© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2009

RED DAWN: THE EMERGENCE OF A RED TEAMING CAPABILITY IN THE CANADIAN FORCES

Matthew Lauder

The concept of red teaming, as it is most broadly understood (i.e. as a challenge function meant to improve blue force performance), is not new; and the use of red teams by the public and private sectors, including the defence and security community, are well documented. For example, red teaming is used by the emergency management community to test the skills of emergency responders during exercises (e.g. against a role-played adversary, such as terrorists), as well as to evaluate the efficacy of emergency response plans. Likewise, red teaming is used by the private sector to evaluate protective systems, including synthetic and physical security networks. However, while there is a legacy of red teaming, in particular in military war-gaming, it remains a developing and evolving concept with numerous definitions, many of which are context-dependent and user-specific.

In fact, red teaming, at least in its current iteration as a decision-support challenge function, has only recently gained traction in the military community. For example, the U.S. Army, after several years of developing and formalizing the red teaming concept, stood-up the Army Red Team Leader (ARTL) course at the University of Foreign Military and Cultural Studies (UFMCS), Fort Leavenworth, in 2006. This course trains military members, usually senior commissioned and non-commissioned officers, to assume and play the role of *the Other* (i.e. a mission-specific adversary) so they may challenge planning assumptions, identify red and blue vulnerabilities, and propose alternative courses of action. For the U.S. Army, red teaming is used exclusively as a decision-support tool for the commander with application limited to planning environments.

Unlike the U.S. military, the Canadian Forces (CF) does not have a program to train red team members in the proper application and utility of the function, nor has it formalized the concept in doctrine. In fact, much of the red teaming performed in the CF is ad hoc and heuristic; and red teams, comprised largely of blue force members tasked to role-play the adversary, are typically assembled at the last minute to meet the needs of the training audience. Most red teaming in the CF has been used in training environments and largely limited to exercises. In other words, red teaming in the CF is applied in a largely haphazard and casual fashion, and a strategy to formalize the concept, and professionalize the activity for application in training, planning, and operational environments, has been absent.

However, the state of red teaming in the CF is about to change. Owing largely to the success of the ARTL course, red teaming has become a hot topic and is receiving significant attention in the Canadian defence and security community. As a result, efforts, albeit nascent, are underway to explore, formalize, and professionalize both the concept and the capability in the CF.

This article has two goals: (1) to briefly identify and explore examples of red teaming from across the private and public sectors; and (2) by drawing upon these examples, to outline the characteristics of red teaming and propose an integrated, and working, definition of red teaming for possible use by the CF.

Opposing Force-based War-gaming

In the context of war-gaming, in which at least one player portrays or serves as the adversary (i.e. opposing force, or OPFOR), red teaming is not a new or recent development.[1] To test or preserve strategy without experiencing the hazards of combat, OPFOR-based war

games, in various forms, date back to the second and third millennium BC. For example, Wei-chi, literally the "surrounding game," dates to approximately 2,200 BC in China. Similar to chess, although the goal of the game was to defeat the adversary by capturing space on the board, Wei-chi was played by generals and statesmen and is reputed to have influenced the development of Chinese military tactics. The origin of contemporary forms of strategic OPFOR-based war games dates to the early 1800s with the development of *Kriegspiel* (literally, "war game"). Developed by George Heinrich Rudolf Johann von Reisswitz, a Prussian military officer, Kriegspiel, which is played using miniatures on a sand table, helped to train Prussian military officers and is, at least partially, credited for the Prussian victory over the French in the Franco-Prussian War (1870-1871). This tradition of war-gaming continued into and throughout the twentieth-century; one of the most notable being the war-gaming of defensive strategies by the staff of the German Fifth Panzer Army in the fall of 1944 using real-time reports from the field.

In the contemporary period, OPFOR-based war-gaming has taken the form of live blue-on-red (force-on-force) exercises and simulations. For example, the British Army developed a training program, under the auspices of the British Army Training Unit Suffield (BATUS), which includes a well-trained, aggressive, and independent (i.e. free-thinking) OPFOR based upon a non-British, all-arms battalion-sized organization. With a focus on genuine force-on-force training against a capable and mission-specific OPFOR, BATUS, which is located at CFB Suffield, includes more than 200 permanent and 640 temporary staff. Realism is further enhanced in force-on-force exercises through the use of direct and area weapons effects simulators, such as laser or infra-red projectors and marker systems (simulated ammunition). However, it should be noted that force-on-force training exercises are not limited to the British military; rather, they have been emulated by militaries around the globe. This same approach is used in the U.S. military and has recently been adopted by the CF for use at the Canadian Manoeuvre Training Centre (CMTC).

