MAD* BEYOND DEFENCE
*METHODOLOGY FOR ASSESSING DISRUPTIONS

Dr. Gitanjali Adlakha-Hutcheon, Defence Research and Development Canada
Canada

Abstract

Advancements in technology are regularly identified, assessed, and classed into emerging and/or potentially disruptive technologies, according to their ability to cause disruptions to defence systems, and in defence. Perhaps this is because defence capabilities centre on grand technology systems deployed at the level of nations. Hypersonic missiles are one example. The testing of a new hypersonic missile or a research program on types of hypersonic drones immediately sparks questions like: which other nations have such capability? or what types of technologies can be used to detect or counter these? In contrast, the ability to identify weak, faint factors that add up and lead to conflict are not brought together in a systematic manner. Nor is it common for there to be a cross-talk between a combination of methods used within military science and technology organizations over in to social sciences related to intelligence and/or conflict. This is a preventable strategic foresight issue relevant for enhancing, planning for, and investing in the security space. This paper describes the MAD (Methodology for Assessing Disruptions) tool, which is adaptable beyond the defence domain. MAD is a scenario-based two-part table-top exercise conducted to identify weak signals that have the potential to cause disruptions, which by consequence may coalesce into challenges for security. Exercising such methods is essential for security professionals to prepare and plan for future conflicts instead of constantly reacting to immediate acute problems.

Introduction

Traditionally, procuring defence capabilities like air and sea carriers requires a long-term time horizon, extending out to a minimum of 10-15 years into the future. Therefore, it is essential to identify and/or anticipate the needs of operators and the ability of providers to fulfill these requirements, as the absence of such awareness could be disruptive; militaries around the world are known to plan ahead. Even the largest military alliance of the world, the North Atlantic Treaty Organization (NATO), specifically its Science and Technology Organization (STO), uses tools like the Disruptive Technologies Assessment Games (DTAG) (Rademaker et al., 2008, 2012) to ascertain the types of technologies that are emerging and/or disruptive to gain a competitive advantage for itself and its member states. In my association with tools from the operational research and analysis domain in defence for over 15 years[1], I have rarely, if ever, come across their use in the realm of safety and security. It is necessary to have similar tools to identify developing security issues, including those that can cause disruptions in safety and security. This paper describes one such tool—Methodology for Assessing Disruptions (MAD)—and presents opportunities where security personnel can use MAD.

What Is MAD?

MAD is a strategic foresight exercise that uses the Science and Technology (S&T) lens to systematically examine concepts and/or systems that could disrupt operations (Adlakha-Hutcheon et al., 2012, 2017, 2020; Adlakha-Hutcheon, 2018; Adlakha-Hutcheon & Hubbard, 2010; Adlakha-Hutcheon & Masys, 2022).

MAD is a hybrid form of a wargaming method and military table-top exercises that was created to discover system-based opportunities or threats to the operations, force development, intelligence, and S&T communities. It enables organizations to conduct exploratory operational research and analysis in a creative manner within a scientific framework; it is multi-disciplinary and multi-modal. This method was developed within Defence Research and Development Canada (DRDC), an agency of the Canadian Department of National Defence, and it is a planning aid used by the force development communities as they plan for investments in large defence capabilities.

MAD – The tool

MAD is conducted in two parts. The MAD Part I is creative and divergent. It focusses on the generation of concepts of technical systems or policy concepts called Conceptual Systems (CS). The CS take the form of futuristic system cards. In contrast to Part I, Part II is a conventional form of table-top exercise which brings convergence. In Part II, operators are engaged to determine the cards of relevance and their potential to be disruptive when applied to future operational scenarios. Part II is similar to the NATO DTAG (Rademaker et al., 2008, 2012).

The purpose of the exercise of MAD is to provide the home team, or the Blue Force, with an operational advantage. MAD yields several outputs including a set of system cards available to the Blue Force to use at any time in the planning continuum. MAD yields CS cards, which are assessed in terms of their ability to

[1] Adlakha-Hutcheon, 2017, 2018; Adlakha-Hutcheon et al., 2012, 2016, 2020; Rademaker et al., 2008, 2012.

cause disruption. Furthermore, the cards may also be categorised further as being conceptual, ready for development, or requiring additional experimentation. Such type of categorization is utilized by militaries to assign a developmental timeline for readiness to technologies. Additionally, the creation, use, and assessment of CS by relevant personnel facilitates development of appropriate countermeasures against the adversary that would not necessarily have occurred without such interaction.

MAD is a part of the strategic foresight toolbox, with a foot in the identification of emerging S&T trends, which in and of itself is desirable for organizations like NATO that publish their S&T trends periodically (NATO Science & Technology Organization, 2020).

