Canadian Security Interests

Les intérêts du Canada en matière de sécurité

cda institute analysis
analyse l'institut de la cad

Papers from the 15th Annual Graduate Student Symposium

Looking Beyond — Un regard au-delà

Communications tirées du 15e Symposium annuel des étudiants diplômés

Bill McAuley | University of Calgary
Meaghan Williams | Queen's University
Geoff Keelan | University of Waterloo

Edited by: Paul Hillier

Institut de la Conférence des associations de la défense

L'Institut de la Conférence des associations de la défense est un organisme caritatif et non partisan qui a pour mandat de promouvoir un débat public éclairé sur les enjeux notre sécurité et de la défense nationale.

Institut de la Conférence des associations
de la défense
151 rue Slater, bureau 412A
Ottawa (Ontario)
K1P 5H3

613 236 9903
www.cdainstitute.ca
cda@cda-cdai.ca

Conference of Defence Associations Institute

The Conference of Defence Associations Institute is a charitable and non-partisan organisation whose mandate is to promote informed public debate on national security and defence issues.

Conference of Defence Associations Institute

151 Slater Street, suite 412A
Ottawa, Ontario
K1P 5H3

613 236 9903
www.cdainstitute.ca
cda@cda-cdai.ca

CANADIAN SECURITY INTERESTS: LOOKING BEYOND

Papers from the 15th Annual Graduate Student Symposium

LES INTÉRÊTS DU CANADA EN MATIÈRE DE SÉCURITÉ : UN REGARD AU-DELÀ

Communications tirées du 15e Symposium annuel des étudiants diplômés

Foreword

The CDA Institute Graduate Student Symposium has matured from its creation some 16 years ago by our Executive Director Col (Ret'd) Alain Pellerin, to what is now acknowledged as an event to be widely attended by the defence & security community. It is a class event from which former presenters continue to become prominent professionals in academia, government, military, industry and media circles.

Over the years, the Symposium has become the cornerstone of the CDA Institute's commitment to the next generation of defence and security leaders, and I am very pleased to endorse this first publication resulting from the event. The three students that are highlighted in the publication worked tremendously hard with our research advisors and staff to develop their presentations into these fine analyses.

The past 12 months have brought about a number of fruitful changes to the Institute that have benefited greatly from the contribution of young analysts. The CDA Institute launched its Defence and Security Blog, which profiles issues briefs, many of which are written by young professionals. Drawing from contributors residing across Canada and managed by our Research Coordinator, Paul Hillier, we have seen this blog become a key tool for discussion and the exchanges of ideas.

Additionally, we are very pleased to have launched the CDA Institute's Internship Programme. Working with our Research Coordinator, several recent graduates as well as current students are given the opportunity to conduct research on topics of their own choosing; these junior policy analysts will provide a dynamic new capacity to the Institute that we would not otherwise enjoy and we welcome them to the team.

These developments over the past year have been exciting, and have focussed on providing opportunities for the next generation. I am personally looking very much forward to hosting the 16th Annual Graduate Student Symposium in Kingston on the 24th and 25th of October, 2013 and invite you to join me at Royal Military College of Canada for the event.

Ray Henault, CMM, MSC, CD
General (Ret'd)
President, CDA Institute

Préface

Le Symposium des étudiants diplômés présenté sous l'égide de l'Institut de la CAD a mûri : depuis sa création il y a quelque 16 ans par le Directeur Exécutif le Colonel (ret) Alain Pellerin, il est maintenant reconnu comme une rencontre à laquelle un grand nombre de personnes des milieux de la défense et de la sécurité se font un devoir d'assister. C'est une manifestation de classe qui a vu certains de ses anciens présentateurs devenir des professionnels éminents, à l'université, dans l'armée, l'industrie et les médias.

Au cours des années, le Symposium est devenu la pierre d'angle de l'engagement de l'Institut de la CAD envers la génération suivante de leaders de la défense et de la sécurité, et je suis très heureux d'appuyer cette première publication résultant du Symposium. Les trois étudiants qui sont mis en lumière dans cette publication ont travaillé extrêmement fort avec nos conseillers en recherche et notre personnel pour développer leurs présentations et les transformer en des analyses fines.

Les 12 derniers mois ont amené à l'Institut un certain nombre de changements fructueux qui ont grandement bénéficié de la contribution de jeunes analystes. L'Institut de la CAD a lancé son blogue sur la défense et la sécurité, qui présente des profils de notes sur les actualités, dont plusieurs sont écrits par de jeunes professionnels. Alimenté par des collaborateurs résidents à travers le Canada et dirigé par notre coordonnateur de la recherche, Paul Hillier, nous avons vu ce blogue devenir un outil clé de discussion et d'échange d'idées.

En plus, nous sommes très heureux d'avoir lancé le programme de stages de l'Institut de la CAD. En travaillant avec notre coordonnateur de la recherche, plusieurs diplômés récents ainsi que des jeunes qui sont encore aux études ont ainsi l'occasion d'effectuer une recherche sur des sujets qu'ils ont eux-mêmes choisis ; ces analystes de politiques juniors vont donner à l'Institut une nouvelle capacité dynamique dont nous ne bénéficierions pas autrement et nous sommes heureux de les accueillir dans l'équipe.

Ces développements de l'année qui vient de s'écouler ont été passionnants et on insisté principalement notre volonté d'ouvrir des possibilités à l'intention de la prochaine génération. Personnellement, c'est avec un plaisir anticipé que je serai l'hôte du 16e Symposium annuel des étudiants diplômés, à Kingston, les 24 et 25 octobre 2013, et je vous invite à vous joindre à moi, au Collège militaire royal du Canada, à cette occasion.

Ray Henault, CMM, MSC, CD
Général (ret)
Le président de l'Institut de la CAD

Introduction

In the best tradition of graduate work, the papers in this collection ask us to question our assumptions, and give us fresh perspectives that allow us to address the many dichotomies that govern security studies.

Whether it is redefining Canada's involvement in Afghanistan as having been exclusively tactically driven, addressing cyber security through the lens of information war, or reshaping the way we appreciate relationships between women and insurgent movements, the following analyses take three unique topics and examine them in a new light.

Each October, the CDA Institute's Graduate Student Symposium is held at the Royal Military College of Canada, drawing master's and doctoral students from across Canada and abroad to present their research on issues relevant to Canadian defence and security. This past year at the 15th annual symposium, three papers stood out as exceptional and deserving of publication.

Bill McAuley's paper, "Canada's Tactical Fixation? Rethinking the IED Phenomenon" presents and defends one haunting assertion: that for much of Canada's combat mission in Kandahar, the counter-IED battle left no room for strategic considerations. In his words, "Canadians spent more than half of their Kandahar deployment fighting for their own lives because too few resources were committed over too large an area." While the Canadian Forces were not the only western power to be manipulated by the Taliban into being consumed by the battle against improvised explosive devices (IEDs), McAulay writes that it was a poorly defined national interest that led Canada to volunteer itself to handle an enormous 54,000km^2 territory.

"Hell on Heels: the Intersection of Women, Terror & Insurgency," by Meaghan Williams studies the strategic role women play as suicide bombers. Making important differentiations between insurgent groups and terror networks, she begins by questioning why women have been allowed by these groups to partake in conflict, which is generally a male-dominated area. She argues that western media has grossly distorted the issue, focusing on exclusively personal motivations and "reconstructing these women as less than women or less than psychologically sound." This has led to a neglect of the strategic asset female suicide bombers represent over their male counterparts. By causing western audiences to struggle with reconciling and rationalizing these women's actions, Williams contends that these organizations achieve a tremendous victory, as sympathy and empathy will always be more powerful than fear alone.

Geoff Keelan's "Information War: The Historical Precedents of Cyber Operations" takes the catchwords of today—cyber security and cyber war—and places them in the context of the centuries' old 'information war.' Drawing parallels between the eruption of easily accessible data during the cyber era and the 15th century proliferation of books through the printing press, he contends that, "both represent different steps in the historical development of the 'information society'." With this basis, he

then compares information warfare in the cyber domain (with its vulnerabilities to penetration) to the historical use of cartography (where theft and disruption of maps had significant security impacts). While both require trained experts as well as a base level of understanding among users, an important difference is that with cyber, those not directly involved in the field represent potential breaches into the system through ignorance or malice.

The annual theme of the symposium, *Canada's Security Interests*, calls upon graduate students to examine what security interests might look like for Canada. These papers go a step further, asking us to critically examine whether Canada approaches its interests in a strategic manner. The authors, in challenging us to rethink their chosen topics, have drawn together one common theme: *does Canada have strategic vision?*

McAuley questions whether we were so governed by our desire to be prominently placed in Kandahar that we undertook too much, and ended up overstretched, focussing on tactical rather than strategic impacts. Meanwhile, Williams presents us with the dilemma that our understanding of the recruitment of female suicide bombers may look only at the tactical benefits for organizations—namely, doubling the number of potential candidates to detonate explosives—when, instead, it must be recognized that recruiters have strategic motivations such as creating empathy. Keelan draws our attention to the converse of these, which is that even if a country has a strategic vision and drafts, for example, a cyber security strategy, it represents a failure if little progress is made in adopting its recommendations.

The core mandate of the CDA Institute is to promote informed public debate on issues of defence and security. In this vein, promoting research and analysis by young academics and professionals rests at the core of the Institute's mission. As we continue to tackle a wide array of topics and challenges, we return to these same issues: *what are our security interests, and how do we conceptualize a strategic vision to meet these interests?*

We hope these papers go some way in advancing discourse and thinking on these topics.

Paul Hillier
Research Coordinator

Introduction

Dans la meilleure tradition des travaux de deuxième cycle, les communications faisant partie de cette collection nous demandent de remettre en question nos hypothèses et nous proposent de nouveaux points de vue sous lesquels aborder les nombreuses dichotomies qui gouvernent les études portant sur la sécurité.

Qu'il s'agisse de redéfinir l'implication du Canada en Afghanistan comme ayant été exclusivement déterminée par la tactique, d'aborder la cybersécurité à travers la lentille de la guerre de l'information, ou de remodeler la façon dont nous apprécions les relations entre les femmes et les mouvements insurrectionnels, les analyses qui suivent prennent trois sujets uniques et les examinent sous un éclairage nouveau.

Chaque mois d'octobre, le Symposium des étudiants diplômés, de l'Institut de la CAD, se tient au Collège militaire royal du Canada, et attire des étudiants à la maîtrise et au doctorat de partout au Canada et de l'étranger pour présenter leurs recherches sur des enjeux qui ont une pertinence à la défense et à la sécurité du Canada. L'année passée, lors du 15^{e} symposium annuel, trois communications se sont démarquées par leur qualité exceptionnelle au point de mériter publication.

