aid comprehension and understanding of the field. The framework was developed from an aggregation of sources, listed in Section 6. It offers a structured perspective, which can be used to broadly categorise the techniques, fields of study, methods and practices from CRT. The utility of the framework for this application is yet to be put to the test and additional work will be required to confirm its completeness.

Now that the framework has been presented, we can broadly explain how it might be employed and tested. For example, it is possible to propose a mapping between the framework taxonomy elements and tasks conducted within a specific program or work or campaign of experimentation.

Within the JOD of DSTO, there are opportunities to conduct such a mapping within each of its Major Science and Technology Capabilities: Joint Systems Analysis; Joint Operations Analysis; and Joint Simulation. For example, the mapping could assist the division to rationalise its support to the Force Structure Review or manage and understand how the division supports key Defence Projects.

In the JOD CRT program, the framework taxonomy elements could also assist planning activities and direct longer term research in specific focus areas. This leads us to recommend the following approach.

Recommendation 1:

> The JOD Executive should consider initiating a scoping study of one targeted task within the division. This study would apply the taxonomy developed in this report, in order to identify where CRT tools and techniques could add-value (or otherwise contribute) to the task.

A likely candidate for such a scoping study is within the JOD Task at the Joint Decision Support Centre. This centre has perhaps one of the most diverse portfolios of work and is currently undergoing a range of software development activities, in support of the Force Structure Review and defence capability planning within the Capability Development Group.

Moving Forward with Computational Red Teaming

This research has been conducted as part of the JOD program of work into the study and development of CRT following from Gowlett (2011). It addresses Gowlett's principle finding[14] and implements his key recommendation for rigorous scoping the field from first principles.

The next logical step is to implement Gowlett's second key recommendation. Gowlett called for the development of a divisional concept demonstrator. This demonstrator would take the form of an executable model. He argued that a niche capability might be developed in a specific targeted area.[15] Should that effort prove successful, a wider program of research could be initiated.

Gowlett's recommendations are still relevant today. We recommend the following approach is adopted within the future work program of the JOD CRT Task.

Recommendation 2.

> The JOD Executive should consider supporting the development of an executable prototype model for CRT. This prototype should be narrowly focused, as a concept demonstrator, and designed formally through adoption of Software or Systems Engineering practices. This approach will ensure best practice is followed in design and that minimal resources are consumed.

An appropriate application area for this prototype is in the study and assessment of ADF capability. The preferred application domain for the program is to study countering Improvised Explosive Devices in Afghanistan.

5. Acknowledgements

Thanks are extended to all of those who contributed to this report. There have been almost too many to mention individually. However, special mention is provided to key personnel in Appendix C. Thanks are also extended specifically to my colleagues within the CRT task, both current and past.

[14] Being that that the field of research was comparatively new and was beset by problems of understanding.

[15] Gowlett recommended Operations Analysis and Operations Research as areas for research and development with specific application to cognitive and social modelling within the Defence Operations Support Centre.

6. References

H Abbass and M Barlow (2010). *Computational Red Teaming for Counter Improvised Explosive Devices with a Focus on Computer Games*. Contractors report submitted to DSTO, Defence and Security Applications Research Centre, University of New South Wales @ The Australian Defence Force Academy.

H Abbass, A Bender, S Gaidow and P Whitbread (2011). Computational Red Teaming: Past, Present and Future. *IEEE Computational Intelligence Magazine*, Vol 6(1), pp. 30-42.

AIIM (2011). Association for Information and Image Management. Online resource accessed June 2011: http://www.aiim.org/What-is-Information-Management.

Army Headquarters (2009). *Army's Future Land Operating Concept*. Head Modernisation and Strategic Planning – Army. Canberra, Australia.

Australian Army (2001). *The Military Appreciation Process*. Land Warfare Procedures – General, LWP-G 0-1-4. Combined Arms Training and Development Centre. Melbourne, Australia.

JC Beck (2000). Responding to Global Crises using the Change Cycle. In *Thunderbird on Global Business Strategy*. The American Graduate School of International Management. John Wiley & Sons, NY.

M Berryman (2008). *Review of Software Platforms for Agent Based Models*. Defence Science and Technology General Document, DSTO-GD-0532, Edinburgh, Australia.