MAD thereby brings cohesion and better understanding of horizon scans and technology watch initiatives. It also assesses concepts of relevance to the end-user; provides a challenge function by applying the lens of science and the end-users'; and finally, provides insights for the formulation of future programs. In essence, MAD has three objectives:

1. To identify potential weak signals that have the potential to cause disruptions,
2. To identify potential capabilities to address threats (opportunities), and
3. To assess the potential of the weak signals identified for causing disruptions in operational theatre with scientific rigor.

To achieve the above objectives from a threat-centric perspective for technology-triggered threats, MAD was specifically adapted into Methodology for Assessing Technology Triggered Threats (MAT3). It should be noted that MAD/MAT3 will be used interchangeably given that both provide the results from the opposing perspective.

MAD – Methodology

A detailed description of the MAD methodology is available in Adlakha-Hutcheon, et. al. (2012). The MAD tool is a combination of wargaming, red teaming, structured brainstorming, and gamestorming, which is defined in the next section (Gray, et al. 2010). To a certain extent, it also leverages the DTAG (Rademaker, et al., 2008, 2012).

The raison d'etre for MAD is described as follows:

> The MAD methodology was designed to fill existing needs within the Defence Enterprise. The observation that a means for the S&T and intelligence personnel to interact with operators early in defining requirements for capability plans was required; a means that would enable one to assess impact of developing certain technical systems that will be used by the operators down the road, and thereby plan for eventualities. There was also a need to provide scientific evidence to decision-makers for making informed investment decisions about resource or capability-based planning. (Adlakha-Hutcheon, 2016)

MAD is cited as an innovative adaption of wargaming by Caffrey in his recent book *On wargaming* (Caffrey, 2019, p. 207-208).

MAD is primarily based on the general practice of board or social games with a wargaming perspective since there is evidence that gaming harnesses creativity and tests concepts which can be applied to real world problems (McGonigal, 2011). That gamification (related primarily to reward-based incentive games) develops problem solving skills (Zichermann, 2011). The data collected for the Entertainment Software Association (Ianrl1989, 2015) shows that an average aged American spends approximately 6.5 hours/week, or 327.5 hours/year, playing video games. Furthermore, recent data points that 66% of Americans—more than 215 million people of all ages and backgrounds—play video games regularly: three quarters of players being over 18, with the average age of a video game player being 33 (Entertainment Software Association, 2022). Across all ages, players are about half female and half male (48 and 52 percent, respectively, as of June 2022). Given that as much as three billion hours a week (McGonigal, 2011) are spent on gaming worldwide, there is a reason to believe that it would not be too difficult to solicit participation in gaming-based exercise (Adlakha-Hutcheon, 2016).

MAD Part I

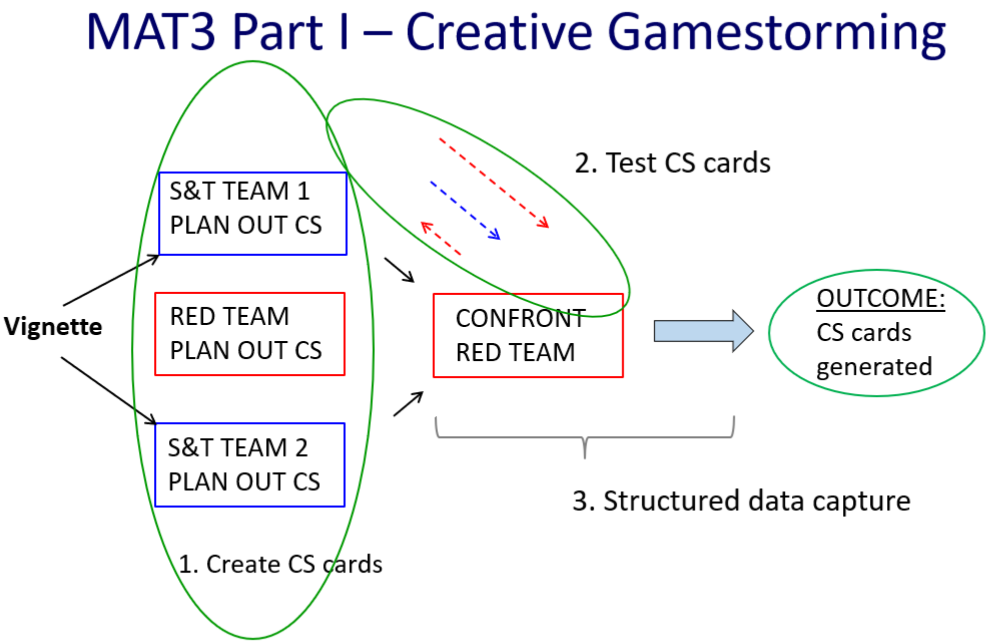
The play of MAD Part I utilizes gamestorming (Gray et al., 2010), a process based on structured brainstorming, which is used in conjunction with gameplay similar to the style of board games that utilize cards. Through it, the creativity of scientific, technical, and intelligence staff is harnessed to innovate and generate futuristic CS cards of technical systems, scientific concepts, or policy. Problem sets are situated in the future (five years or more from the present) within a larger operational mission scenario. These are presented in the form of vignettes to three teams, (2 Blue and 1 Red which represents the adversary). Both Blue teams are made up of Scientific, Technical, or Intelligence staff, while the Red Force comprised members of the armed forces or could even be security professionals. Having the adversary played by operators by profession and having the Blue team comprising S&T or Intelligence personnel is intentional. This type of team make-up, while being counterintuitive, is designed to stimulate out-of-the-box thinking. It allows Blue team personnel to exercise creativity by putting themselves in the shoes of the adversary regardless of their size: a representative of a state, a radicalized youth, or even a member of a small agile terrorist group.