La communication de Bill McAuley, *Canada's Tactical Fixation? Rethinking the IED Phenomenon* présente et défend une affirmation lancinante, à savoir que, pour une grande part de la mission de combat à Kandahar, la bataille contre les engins explosifs improvisés n'a laissé aucune place à des considérations stratégiques. Selon lui, « Les Canadiens ont passé plus de la moitié de leur déploiement à Kandahar à se battre pour sauver leur peau parce que trop peu de ressources avaient été engagées sur une trop grande superficie. » Bien que les Forces canadiennes n'aient pas seulement été la seule puissance occidentale à être manipulée par les Taliban et à être consommée par la bataille contre les engins explosifs improvisés, McAulay écrit que c'était un intérêt national mal défini qui a mené le Canada à se porter volontaire pour prendre charge d'un énorme territoire de 54 000 km^{2}.

Hell on Heels: the Intersection of Women, Terror & Insurgency, de Meaghan Williams, étudie le rôle stratégique que les femmes jouent comme kamikazes. Faisant une importante distinction entre les groupes d'insurgés et les réseaux de terroristes, elle commence à mettre en question les raisons pour lesquelles ces groupes ont permis aux femmes de prendre part à ces conflits, qui sont généralement un domaine dominé par les hommes. Selon elle, les médias occidentaux ont grossièrement déformé la question en portant l'attention exclusivement sur des motivations personnelles et en « reconstruisant ces femmes comme moins que des femmes ou moins que psychologiquement saines ». Ce point de vue a fait qu'on a négligé l'actif stratégique que les kamikazes féminins représentent sur leur vis-à-vis masculins. En faisant en sorte que les auditoires occidentaux se débattent, aux prises avec la réconciliation et la rationalisation des gestes de ces femmes, Williams soutient que ces organisations remportent une prodigieuse victoire, parce que la sympathie et l'empathie seront toujours plus puissantes que la peur à elle seule.

L'article *Information War: The Historical Precedents of Cyber Operations*, de Geoff Keelan, prend les mots à la mode aujourd'hui—cybersécurité et cyberguerre—et les place dans le contexte de la vieille 'guerre de l'information' qui remonte à des siècles. En tirant des parallèles entre l'éruption de données

faciles d'accès, à l'ère de la cybernétique, et la prolifération des livres, au 15e siècle, due à l'invention de la presse à imprimerie, il soutient que « les deux représentent différentes étapes dans le développement historique de la 'société de l'information'. »

Avec cette base, il compare ensuite la guerre de l'information dans le domaine cybernétique (avec ses vulnérabilités à la pénétration) à l'usage historique de la cartographie (où le vol et la perturbation des cartes avaient des conséquences significatives sur la sécurité). Tandis que les deux modes nécessitent des experts formés ainsi qu'un niveau de base de compréhension chez les usagers, il existe une importante différence entre les deux : avec la cybernétique, ceux qui n'ont pas directement à voir dans le domaine représentent des infractions dans le système, par ignorance ou par malice.

Le thème annuel du symposium, *Les intérêts du Canada en matière de sécurité*, demande aux étudiants diplômés d'examiner de quoi les intérêts de sécurité pourraient avoir l'air pour le Canada. Ces communications vont un pas plus loin en nous demandant de nous interroger de façon critique pour savoir si le Canada approche ces intérêts d'une manière stratégique. Les auteurs, en nous mettant au défi de repenser ces sujets choisis, se sont rassemblés sous un thème commun : *le Canada a-t-il une vision stratégique ?*

McAuley se demande si nous avons été menés par notre désir d'être bien placés à Kandahar au point d'avoir trop entrepris, pour finir par être débordés, concentrés sur le niveau tactique plutôt que sur les impacts stratégiques. Pendant ce temps, Williams nous présente le dilemme à l'effet que notre compréhension du recrutement de kamikazes féminins peut ne concerner que les bénéfices tactiques des organisations—c'est-à-dire doubler le nombre de candidats potentiels pour faire détonner les explosifs—alors qu'on doit plutôt reconnaître que les recruteurs ont des motivations stratégiques, comme celle de créer de l'empathie. Keelan attire notre attention sur l'inverse de ces situations en disant que, même si un pays a une vision stratégique et des ébauches de stratégies, comme une stratégie de cybersécurité par exemple, il court à l'échec si peu de progrès est réalisé dans l'adoption de ses recommandations.

Le mandat essentiel de l'Institut de la CAD est de promouvoir un débat public éclairé sur les questions de défense et de sécurité. Dans cette veine, la promotion de la recherche et de l'analyse par de jeunes universitaires et professionnels repose au cœur de la mission de l'Institut. Alors que nous continuons à nous intéresser à une large gamme de sujets et de défis, nous retournons à ces mêmes questions : *quels sont nos intérêts en matière de sécurité, et comment conceptualisons-nous une vision stratégique afin de répondre à ces intérêts ?*

Nous espérons que ces communications nous permettent dans une certaine mesure de faire avancer le discours et la réflexion sur ces sujets.

Paul Hillier
Coordinateur de la Recherche

Canada's Tactical Fixation? Rethinking the IED Phenomenon

> Pre-occupied with protection of our own forces, we have operated in a manner that distances us—physically and psychologically—from the people we seek to protect. In addition, we run the risk of strategic defeat by pursuing tactical wins that cause civilian casualties or unnecessary collateral damage. The insurgents cannot defeat us militarily; but we can defeat ourselves.[1]
>
> General Stanley McChrystal, Commander, NATO ISAF (2009-2010)

Introduction

Canadians spent more than half of their Kandahar deployment fighting for their own lives because too few resources were committed over too large an area. This condition left Canadians perpetually focused on the tactics of mitigating physical threats. This threat-based focus promoted a form of tactical myopia, or *strategic blindness*. By late 2006, the Canadian Task Force became fixated on a tactical fight against an improvised explosive device (IED) threat and became conditioned to perceive short-term raids and company-level searches targeting IED cells as the means to ensure its personnel's survival in Kandahar province. This tactically fixated campaign pattern in Kandahar did not change significantly until the latter-half of 2009, when a reassessment of NATO operations and strategy was conducted by incoming International Security Assistance Force (ISAF) Commander General Stanley McChrystal, and significantly more American resources were deployed to Kandahar province.[2] It was this change in the overall strategic situation that provided the framework within which then-Brigadier-General Jonathan Vance was at last able to salvage Canada's Kandahar mission by consolidating Canadians efforts in a single district and initiating focused counterinsurgency (COIN) operations at the village level.[3]

That a form of *tactical fixation* shaped Canada's Kandahar operations from 2006 to 2009 is perhaps understandable within the context that, in comparison with British and US forces, Canada experienced a disproportionately high *per capita* number of casualties in Afghanistan from May 2006 to May 2009 and upwards of 60% of Canadian casualties were associated with IEDs.[4] In comparison with relatively low-risk peacekeeping and peace enforcement missions such casualty rates were certainly a new phenomenon for Canada and merited a serious response. Lacking sufficient troop densities in Kandahar to execute and sustain ISAF's 'clear, hold, build' strategy over the entire 54,000 square kilometers of Kandahar Province, the counter-IED battle became the de facto *raison d'être* for Canadians in Kandahar until late 2009. Soldiers and their civilian counterparts naturally focused on the one mission objective that persisted regardless of limited manpower resource allocations: the fight to ensure their own survival.

A threat focused counter-IED battle was perhaps exactly the condition that the insurgents wanted to inflict upon Canadian and Coalition contingents because this predominantly tactical emphasis precluded any serious attention to strategy. It distracted focus away from the most critical driving factor behind the insurgency: the growing perception among Afghans that coalition forces were

complicit in sustaining a corrupt and unjust Afghan government.[5] Canada's adversaries were using explosive devices to encourage the use of tactics, techniques, and procedures (TTPs) so fixated on force protection that tactical operations and effects would become disconnected from political and strategic objectives. The Canadian contingent became caught in the untenable position of having to employ all available resources against a single insurgent capability – the IED – while simultaneously neglecting the strategic objectives for which they were ultimately deployed. Attacking the IED networks, defeating the individual devices on the ground, and training the force to survive in an IED environment were critical tasks for ensuring force protection, but did not in themselves generate the population-centric conditions requisite for the pursuit and sustainment of governance and development objectives.[6] But without the manpower density required to both *clear* and *hold* in the interests of providing a secure environment for the population of Kandahar province, the counter-IED battle became the means by which the Canadians could at least demonstrate some form of deliberate activity against a growing insurgency. While this tactical activity had tangible localized effects against insurgents, it could not automatically translate into real strategic effects against the underlying causes of the insurgency.[7]

1. Assessing Canada's Legacy in Kandahar

Canada's whole-of-government campaign did eventually adapt and evolve to achieve a notable level of proficiency in planning and execution by the time the Canadian Kandahar mission concluded in 2011.[8] Positive security, governance, and development gains at the village level were undoubtedly being realized by 2010-11 as a result of an important shift in military focus in 2009 and the subsequent revitalization and reinforcement of the development and governance lines of operations. However, these achievements occurred within the context of an extensively reduced area of operations in comparison to the 54,000 square kilometres for which Canada originally assumed responsibility. The hard-won lessons in terms of how successful whole-of-government activities must be conceived, coordinated, and resourced are indeed invaluable for future endeavours, but these lessons of organization and coordination must be continuously assessed within the wider coalition context. Recognition that Canadian successes at village and district levels were ultimately enabled by US re-engagement and an enormous reduction of security responsibilities in Kandahar province is critical when interpreting Canada's legacy.

Efforts after 2009 enjoyed significantly greater territorial focus and allowed for much more favourable allocations of limited resources. It was this fundamental change that was effectively exploited to produce more tangible effects with the implementation of a Key Villages Approach (KVA) and retooling of Counterinsurgency (COIN) efforts. Remarkably, it appears that this fundamental shift in focus was driven mostly from the Canadian leadership in theatre against a reluctant Ottawa that required positive attention from NATO and ISAF leadership to concede that a mid-course correction was required.[9] This background context has considerable relevance to future policy aspirations and formulation, as it may provide greater understanding of what is realistic and feasible to achieve within

the context of Canada's political will and resource limitations, regardless of how well the whole-of-government effort is organized and coordinated.

The period between late 2006 and late 2009 is perhaps the most illustrative period for understanding the limits of Canada's ability to transform tactical performance into operational and strategic effects. This period represents a critical period during which government aspirations appear to have remained inconsistent with the Canadian contingent's ability to gain control of the tactical balance within Kandahar province. Ottawa seemingly allowed Canadian blood and treasure to be committed and expended without a carefully considered strategy to synchronize available ends and means.[10] This mismatch between policy aspirations, strategy, and resource allocation was exploited through the insurgents' use of IEDs to continually manipulate the tactical balance in Kandahar province. An apparent acceptance of this situation has appeared through the development of a national narrative that has the undermanned Canadians bravely "holding Kandahar for more than three years" while waiting for reinforcements.[11] That a tactically-fixated pattern of "whack-a-mole" [12] against IED cells was carried on for years at considerable cost in lives and resources suggests that revisiting how IEDs impacted decision making is particularly relevant to understanding how well Canada is actually prepared to deal with the realities of contemporary conflict.