Contemporary OPFOR-based war games are not limited to the physical realm. Advancements in computer technology have led to the development of highly detailed virtual-world and immersive environments. The U.S. Army created the Dismounted Battlespace Battle Lab (DBBL), which allows soldiers to enter an immersive environment (i.e. a virtual battlefield) and manoeuvre through a variety of challenging situations while interacting with simulated adversaries. The primary emphasis of these force-on-force synthetic training environments is to develop and enhance tactical behaviours (i.e. improve individual battle task standards) for soldiers, and to examine how soldiers move and conduct themselves on the battlefield. These immersive and networked environments, which can accommodate up to 13 soldiers in individual virtual simulators, allow soldiers to interact with each other (as they would in the real world) and come complete with dynamic physical and human terrain features, including simulated adversaries and civilians. Other immersive training environments, such as ELECT BiLAT (developed by the Institute for Creative Technologies), focus on the soldier's *social interaction* with synthetic agents in a virtual world. Referred to as a social simulation, the objective of the training environment is to provide participants an opportunity to practice interpersonal skills such as negotiation and issue recognition. In the immersive environment, participants assume the role of a U.S. Army officer who must conduct a meeting with local leaders to achieve mission objectives or collect information on social relationships among the characters.

But, the question must be asked: Are OPFOR-based war games and simulations, such as those outlined above, examples of red teaming? Or, is red teaming something more than merely pitting blue and red forces against each other in an exercise or training environment? I will return to, and hopefully answer, these questions later in this paper.

Some Examples of Red Teaming from the Public and Private Sectors

Although red teaming is a term commonly used across the public and private sectors to identify, in very broad terms, a type of challenge function (e.g. to challenge a skill or a plan),

red teaming is not applied in a common or consistent fashion across the sectors. To work towards a common and more focused understanding of, and approach to, red teaming, the various applications of the concept (i.e. red teaming as it is most broadly interpreted and applied) must first be identified and briefly examined.

Civilian Applications

Jack Davis, of the Sherman Kent Centre, an institute of the Central Intelligence Agency, uses the term *red team* to denote a specialized team comprised of external, "substantive" (i.e. area) experts and analytical thinkers, who "work with [intelligence] analysts to study assumptions, mirror-imaging, and complex analytical processes."[2] For Davis, red teams role-play the adversary's calculations. It should be noted that Davis refers to the overall activity as *alternative analysis*, but not as red teaming. Davis does, however, identify red teaming as a technique, along with *Devil's Advocacy* (i.e. the deliberate challenging of an analyst's views) and *Team A-Team B* analysis (i.e. competitive assessments using a different set of assumptions), used under the umbrella of alternative analysis (i.e. red teaming, along with Devil's Advocacy and Team A-Team B analysis, is a specific type of challenge technique that falls under the broader category of alternative analysis).[3]

In the context of information systems security, Sandia National Laboratory, a national security laboratory of the U.S. Department of Energy, refers to red teaming as an "assessment" that considers malevolent intent rather than system design or structure, and the application of that knowledge, by a specific team of role players (red teams), to test the weaknesses and vulnerabilities of information systems.[4] For Sandia Labs, red teaming is the activity that involves ethical (i.e. white hat) hacking from a *black hat* perspective, using hacker personality templates (i.e. adversary behavioural templates). Black hat hacking is a colloquial term to describe malevolent hackers. White hat (i.e. ethical) hacking involves penetrating a computer system using the techniques, approach, and intent of malevolent hackers. However, the goal of the ethical hacking is to identify security vulnerabilities and to leave the system intact. Likewise, the National Security Agency (NSA) developed a specialized red team that provides adversarial network service (e.g. network security penetration analysis). The purpose of the NSA's red teaming effort is to assume the mindset of the adversary and penetrate a synthetic network undetected and identify security gaps so that the customer (i.e. the client) can take appropriate defensive measures. A spokesperson for the NSA notes that the first rule of red teaming is to "do no harm," and that the perfect *red teamer* possesses "technical skills, an adversarial mindset, perseverance, and imagination."[5] Similarly, IBM describes red teams as a highly specialized group of people assigned with the task of assuming the "role of the outsider" and challenging assumptions, examining systems for unexpected outcomes, proposing alternatives or new approaches, or identifying vulnerabilities of new ideas or approaches.[6] For IBM, the critical characteristic of red teaming is that the teams are able to assume an "adversarial posture, taking the perspective of the enemy or competitor."[7]

Although not restricted to synthetic networks, similar penetration tests are conducted by the Forensic Audits and Special Investigations Team (FSI) of the U.S. Government Accountability Office (GAO).[8] Created in 2005, the FSI conducts covert evaluations of executive branch security systems and government program activities to identify vulnerabilities and internal control weaknesses that could be exploited by terrorists or criminals. These covert evaluations are conducted as "red team operations," meaning that the team adopts the capabilities, resources, and mindset of the adversary (i.e. they behave as the adversary would), and that the target of the investigation is completely unaware (i.e. not notified in advance) of the test.[9] Moreover, these evaluations occur in the actual work environment during normal operational periods; meaning that they do not take place in a simulated or replicate environment, nor are they exercises or training events. In other words, these are live red teaming events.