All three teams create concepts after being briefed the same vignette. The teams are tasked with developing CS cards while thinking three moves ahead of the opponent (Blue Force or Red Force; please see Figure 1 below). Once they have developed cards, one Blue team engages at a time in a refereed red teaming step with the Red team in volleys of moves and countermoves (shown as red and blue arrows in the schematic), which enables finessing the cards for their practical applications. Technical referees preside over this part to allow/disallow these moves. The overall play of each vignette takes three hours. The duration may be reduced to two hours, especially after participants get familiar with the process after playing the first vignette. The entire MAD Part I can be played out over the course of one to two days with a play of three to four vignettes.

Subject matter experts are consulted after MAD Part I to determine the technical plausibility of the CS cards generated.

Figure 1

Schematic Illustration of the Play of MAD Part I

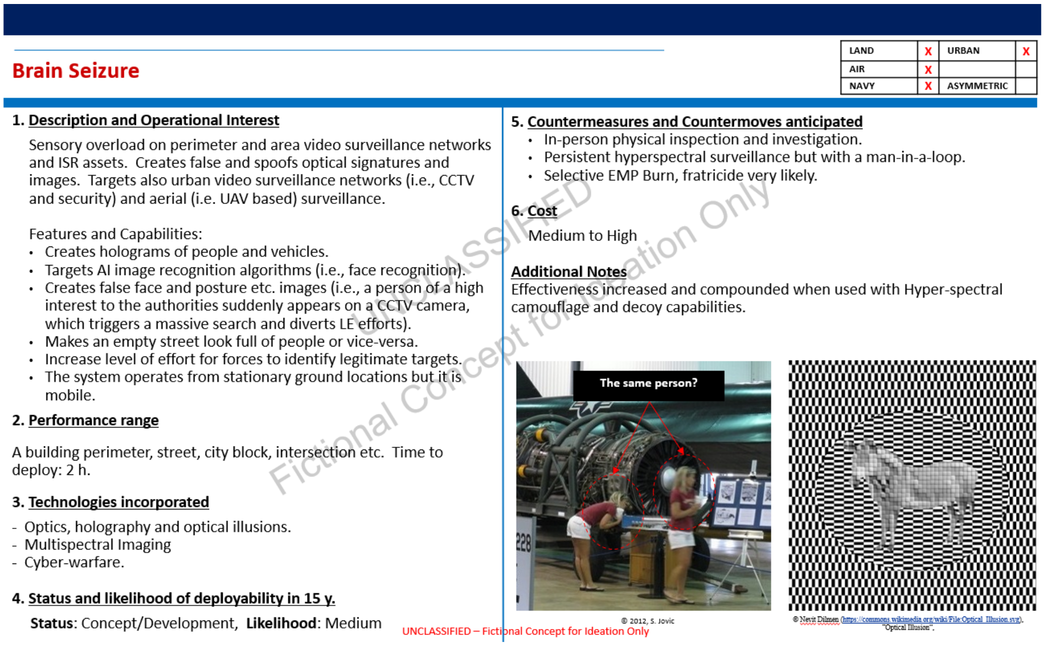

MAT3 Part I – Creative Gamestorming

As shown in Figure 1, there are three steps in Part I: creation of CS cards, testing realism of the cards, and a structured data capture by observers and/or analysts.

The teams have full license in creating the conceptual cards. They can create cards which are capabilities, concepts of policy, or technical systems built from new technologies alone or in combination with pre-existing technologies. Thus, overall, the CS cards represent futuristic concepts available for use in MAD Part II by either Red or Blue teams and as a reference for the future. A sample of a CS is available in Figure 2. The card takes the format of a single slide. The participants fill out the slide template with as much detail as they can for a futuristic concept using the internet and other resources (books, journal articles, or descriptions of tools of the trade) made available to them. They are also asked to give a creative name to their concept.

Figure 2

Sample Concept System Card Created During an Iteration of MAD Part I



Brain Seizure

LAND	X	URBAN	X
AIR	X		
NAVY	X	ASYMMETRIC	

1. **Description and Operational Interest**

Sensory overload on perimeter and area video surveillance networks and ISR assets. Creates false and spoofs optical signatures and images. Targets also urban video surveillance networks (i.e., CCTV and security) and aerial (i.e. UAV based) surveillance.