P Campbell (2010). *A Literature and Tool Review for IED Computational Red Teaming*, Contractors report submitted to DSTO, Defence and Systems Institute, University of South Australia.

KM Carley, N Altman, B Kaminsky, D Nave & A Yahja (2004). *BioWar: A City-Scale Multi-Agent Network Model of Weaponized Biological Attacks.* Centre for Computational Analysis of Social and Organizational Systems Technical Report, CMU-ISRI-04-101.

CASOS (2011). Computational Analysis of Social and Organizational Systems. Online resource accessed June 2011: http://www.casos.cs.cmu.edu/projects/biowar/index.html

AF Chalmers (1999). *What is this thing called Science?* Third Edition. McPherson Printing. Queensland, Australia.

CS Choo, CL Chua and SHV Tay (2007). Automated Red Teaming: A Proposed Framework for Military Applications, In Proceedings of the Genetic and Evolutionary Compuation Conference (GECCO), London, England. pp. 1936-1942.

CL Chua, WC Sim, CS Choo and V Tay (2008). Automated Red Teaming: An Objective-based Data Farming Approach to Red Teaming. In *Proceedings of the 2008 Winter Simulation Conference: Global Gateway to Discovery,* Miami, FL, December 7-10. pp. 1456-1462.

I Cil and M Mala (2010). A Multi-agent Architecture for Modelling and Simulation of Small Military Unit Combat in Asymmetric Warfare. *Expert Systems with Applications*, Vol 37(2), pp. 131-1343.

PA Corning (2002). The Re-emergence of Emergence: A Venerable Concept in Search of a Theory. *Complexity*, Vol 7(6), pp. 18-30.

S Craig (2007). Reflections from a Red Team Leader. *Military Review*. March-April, pp. 57-60.

J Decraene, F Zeng, MYH Low, S Zhou and W Cai (2010). Research Advances in Automated Red Teaming. In *Proceedings of the 2010 Spring Simulation Multiconference*, Orlando, FL, April 11-15.

Department of Defense (2000). *Doctrine for Intelligence Support to Joint Operations.* Joint Operation Planning, JP 2-0. US Joint Chiefs of Staff, Washington, DC.

Department of National Defence (2007). *Land Operations 2021: Adaptive Dispersed Operations*. Directorate of Land Concepts and Design, Ontario, Canada.

DSARC (2008). *New Analytical and Synthetic Techniques Applicable to Capability Planning and Decision Making*. Contractors Report to Joint Operations Division, DSTO. Defence & Security Applications Research Centre, University of New South Wales, Australian Defence Force Academy, Canberra, Australia.

W Fishbein and G Treverton (2004). Rethinking "Alternative Analysis" to Adress Transnational Threats. *Occasional Papers of the Sherman Kent Center for Intelligence Analysis*. Volume 3 (2).

B Gladman (2007). *The 'Best' Practices of Red Teaming*. DRDC CORA TM 2007-29. Centre for Operational Research & Analysis, Canada Command Operational Research Team, Ottawa, Canada.

T Gold and B Hermann (2003). *Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities*. Office of the Under Secretary of Defense for Acquisition Technologies and Logistics, Washington, DC.

P Gowlett (2011). *Moving Forward with Computational Red Teaming*. DSTO General Document, DSTO-GD-0630.

CM Henein and T White (2005). Agent-Based Modelling of Forces in Crowds. *Lecture Noters in Computer Science: Multi-Agent and Multi-Agent-Based Simulation*. Vol 3415, pp. 173-184.

PF Hingston (2010). Computational Red Teaming: A Literature Survey and Computational Tool Review. Contractors Report to Joint Operations Division, DSTO. School of Computer and Security Science, Edith Cowan University, Australia.

A Kott and WM McEneaney, Eds (2007). Adversarial Reasoning. *Computational Approaches to Reading the Opponent's Mind.* Chapman & Hall, CRC Computer and Information Science Series, Boca Raton, FL.

A Kott and M Ownby (2005). Adversarial Reasoning: Challenges and Approaches. In Proceedings of SPIE, Vol 5805. *Enabling Technologies for Simulation Science IX*. Dawn, Trevisani, and Sisti (Eds.), May 2005, pp. 145-152.