2. The Dangers of Tactical Fixation

The insurgents' use of IEDs against Canadians in Kandahar province can best be understood as an attempt to manipulate decision making processes.[13] Western staff colleges train military officers to *seize the initiative* through manoeuvre and surprise in order to get inside their adversary's Observation-Orientation-Decision-Action [OODA] Loop.[14] This is exactly what the insurgents did in Kandahar. John Boyd's theory of conflict underpinning the OODA Loop concept suggested that all actions are reached by going through an imbedded hierarchy of OODA loops: "in order to win, we should operate at a faster tempo or rhythm than our adversaries - or better yet, get inside [the] adversary's OODA time cycle or loop and beat him by making more and faster decisions thereby seizing the initiative."[15] The ability of the insurgent IED campaign in southern Afghanistan to take the initiative away from the Canadians in Kandahar from 2006 to 2009 should be considered an example of insurgents neutralizing technological advantages at the tactical level by successfully getting inside the Canada's hierarchy of OODA Loops. In essence, the insurgents imposed sufficient *friction* for the Canadian's OODA process to run in reverse.[16] By forcing Canadian to react to IEDs, tactical decision making was preconditioned towards force protection, orientation became presupposed by reactive decisions already made, and observations become filtered through the lens of this orientation. Since the tactical OODA Loop is connected to a hierarchy of decision making processes at the operational, strategic, and political levels, the friction imposed by insurgents at the tactical interface transferred through the system and forced these OODA Loops to run in reverse [see Figure 1].

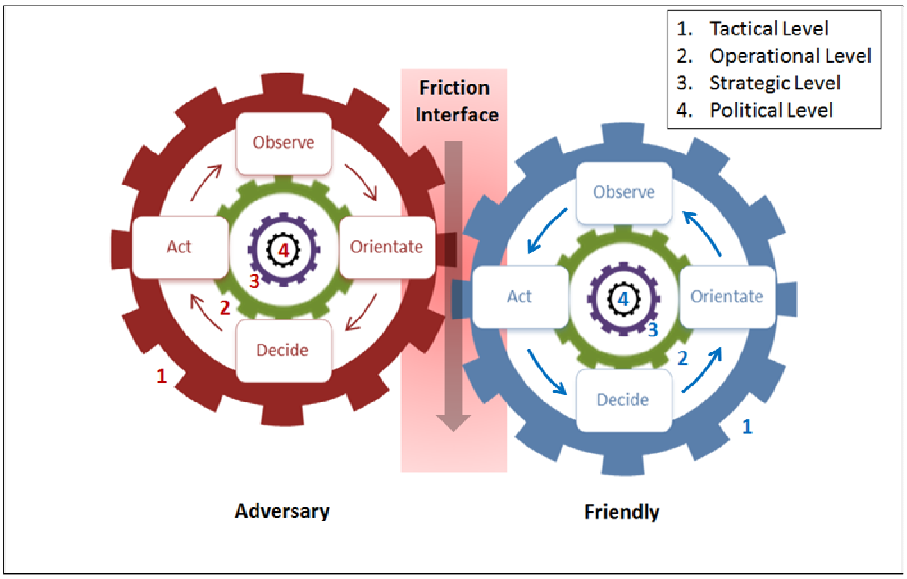

Figure 1. The Friction Interface between Imbedded OODA Loops[17]

What is significant is that the IED is not a tactic or strategy in itself; the IED is merely a tool to increase the amount of friction applied to the adversaries' decision process. Linking Boyd's insights with David Kilcullen's[18] tactical level guidance for counterinsurgency—in which he emphasizes fighting the enemy's strategy and always maintaining the initiative—in order to recover the initiative requires sufficient 'torque' to be applied through an inherent synergy between imbedded OODA cycles. Canada was unable to achieve sufficient torque from 2006 to 2009 because its tactical interface in contact with the insurgent's friction was not sufficiently robust to survive sustained exposure. This subsequently caused OODA loops at the operational, strategic, and political levels to run in reverse. As such, the need to react to IEDs influenced decisions, these decisions influenced force orientation towards counter-IED efforts, and this orientation influenced observations and assessments throughout the chain of command. Counterproductively, then, this further reinforced the original cause of this problem: the propensity to focus on tactical action against a mere source of friction, the IED.

The observation that too few resources were committed over too large an area in Kandahar, which may have caused Canadian decision making processes to run in reverse and fixate on a mere source of friction for some three years, suggests that the Canadian policy and strategy in Kandahar be further scrutinized. The question that remains is whether there was a strong and synergetic core of policy, strategy, and operational level planning acting to drive tactical decision making processes in the proper direction. That Canadians were allowed to remain under-resourced and continue fighting essentially for their own survival for over three years would appear to provide evidence of a significant gap between policy and the tactical interface. The logical conclusion that this situation suggests is that Canadians carried on in a state of tactical fixation for so long because the actual performance at the

tactical interface was not directly linked to policy objectives. This could only have been the case if the strategic value of simply 'being in Kandahar' was perceived as enough to achieve the political objectives behind the Kandahar deployment.

A desire for 'profile' and 'international visibility' has indeed been cited as a prime motive behind Canada's dismissal of the suggestion from NATO to deploy a Provincial Reconstruction Team (PRT) to the remote Chaghcharan region of Afghanistan in early 2005.[19] This choice has been suggested to have been justified by the military on the basis of the Chaghcharan region being too operationally challenging and risky.[20] If this were indeed the case, what possible justification could have existed for assuming responsibility for the even more operationally challenging and risky ISAF command in Kandahar? That the Canadians' tactical OODA cycles were forced by insurgent friction to run in reverse appears to have been of lesser concern in Ottawa because the mere act of taking on such a high profile task was expected to achieve the desired political outcome of increased Canadian influence with the United States and the international community.

Ultimately, insurgents were able to exploit the weak match between Canadian policy-strategy. Whether by deliberate design, persistent luck, or probably some combination of both, insurgents forced a succession of revolving Canadian contingents in Kandahar into a classical dilemma of operational art.[21] For much of its Kandahar deployment, the Canadian contingent was forced to choose between the dispersal of forces enshrined in the population-centric counterinsurgency (COIN) doctrine and the need to concentrate forces in order to achieve short-term tactical kinetic effects in the interests of their own force protection. A preference towards the latter persisted until the strategic context of operations in southern Afghanistan fundamentally changed in 2009 as a result of bolstered US strategic leadership and reinforced US troop commitments.

Causing the small Canadian force to focus the majority of its resources on reducing IED attacks and casualties could help insurgents prevent implementation of effective reconstruction, development, and counterinsurgency efforts. The IED simply became the perfect tactical means by which to attack a vulnerability created by the mismatch between Canadian foreign policy ambitions and its ability to generate and project real strategic power. An apparent ignorance of the considerable distance between ambition and ability made Canada relatively more vulnerable to manipulation through friction and placed the Canadian contribution to ISAF at considerable disadvantage in terms of attempting to seize the initiative in Kandahar province with an available Canadian force density of a meagre 0.05 soldiers per square kilometer.[22] It is in terms of this vulnerability that the fundamental lesson from Canada's foray into southern Afghanistan is perhaps to be found. Canada has considerable work to do in terms of making itself less vulnerable to manipulation by an adversary. Recognition that the IED was effectively utilized against Canadians as a tool to manipulate tactical decision making and disrupt the generation of Canadian strategic power is critical for turning the Kandahar experience from 2006 to 2009 into a constructive lesson for future whole-of-government expeditionary operations.

3. Translating Tactical Contribution into Strategic Effect

The initial policy context for Canada's engagement in Kandahar flowed from the rationale underpinning *Canada's [2005] International Policy Statement: A Role of Pride and Influence in the World*.[23] Prime Minister Paul Martin expressed the Government's desire to enhance Canada's status as a responsible and contributing member of the international community, focus expeditionary capabilities on failed or failing states, assume a greater leadership role when in Canada's interest (and ability to do so), explore new and innovative ways to enhance relations with the United States, and pursue an integrated strategy that draws on Canada's diplomatic, development and defence resources.[24] To achieve these goals of status, leadership, and enhanced relations with the United States, the Canadian 'strategy' in Afghanistan took the form of a pledge to take over a US Provincial Reconstruction Team (PRT) in 2005 and subsequently assume command of ISAF forces in Kandahar Province.

It has been suggested that Canada simply slipped unexpectedly into war in southern Afghanistan.[25] Observers have also suggested that through ignorance of its inherent military limitations in terms of manpower, equipment, and civil-military preparedness, Canada committed its limited resources to an undertaking that was well beyond its actual capabilities.[26] This apparent inconsistency between expectations, aspirations, and objective self-assessment of abilities is not actually new, but the complexities of the Kandahar mission represented a set of conditions that were substantially different from previous peacekeeping and conventional expeditionary activities. An argument can be made that Canada's primary strategic objective in Kandahar was to gain *prestige* on the world stage and the initial thinking in Ottawa was that the mere *presence* of a high profile Canadian deployment in Kandahar was the means to this end. Kandahar provided a considerable shock to a nation unprepared for anything beyond 'contribution warfare', a type of limited liability warfare whereby national strategic objectives are limited exclusively to those that can be met by the mere commitment, deployment, and presence of resources.

Canada's inability to move defence planning beyond a 'strategy of commitments', or the belief that the mere *participation* of Canadian tactical forces is sufficient to meet the national objective of being seen to be a responsible international actor, has long been part of Canadian thinking on defence.[27] In 2000, Douglas Bland observed:

> The essence of Canadian defence policy for the last 50 years has been to contribute to allied efforts – in effect "to lend troops" where needed. Within this framework, the size and capabilities of the contribution are never too important and neither is the credibility of the military force as defined in military terms. These factors hardly matter to politicians or mandarins. Getting there is the strategic objective.[28]

Rather than measuring a tactical force's *performance* in terms of its ability to translate tactical action into national strategic objectives, tactical *presence* in a theatre of operations would appear to have remained the fundamental measure of mission success for Ottawa on the eve of the Kandahar commitment.[29] It is this precedence that arguably created a situation by which Canada's blood and

treasure was committed to Kandahar between 2006 and 2009 without much incentive for detailed examination of the real ends that were to be achieved within the full context of political, cultural, logistical, and geographic constraints.

While an authoritative narrative on the post-9/11 Afghanistan war is likely some years off, the increased stature for Canada that was thought to be inherently tied to the Kandahar deployment may not actually be materializing as envisioned. Assessment of *performance* has eclipsed the calculations of mere *presence* as allies attempt to distil the true lessons of Afghanistan. A theme that Canada's contribution to Kandahar had little operational and strategic impact has begun to appear as a standard narrative in Afghanistan studies published by American and British observers such as Sandy Gall, Sherard Cowper-Coles, and Rajiv Chandrasekaran.[30] While it must be acknowledged that attempts to shift responsibility for disappointments in Afghanistan may be part of any coalition landscape, it would appear that there is some basis to claims that Canada's involvement was strategically ineffectual.

A key lesson from the Kandahar experience seems to be that the Canadian government's reliance on a 'strategy of commitment' left the Canadian contingent *tactically fixated* and at the mercy of an adversary that learned to effectively translate tactics into strategic effect using a loosely sequenced campaign of friction. The employment of the IED as the insurgents' weapon of choice went beyond its tactical kinetic effects. The IED allowed insurgents to manipulate the Canadians by saturating their sensors and overwhelming their limited resources with fleeting tactical objectives.