Features and Capabilities:
- Creates holograms of people and vehicles.
- Targets AI image recognition algorithms (i.e., face recognition).
- Creates false face and posture etc. images (i.e., a person of a high interest to the authorities suddenly appears on a CCTV camera, which triggers a massive search and diverts LE efforts).
- Makes an empty street look full of people or vice-versa.
- Increase level of effort for forces to identify legitimate targets.
- The system operates from stationary ground locations but it is mobile.

2. **Performance range**

A building perimeter, street, city block, intersection etc. Time to deploy: 2 h.

3. **Technologies incorporated**

- Optics, holography and optical illusions.
- Multispectral Imaging
- Cyber-warfare.

4. **Status and likelihood of deployability in 15 y.**

Status: Concept/Development, **Likelihood**: Medium

5. **Countermeasures and Countermoves anticipated**
- In-person physical inspection and investigation.
- Persistent hyperspectral surveillance but with a man-in-a-loop.
- Selective EMP Burn, fratricide very likely.

6. **Cost**

Medium to High

Additional Notes

Effectiveness increased and compounded when used with Hyper-spectral camouflage and decoy capabilities.

© 2012, S. Jovic

© Nevit Dilmen (https://commons.wikimedia.org/wiki/File:Optical_Illusion.svg). "Optical Illusion".

UNCLASSIFIED – Fictional Concept for Ideation Only

Source: Adlakha-Hutcheon, 2018 presentation at CORS

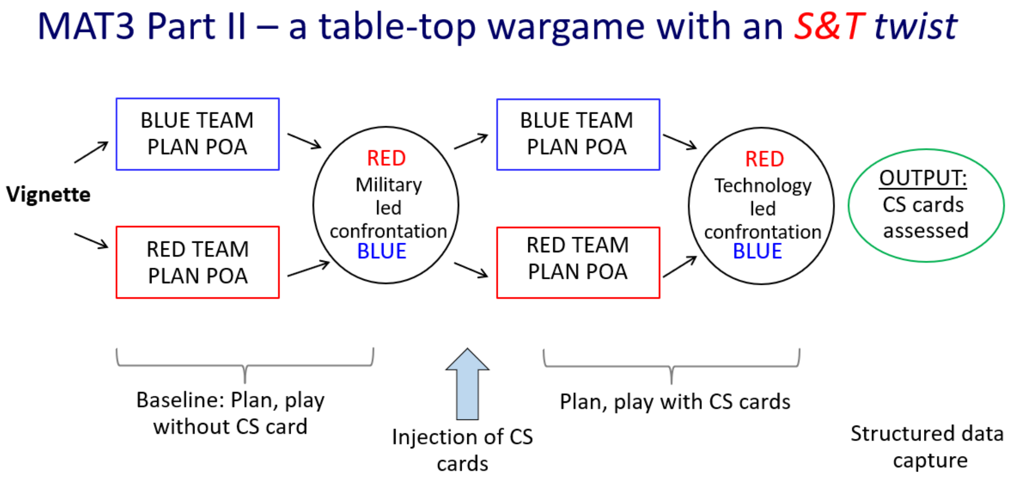
MAD Part II

In Part II, the disruptive impact of selected CS cards formulated in Part I is assessed by two teams of experienced operators, mostly uniformed personnel, in a series of realistic operational vignettes. The entire MAD exercise is set 10-15 years into the future to enable free play by the participants. The number of years into the future for situating the scenarios and vignettes may vary by subject. For example, for cyber concepts, three years from now is already considered the far future.

MAD Part II plays out as a seminar table-top wargame, where two teams develop outlines of their respective Plan of Action (POA) in response to an operational/ tactical vignette set in the future. They are then provided with CS cards to refine their plans with the knowledge of the opponent's POA (see Figure 3). Typically, a vignette takes around 3 hours from start to finish. Both the Red and Blue teams comprised military officers of the rank of Major or equivalent that hail from all three environments. By design, the Red Force's moves and counter moves have a wide degree of flexibility (i.e., akin to the *asymmetric edge*). On the other hand, the Blue Force's moves are limited in the gameplay by having to respect international legalities such as the Laws of Armed Conflict (LOAC), the Geneva Convention, etc. If the participants include military personnel, then the MAD design can also enforce the Canadian Armed Forces Doctrine together with Tactics, Techniques, and Procedures (TTPs) when they access current or near-term technological systems. For security personnel, relevant laws and rules of engagement can be added more suited to their function.

Figure 3

Schematic Illustration of the Play of MAD Part II


MAT3 Part II – a table-top wargame with an S&T twist
Vignette
BLUE TEAM PLAN POA
RED TEAM PLAN POA
RED Military led confrontation BLUE
BLUE TEAM PLAN POA
RED TEAM PLAN POA
RED Technology led confrontation BLUE
OUTPUT: CS cards assessed
Baseline: Plan, play without CS card
Injection of CS cards
Plan, play with CS cards
Structured data capture

The two parts of MAD are contrasted in Table 1 below.