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

V de Ligt (2010). Practical and Conceptual Issues in the Use of Agent-based Modelling for Disaster Management. PhD Thesis, University of Nottingham.

MAJ DF Longbine (2008). *Red Teaming: Past and Present*. School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, Kansas.

D Lowe, S Batley, D Byrne, J Caunce, J Dinale, M Galister, K Johns, S Long, A Ween (2008). *A Survey of Tools with Potential for use in Force Structure Analysis in 2008.* Defence Science and Technology Organisation, Unpublished brief to Director General Capability and Plans.

C MacNish (2010). Computational Red Teaming: A Review for the Defence Science and Technology Organisation. Contractors report submitted to DSTO, Faculty of Engineering, Computing and Mathematics, University of Western Australia.

COL TG Malone and MAJ RE Schaupp (2002). The 'Red Team': Forging a Well-Conceived Contingency Plan. *Aerospace Power Journal*. Summer 2002.

M Mateski (2008). A Call for a Red Teaming Surge. *Red Team Journal*.

M Mateski (2009). A Short Introduction to Red Teaming 1.0. *Red Team Journal*.

Ministry of Defence (2006). *The UK Joint High Level Operational Concept*. JDN 4/05. Joint Doctrine and Concepts Centre, Swindon, UK.

MAJ PS Oh (2009). Future Strategic Environment in an Era of Persistent Conflict. Military Review. July-August, pp. 68-79.

J Parker (2007). A Flexible, Large-Scale, Distributed Agent Based Epidemic Model. In *Proceedings of the 2007 Winter Simulation Conference*, Washington, DC, December 9-12.

Red Team Consulting Pty Ltd (2011). *What is "Red Teaming"*. Online resource accessed June 2011: http://www.redteamconsulting.com.au/red-teaming

Red Team Journal (2009). Red Teaming and Alternative Analysis. *Red Team Journal*. Online resource accessed June 2011: http://redteamjournal.com

Ryan A (2006). *Making Independent Red-Teaming the Foundation for Successful Strategy*. Noetic Paper 01-06. Noetic Solutions Pty Ltd.

Sandia National Laboratories (2011). *Information Design Assurance Red Team (IDART)*. Online resource accessed June 2011: http://idart.sandia.gov

J Sandoz (2001). *Red Teaming: A Means to Military Transformation*. Institute for Defence Analysis, Alexandria, VA.

B Schwartz (2004). *The Paradox of Choice: Why More is Less*. Harper Perennial Publisher, NY, NY.

H Simon (1955). A Behavioural Model of Rational Choice. *Quarterly Journal of Economics*, Vol 69(1), pp. 99-118.

MJ Skroch (2009). Modeling and Simulation of Red Teaming, *Red Team Journal*.

SourceForge (2011). *Repast: Recursive Porus Agent Simulation Toolkit*. Online resource accessed June 2011: http://repast.sourceforge.net/repast_3/index.html

The Technical Cooperation Program (2006). *Guide for Understanding and Implementing Defense Experimentation. GUIDEx*. Joint Systems Analysis, Action Group 12. Version 1.1.

GF Treverton (2005). *The Next Steps in Reshaping Intelligence*. RAND Corporation, Occasional Paper, Santa Monica, CA.

US Army (2008). *Red Team Education and Training*. Army Posture Statement, Information Papers (Prepare). US Department of Defence.

US Marine Corps Warfighting Laboratory (2011). *Project Albert*. Online resource accessed June 2011: http://www.projectalbert.org

Wheeler (2005). *On the Suitability of Netlogo for the Modelling of Civilian Assistance and Guerrilla Warfare*. Defence Science and Technology Technical Note, DSTO-TN-0623. Land Operations Division, Edinburgh, Australia.

Wheeler (2010). *Use of Scenarios in Support to Operational Concept Document Development: Application to JP 154*. Defence Science and Technology Client Report, DSTO-CR-2010-0012. Joint Operations Division, Fairbairn, Australia.