A 2009 report by the Washington-based Institute on the Study of War suggested, looking back on the first three years of Canada's deployment in Kandahar, that the "[t]he IED campaign in Zhari and Panjwai [districts of Kandahar Province, Afghanistan] had the net effect of taking the initiative away from the Canadians, whose military resources were increasingly focused on force protection and targeting of IED cells, rather than on separating the Taliban from the local population through counterinsurgency operations."[31] The implication that the Canadian approach to countering the IED threat allowed insurgent groups to further a perceived operational objective of exerting control over Kandahar city has been stated by Carl Forsberg as follows:

> In the face of this growing enemy threat, the small Canadian force transitioned in 2008 from holding terrain and protecting the population in Taliban-controlled areas, to operations designed to disrupt the Taliban by targeting IED cells and their logistics through raids. But operations targeting IED cells did little to counter the Taliban's control over the population, and as long as Taliban control persisted, ISAF operations had only marginal effects on the capabilities of the Taliban fighters.[32]

Colonel Bernd Horn aptly sums up the dilemma that the insurgents ultimately created for the Canadian contingent in the following passage:

> The nature of the conflict fuels a spiral of antagonism. In essence, it is a vicious circle. As coalition forces continue to be targeted by IEDs and suicide bombers, they have no choice but to take the necessary actions to protect themselves. This, however, comes with a cost. As convoys drive aggressively down the centre of the road, they force local Afghan traffic to scurry for the shoulder. As they physically bump traffic out of the way, or threaten vehicles who follow too close by pointing weapons, or create collateral damage due to attacks against them and/or defensive or offensive operations – they risk alienating Afghan nationals. With every action taken against the population at large, regardless of justification or cause, a cost is incurred. Coalition actions could potentially push Afghans to support the Taliban, or at least cause them to turn a blind eye to Taliban activities. Yet, to do nothing and continue to be hit without taking some action – feeds soldier disillusionment and the potential to lose Canadian public support for the conflict, if it appears that the country's troops are put at risk without the ability to take the necessary steps to defend themselves. Moreover, if a safe and secure environment is not created for the local population, there is almost no hope of creating support for the new Afghan national government.[33]

4. Insurgent Strategy?

Canadian limitations in terms of manpower, equipment, and civil-military preparedness ultimately made ambitious and ever expanding tactical objectives of the Kandahar mission all but impossible to achieve without a coherent strategy to connect ends and means. Whether the actual strategic situation in Kandahar and the operational and strategic objectives towards which Canadians would be directed were seriously assessed is a subject for continued debate.[34] Military commanders appear to have essentially been dictated a force structure justified on concerns of political palatability and comfortable sustainability rather than the detailed assessment that a coherent strategy would require. Even with the help of allied contingents under their command, Canadians lacked sufficient troop densities from 2006 to 2009 to adequately sequence all phases of the 'clear, hold, build' counterinsurgency (COIN) doctrine throughout Kandahar province.[35] The insurgents quickly developed capabilities and plans to attack and manipulate this vulnerability.

Although it is difficult to superimpose western concepts of strategy onto a complex insurgency composed of a variety of actors, issues, and causes, Afghan insurgents appear to have used the IED in a manner consistent with Boyd's assessment of the overall goal of strategy: to "[c]ollapse [the] adversary's system into *confusion* and *disorder* by causing him to over or under react to activity that appears simultaneously *menacing* as well as *ambiguous*, *chaotic*, or *misleading.*"[36] The IED tactics used by insurgents also have remarkable consistency, with Boyd's vision of effective tactics being an ability:

> To observe-orient-decide-act more inconspicuously, more quickly, and with more irregularity as basis to keep and gain initiative as well as shape and shift main effort; to repeatedly and unexpectedly penetrate vulnerabilities and weaknesses exposed by that effort or other effort(s) that tie-up, divert, or drain-away adversary attention (and strength) elsewhere.[37]

The IED simply became the perfect tactical means by which to attack, since causing the small Canadian-led force to focus the majority of its resources on reducing IED attacks and casualties would prevent implementation of effective counterinsurgency efforts throughout Kandahar.

Boyd's framework provides the impetus to conceptualize adversarial strategy beyond solely 'device-centric' or 'enemy-centric' approaches, which arguably lead to *tactical fixation* and loss of initiative. Within southern Afghanistan, it is clear that the insurgent IED campaign against Canadians was not a means and ends to itself. The Quetta Shura Taliban (QST), whose campaign plans are allegedly formulated by the *rahbari shura* (leadership council) and the *majlis al-shura* (consultative council), have pursued a strategic aim of neutralizing the Kabul government's legitimacy and ability to govern in southern Afghanistan. Since 2004, all operations attempting to isolate, infiltrate, and eventually capture a legitimate seat of power in Kandahar City have essentially been part of this greater strategic framework.[38] Insurgent IED campaigns have simply been a means to pursue this strategic aim. Canadian efforts to defeat devices and attack IED networks from 2006 to 2009 ultimately did little to defeat this strategy as they distracted critical resources away from applying their energies towards increasing the government's legitimacy and ability to govern.

Allowing the IED threat to become the main focus for intelligence and military operations allowed the QST to increase tactical fixation on a mere weapons system and then subsequently outmanoeuvre the Canadian Forces in Kandahar Province at the operational and strategic levels. The Institute for the Study of War observed:

> Because of the Taliban's success in tying down the Canadians in Zhari and Panjwai, they were able to pursue two key goals in Kandahar. The Taliban were able to develop institutions of governance in Taliban-held areas of Kandahar, especially in Zhari and Panjwai, as a means of winning legitimacy for the Taliban movement. The Taliban were also able to wage a successful offensive to move into Kandahar City from the north through the Arghandab District circumventing the ISAF deployment in Zhari and Panjwai.[39]

The initiative in relation to governance was allowed to remain with the insurgents. The QST ultimately achieved a level of operational and strategic success over Canada by preventing the Canadian contingent from implementing an adequate counter-strategy in Kandahar for almost three years.

In essence, the mission objectives quickly became secondary to force protection. Although similar consequences occurred for other coalition force members, unique Canadian vulnerabilities (beyond obvious limitations in force numbers) made this dilemma more pronounced for the Canadian Forces, and therefore much more exploitable and apt for manipulation by the QST leadership. The overarching Canadian vulnerability is the overreliance on strategies of mere 'commitment' and the subsequent lack of civil-military experience in strategy formulation that this outlook nurtures. A second major Canadian vulnerability further contributes to Canada's stale strategic culture: a lack of intelligence collection

capability beyond the tactical level. As good situational awareness is key to coherent strategy formation, it is perhaps here that the path towards a stronger strategic culture in Canada commences.

5. Intelligence Saturation

In a study of Canadian Forces military intelligence organization and capabilities, David Charters suggests that the significant transformation and "adaptation-while-fighting" occurred during the various phases of engagement in Afghanistan and this enabled the Canadian Task Force to plan and execute successful intelligence-led-operations (ILO);[40] however, it remains unclear whether these ILOs resulted in tangible strategic effects. Charters has observed that some anecdotal information exists to support a critique that the trumpeted Canadian All Source Intelligence Centre (ASIC) did not "serve the campaign overall, but [was] focused more narrowly on specific aspects of the tactical battle for control."[41] If the primary intelligence apparatus did indeed become tactically fixated, the trend towards tactical fixation of the entire contingent would have been extremely difficult to overcome.

David Kilcullen's thoughts on the nature of victory in counterinsurgency provide the basis from which a mindset beyond tactical fixation must be established:

> [C]ombat victory depends on the enemy being stupid enough to present you with a clear-cut target, which is a rare windfall in counterinsurgency. Instead, you may achieve a victory by resolving long-standing issues your predecessors have failed to address, or by co-opting a key local leader who has resisted cooperation with our forces.[42]

What is impeding this is what Norman Dixon would describe as "an almost total lack of information about the enemy,"[43] which subsequently causes an inability to perceive that the enemy may in fact have a strategy and campaign plans aimed at manipulating tactical behaviour. Former British Ambassador Sherard Cowper-Coles certainly suggests that Canadians who briefed him and US Secretary of State Condoleezza Rice in Kandahar appeared to live in a particular world of "cautious optimism" that was arguably detached from the operational and strategic realities of southern Afghanistan.[44] This was perhaps not a uniquely Canadian problem as indicated by a January 2010 report by ISAF Deputy Chief of Staff, Intelligence (CJ2), US Major General Michael T. Flynn, and Paul Batchelor of the US Defense Intelligence Agency, which concluded that the intelligence community had been baited into reacting to insurgents tactics such as IEDs and this preoccupation had caused a failure to identify "ways to strike at the heart of the insurgency."[45]

As highlighted in considerable detail in COIN doctrine, human intelligence (HUMINT) capabilities are considered critical in understanding and identifying ways to strike at the heart of an insurgency.[46] Although Canadian human intelligence (HUMINT) collection and the Canadian military's approach to intelligence fusion through the ASIC concept have been praised for their tactical impact,[47] some evidence leads us to conclude that Canada's HUMINT collection resources appear to be remarkably thin.[48] This undoubtedly leaves Canada vulnerable to 'sensor saturation', whereby field collectors

become overwhelmed by the persistent information demands from tactical, operational, and strategic levels consumers. This problem becomes even more critical once force protection is allowed to become the dominant objective and directing scarce assets to collect anything other than threat intelligence is extremely difficult to justify when personnel are perpetually in harm's way. This is a significant hurdle to overcome for the astonishingly small cadres of HUMINT operators that Canada deploys.

With HUMINT, the number of collectors available is directly linked to the range, quantity, and quality of sources that can be effectively developed and managed. As limited collection assets are forced to react to tactical enemy-centric issues such as IEDs, almost no surplus HUMINT collection capability is available to direct towards non-tactical issues such as governance and development in support of efforts by agencies such as DFAIT and CIDA who lack sophisticated HUMINT collection assets of their own. Successful HUMINT is ultimately about asking the right questions to people who have access to the information being sought. If sources of corruption and other detrimental actors are to be recognized, understood, and countered, collectors must be available to identify, recruit, and systematically extract information of intelligence value in areas other than the tactical realm. If all HUMINT collection is tactically fixated, the commander's (and Ottawa's) overall situational awareness is necessarily limited.

A March 2010 study by the Kabul-based Stability Operations Information Centre suggested two risks associated with the flood of development aid into Kandahar after 2009: that the flood of additional aid dollars would fuel corruption and therefore undermine, rather than create, stability; and, that the central government's involvement in dictating staffing for district level development programs could have detrimental impacts at the local level.[49] These kinds of problems are actually more vital strategically if ISAF is to actually achieve its mission of leaving behind a functioning and sustainable government. Although Canadian COIN doctrine clearly reinforces the importance of intelligence – and particularly HUMINT – in relation to these types of problems,[50] it is not clear that this aspect of COIN has fully penetrated the cultures of DND, DFAIT, or CIDA to the degree that may be necessary to break away from mere tactical fixation. IEDs and other sources of friction and uncertainty are destined to exist in any future theatre of expeditionary operations and these challenges will undoubtedly require a sufficient level of resourcing in order to be addressed and overcome. There must also be sufficient surplus capability, both in terms of boots-on-the-ground and field intelligence, to go beyond simply dealing with this friction.