Military Applications

John F. Sandoz, of the Institute for Defence Analysis, describes red teaming as a "management tool" to "challenge assumptions" and "avoid group-think."[10] Likewise, the UFMCS defines red teaming as "a function … that provides commanders with an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the operational context" from a range of perspectives (e.g. partners, adversaries, and others).[11] For the UFMCS, the goal of red teaming is to enable planners and decision-makers to avoid group-think, mirror-imaging, and cultural miscalculations. Susan Craig, a recent graduate of the UFMCS Red Team Leader course,[12] describes a red teamer as "not an intelligence analyst," but rather like a historian and anthropologist, possessing excellent communication skills and ready to question assumptions and voice dissent.[13] Moreover, Craig notes that red teamers understand how the blue force shapes the environment, and examines those attempts (by blue force) to shape the environment through the "lens of the adversary."[14] In other words, red teaming is about accessing and utilizing the adversary's culture and world view and seeing blue (i.e. *the Self*) through the eyes of red (i.e. *the Other*).

Although most practitioners agree that red teaming is a type of challenge function, there is some disagreement on the level of application within an organization. For example, the U.S. Defense Science Board Task Force report on red teaming indicates that red teams can be employed at "multiple levels within the enterprise," specifically: (1) the strategic level to challenge assumptions and vision; (2) the operational level to challenge force postures and plans; and (3) the tactical level to challenge military units during collective training.[15] In contrast, Colonel (retired) Gregory Fontenot, the Director of UFMCS, and Colonel T.G. Malone and Major R.E. Schaupp expects red teaming to be used exclusively as a planning and decision-support tool (i.e. red teaming is about developing a more robust plan at the operational or strategic levels).[16] At least as far as the UFMCS is concerned, the purpose of red teaming is to assist the commander, and the staff, in planning and operations by providing alternative, and holistic, perspectives and insights, in particular from the adversary's point of view or by taking the cultural nuances of the operating environment into consideration. It is unknown as to whether the U.S. Army intends to utilize red teaming at the tactical level, or outside of the planning and decision-support role (e.g. role-playing the adversary in war games or exercises). However, it appears that red teams, in so far as the U.S. Army is concerned, do not actually *play OPFOR* in war games or exercises.

Red Teaming in the Canadian Forces

Unlike the U.S. military, red teaming (again, broadly defined) in the CF is done in a much more informal and irregular manner, and more often in a tactical-training setting. For example, The Argyll and Sutherland Highlanders of Canada (Princess Louise's), a reserve infantry unit, developed a dedicated team which, in collaboration with the blue-force commander, designs field training exercises, trains the OPFOR to accurately represent and role-play adversaries and neutrals (and other agents found in the operating environment), serves as exercise controllers and key role-players (e.g. insurgent leaders), and provides feedback on performance and identifies opportunities and areas for improvement. The purpose of this red teaming effort is two-fold. First, it is to accurately represent the adversary and other agents, in this case insurgents and civilians, in order to challenge blue's assumptions about the human terrain, in particular culturally-specific behaviour. Second, it is to create a physically and psychologically challenging learning environment; one which challenges, but not overwhelms (i.e. breaks), the primary training audience.

Another example is the CMTC, which employs both military members and civilians to role-play adversaries and neutrals (including religious leaders, local politicians, and aid-workers) during pre-deployment training for Afghanistan. However, it should be pointed-out that, while military role-players receive some training in Afghan culture and Taliban tactics, and many of the civilian role-players are native-born and speak languages indigenous to Afghanistan, the red teaming effort, in this instance, is exclusively applied to

the collective training environment for individual battle task standards and not to planning or operational decision-support.

Red teaming has also been used by the CF for major event preparation, specifically by the Joint Task Force Games (JTFG) Red Team[17] during command group table-top exercises (e.g. red team TTXs) in preparation for the 2010 Winter Olympics. Red Team TTXs are a specific type of TTX exercise in which the red team designs, coordinates, and conducts the exercise. The purpose of these TTXs is to create and maintain an environment of open and candid discussion of existing or emerging issues, challenges, and concerns. Most importantly, red team TTXs allow the command group, or senior decision-makers, to discuss and think-through a number of novel issues in a *team environment* and to contemplate and consider the various cascading effects or downstream consequences of blue and red actions. It should be noted that team involvement is essential to this endeavour. Not only should the entire team be present, including the commander or senior decision-maker, but the exercise should allow for open, candid, and non-hierarchical discussion between team members.