Table 1

Contrast of the Two Parts of MAD

	MAD Part I (1-2 days)	MAD Part II (2-3 days)
Style of play	Divergent	Convergent
Instruction to participant	Be Creative	Be a Detective
Basis of play	Gamestorming	Table-top seminar wargame Red teaming
Outputs	Generates Conceptual System (CS) cards	Assessment of impact through ascertaining the potential for causing disruption, and a validation of operational relevance of CS by the end-user
	Concept generation	Scopes out weak signals and consequent future projects
Overall outcome	Through creation of concepts and an assessment of their potential impact, the awareness of cross-discipline and operational practitioners is raised concomitantly generating a community of practitioners.	

Methodology: Types of Analysis

Data collected at the end of both parts of MAD can be analyzed in several ways. Thus far, most often it has been analyzed in three ways. First, assessing the potential of a CS card to be disruptive; second, the added relevance (value) of the card to the military and/or operator is determined through the construction of move-countermove trees; and finally, the cards are categorized for their readiness for use by operators. The timescale of the availability of cards to the operators is determined in terms of the time taken for their development on the concept maturity continuum, which extends from an exploration of a Concept, its Development, and Experimentation or CD&E, and their final validation for exploitation. These three phases are also referred to as Concept, Development, and Experimentation (C, D & E, respectively). Each of these analyses is described below.

Determination of Disruptive Potential

Disruption is a commonplace occurrence within the public security and operational military milieu; however, it is not often that it is studied scientifically or in combination with innovation (Adlakha-Hutcheon & Masys, 2022). This essential fact was the critical gap that formed the basis for this analysis.

In MAD, the potential of a card to be disruptive is assessed by determining the difference in a team's POA in the presence of cards relative to the baseline POA established in the absence of cards or the baseline. It is done during play and more formally after the exercise is over. It uses the basic arithmetic formula of

Potential for causing disruption = $\text{POA}^{\text{with card}} - \text{POA}^{\text{baseline}}$

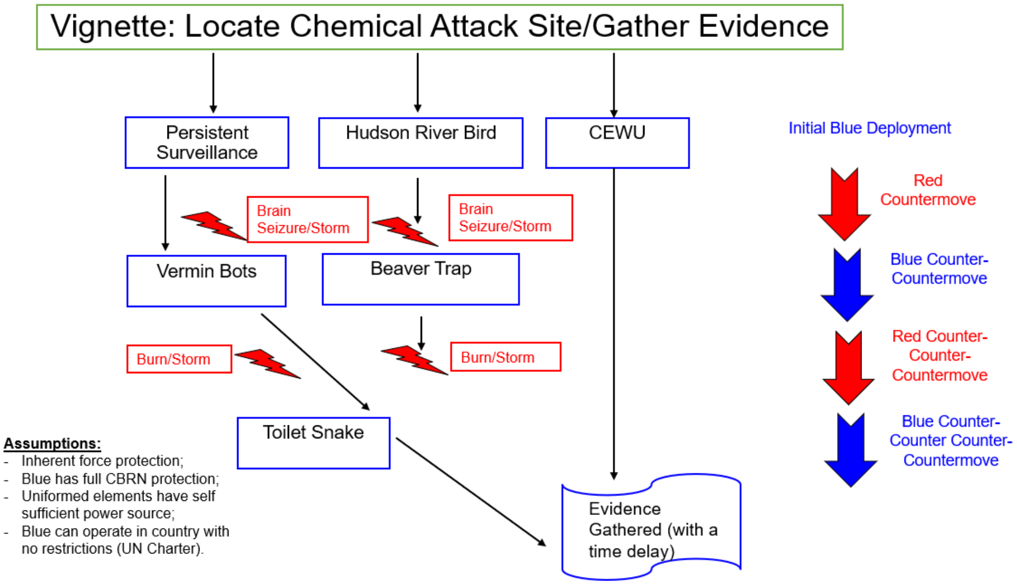
As an example, in an iteration of MAT3 centered on non-kinetic sciences, the concepts based on exploitation and suppression of persistent full spectrum electronic surveillance and the shaping of behavior via social media were found to be potentially disruptive technologies. The CSs generated were tested at the NATO's International Concept Development and Experimentation Conference workshop (Adlakha-Hutcheon et al., 2020). Such a non-kinetic theme based MAT3 has direct applicability beyond military to security. Since 9/11, the use of non-military centric technologies, like homemade devices and improvised tools by terrorists and/or small organizations with minimal budgets, is publicly known. Not only are these used contemporarily, but they also raise the alarm for training security personnel into readiness. MAD is a pragmatic tool that can, through red teaming, train them in being able to beat the adversary at its own game.