6. Conclusion

As has been noted by Richard Livingstone in his introduction to the writings of Thucydides: "Athens was ruined by bad leadership. It was her politicians who lost the war."[51] In a similar fashion, Canadian politicians and policymakers and their lack of strategic skill are perhaps the ultimate cause of the Canadian military's tactical fixation on IEDs and subsequent failure to maintain the initiative in Kandahar from late 2006 to 2009. For the Canadian military, a lack of higher vision and strategic

culture at the political level has translated into an emphasis on process versus intent, what Norman Dixon has described as a predilection to emphasize events rather than ideas, thereby becoming "wrapped in cocoons of catastrophic ignorance."[52]

While it is acknowledged that the impact of IEDs on the Canadian Forces eventually declined due to the 2009 surge of US forces that allowed Brigadier-General Jonathan Vance to consolidate the small Canadian force and initiate focused COIN operations in Dand district,[53] it is unlikely that the threat of IEDs is going to disappear on future expeditionary operations. In order to prepare for the next IED campaign waged against Canadians, it must be recognized that exploitable vulnerabilities exist in how Canada perceives its expeditionary commitments. These vulnerabilities will be exploited by adversaries who can easily recognize them. The IED itself was not the enemy of Canadian troops in Kandahar; it was merely part of an insurgent strategy that was perceptive enough to attack Canada's lack of ability to deal with and overcome friction.

The reality that Canada's international deployments have historically been perceived as based on strategies of commitment rather than detailed assessments of how to most effectively employ national means for chosen ends has led to a stagnant strategic culture. This stagnant strategic culture must be recognized as being a liability in that it ultimately leads to weak policy-strategy matches and incompatible resource allocations. Once Afghan insurgents were able to perceive and adjust to the Canadian military's tactical strengths demonstrated in 2006, the IED was used to manipulate this obvious gap between political aspirations and capabilities. Canada must seek to make itself less vulnerable to this type of manipulation by an adversary. Recognition that the IED was effectively utilized against Canadians as a tool to manipulate the tactical balance and disrupt the generation of Canadian strategic power is critical for turning the Kandahar experience into a constructive lesson for future expeditionary operations.

Canada must not only be able to recognize when it is being manipulated, but must also make significantly better efforts to understand the full dynamics of engagements and how its own capability limitations need to be mitigated. Friction will always be present in some form and strategies will always need to be found to ensure an adversary's instruments of friction are not allowed to adversely manipulate behaviour. Securing a breach through a minefield is akin to merely occupying a kill zone unless sufficient capability is brought to bear to move through the breach and attack the true objective. If capacity to move beyond the obstacle does not exist, it might be advisable to avoid engagement in the kill zone and develop another strategy. Fortunately, the challenge of strengthening Canada's strategic culture lies with Canada itself.

Recommendation 1 –

Canada's whole-of-government efforts did eventually adapt and evolve to achieve positive security, governance, and development gains at the village level by the time the Kandahar mission concluded in 2011. These gains should not be viewed in isolation from fundamental changes in the strategic situation that occurred in Kandahar province after 2009. Canadian achievements occurred within the

context of an extensively reduced area of responsibility from that Canada originally assumed charge of. In order for the lessons of Kandahar to be truly transferrable to future expeditionary operations, care must be taken not to over embellish Canada's actual impact in Kandahar province by confusing activity with lasting achievement.

Recommendation 2 –

Canadians must be realistic about what can be achieved within the limits of their ability to generate military, diplomatic, and development resources. Scenarios where 'a presence in the line' or 'a presence in the area' will by itself achieve tangible influence among allies are likely to become the exception rather than the rule. Being there while being tactically fixated may in fact have counterproductive consequences in terms of influence. As influence becomes tied more closely to actual performance greater attention will need to be paid to the synergy between policy and strategy. Policy aspirations must remain consistent with the Canada's actual ability to deal with friction and translate tactical action into operational and strategic effects. Canada's blood and treasure should only be committed when underwritten by a carefully considered strategy to synchronize available ends and means.

Recommendation 3 –

Strengthening Canada's ability to translate tactical action into operational and strategic effects means becoming as well informed about potential adversaries and operating environments as possible. This requires good intelligence at levels beyond the tactical. Human intelligence (HUMINT) collection capabilities are likely to become increasingly vital for navigating the future security environment and require continued investment. The tactical field HUMINT capabilities that the Canadian Forces honed in Afghanistan must not be allowed to atrophy as a result of current budgetary constraints. Consideration should be given to expanding these capabilities to provide insights beyond the tactical level. An ingrained culture that recognizes the force multiplication advantages and inherent limitations of HUMINT must also be developed within the entire whole-of-government team if limited intelligence resources are to be employed to greatest effect.

Hell on Heels: The Intersection of Women, Terror and Insurgency

> *Then she pulls a veil over her face and adjusts the belt around her waist before stepping out. One of the men in the car whispers, "God is great!" She doesn't respond or look back. As the car drives away, the video, shot through the rear window, shows her approaching the checkpoint. She is quickly obscured from view by the dust trail behind the car. Nearly a minute later there's a flash, a muffled boom and a column of black smoke. "God is great!" says the cameraman. "The stupid woman did it."*[1]
>
> *Bobby Gosh*

Introduction

The narrative of terror attacks as being among the most prevalent threats to freedom and democracy has dominated media, policy and academic discussion, garnering significant attention to "terrorism" writ large. The project to explain "terror" as both a strategy and a tactic has resulted in numerous definitions, rendering a concrete understanding of its use and prevalence largely elusive. One of the most commonly cited definitions is that of the United Nations Security Council's Resolution 1566, which condemned terrorism as

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.

Perhaps then the more useful project is conceptualizing one aspect of terrorism, and exploring the elements of that component that lend both meaning and utility to the efforts to combat terrorism at a broader level. The purpose of this paper will be the exploration of one such component: female suicide bombers.

Focusing on female suicide bombers as a single analytical element of the range of activities largely classified as "terrorist" in nature is useful for two key reasons. First, at present, analysis of female suicide bombers specifically is significantly lacking. While academics and researchers in the field of terrorism studies have increasingly measured suicide terrorism's prevalence and assessed its effectiveness, a quick survey of the literature and public policy discussions on suicide terror indicates that the female suicide bomber phenomenon is relegated to the sidelines, representing a crucial imbalance in the burgeoning field. The reach—both in terms of the spectrum of motivations and geographical spread of female suicide bombers—is especially concerning as it makes all the more necessary the development of an underlying commonality. The definition of this commonality is the

second important contribution of this paper, as it links the specific use of women as suicide bombers uniquely and specifically to insurgency. Understanding this link frames the way in which policy related to counterinsurgency efforts is developed. Developing a body of literature related to female suicide terrorism that assesses the relationship between women and insurgent movements informs the strategies that organizations can rely on to counteract this trend.

Exploring first the specific phenomenon of female suicide terror, including the history and context in which it becomes more common (in addition to the limitations of its use), this paper will proceed to define the power of such a terror tactic. Finally, it concludes with a discussion about the kinds of "ground-level" counterinsurgency strategies that must be employed if this frightening development in suicide terror is to be effectively contained. Furthermore, this paper will demonstrate in part that some of the ineffectiveness to date regarding countering female participation in insurgency-linked suicide terror is due to a misunderstanding of two key factors: the personal set of motivations that drive participation in suicide terror by women in insurgent-laden societies, and the organizational imperative that drives male-dominated insurgent groups to recruit women.

1. "Insurgent" versus "Terrorist"

An insurgency is "an organized, protracted, politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control."[2] Understood according to this definition the use of female suicidists is, at least contemporaneously, a tactic employed by insurgent groups specifically as part of a broader campaign to advance specific political ends. Global terror organizations, such as Al Qaeda and its affiliated branches, are global manifestations of long-established regional terror-based insurgent groups. Chechnya, Palestine and Sri Lanka are of particular relevance, but as the term 'global' implies, certainly not contained exclusively to these regions.

Everyday post-9/11 usage has largely rendered the term "insurgent" synonymous with "terrorist." The nature of their lawless tactics draws criticism from the range of state and non-state actors due to the dangers these tactics pose to civilians. It is important to note, however, that insurgency does not necessarily rely on terror tactics; rather, insurgent groups are likely to identify with a sense of being "occupied" and employ a range of political, social and economic strategies to overcome the obstacles in their way. Only the most radical of insurgent groups may make use of terror tactics at all, and among these, even fewer rely on female suicide bombers. Nonetheless, in the introduction of this paper, it is important to distinguish between the two terms: not all terrorists are insurgents, nor are all insurgents terrorists.

What then explains the employment of female suicide bombers by a select few insurgent groups? How are these women used, and why? What are the limits on the use of female suicidists? The exploration of these questions in particular will lead to a clearer understanding of the foundations of both terrorism and insurgency from a conceptual, motivational and organizational standpoint.

2. Foundational Understandings

When the dynamics of global security shifted on September 11, 2001, international terrorism came to the fore as, arguably, the largest threat to security in the West. The "war on terror," enacted in Afghanistan and Iraq, has facilitated the fear and fascination that terror activities hold in contemporary society. The particular use of suicide bombings gained widespread media attention and the turbaned man with a hefty beard crying "Allahu akbar" has become the imagined face of the global threat to security, peace, freedom and democracy.

The existence of terror tactics and individual terrorists dates back thousands of years, from Nizari-Ismaili Assassins to the Hindu Thugs, and from the Jewish Sicarii to the Japanese Kamakazi.[3] However, it is the more recent uses of terror within explicitly insurgent organizations that are the focus of this paper. For our purposes, this paper will narrow its scope of interest to "modern" terrorism, defined primarily by the period that follows the 1983 truck bombings in Beirut, Lebanon.

Also referred to as the Beirut Barracks Bombings, the events of October 23, 1983 resulted in the deaths of 299 American and French servicemen of the Multinational Force in Lebanon housed at two separate locations, each struck by truck bombs detonated by suicidists. It was following this attack that suicide bombing in particular became a specific tactic employed by various political organizations. The truck bombings represented a new age in suicide attacks, which saw the specific use of explosive devices, carried by an individual disguised as a civilian or transported in a civilian vehicle to a specific site. As this technique gained in notoriety in the 1980s, it spread to other regional insurgent organizations. In the three decades since, insurgent groups employing terror tactics have appeared throughout the Middle East and across the world, including the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka, Hezbollah in Lebanon, Hamas in Israel-Palestine and nationalist groups in Chechnya. These and other insurgent movements date their founding to the period from the early 1980s onward, hence representing the era of modern terror tactics in an insurgent context.

The motivations of most insurgent organizations have been classified as either religious or secular.[4] However, the modern era of insurgency has rendered this dichotomy an oversimplification as insurgent movements harmonize the two motivations for an even stronger presence in their respective regions. The result is that traditionally secular insurgent movements, such as those in support of nationalist goals or aims advancing autonomous territorial status, now also increasingly invoke religious texts and clerical authorities, while maintaining a secular commitment to distinct political ends. In this way, the religious aspect of each group's agenda is an important consideration in the understanding of what is, essentially, a political (and formerly secular) message. While it is tempting to regard religion as the primary motivation for involvement in these activities, and indeed as the primary tool of recruitment, to do so would ignore the much larger and much more complex socio-political context that drives young men and women to join the ranks of terror groups.