Led by a facilitator, red team TTXs may take the form of a series of scenarios, which are usually framed by the upcoming event or operation and gradually increase in difficulty or complexity. The role of the facilitator is to solicit and maintain group discussions, as well as to keep the blue force focused on the larger context and strategic issues and directed towards a particular end-state or goal. Red team TTXs are characterized by a "push" red-blue relationship. In essence, the red team is actively engaged in the entire TTX and pushes blue to think about a particular issue in a particular manner. In this situation, red *pushes* information to blue for consideration. (In red team supported TTXs, whereby the red team supports the decision-making process, the relationship between red and blue is much more "push-pull." For example, red could push information to challenge blue assumptions, or blue could request assistance or support from red). Moreover, the facilitator does not play the role of neutral observer (which is typical in TTXs), but rather plays the role of agent-provocateur (i.e. an inciting agent). In fact, there is nothing neutral about the role of facilitator in this type of red teaming exercise. This, however, does not mean that the facilitator plays the role of *contrarian* who purposely assumes a combative, confrontational, or oppositional stance. (In fact, to do so would create a negative learning environment). Rather, the facilitator plays the critical role of guiding the training audience to a particular end state (the end state or goal of the red team TTX must be negotiated and agreed upon by the facilitator and the blue commander), and ensuring that the training audience remains objective and does not engage in group-think or mirror-imaging. This is achieved through the selective use, or manipulation, of information. In other words, the role of the facilitator is to influence and guide discourse and to help blue achieve the end state.

To avoid the blue force rejecting the facilitator, or dismissing the scenarios as unrealistic, it is important that the commander both sanction the red teaming effort and play the role of confidant during the exercise. That is, the commander will be a trusted (i.e. inside) agent and will assist the facilitator, through clandestine or subtle means (e.g. unobtrusively re-directing conversation or supporting the points made by the facilitator), by guiding the discussion towards the end state. It is also important that the facilitator and the confidant work cooperatively to nurture and maintain a positive, constructive, open, and egalitarian setting.

Synthesis of Red Teaming Approaches

Although this examination is not exhaustive, it provides an overall idea of what red teaming is and how it is applied across the public and private sectors. In general, civilian applications tend to use red teaming on the tactical level (in particular, but not exclusively, to test physical or synthetic networks, systems, or operational programs), whereas military applications tend to be employed on the operational and strategic levels, and largely within a planning setting or in a decision-support role (although, in the CF, red teaming appears to be most often utilized in exercise or training environments). It is clear that, while application of the red teaming concept may differ across sectors, both the civilian and military communities

utilize red teaming in an *active*, rather than a *passive*, fashion, and that red teamers must possess a deep understanding of the adversary (i.e. thinking and behaviour) for the purpose of role-playing the adversary (or, advising as to what the adversary may think and do) in training, planning, or operations (i.e. live) setting. Moreover, it is apparent that red teamers must see themselves as integral parts of the learning process; that they play a critical role in making blue better.

Why is Red Teaming Important?

There are two interrelated reasons why red teaming is important.[18] First, red teaming mitigates complacency, group-think, and mirror-imaging (i.e. imposing blue force behaviours and tactics on the adversary; in other words, seeing the adversary as we see ourselves).[19] Second, red teaming is a process by which blue force may be able to deepen its understanding of, and therefore the ability to respond to, the adversary.[20] This is particularly important in the contemporary security environment, which is characterized by multiple, relatively unknown, dynamic and highly-adaptable adversaries (in particular, but not limited to, non-state actors possessing asymmetric tactical advantages used against conventional forces and civilian populations) in non-contiguous battlespaces. In essence, we now face multiple adversaries that operate across international boundaries and in an unorthodox fashion, adopting and modifying military doctrine from a range of militaries, or dispensing with convention altogether, in an effort to gain an advantage over technologically and numerically superior opponents. As such, this situation requires the blue force to acquire a deep understanding of the mindset, behaviour, and culture of the adversary, as well as a level of self-knowledge to critically examine and identify the vulnerabilities and weaknesses in blue force networks, systems, approaches, activities, programs, thinking, and plans (i.e. to be introspective; to look from within). The purpose of red teaming is to deepen our understanding of ourselves and of the adversary and, by doing so, open our eyes to our own stereotypes and weaknesses; in other words, to see the world from outside one's own experiences.