Wikipedia (2011). Verification and Validation. *Wikipedia*. Online resource accessed June 2011: http://en.wikipedia.org/wiki/Verification_and_validation

S Wu, L Shuman, B Bidanda, M Kelly, K Sochats and C Balaban. Agent-Based Discrete Event Simulation Modeling for Disaster Responses. In *Proceedings of the 2008 Industrial Engineering Research Conference*. Vancouver, Canada, May 17-21.

A Yang, HA Abbass and R Sarker (2006). Characterizing Warfare in Red Teaming, *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, Vol 36(1), pp. 268-285.

Appendix A: Selected Definitions of Red Teaming

"Red teams are organizational elements comprised of trained, educated, and practiced experts that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others."

Department of Defense (2000)

"Red teaming is an organizational process support activity undertaken by a flexible, adaptable, independent and expert team that aims to create a collaborative learning relationship by challenging concepts, assumptions, plans, operations, organizations and capabilities through the eyes of adversaries in the context of a complex security environment"

Lauder (2009)

"Red Team: a group of subject-matter experts (SME), with various, appropriate … disciplinary backgrounds, that provides an independent peer review of products and processes, acts as a devil's advocate, and knowledgeably role-plays the enemy and outside agencies, using an iterative, interactive process during operations planning."

Malone & Schaupp (2002)

"Defined loosely, red teaming is the practice of viewing a problem from an adversary or competitor's perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate."

Red Team Journal (2009)

"The term red teaming is commonly used to depict processes designed to bring a devil's advocate perspective by exposing flaws and gaps in our ideas, strategies, concepts, and other new proposals."

Sandoz (2001)

"Red teaming is authorized, adversary-based assessment for defensive purposes."

Sandia National Laboratories (2011)

"'Red-teaming' is seeking to get inside the heads of adversaries, not asking what we would do if we were them but creatively trying to ask what they might do given their own goals, culture, organization, and the like."

Treverton (2001)

Appendix B: Selected Definitions of Automated / Computational Red Teaming

"CRT is … the computational side of RT, be it to carry out the whole activity in silico or be it to augment a human-based RT exercise with computational models and methods. CRT is a natural advancement of computational models and methods that support decision making and planning in business, government and defense."

Abbass et al (2011)

"Computational Red Teaming is… the use of computer models and/or other mathematical techniques, using a variety of modelling approaches, that provide support to the red team in exploring and understanding the complex interactions… and the local population within which the actions are taking place in order to provide useful information to blue force."

Campbell (2010)

"CRT is a set of methodologies and computational models that augment a human based red teaming exercise or perform a computer based, more abstract red teaming exercise."

Chua et al (2008)

"CRT is a framework built upon a set of computational models that assist a human based red teaming exercise smartly and responsibly."

Cil & Mala (2010)

"ART is an automated vulnerability assessment tool which is employed to uncover the hard-to-predict and potentially critical elements of military operations."

Decraene et al (2010)

Appendix C: Third-level Functions

C.1 Information Management

Information Management "is the ability of organizations to capture, manage, preserve, store and deliver the right information to the right people at the right time." (AIIM, 2011). In the CRT framework, we broadly categorise this function as the *Collection, Capture, Storage and Retrieval of Information*. This includes a range of activities, including:

- Archival & search
- Information integrity
- Integration & fusion
- Publication & dissemination
- Security.

These activities underpin robust red teaming capability. For our application domain, we also specifically include *Data Design, Architectures & Structured Representations* as a separate category under Information Management. This is not a part of collection, capture, storage and retrieval as much as a mechanism by which it is achieved. In any sense, one cannot be conducted without the other.

For our purposes, we demarcate between information based activities (as per above) and the knowledge building activities (which are included here). Data Design, Architectures & Structured Representations includes:

- Business processes & improvement
- Collaborative & virtual environments
- Corporate knowledge & capability
- Enterprise architecture frameworks
- Standardisation & data control.

Hence, we include capability building activities within this category along with the functions of design and representation.

Visualisation & Replay is the item which denotes the use of the information. While the first two items describe the information and knowledge building activities, this item focuses on direct outcomes for Red Teaming.

Visualisation & Replay includes:

- Application development
- Infrastructure & maintenance

- Model instantiation & execution
- Synthetic & immersive environments
- Systems integration.