3. Suicide Bombings, Women and Insurgency

Insurgent groups employing terror tactics have only recently begun the use of suicide attacks, predominantly recruiting men to undertake suicide missions. In the 1980s, there were fewer than five suicide attacks worldwide per year. But in 2001, 81 suicide attacks were recorded. This jumped to a record 460 in 2005.[5] While constructed primarily as an Islamist insurgency terror tactic, suicide bombing has also been used by the LTTE in Sri Lanka. It is also notably common in insurgent groups in Chechnya, against Russian forces and particularly as a response to the Second Chechen War. The "occupied" peoples of Palestine, Afghanistan and Iraq have all made particular use of suicide bombing as a tactic as well.

In order to obtain a comprehensive picture of the role of women in insurgent organizations, particularly with regard to their participation in suicide attacks, we must consider two key questions. First, *what motivates women to engage in suicide terror activities*? Second, *why are terror organizations allowing this expansion in their ranks, particularly in societies where the role of women has been confined to the "private," apolitical sphere?*

The role of women as weapons in insurgent organizations, while increasing, largely has been marginalized and minimized by most studies of terrorism and insurgency. Several scholars have attempted to explain the lack of academic and real-world attention given to this growing phenomenon. Their explanations are varied: (1) suicide terror is a recent trend overall and academia simply has not caught up; (2) the thought of involving women in such tactics goes against the very traditional view of female combat roles in the vast majority of Western societies; and (3) there is little data concerning the motivations and specific involvement of women in insurgent and terror activities.

Notwithstanding these and other ambiguities, it is no longer possible to ignore the increasing participation of women in suicide terror activities. Not only is female participation in political violence a relevant commentary on the cultural, religious, political and socio-economic context of the region in which it occurs, but it is also a study that is imperative to the understanding of a broader dynamic within terror-based insurgent organizations: what drives the motivations behind recruitment strategies of these organizations?

Because military and paramilitary conflict has traditionally been conceived of as a male-dominated sphere, the rise of female involvement in terror activities is largely a phenomenon of modern insurgent organizations. Starting in the 1980s, in Southern Lebanon female suicide bombers emerged on the scene, employed predominantly by the Syrian Social Nationalist Party (SSNP).[6] In the mid- to late-1990s, two-thirds of the attacks undertaken by the Kurdistan Workers' Party (PKK) were by women. Finally, in the early 2000s, a small collection of Muslim clerical leaders began to issue edicts approving female suicide attack missions. As a result, between 2000 and 2004, 96 Palestinian women were involved in overt political violence, including eight suicide attackers between the years 2002 and 2004.[7] Female suicide bombers represent nearly 15 per cent of the overall number of actual suicide bombers around the world, including those intercepted before the attack.[8] Two key sets of motivations can be

identified: "their primary motivations are often nationalistic and their personal motivations are trauma and revenge driven."[9]

In most cases, as in Palestine, Chechnya and Sri Lanka, years of living under occupation or in the presence of war and conflict creates a socio-political context that, married with cultural, religious or political sentiment, drives female motivation. Women are more likely to be the victims of particular forms of violence accompanying political tension, such as rape (by soldiers or insurgents) or the loss of family members. These emotionally painful issues can exacerbate hatred already felt toward the enemy for political reasons. Particularly in cases where a family's "honour" has been socially damaged (by rape) or where culture demands revenge (as in the case of a death in the family), emotional vulnerability and psychological trauma can easily be exploited by local insurgent organizations. Without question, this is a brief simplification of the motivational context for female participation as suicide bombers in insurgent organizations. The literature on female involvement in suicide terror expands on these motivations in significant detail for which there is little room in the context of this paper to explore.

However, this represents only one side of the equation. Reasons to join may be personal, but why are they being recruited?

This brings us to the question of analytical imperative to this paper: *why would insurgent organizations accept women in their ranks and employ female suicide bombers at all?* As stated above, warfare is a typically male-oriented, male-dominated activity. As such, *what is the value of including females in terror enterprises?* And *how can particularly "gender traditional" constituencies explain this inclusion?*

The participation of women in insurgent and terror operations is increasingly associated with a particular set of strategic advantages.[10] The vast majority of these advantages is attributed to the widespread media and societal attention that women-as-weapons attract. When a woman commits herself to a suicide bombing mission and succeeds, the audience begins to consider her motivation - more so than ever happens with a male bomber. Because terrorism is a powerful psychological weapon,

> the use of female bombers clearly has the effect of increasing the weapon's utility in creating a more horrific impact on the receiving audience and causing the horrified witnessing audience to probe more deeply for her motivation - something that garners far more attention to and often more sympathy for the terrorists' cause.[11]

Therein lies the key utility of a female suicide bomber: sympathy. The most effective weapon of any insurgent group (and the most useful particularly for those engaged in terror activities) is to cut through fear and win sympathy. Because female suicide bombers are more commonly viewed as women expressing their pain at loss or violation, women are more effective weapons in the public relations battle.

While men and women engaging in suicide terror operations do not differ greatly in their motivational sets (i.e. political statements, personal sense of empowerment and accomplishment), their utility from an organization's operational standpoint is drastically different. In a study conducted by Barbara Friedman of American media coverage following female suicide attacks, she found five key motivation explanations that news outlets offered: (1) strategic desirability, (2) the influence of men, (3) revenge, (4) desperation, and (5) liberation.[12]

In the stories that journalists told of these women, it was alleged that they had not volunteered themselves as deadly weapons, playing down the first of these motivations – the strategic desirability. Instead, the media reconstructed these women as less than women or less than psychologically sound: the failure to become a mother or wife, or the loss of a husband or father cultivated desperation in these women, which led them to their tragic final acts.

Whether this is an appropriate description of these women's motivations (which, arguably, it is not - given the many instances of determined, politically-motivated young women engaging with terror-based organizations), nonetheless, an insurgency that succeeds in portraying its female suicide bombers as such has claimed a great victory. The audience is working to uncover the reasons behind this female suicide-bomber's final moments. She is neither imagined as a monster nor a passive stander-by: she is a woman who has been rendered emotionally distraught by the circumstances she has lived in for years, driven to the breaking point and desperate to make a final statement about her pain.

Palestinian Wafa Idris was the first woman declared a suicide bomber by the Israelis in February 2002, following her suicide attack in January of that year. She has come to represent the archetypical Palestinian female bomber, and her name lives on in a way that most male suicide bombers' reputations have not. In the wake of her attack, media attention was widespread, instilling not only fear but also powerful sentiments of sympathy. Her effectiveness cannot be understated because, as one observer noted following the bombing, "it's the women we remember."[13] The abnormality and shock of a female bomber is of irrevocable value to insurgent organizations. So long as the reasons behind her attack have an opportunity to be "explained" to the public, the insurgency may craft a compelling message as the audience seeks to find understanding. Meanwhile, there is comparatively significantly less attempt made by the general Western public to understand male suicide bombers.

While terrorism and suicide attacks are not unprecedented in insurgency studies, the changing dynamic of insurgent organizations and the tactics used have left the academic and policy worlds largely struggling to keep pace. In a world inundated with technology and the digitization of media, insurgencies have found a new medium with which to convey their message and increase recruitment. Suicide bombing has fast become the attack method of choice for a number of reasons. Stated simply, it is the most effective technique for garnering media attention and triggering fear within entire populations. Due to the unpredictable and flexible nature of these attacks, including the method's disregard for human life, suicide-terror indicates fanatic commitment to a cause. This is particularly

disturbing to many people across societies because such psychological power forces us to ask the question: what weapon can effectively combat a determined mind?

4. Counter-Female-Insurgent-Bomber-Strategies

Having explored suicide terror tactics within the context of insurgency, we can now proceed to a discussion about strategies to counter the terror tactics of insurgent groups. While at the broadest level the range of tactics, strategies and methods employed to defeat insurgencies can be termed as 'counterinsurgency,' the focus of this paper will be primarily those counterinsurgency measures that will be particularly useful in countering the rise of female involvement in suicide terror.

It is important to understand female participation in suicide terror as a small element of the broader insurgent strategy. Women acting as weapons is a relatively new phenomenon (as stated above, dating to around 2000 in the modern era of terrorism), and from the organizational perspective this filled a number of needs. A drop in male recruitment, a lack of media-related effectiveness, or a desire to achieve tactical surprise may all be contributing factors. The key point here is that women suicidists will only be used as a technique by male-dominated insurgent groups as long as the technique proves practical and effective. The reality is that, to date, female terror has not occurred outside the realm of traditional, male-oriented insurgent organizations: "it is part of a male engineered, male dominated activity and... [there is] remote likelihood of it changing."[14]

Drawing on the work of David Kilcullen in the field of counterinsurgency, the primary task of any counterinsurgent effort aimed at radically reducing and preemptively countering the recruitment of women into terrorist organizations, will be to minimize the alienation of the population as a whole, and in this case women in particular.

Female involvement in suicide terror is more common in regions that have seen prolonged conflict and where insurgent organizations have been a part of everyday life for decades. Insurgents often argue that they are responding to years of failed governments and, frequently, foreign occupation or direct political involvement. Such a contentious political climate is conducive to the recruitment of new members, and women, as they are subjected to the "liberating" policies of outside (predominantly Western) forces – in response, they may envision combative roles for themselves. Understanding such a context, it is absolutely imperative that counterinsurgent strategies work with local populations, especially (perhaps even primarily) women. In particular, the role of women in most societies is so foundational that "winning" the support of the women in the community who are tired of watching their husbands, brothers and sons die in vain attempts at political change will be crucial.

Most psychological literature suggests that women are "more idealistic" than men; they are prepared to support and sustain an ideal longer than men are, and are much less affected by cynicism.[15] While this can work in favour of insurgencies as they recruit women, it can also be a useful strategy employed by counterinsurgent efforts. In presenting an alternative ideal, or in constructing an image of what a

real future could actually be if women engaged in less violent tactics aimed at political change, the capacity for terror-based organizations to recruit women (and perhaps even men) would be seriously undermined.

Furthermore, top-down, hierarchical approaches to counterinsurgency often fail to eliminate the base support for insurgent groups, and can even motivate locals—who view the state as an imposition—to support insurgencies. State soldiers are often unknown faces; insurgents are family and friends. If counterinsurgency efforts stand a chance at being successful, they must employ "bottom-up, civil-society-based programs that focus on peace-building, reconciliation, and the connection of legitimate local non-state governance structures to wider state institutions."[16]

5. Conclusion

The rise of the female suicide bomber heralds a new age of modern terrorism. It is the result of a convergence between personal motivations indicative of the female experience in war-torn, conflict-ridden societies and the strategic needs of terror-based insurgent groups throughout the world. This convergence has created a dangerous environment in which insurgencies now have access to a second cohort of vulnerable individuals.