Red Teaming Conceptual Framework

In a recent article, Mark Mateski, who attempts to balance the use of red teams by the military community with that of the larger public and corporate sectors, defines red teaming as "any activity—implicit or explicit—in which one actor…attempts to understand, challenge, or test a friendly system, plan, or perspective through the eyes of an adversary or competitor."[21] Although recognizing that various approaches to red teaming are used across sectors, Mateski notes that red teaming generally serves one of four purposes (i.e. to understand, anticipate, test, or train) and further indicates that these purposes are cumulative, each building upon the previous purpose. Mateski also separates the purposes into two broad categories or approaches; that of *passive*, the other *active*. Mateski notes that the primary difference between these two broad categories is that active approaches "play-out" adversary actions against a blue force in an operational (i.e. live) setting; and he further notes that red teaming, in the active approach, "tends to more interactive than passive."[22]

Although Mateski's framework provides a detailed account of various ways in which red teaming is used across sectors (e.g. in military and corporate planning versus exercises and penetration tests), there are two critical issues that must be highlighted. First, Mateski's identification of passive versus active approaches to red teaming appears to run counter to the generally-accepted purpose of red teaming (i.e. to challenge conformity, convention, and orthodoxy and to encourage self-discovery and learning, red teaming requires high levels of interactivity and exchange between red and blue forces). Red teaming, by its very nature, is a collective, and therefore social, activity which implies a level of cooperation, interactivity, and reciprocity. Second, Mateski's assertion that purposes are sequential and cumulative (i.e. building upon the previous purpose) does not reflect red teaming in the applied environment. For example, tests and evaluations, such as the penetration or probing of blue systems or networks, in addition to teaching blue to understand and anticipate red patterns of activity, prepare blue to respond to red actions (i.e. both teaches and trains countermeasures). Rather than having a cumulative effect, I argue that the various purposes (i.e. to help blue understand, anticipate, test, and train) exist across all red

teaming activities; that is, every time you red team, a combination of purposes and functions are realized.

Recognizing the various manifestations of red teaming across the public and private sectors, and the levels of application (i.e. tactical, operational, and strategic), I argue that the basic purpose of red teaming is to create a *collaborative learning environment*.[23] At its very core, red teaming is about learning; not only about *the Other*, but also *the Self,* in a participatory and interactive fashion. In essence, an effective red teamer is, first and foremost, a coach or mentor; that is, one who instructs and teaches while strategically directing the team towards a specific goal.

Taking into consideration red teaming applications from across the public and private sectors, as well as the basic purpose of red teaming, the following table (Table 1) provides a description of red teaming categorized by four broad and generic organizational processes (i.e. Innovation, Planning and Analysis, Training and Professional Development, and Operations).

Organizational Process	Description	Method / Technique	Example
Innovation	• Policy, concept, program, or product development leading to transformation	• Peer review / critical analysis • Experimentation	• Red teams test the validity and applicability of a new concept
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 • Adversary role playing (surrogate adversary)	• Red teams assess the vulnerabilities of a plan by role playing the adversary during war-gaming • Red team advises planners during design phase of adversary capabilities and limitations
Training and Professional Development	• Individual and collective training, typically in an exercise environment	• Adversary role playing in a blue versus red environment • Advisory role • Peer review / critical analysis (e.g. during after-action reviews)	• Red teams design and coordinate training exercises, as well as role play all agents in the exercise scenario • Red team can play a support role in exercises, serving to challenge or advise blue when necessary
Operations	• Assessment of live / operational (cyber or physical) activities, systems or networks (e.g. computer networks, physical access systems, or environmental security elements of critical infrastructure or other asset)	• Tiger teams (red versus blue) • Ethical hacking (white and black hat hacking) • Peer review / critical analysis (attack the whiteboard)	• Red teams conduct penetration tests of a live or replicated computer network, or tiger teams attempt to gain entry into secure areas of a physical asset (e.g. airports, military bases, etc.)

Table 1: Red Teaming Conceptual Framework

Characteristics of Red Teaming

The use of red teaming is based upon client needs, available resources, and the context of the operating environment. As evidenced by the various manifestations of red teams across the public and private sectors (i.e. multiple horizontal and vertical applications), there is no single definition of, or format for, red teaming. As such, I believe it necessary to resist the urge to be overly prescriptive in the definition, purpose, doctrine, and the application of red teaming, even if the application is limited to the military environment within a specific context (i.e. limited to planning or training settings). We must be able to provide enough space for the concept to be useable in a variety of settings (so that we do not marginalize the military community from wider application of the concept, especially the civilian public and private sectors)[24] and for the red teaming concept to develop further so that it may respond to the changing security environment (i.e. emerging technologies or adversary capabilities). In other words, red teaming should not be a considered a static or single-purpose capability; rather, red teaming implies dynamic application across settings, organizations, and levels. Moreover, red teaming implies multifaceted representation (i.e. multiple adversary or agent perspectives) and a capability that can be utilized to respond to a range of problem-spaces (e.g. not just for counter-insurgency operations). It is for these reasons (i.e. to emphasize its multi-setting, multi-level application and the need for future development) that red teaming should remain, above all else, a highly flexible concept and an adaptive capability in the CF.