Move-countermove Tree

As noted earlier, in Part II, a volley of moves and countermoves takes place. Each team and analysts are provided with move/countermove or measure/countermeasure tree templates to note down the play of cards within the narrow constraints of the played vignette. A gap is signalled when no further countermove can be made in the gameplay. A stop in play could arise due to a lack of availability of a suitable CS card; existing equipment; or lack of use of technology, a concept, or a response to an unforeseen manoeuvre by the opposing force. Consequently, these trees are useful visual representations that reveal capability strengths and vulnerabilities as illustrated in Figure 4. Through the trees, the potential of a system to be a future capability or a threat is also obtained. For example, as indicated in Figure 4, the ability of the Blue Team to be able to counter the sample card Brain seizure (Figure 2) suggests an existing capability, while this is not true for the Burn Storm card, indicating a vulnerability for the Blue Team. By extension, the Blue side would want to explore means to address such gaps through targeting investment in research and/or a program.

Figure 4

Example of a Move-Countermove Tree for Three Conceptual System Cards


Vignette: Locate Chemical Attack Site/Gather Evidence
Persistent Surveillance
Hudson River Bird
CEWU
Initial Blue Deployment
Brain Seizure/Storm
Brain Seizure/Storm
Red Countermove
Vermin Bots
Beaver Trap
Blue Counter-Countermove
Burn/Storm
Burn/Storm
Red Counter-Counter-Countermove
Toilet Snake
Blue Counter-Counter Counter-Countermove
Evidence Gathered (with a time delay)
Assumptions:
- Inherent force protection;
- Blue has full CBRN protection;
- Uniformed elements have self sufficient power source;
- Blue can operate in country with no restrictions (UN Charter).

Source: Adlakha-Hutcheon, 2018 presentation at CORS

Categorization

Categorization is a third type of analysis. It is conducted post-exercise in consultation with subject matter experts and operators. The cards are categorized for their relevance based on their readiness for use on the CD&E or concept maturity continuum.

Methodology: Types of Outputs

In summary the MAD exercises yield five different outputs. These are:

1. A dataset of CS cards (Part I) which are available for use, when appropriate, in other iterations of MAD exercises with different sets of vignettes;
2. A sub-set of cards assessed to be disruptive within the context of the vignettes played;
3. A move-countermove tree for CS cards used by the participants (i.e., found to be useful to the end-user);
4. Evidence useful to decision-makers to determine which S&T capabilities to advance, and finally;
5. A community of practitioners developed among scientists, technical, intelligence personnel, and operators/officials that have experienced MAD methodology together. On an experiential level, these participants gain first-hand experience in gamestorming, red teaming, and wargaming—techniques that are not often available simultaneously to such communities.

Relevance of Outputs

These outputs are relevant because together they allow an identification of applications of technologies integrated into conceptual system cards; an assessment of concepts through a scientific lens for purposes of further development by S&T, operators, and intelligence personnel; an assessment conducted by the end-user of scenarios, futuristic conceptual systems comprising old and emerging technologies or even tools for that matter and capabilities; and an opportunity to engage S&T + operator (+ intelligence/policy) personnel early and at low cost, as well as the creation of communities of practice that have exercised MAD together. MAD also generates intangible, qualitative insights that can influence not only the thinking of participants, but also provides evidence for management to make informed decisions. As an example, observing how participants react to different vignettes within the exercise offers insights into how they will react in a real situation, which could help in planning future training needs, all of which enhance the operators' CD&E perspectives.

The type of personnel that would benefit the most from exercising MAD regularly include:

Emergency personnel that do not systematically train to be creative or those that are not used to exercising their standard operating procedures (SOP's). For example, those that counter chemical or biological spills. While the police, firefighters, and paramedics participate in table-top exercises, they do not train to get S&T input in planning their requirements for the future and associated research programs 10 or 15 years out into the future. In addition, IT personnel and security personnel who maintain infrastructure also stand to benefit greatly.

Security and intelligence personnel could potentially use MAT3 exercises for the following purposes:

- Identifying previously unknown gaps in intelligence knowledge;
- Identifying indicators to aid in assessments of weak signals that may coalesce;
- Identifying key issues to add to future intelligence collection efforts; and
- Identifying new potential sources where complementary information may be found to aid in intelligence assessments.

Furthermore, MAD can be tailored to client requirements on specific topics of interest.

MAD can be conducted at a classified or unclassified level. The results of MAD/MAT3 add to the evidence for evidence-based decision-making on investments. All the above attributes of MAD/MAT3 aid the formulation of programs of work for practitioners be they researchers or operators.

MAD facilitates a conversation between science and technology experts and operators spanning across safety and security. Of course, the use of S&T to aid planning and training in tactics[2] is not new and dates back to the Hellenistic age, 500–100 BC. MAD/MAT3 may even be held virtually to engage wider participation across geographically distributed personnel.