In exploring both the history of terrorism and the growing phenomenon of female suicide terror in particular, this paper offers insight into the motivations that brought about this terror phenomenon as well as the tactical and strategic advantages that organizations themselves seek in the use of women. While many groups, including Al Qaeda, have not made overt use of women in their tactics to date, it is clear that the growing use of female suicide bombers by other insurgent organizations attracting global attention will facilitate the same phenomenon within groups on a more global scale. And recruitment will not be limited to these war-torn areas. Young women in the West who are "liberated" and therefore already invoke a political presence are also susceptible to the propaganda of terror-based organizations that employ increasingly complex web-based media and outreach strategies.

Not only must societies, as well as both state and non-state organizations continue to condemn political violence, but counterinsurgents must recognize that neglect of this trend has fed outdated policies which no longer respond to the on-the-ground realities that facilitate female recruitment and participation. In order to be effective, counterinsurgency strategies must work beside communities and women in order to feed hope and non-violence from the bottom up. In providing women with nonviolent alternatives at the communal level, not only can the phenomenon of female terrorism be countered, but the entire range of violent tactics employed by insurgencies may be undermined.

Recommendation 1 –

The Department of National Defence, the Department of Foreign Affairs, Trade and Development, and other government departments operating overseas should engage local women in community reconstruction efforts, encouraging them to take the lead developing local initiatives which focus on political "future-building." The evolution of formal and informal grassroots models of community

governance that create a non-violent political space in which women can define and act on their ideas for community development may contribute an important counterbalance to the power of the ideals espoused by insurgent organizations.

Recommendation 2 –

The Government of Canada should establish a whole-of-government intelligence database and an international intelligence network that focuses specifically on female participation in insurgent activities, particularly those insurgent groups making use of terror tactics. The nature of female involvement, from fundraisers to combatants, and right up to suicide bombers needs to be tracked. Undertaking this research and tracking will crystallize the process by which women's motivations to participate evolve, as well as the organizational "imperative" for female suicidists.

Counterinsurgency tactics are largely aimed at male-dominated organizations, but if counterinsurgency operations are to be effective at discouraging female participation in terrorism and political violence more broadly, they must create culturally-specific, on-the-ground tactics which remove and channel into other arenas as many of their motivations as possible. Counterinsurgency strategies must integrate non-violent, local institutions to replace the insurgent model. It must also be about constructing counterinsurgent ideals: women seek out a strong sense of community, and in creating not only legitimate institutions but viable ideals, women can be recruited to work within non-violent parameters for political change and stability.

Recommendation 3 –

Counterinsurgency strategies must be updated to recognize important differences rather than, as they have been, grossly dichotomized, such as religious versus secular and victim versus perpetrator. Such oversimplifications have made their way into counterinsurgency efforts, largely through Western media. Western media sources have created narratives not connected to the information on the ground, and are at least partially responsible for these false dichotomies. Counterinsurgency strategies must replace them with more astute clarifications of the regionalized, socio-historically specific, culturally framed "imperatives" propagated by local insurgent organizations that have come to drive female participation. While this will make counterinsurgency strategies less theoretically transferable, it will make them more regionally effective.

Information War:
The Historical Precedents of Cyber Operations

Introduction

The greatest problem facing strategists of cyber operations is its evolving and changing nature. Twenty years ago, cyber operations meant war through secured or limited computer networks. Ten years ago, widespread public access to the internet expanded cyberspace by leaps and bounds. Five years ago, social media dominated our lexicon as Facebook and Twitter began to reshape the role of the internet in our public interactions. Analysts and scholars of cyber operations have struggled with many of the questions these changes have raised. Are cyber operations limited to only state actors? Does it include only attacks on networks crucial to state infrastructures? Should we include military networks but not civilian ones? Does it include activists and criminals? Even though the answers to these questions and many others have gradually become clearer as the definition of cyber operations has been clarified, none have endeavoured to connect them to similar historical dilemmas.

Militaries and intelligence agencies face the ongoing challenge of how to wage war and how to defend themselves in the virtual realm of cyber space. Cyber operations are an integral aspect of all nations' security policy and cyberspace has been named by the United States as the "5th battlespace" alongside land, air, sea and space.[1]

Most scholars of cyber operations, if not all, tie it to the electronic and computer age. While this may seem intuitive, cyber operations also reflect a far older form of warfare: information war. Information war is most frequently linked to propaganda though it is today called Information Operations or Influence Operations. While once connected directly with cyberspace operations, electronic warfare is in its own category of warfare, now separated from "information war." This article uses a historical definition of "information war," broader than its modern definition and connected to an "information society."[2] One element of cyber operations is about the creation, control and manipulation of information—bytes of data on a computer network—be it espionage, sabotage, propaganda, or even simple dissemination of select information. A separate domain, outside the scope of this paper, is the networks and critical infrastructure (from power grids to telecommunications lines) that while also facing some potential risk are a different matter. A specially trained group of experts, such as programmers and Information Technology specialists, are crucial to understanding the medium of that information – the way it is transmitted. Their expertise informs the analysts, regional experts, linguists and other specialists who carry out operations or develop policy alongside them. A broader definition of information war that places it within the context of the "information society" that led to its creation reveals that the circumstances surrounding cyber operations are not new. Information war as described here has a much longer history than that of the internet or computer. It expands to include the entire history of "information society," and the idea of "information war" could easily apply to cartographers or scribes from centuries past.

This paper presents a historical perspective for strategists, policy makers and academics in their approach to cyber operations and their understanding of its significance in the broader

military and political realm. Using selected historical examples to examine the history of information media[3] can reveal how Western society adapted to the first Information Revolution of the printing press and how cartography and maps reflect similar concepts that underlie cyber operations as information war today. From this we can draw conclusions towards a new conceptual understanding of cyber operations and how to shape Canadian policy accordingly.[4]

Ultimately, current policy would be better informed if viewed within a historical context. While questions about the characteristics of cyber operations, such as the inclusion of non-state actors, or if cyber operations are any attacks on any network, or even the definition of "cyber war" are important, they are not the right questions with which to begin. First we must answer questions about the changing nature of 21st century society to properly understand how individuals and nation-states interact today.

1. The Renaissance and the Printed Book

Despite the vast differences in technology, society and culture, there are surprising links between the world of the computer and the world of the printing press. Each age reacted to new information media, be it the book or the computer, in a similar way. Both struggled with an excess of information and how to process it more efficiently and both societies were transformed as a result. Their differences, such as centuries of large-scale book printing versus a few short decades of the digital age, do not negate the significant parallels between them. They both represent different steps in the historical development of the "information society."

The origins of large scale production and categorization of information can be found in the intellectual culture of early modern Europe. Large scale information collection in the West began during the Renaissance, as scholars actively sought to gather and manage as much information as possible.[5] Before the invention of the printing press, Europeans had indexed and organised information from different manuscripts and libraries throughout Europe as a matter of necessity. Immense manuscripts were filled with knowledge cut and pasted from books that were rare or inaccessible. The rediscovery of knowledge from Antiquity led a generation of scholars to realise how much knowledge they had almost permanently lost. Only a small percentage of texts from the Roman and Greek eras were recovered from the long centuries after their empires crumbled. As works that had been preserved in Arabic slowly filtered into Europe, Europeans realised how much the breakdown of education and scholarly institutions had cost them.

Their realization resulted in putting every scrap of information they could find down in writing and reference texts, soon called encyclopaedias, which were collated together from wide source bases. The effort to preserve knowledge and the rebuilding of Europe's scholarly community was paramount to future scientific discoveries. New information was also recorded and added to the encyclopaedias. Scholars listed the newly discovered plants and animals, languages, historical events, and much of what we find in an encyclopaedia today. This drive was a reflection of a new cultural attitude towards compiling information.[6] Through the work of generations of Renaissance scholars, these vast texts

grew as each generation added to the knowledge of the "whole." Some were driven to compile the information from their excessive note-taking, others for financial gain or patronage, but all revealed the same commitment to reading, intensive labour and intellectual judgement.[7] Yet the cultural shift towards information preservation would remain restrained without an accompanying outlet for their endeavours. Only when matched by a new medium for information, the printed book, was one of the world's first Information Revolutions underway.

The creation of the printing press and the rise of "print culture" allowed scholars to move away from manuscripts. Handwritten manuscripts had been painstakingly produced by an army of scribes, but the printing press made such arduous methods extinct. Within sixty years of its invention in 1450 by Johann Gutenberg in Mainz, Germany, the printing press had spread across much of Europe. As the printing press became more accessible, larger and larger amounts of written material was published. Books, no longer the purview of dedicated scribes, became part of a new publishing industry motivated not only by the preservation of knowledge, but also the desire to make money doing so. Publishers and authors flooded the market with their work. An unexpected consequence of these technological and commercial developments was the sheer number of works that began to be distributed. Soon they far out-produced the centuries of manuscripts produced by scribes. Much like those who today worry about the consequences that the internet's seemingly infinite number of blogs, news articles and comments might have on our ability to find and process important information, Europeans scholars were also worried about the overabundance of information. Humanist scholar Erasmus asked in 1526, "is there anywhere on earth exempt from theses swarms of new books? [Printers] fill the world with pamphlets and books [that are]…foolish, ignorant, malignant, libellous, mad, impious and subversive; and such is the flood that even things that might have done some good lose all their goodness."[8] As books became easier and easier to create and preserve, it seemed as if too many books, good and bad, would overwhelm the learned.

The solution then, as it is now, was not to set about the impossible task of reducing the number of sources of information. Instead, the solution was in new ways of reading and absorbing information.[9] The advent of print society allowed Europeans to begin collecting important information into mass-produced books rather than in a multitude of hand-crafted manuscripts. As information became easier to access and a greater volume of information was available, how Europeans read also changed. By the 18th century noted English literary critic and writer Samuel Johnson could describe four different kinds of reading used to best learn different types of information. One, "hard study" for learned books read with pen in hand; two, "perusal" for close reading for specific information; three, "curious reading" for leisurely reading of fiction; and four, "mere reading" for quickly scanning text for information.[10] Each reflected the book being read and the purpose of the reader. Only if a reader was better equipped to process information could they begin the task of categorizing it. The end result of the first Information

Revolution, the transformation of the "reader," (that is, the changing effects information media has on the society that furthers it) is important and has been repeated in the second Information Revolution.

2. What can we learn from the first Information Revolution?

Today, those best equipped to operate in the world of computers and the internet are those who have changed, consciously or unconsciously, how they absorb and find information. A skilled "reader," or perhaps the better term might be "user," today knows how to find information on the internet, or how to best use electronic devices to record it, or how best to search through documents: the proper use of search terms on Google, scanning texts into searchable documents using optical character recognition, and creating databases to categorize large amounts of information may all seem simple to those familiar with technology, but they represent an enormous change in the ability of an individual user to process information. They are skills that are absolutely necessary for the modern user. Just like the readers who could read through more books and remember more from them, the users who can effectively use the internet or computers today are a product of their age. Their skills allow them to operate in the midst of an overabundance of information.