From an examination of red teaming initiatives from across a range of settings, the following table (Table 2) lists, what I believe to be, the six key characteristics of red teaming.

Characteristic	Description
Trust	The effectiveness of red teams will be dependent upon building a level of rapport, trust, and credibility with blue force members. Without trust, the blue force will dismiss red involvement in planning activities, decision-support, and exercises. Red team members must develop trust in order to create an environment of joint-ownership. Blue members must be able to trust that red teamers are there to help and guide (i.e. do no harm), rather than to overwhelm, unfairly criticize, or break blue efforts.
Positional Authority	To ensure buy-in, the blue commander must sanction the red teaming effort and must make blue members aware that the red team functions at the highest level.
Relative Independence	Strict independence of the red team is only required in special circumstances. Red team performance and activities should be continually negotiated between the red commander and the blue commander to ensure that the experience is of value to blue (i.e. that red teaming remains a high-value training aid).
Expertise	Red team members should have a deep understanding of the human and physical terrain of the operating environment (in particular, the adversary, including adversary thinking, behaviour, culture, etc.), knowledge of alternative and adult learning methods, and advanced knowledge of the blue force, including blue thinking, behaviour, culture, and the system, product, program, or activity being examined.
Adaptability	Red teams must play a role that is fully immersive and participatory (active rather than passive) and that they should be permitted to adapt to, and counter, blue force actions, as appropriate. To ensure learning value, red teams and the blue force must continually interact and negotiate continued participation.
Flexibility	Red teams should be used in a variety of settings (functions) at all levels (tactical, operational, and strategic), and in response to a range of problem-spaces.

Table 2: Red Teaming Characteristics

Integrated Definition of Red Teaming

Based upon the conceptual framework (Table 1) and the key characteristics (Table 2), the following integrated and working definition of red teaming is proposed for use by the CF:

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 assumptions, concepts, plans, operations, organizations, and capabilities through the eyes of adversaries in the context of a complex security environment.

This definition, although developed with the military community in mind, provides significant latitude for use by the civilian community across the public and private sectors. Moreover, the definition allows for use at all levels (i.e. tactical, operational, and strategic) and across all organizational processes (i.e. depth and breadth of processes; see *Table 1*) rather than for use by a single community in specific setting, such as planning or operational decision-support, and for a specific problem-space. Lastly, this is a *working* definition because it is recognized that, as our experience and knowledge of red teaming develops, the definition will evolve and mature.

Preliminary Observations from the Field

At present, there is very little systematic research being conducted on red teaming. However, a few preliminary observations from red teaming activities are worth mentioning. First, anyone can be a critic or a contrarian and disagree with a particular position and put forth an opposing viewpoint, but not everyone can be an effective red teamer. Red teaming takes a particular type of individual, mind-set, and approach. Most importantly, red teamers must be able to *check their ego at the door*. The finished product of red teaming, whether that product is a robust plan or an enhanced skill-set, is not about the red teamer; that is, the red teamer does not have ownership of that product. Rather, the goal of the red teamer is to help blue learn and improve. To do this, red teamers must be sociable, gregarious, likeable, perceptive, empathetic, understanding, and have a balanced personal-touch (i.e. know when to push or advocate for an issue and when to lay-off). Furthermore, red teamers must be able to recognize the limits of their knowledge and experience and seek additional expertise, whether that is an indigenous asset or an external subject matter expert, when appropriate. Red team members must possess and maintain credibility throughout the entire red teaming endeavour.

High-level or strategic red teaming (e.g. for command personnel or persons in senior leadership positions) appears to be a good add-on or augmentation to existing exercises and training programs rather than as a substitute. In essence, the red teaming activity (e.g. a red team TTX) allows for greater discussion of pre-existing or emergent issues and challenges. Although not a hot-wash or after-action review, red team TTXs allow the participants to take issues (that are identified during a larger exercise) and to think through the problem-space and consider alternative options and courses of action (which were not used in the larger exercise). Red team TTXs appear to be most valuable when conducted in an intimate and impartial setting, and towards the end of, or immediately following, an exercise (but before a hot-wash) when memories are fresh and information and resources are readily at-hand.