This item includes all of the requisite supporting activities in building physical systems for the use of the Red Team and running software on those systems.

The function of Information Management largely benefits from technical expertise in Engineering and Computer Science. Four specific disciplines; Computer & Information Sciences, Information Engineering, Software Engineering, and Systems Engineering; support this function.

C.2 Conduct and Execution[16]

We define the function of *Adjudication* quite broadly. This category is designed to include the traditional role of the adjudicator, as in seminar wargaming, and also the role of the facilitator, who may not otherwise be responsible for adjudication but who might enforce the methodology, the established rules for the activity, and time limits. The facilitator is also logically separated from the role of activity lead; who provides guidance and direction to the Red Teaming activity throughout the course of the activity.

Adjudication includes a range of activities, including:

- Activity management
- Adjudication, arbitration & mediation
- Facilitation & moderation
- Shaping, guidance & direction
- Stakeholder management.

All of these responsibilities may be conducted by a single individual, or a team. The extended concept of stakeholder management also includes the idea that the adjudicator is responsible for supporting outcomes. This includes balancing participations contributions, maintaining engagement, and fostering interpersonal interactions and *team spirit* within the group.

Knowledge Discovery is defined to encompass activities focused on adding value to information and raw data. This includes information based tasks like processing and analysis but also the capture of the information.

[16] TTCP (2006) is an excellent reference for the conduct and execution of experimentation in defence. This document was developed in collaboration between the *five-eyes* nations (Australia, Canada, New Zealand, United Kingdom, United States). It presents the principles of experimentation as a theory and then demonstrates those principles through case studies.

The process of knowledge elicitation is also essential leading into, during and after Red Teaming activities. Knowledge Discovery includes:

- Analysis, processing & exploitation
- Correlation & fusion of information
- Data capture
- Elicitation
- Program management.

In this category, we also include concepts from management science. However, only those functions relating to management of the program, activity or experimental campaign which derive or manipulate information belong here.

The precursor work towards executing a Red Teaming activity and supporting it with CRT is conducted under *Problem Scoping & Structuring*. This function includes all of the initial work engaging stakeholders, determining their needs and structuring the problem appropriately for Red Teaming.

Problem Scoping & Structuring includes a range of activities, including:

- Client engagement
- Problem decomposition
- Problem definition & statement
- Requirements & needs elicitation
- Representation.

In problem decomposition, the phasing of the problem and its break-down into work-able units is also addressed. This category is then broader than statement of the problem because that statement must be developed in a form fit for program management. It is also useful to be mindful of the future evolution of the problem into potential follow-on work programs.

In *Quality Control & Management*, the aspects of program management impacting on the quality of the outcome of CRT are identified.

Quality Control & Management includes:

- Constraints & controls
- Correction & prevention
- Operating practices
- Standards assurance

- Test & evaluation.

It might be assumed that the incorporation of *lessons learnt* is an important part of this function. However, that process also appears as a fundamental enabler. We do not include the development of capability through lessons learnt here.

There are a wider field of scientific disciplines which underpin the function of Conduct & Execution. All branches of science for experimental practice apply. The conduct of the Red Teaming activity in a defence application also depends on subject matter expertise gained through military service.

C.3 Scrutiny and Analysis

Adversarial Reasoning (Kott & Ownby, 2005; Kott & McEneaney, 2007) encompasses a wide range of tools, techniques and methodologies. The two principle approaches applying to Red Teaming are playing the Devil's advocate and directed challenge by contest and dispute.

Adversarial Reasoning includes:

- Devil's advocate
- Directed Challenge
- Exploitative play
- Role play & re-enactment
- Shaping & influencing.

Adversarial Reasoning provides a means by which participants in a Red Teaming exercise can learn, through experiential game play. It then includes the two broad techniques of role play and re-enactment, and exploitative play. While role play might not involve a contest of wills, exploitative play refers specifically to an environment where participants in a contest learn through the act of facing off against each other. More generally, Adversarial Reasoning includes approaches which shape or influence participants towards better planning, decision making and outcomes.