The MAD exercise can be tailored within strategic, operational, or tactical scenarios, depending on the needs of the client. In order to conduct MAD at a strategic level, there would need to be an equivalency between the Blue and Red sides, in terms of research funding, time toward the development of research programs, and an overall scenario setting addressing a nation-to-nation or state-versus-state problem set involving strategic competition. Such type of MAD is referred to as Methodology for Assessing Political States or MAPS. The strategic level of play associated with MAPS, which tends to change political maps, is beyond an easily transferrable scope and irrelevant to safety and security

[2] Simulations Publications, Inc. was an American print-wargame pioneer, developer, and publisher operating from 1969 to 1982 (The Tactical Wargamer, n.d.).

personnel, and thus not discussed in this paper. Here, the focus lies on gaining operational and tactical advantage for the security personnel through the use of a tool used within the military as illustrated in Figures 2 and 3. The concept of generating an optimal sensory overload is captured in the Brain seizure CS card (see Figure 2). The manner in which the Brain Seizure card may be employed is shown in Figure 3, whereby it defeats electrical surveillance by oversaturating it with input. Other examples of CS cards created as a consequence of MAD that may be applicable within safety and security operations are indicated as sequential tactical moves in red and blue.

MAD is adaptable to client needs, both the scale and timeline of their needs. The ability to tailor MAD to client requirements is derived from writing scenarios and vignettes to match the needs. For instance, if the client needs fixes for an informational technology problem that is expected to arise in the next 5-10 years, then the scenarios are situated within this time. This type of MAD was exercised in 2012-13 for the interdepartmental Canadian Telecommunications Cyber Protection Working Group of the Government of Canada and the communication industries. IT personnel from the government and telecommunication industries, none of whom were uniformed personnel but hailed from the world of IT responsible for IT security, participated. The telecommunication industries have communicated that they have since started using MAD to develop their in-house future technical capabilities.

Scenarios and vignettes need to be tailored specific to each type of problem. In addition, the selection of participants plays an important part in the success of MAD. For instance, when MAD is run for the Air force, even though participation is joint, which is to say that officers are also invited from the Army and Navy in addition to the Air Force, the scenarios and vignettes seek solutions geared toward utility by the Air force. The cards created in MAD Part I are assessed by subject matter experts for their relevance and only then included for play in Part II. In each run of MAD Part II, cards are rejected either for their implausibility or lack of demonstrable utility to the client. As a result, designing MAD appropriately demands a good understanding of the client problem and preparation toward achieving it. This said, the actual table-top exercise itself is low technology with a few demands other than participation from S&T, intelligence, safety, and security operational personnel. Each team ideally should include 6-8 participants for a total of 18-24 in Part I and 12-16 in Part II. MAD requires analysts to support data gathering, as well as two types of referees (one with operational and the other with technical expertise) in Part II.

Therefore, in summary, MAD needs no more than 20 participants in total in each of its Parts I and II, a few subject matter experts, and a very small budget to cover the temporary duty travel for personnel for its execution. It is neutral or separate from and not related to the budget of the client organization.

It should be pointed out that the use of MAD is not impacted by the size of the client organization or the time frame within which they wish to develop their future needs or train their personnel. Through the MAD tool, an organization responsible for safety and security, large or small, can use MAD to exercise the creativity of available personnel on their team or the Blue side. This play also overrides the size of the budget in the client organization to understand, detect, and defend against an adversary that is agile. In addition to the training of personnel by the regular and periodic conduct of MAD, there are at least two other opportunities to become nimble in the face of a lesser-known adversary, especially one that includes small groups or cells of terrorists. The first one is during Part I through the creation of cards by all participants. The second one is during Part II, when and where all participants train to defeat the opponent through the selection of cards thus the participants get to know the card, determine what an opponent might do without having to follow the rules of law, and learn the best way to play within the rules of engagement with limited resources. MAD affords an overall training in readiness including against the winning hand of lawfare.

Implications Beyond Defence

The MAD methodology facilitates the use of S&T by steering the creation of CS cards with input from emerging technologies resulting from technology watch and horizon scanning activities of their assessments by operators. This feature has been used to their advantage by military organizations such as NATO. For example, the scientific evidence resulting from DTAG and MAD has been used to support decisions on investments (Bexfield, 2013). Scientific organizations have also taken up development of capabilities based on pointers from MAD indicating direct utility to the operators (i.e., the end-users).

For the military, the usefulness of the tool lies in familiarizing operators with what S&T can bring to operations, especially as it can also help identify possible future disruptions that might have a serious impact on defining capability requirements or operational concepts. Therefore, it would be advantageous to extract the value (Gordon, 2009) of this methodology and use it to support capability-mix studies at strategic and operational levels, in particular for those looking more than 15 years ahead. Its other possible applications include advancing capability-based planning and assessment and/or concept development.

Recommendation

MAD is a tool developed within DRDC, the outputs of which provide end-user validated evidence for decision-makers to plan, prepare, and make informed investment decisions. Conducting periodic MAD is a step in the right direction to plan ahead, identify, and combat all forms of disruption, particularly ones overlooked in conventional security fora. It also facilitates a better understanding amongst participants of the potential for concepts to coalesce in a manner that is a threat that demands consideration of solutions or presents opportunities.