So, to return to my early question: Are OPFOR-based war games and simulations examples of red teaming? The short answer is: *It depends*. In essence, it depends upon how well-trained or knowledgeable the OPFOR is in adversary culture and behaviour, how war games and simulations are structured (i.e. are they interactive and collaborative learning environments), and whether the OPFOR is attempting (first and foremost) to challenge preconceived ideas, assumptions, or concepts rather than to simply defeat or crush the opposition (i.e. blue). In the broadest interpretation of the term, OPFOR-based war games (i.e. simple blue versus red events) can be considered a form, albeit a basic form, of red

teaming; but the key to red teaming, at least as it is conceived in the contemporary operating environment, is about creating opportunities to self-reflect (i.e. gain self-knowledge) and to improve blue performance through an accurate representation of the adversary as well as an accurate perception of the blue force through the eyes of adversary. In other words, if the role of the red team (in war-gaming or during the planning process) is to simply antagonize, criticize, castigate or defeat (or even to validate) blue, then these activities are less red teaming endeavours and more banal competitions (i.e. there must be learning value associated with the endeavour). The danger of competitions is that it often creates a negative learning environment. The overall objective of red teaming is to maximize learning in order to enhance performance.

To that end, I believe that there are two general forms, or categories, of red teaming: basic; and advanced. Basic red teaming usually involves a role-played adversary; and, while there may be some learning value associated with basic red teaming, the learning agenda is informal and relatively unstructured. For example, simple competitions between blue and red forces in an exercise environment may be regarded as a basic form of red teaming. In contrast, advanced forms of red teaming involve experts who not only role-play the adversary (or look at a problem from the adversary's perspective) but who purposively create and maintain a learning environment that is both well-structured and highly formalized. Moreover, advanced red teaming is characterized by set goals and learning objectives (i.e. a particular end state that is negotiated by blue and red commanders). It should be noted that advanced red teaming is not exclusive to planning environments or the operational and strategic levels; that such learning environments can be created at the tactical level and in exercise environments.

Areas for Further Investigation

Although a number of articles have been written on the topic of red teaming (in particular, in military and defence publications), and red teams have been put into use across the public and private sectors, there is a paucity of data on the effectiveness of red teaming to achieve specific goals (i.e. there are no studies validating the effectiveness and efficacy of red teaming as a process). In fact, much of the literature on red teaming is anecdotal and descriptive, focusing, from a practical perspective, on best-practices or approaches to applying the concept by a specific community and in a specific context (i.e. by the military in a planning setting). The following are a number of areas that require further investigation:

- What are the qualities and characteristics of good and effective red teamers and how are red teamers selected?
- What type of training is required for red teamers?
- Is there a particular red team composition that is more effective than others?
- What kind of learning environment is most effective?
- Does the role of the red team differ in certain environments (i.e. does the role differ across settings and levels)?
- What type of interaction is necessary (between red and blue) to encourage learning?

Does red teaming really work? We assume that red teaming makes blue better (i.e. more robust plans or more effective soldiers), but does it really? Is there evidence to support the claim that red teaming actually improves plans or behaviour? Some evidence suggests that red teaming may be a barrier to learning because participants revert to a competitive approach aimed at short-term gain (in spite of the overalls goals or content of the course).[25]

Conclusions

The concept of red teaming is neither new nor is it commonly applied across the public and private sectors. For the civilian community, red teaming is often, but not exclusively, used to test physical and synthetic networks and systems, such as security and information systems, at the tactical level. In contrast, red teaming is commonly used by the military community at the strategic and operational levels and within a planning setting (although there are examples of both tactical level and training applications), largely to challenge assumptions. In essence, red teaming is an evolving concept, tailored to meet the specific needs and environment of the end-user. A cross-sector examination of red teaming reveals it is used in four broad organizational processes:

- innovation;
- planning and analysis;
- training and professional development; and
- operations.

In addition, this cross-sector examination reveals that red teaming, regardless of the level or setting of application, involves a specially trained team that assumes the role of (or can at least speak to the thinking and behaviour) the adversary. This role-playing requires a deep understanding of the mindset, behaviour, and culture of the adversary. Most importantly, the examination also reveals that the purpose of red teaming is to facilitate collaborative learning. Since red teaming has broad (i.e. horizontal and vertical) application across the public and private sectors, and since the CF have entered an era of deep civilian-military integration (in particular, in response to emergencies and humanitarian crises), it is recommended that the military develops an inclusive and agile red teaming framework with flexible and adaptable guidelines for the application of a red teaming capability at all levels and across the four organizational processes.

About the Author...

Matthew A. Lauder is a cultural theorist and applied social anthropologist who earned his BAH in Psychology and Religious Studies at Queen's University, a Master's in Religion and Culture at Wilfrid Laurier University, and a Master's of Philosophy (MPhil) in Religious Studies from Lancaster University (UK). His research has been broadly on the anthropology of religion, with a focus on the use of qualitative research methods to explore indigenous social networks, the social reality of groups existing on the margins of society, myth and ritual, new religious movements, and the intersection between politics and religion. Matthew is currently a Defence Scientist in the Adversarial Intent Section, Defence R&D Canada (Toronto), and undertaking theoretical and applied research in the cultural context of conflict, cultural support to operations, irregular warfare, radicalization and extremism, and red teaming.