Assumptions Testing is crucial to understanding how the hypothesis, conclusions or outcomes of Red Teaming are related to the underlying assumptions, axioms or assertions. Most importantly is the understanding of how the validity of those underlying assumptions affects outcomes. Testing assumptions also helps participants in the activity to be aware of their own internalised belief structures and to open them to a range of alternative or competing beliefs which may be equally valid (or valid should specific circumstances arise).

Assumptions Testing includes:

- Consequence & implication testing
- Debate & critical review

- Deductive argument & logic
- Feasibility studies
- Hypothesis testing & experimentation.

Assumptions can be tested by any manner of means, including open or closed debate, in groups or by individuals. Assumptions Testing can also be conducted over short or long term studies, which may be used to as inputs to the Red Teaming activity or cued after the activity to answer specific targeted questions or gaps in knowledge.

All types of computerised and algorithmic-based search techniques are included within the category of *Data Mining*. These techniques are designed to facilitate the processing of large sets of data and to determine patterns within that data either in the form of interdependencies (such as clusters) or anomalies (such as extreme points).

Data Mining includes:

- Anomaly Detection
- Assisted Search
- Cluster & structure recognition
- Metrics & heuristic evaluation
- Statistical analysis.

If the data to be processed is includes time-series events; that is, the data is ordered sequentially in time then, the data mining process may also be used to determine or extract *causal chains* within a sequence of events. Such an approach is particularly interesting in military applications because of the obvious synergy with *branches* and *sequels* in military planning (Australian Army, 2001). This type of application can be used to suggest *decisive events* or to critique a *military plan*.

We also include statistical analysis within this category; although strictly speaking, statistical analysis is not traditionally considered to be a data mining technique. However, it does fit well within the concept of processing large quantities of information for the purposes of measurement or the determination of structure.

Appendix D: Subject Matter Contribution

List of parties that have contributed to the outcomes of the report

Specialist Consultants

Name	Role	Organisation
Dawn Hayter	Managing Director	IGOR Human Sciences
John Wiese	Director Defence Systems	Thales Australia Perth
Tess McCarthy	Criminal Intelligence	Australian Federal Police

DSTO Subject Matter Experts

Name	Role	Organisation
Andrew Gill	Lead Geographic Profiling	JOD Edinburgh
Gary Bullass	Lead Discovery Team	JOD / JDSC Fairbairn
Jon Rigter	Lead Systems Studies	JOD / JDSC Fairbairn
Paul Gaertner	Head Emerging Technology	JOD Edinburgh
Piers Duncan	Lead Red Teaming	MOD / Edinburgh
Russell Connell	Lead Red Teaming	AOD / Fishermans Bend

Internal JOD Computational Red Teaming Program

Name	Role	Organisation
Coen van Antwerpen	Lead Corporate CRT	JOD Edinburgh
Paul Whitbread	Lead Divisional CRT	JOD Fairbairn
Phil Gowlett	Science Lead CRT [prior]	JOD Edinburgh
Phil James	Research Leader COPS	JOD Edinburgh

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Moving Forward with Computational Red Teaming

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Scott Wheeler

5. CORPORATE AUTHOR

DSTO Defence Science and Technology Organisation
Fairbairn Business Park Department of Defence
Canberra ACT 2600 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TN-1104	AR-015-352	Technical Report	July 2012

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2012/51911/1	CDF 07/331	COMD CIED TF	34	63

13. DSTO Publications Repository

http://dspace.dsto.defence.gov.au/dspace/

14. RELEASE AUTHORITY

Chief, Joint Operations 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

18. DSTO RESEARCH LIBRARY THESAURUS http://web-vic.dsto.defence.gov.au/workareas/library/resources/dsto_thesaurus.shtml

Computational Analysis, Decision Support Systems, Red Teaming, Automated Reasoning

19. ABSTRACT

The term Computational Red Teaming has recently arisen within the literature to describe the application of new and innovative analytic techniques, tools and methodologies in support of Red Teaming Activities. This report explores Computational Red Teaming as a concept, which is itself undergoing transformation and growth within the practicing community. It describes just what Computational Red Teaming is, how it is applied, and its benefit over traditional Red Teaming practices and techniques. A framework of three key activities: Information Management; Conduct and Execution; and Scrutiny and Analysis; is then developed and decomposed into constituent functions for analysis.