References

Adlakha-Hutcheon, G. (2016, October 17). *The MAD way.* Proceedings of the Tenth Annual NATO Operations Research and Analysis Conference 2-3. NATO Science and Technology Organization. Defence and Research Development Canada, NATO MP-SAS OCS-ORA-2016-11.

Adlakha-Hutcheon, G. (2017). *The MAD way.* The Tenth Annual NATO Operations Research and Analysis Conference 2-3. NATO Science and Technology Organization. Defence and Research Development Canada, DRDC-RDDC-2016-P172, NATO MP-SAS OCS-ORA-2016-11.

Adlakha-Hutcheon, G. (2018, June 5). A foresight method for countering irregular warfare threats. In C. MacDonald & P. Vanberkel (Chairs), *60th Annual CORS Conference,* Canadian Operational Research Society, Halifax, Nova Scotia, Canada.

Adlakha-Hutcheon, G., Elsaesser, D., & Wallace, B. (2017). *Methodology for assessing technology triggered threats exercise for non-munitions targeting sciences 2016–17, Part I: Scenario and vignettes.* DRDC-RDDC-2017-D019. Defence Research and Development Canada [Archived in DRDTIS Information Holdings and Services].

Adlakha-Hutcheon, G., Hazen, M., Hubbard, P., Mclelland, S., & Sprague, K. (2012). *Methodology for assessing disruptions (MAD) Part I: Report and analysis.* DRDC Corporate TM 2012-009. Defence Research and Development Canada – Corporate Office [Archived in DRDTIS Information Holdings and Services].

Adlakha-Hutcheon, G., & Hubbard, P. (2010). *Disruptive technologies assessment game: A pilot for DRDC and an S&T outlook tool for assessing the disruptive potential of technological systems.* DRDC Corporate TM 2010-011. Defence Research and Development Canada – Corporate Office [Archived in DRDTIS Information Holdings and Services].

Adlakha-Hutcheon, G., & Masys, A. J. (2022). Understanding the landscape of disruption, ideation and innovation for defence and security. In G. Adlakha-Hutcheon & A. Masys (Eds.), *Disruption, ideation and* *innovation for defence and security* (pp. 1-9). Springer. https://doi.org/10.1007/978-3-031-06636-8

Adlakha-Hutcheon, G., Wallace, B. & Jovic, S. (2020). *Exercising MADness – Countering civil unrest: Results of workshops conducted at the International Concept Development and Experimentation Conference.* Scientific Letter, DRDC-RDDC-2020-L289. Defence and Research Development Canada [Archived in DRDTIS Information Holdings and Services].

Bexfield, J. N. (2013). Operations assessment and planning for transition stages. In A. Williams, J. Bexfield, F. F. Farina & J. De Nijs (Eds.), *Innovations in operations assessment: Recent developments in measuring results in conflict environments.* North Atlantic Treaty Organization.

Caffrey, M. B. (2019). *On wargaming: How wargames have shaped history and how they may shape the future.* Newport Papers. 43. Naval War College Press.

Entertainment Software Association. (n.d.). *2022 Essential Facts About the Video Game Industry*. https://www.theesa.com/resource/2022-essential-facts-about-the-video-game-industry/

Gordon, A. (2009). *Future savvy: Identifying trends to make better decisions, manage uncertainty, and profit from change*. AMACOM.

Gray, D., Brown, S., & Macanufo, J. (2010). *Gamestorming*: *A playbook for innovators, rulebreakers, and changemakers.* O'Reilly Media.

Ianrl1989. (2015, April 25). *ESA 2015 Essential Facts About the Computer & Video Game Industry.* The Sociology of Video Games. https://sociologyofvideogames.com/2015/04/25/esa-2015-essential-facts-about-the-computer-video-game-industry/

McGonigal, J. (2011). *Reality is broken*: *Why games make us better and how they can change the world.* The Penguin Press.

NATO Science & Technology Organization. (2020). *Science & technology trends 2020-2040: Exploring the S&T edge.*

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Rademaker, M. [Multiple authors]. (2008). *Assessment of possible disruptive technologies for Defence and Security*. North Atlantic Treaty Organization. Technical report for NATO SAS-062 [Archived in https://www.sto.nato.int].

Rademaker, M. [Multiple authors]. (2012). *Disruptive Technologies Assessment Game: Evolution and Validation*. North Atlantic Treaty Organization. Technical report for NATO SAS-082 [Archived in https://www.sto.nato.int].

The Tactical Wargamer. (n.d.). *Simulations Publications, Inc.* https://www.tacticalwargamer.com/publishers/spi.htm

Zichermann, G. (2011, June). *How games make kids smarter* [Video]. TED. https://www.ted.com/talks/gabe_zichermann_how_games_make_kids_smarter

Author's corresponding address: Gitanjali.Adlakha-Hutcheon@forces.gc.ca

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/