Endnotes

1. B.W. Gladman, "The 'Best Practices' of Red Teaming," *DRDC CORA TM 2007-29*, Centre for Operational Research and Analysis (2007); and, G. Fontenot, "Seeing Red: Creating a Red-Team Capability for Blue Force," *Military Review* (September-October 2005): 4-8. Gladman uses "opposing force red teaming" to identify the use of role-played adversaries in training environments.
2. Jack Davis, "Improving CIA Analytic Performance: Strategic Warning," *The Sherman Kent Center for Intelligence Analysis*, Vol. 1, No. 1, (September 2002).
3. Ibid.
4. "What We Do," Sandia National Laboratories, www.sandia.gov/iorta/whatwedo.html (accessed 23 October 2008).
5. Glenn Derene, "Inside NSA Red Team Secret Ops with Government's Top Hackers," *Popular Mechanics.com,* 30 June 2008, www.popularmechanics.com/technology/military_law/4270420.html (accessed 23 October 2008).
6. "Red Teams: Toward Radical Innovation, Executive Technology Report," *IBM.com*, July 2005,

www.ibm.com/bcs (accessed 28 September 2008).
7. Ibid.
8. Statement of Gregory D. Kutz, Managing Director, Forensic Audits and Special Investigations, *Investigative Operations: Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse*, United States Government Accountability Office, 14 November 2007, GAO-08-286T.
9. Ibid.
10. John F. Sandoz, *Red Teaming: Shaping the Transformation Process*, (Annotated Briefing), Institute for Defense Analyses (IDA Document D-2590, Log H 01-000776), June 2001.
11. Marcus Spade, "Army Approves Plan to Create School for Red Teaming," *TRADOC News Service*, 13 July 2005,www.tradoc.army.mil/pao/tnsarchives/july05/070205.htm (accessed 22 July 2008).
12. Susan Craig is a Red Team Leader at the Joint Intelligence Operations Center of U.S. Pacific Command.
13. Susan Craig, "Reflections from a Red Team Leader," *Military Review* (March-April 2007): 57-60.
14. Ibid.
15. Defense Science Board Task Force, *The Role and Status of DoD Red Teaming Activities*, Office of the Under Secretary of Defence for Acquisition, Technology, and Logistics (September 2003), Washingston, DC, 20301-3140.
16. Fontenot; and Timothy G. Malone and Regan E. Schaupp, "The 'Red Team': Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal*, Summer 2002,http://findarticles.com/p/articles/mi_m0ICK/is_2_16/ai_90529724 (accessed 2 October 2008).
17. Joint Task Force Games (JTFG) is the purpose-built operational headquarters responsible for the command of the CF contribution to the 2010 Winter Olympics. The major part of the JTFG effort will be directed towards security operations in support of the Royal Canadian Mounted Police (RCMP), which is the lead agency for security for the games. In May 2008, the JTFG stood-up the Games Red Team (GRT) to provide independent peer review (i.e. red teaming) of JTFG plans and preparations. The GRT supports JTFG training through a number of red teaming activities, the purpose of which is to maintain the mental agility and competency of JTFG staff.
18. For a more detailed discussion of the importance of red teaming, see: B.W. Gladman, "The 'Best Practices' of Red Teaming," *DRDC CORA TM 2007-29*, Centre for Operational Research and Analysis (2007).
19. Defense Science Board Task Force.
20. Sandoz.
21. Mark Mateski, "Toward a Red Teaming Taxonomy, 2.0 (2004)," *RedTeamJournal.com,* 4 September 2004, http://redteamjournal/com/2008/09/toward-a-red-teaming-taxonomy-20/(accessed 2 October 2008).
22. Ibid.
23. Collaborative learning is an umbrella term for a range of approaches that emphasizes collective development, both for the students and the teachers. Although activities and techniques may vary, collaborative learning is an active, constructive and inherently social process that involves the immersion of the student in rich contexts and challenging tasks in a cooperative environment. See B.L. Smith and J.T. MacGregor, "What is Collaborative Learning," in *Collaborative Learning: A Sourcebook for Higher Education*, ed. A. Goodsell, National Centre on Postsecondary Teaching, Learning and Assessment, Pennsylvania State University, Pennsylvania, (1992).
24. This is particularly important, given the emphasis currently placed by the CF on domestic and humanitarian response capabilities and JIMP / Whole of Government approaches to operations. See: Chris Thatcher, "Future Force: Incorporating More than the Military," *Vanguard*, 2006, www.vanguardcanada.com/FutureForceThatcher (accessed 23 October 2008).
25. Mike Maughan, Adrian Thornhill and Caroline Maughan, "Using the Red-Blue Exercise to Facilitate Learning Transfer: Theory and Practice," *Journal of European Industrial Training*, 20 (8), (1996): 18-21.