The crucial element of those skills lay in their approach to information: knowing what to read closely, what to skim, and where to find the information required. In Samuel Johnson's words, "knowledge is of two kinds. We know a subject ourselves or we know where we can find information upon it."[11] In the 21st century as we grapple with another Information Revolution we can see how society has already learned from history's lessons. Adapting to new methods of finding and processing information has allowed us to efficiently and effectively operate in the computer age. These skills and tools are essential to our modern "information society" where the categorization of information and the ability to rapidly access and ingest it is paramount. The major difference is the amount of information on the internet and the speed at which it travels; but the fundamental problem and its solutions remain the same. Paper or digital, yesterday or today, our society has developed similar ways of dealing with an excess of information.

The speed and the manner that information is transmitted changes the very individuals and society responsible for transmitting it. The shift from the age of printing to the digital age has brought with it the digital society. All aspects of our daily lives are being affected by digital media. The printing press eventually caused greater and greater literacy rates, and the spread of computers will bring (and has brought) with it greater and greater digital literacy—the capacity to easily navigate computer systems. Being left behind was, and is, a severe handicap. Rather than treating digital media merely as a signpost of some sort of generational divide, the Government of Canada and Canadians must acknowledge that they are all involved in the new digital society, regardless of whether they use computers, a smart phone or a tablet. Just as it was for the scholars who bemoaned the number of printed books in the 16th century, it is already too late to turn back the clock. We must accept the new society of the 21st century and act accordingly. Cyber operations are not simply a new form of engaging in war—they are the predictable by-products of a digital society engaging in warfare.

3. Cartography

Just as the latest development of information society today can be linked to its emergence during the Renaissance, so too can historians connect an older form of information war to today's variant. Before the modern era, information was just as vital and contested as it is for cyber operations. The difference was how that information was transmitted and controlled. One important example is the use of

cartography, the creation and reading of maps. The role of maps in war is another historical precedent that offers lessons on the waging of information war in 2013.

Long before Google Maps and MapQuest made maps and directions instantly accessible, printed maps were highly valued and closely protected. Cartographers, like programmers today, were specially trained individuals who worked with an information medium crucial to government and military leaders. In the Age of Discovery, as the monarchies of Europe explored the lands beyond their kingdoms, maps served as a vital medium conveying precious new knowledge of uncharted lands. The new commercial opportunities and resources that lay there were guarded by the states that had funded expeditions to them. A map of a newly discovered coast could provide ships safe passage through unfamiliar waters. Stealing maps, or copying them surreptitiously, provided nations with economic benefits and military advantages. Even just knowing the route of the enemy's vessels made them far easier to interdict if war did break out. Some nations had laws prohibiting the sharing of cartography with foreign states while others had traditions against sharing these discoveries with outsiders. A famous example is the "Cantino Map" of 1502, which was created by a Portuguese mapmaker at the request of an Italian, Albert Cantino. Cantino convinced the mapmaker to reveal the protected Portuguese voyages to Brazil and Newfoundland at a time when these new worlds were rich sources of fish, gold or other resources.[12] Through bribery or friendship (any way of manipulating people into revealing confidential information that today would be called social engineering) the protected "data" was quickly sold and distributed to other nations of Europe that could now send their own expeditions there. Protective measures, like today's firewalls, can always fall victim to the human breaches.

Maps were equally decisive for military planning and government policy. Without a correct and accurate map, navies could sail into ruin, armies could march into unfavourable terrain, and diplomacy could flounder. To choose just one example is the British reaction to the Ochakov Crisis of 1791 during the one of the many Russo-Turkish wars. The British Foreign Office discovered that they had no accurate charts for the Black Sea, leaving them unclear whether the fortress of Ochakov really controlled the entrance to the river Dnieper. The British could not prove that the return of Ochakov to the Turks was essential to the Ottomans' power in the region since they themselves were not sure of its location.[13] Historian Jeremy Black explains that map information and the detailed planning derived from it was "a source of authority" that could guide policy makers and generals alike; cartography and war were linked to "a developing consciousness about [military] planning" and became a key aspect of any successful campaign or international dispute."[14] They represent the reality of an information society. The ability to accurately (and securely) transfer information is key to operational and political success.

In the 21st century, computer systems and networks occupy a comparable place. They are indispensable to government action and military operations. Likewise, their negation or inaccessibility results in similar disadvantages. A ready example is the Russian cyber attacks on Estonia in 2007 and Georgia in 2008. As an early example of cyber operations, they were an offensive against a medium of information used to communicate with citizens and for government affairs. The self-evident

differences between electronic and print media aside, the same basic principle of communication underlay their utility in times of war and their vulnerability to attack. The inability to receive information from websites or servers has a similar result to that of being unable to find an accurate map for generals of the Napoleonic era. Ensuring prompt access to accurate information or removing the enemy's ability to do so will always be a fundamental part of warfare. Whether it is information from maps or cyber media, both impact state policy and military success.

Maps, as a medium of information like the printed book, also shaped the societies that used them. Cartographers were important stewards of nations' and societies' sense of themselves. In Arthur Jay Klinghoffer's review of the inherent power of cartography, he writes, "cartography is…the intellectualization of space across time."[15] That is, maps are a visual representation of information as the cartographer understands it. They represent not only the world as it exists, but also the world as its makers portray it. An example of this is the Mercator projection of the world map that enlarges the northern hemisphere and unintentionally makes Europe and North America far larger to an observer than reality. In contrast, the Peters projection portrays the continents closer to their real size, emphasizing the "Third World" and minimizing the importance of Mercator's Europe.[16] A more modern and striking example is from the interwar period when German scholars used cartographic manipulation as a means of reinforcing German territorial claims, as well as ethnographic and political ambitions during the uncertain political period following the Treaty of Versailles that ended the First World War.[17] Maps are far more subjective than they might first appear and influence their readers in subtle ways. Moreover, that influence sometimes stems from what information is not presented rather than the information itself. Data on computer networks is a medium of information that can be manipulated, such as censored Google results or biased news aggregate sites. Bytes of information are like ink on a map – alone they are nothing, but together they form information we can understand and can control. Our ability today to control and change computer networks is similar to a monarch's control of cartography in their era, which centuries of military, economic and intelligence success (and failures) have shown.

4. Modern Information War

Thus far, the correlation presented between historic information media and the modern domain of cyberspace underscores the conclusion that the concepts that drive our understanding of 'cyber operations' reflect historical processes. The first Information Revolution of the Renaissance and the printing press unfolded in a similar manner (albeit as it appears now, on a different scale) as the Information Revolution of the computer age. Both reveal a social reaction to how information is transmitted and widespread changes to how individuals interact with it. An examination of cartography reveals that military and state operations being informed by the use of an information medium is not unique to cyber operations. Historic information war demonstrates that its basic concepts can be applied as easily to a printed medium as it can to a virtual one. Cyber operations, then, are a continuation of historic developments. Thus, cyber is a new tool for information war, rather than a new form of war entirely. These links, acknowledged by present-day scholars and analysts will necessarily affect how we approach cyber conflicts.

So far this paper has examined information society in Europe from the emergence of new cultural attitudes towards information in the Renaissance, to the printing press and the rise of print society, to cartography as an example of information society's impact on politics and war. The most recent iteration of information society is the digital society, where computers and networks are integrated into our daily lives. A crucial question to ask is how the cyberspace created by these networks has changed us. The answer sheds light on how a digital society could (or perhaps, should) wage war and reform policies.

Countless books and articles have addressed how cyberspace has influenced society, politics and economics in almost all aspects of our lives. Each offers a definition of cyberspace tooled towards their specific subject, so it is beneficial to present some of the basic ideas that underly these different meanings.[18]

The basic structure of cyberspace can be described by three layers: physical, the actual computer hardware; syntactic, the protocols and software used to send, receive and understand data; and semantic, the actual information presented to computers or users.[19] This definition describes the physical system that forms the virtual medium of cyberspace, but neglects to capture the social conception of cyberspace. Much like saying a book is simply paper, ink and a leather cover, the material explication of a medium reveals little about its role in our digital society.

Like the published book, cyberspace is the result of social technological processes and must be understood as something more than its physical components—in this case, it is more than a network of computers. Daniel Kuehl provides useful insight by adding that beyond these physical characteristics, cyberspace is also a "designed environment, created with the specific intent of facilitating the use and exploitation of information, human interaction, and intercommunication."[20] The users, be they individuals, states, or organizations, shape the "cyberspace" it represents with every textual, visual or auditory communication that occurs in it. While scholars have variously used "domain", "environment" or "realm" to describe the virtual "space" created by computer networks, all of these are limited by the narrowness of their description. They do not infer the basic nature of cyberspace as a virtual space where media is created, manipulated and controlled just as much as its users interact and define it. So although the US Department of Defense defines cyberspace as "a global [man-made] domain within the information environment that encompasses the interdependent networks of information technology infrastructures,"[21] it offers little context to our understanding.
Cyberspace, like the printed book, is a medium that shapes the behaviour of its users. Any aspect of cyber operations that deal with a human element, be it defensive policies or offensive actions, must also involve an understanding of the role of cyberspace in shaping the digital society we live in today. Whether it is the public communicating messages through social media or accessing open source information with a click of a button, society comes to rely upon the speed of the fastest communication. The availability of instantaneous communication and information has in turn had a reflective effect on the society that developed it, by making itself invaluable to our daily lives. It has fundamentally changed how we interact with information and each other, and consequently, inform us

about how we might influence that interaction.

This paper limits its definition of information war to consist of non-kinetic operations that primarily focus on intelligence gathering, such as stealing information, and intelligence deception, such as attacking or manipulating networks and websites. It does not include cyber operations with kinetic results, such as shutting down power grids or, as in the case of Stuxnet, attacking nuclear centrifuges. Those types of cyber operations fall closer to what might be described as "cyber war." The debate over whether cyber operations that fall under intelligence are actually a form of warfare continues, but a historical understanding of information war is vital when addressing this debate and informs our understanding of cyber operations.

Two case studies have often been presented as the "earliest" incidents of true state-on-state cyberwar. The first is the Denial of Service (DoS) attacks against Estonian websites that began in April 2007, and the attacks against Georgian websites in August 2008. Both have been attributed to Russia, though no conclusive proof is available in either case. In early April 2007, Estonia moved the Russian Second World War Tomb of the Unknown Soldier from the centre of the Estonian capital Tallinn to the city's outskirts. In response, the Russian blogosphere began to discuss taking revenge on Estonia. For over three weeks, up to 85,000 hijacked computers were used to bring down Estonian websites with a peak on 9 May as Moscow celebrated Victory Day. Although the Kremlin never definitively claimed responsibility, the coordination between alleged perpetrators, Russian criminals and rogue patriots has led many to suggest some national involvement.[22] Similar DoS attacks were launched against Georgia a year later. As Russia and Georgia approached a state of war over the separatist state of South Ossetia, three types of attacks were launched. One, defacing prominent websites; two, a DoS attack against public and private sector websites; three, spreading malicious software to help the public participate in the attacks against Georgian websites and government emails. Again, Russia was allegedly the organizer for these attacks, but the NATO report on the attacks reported, "there is no conclusive proof of who [was] behind the DDoS attacks as was the case with Estonia."[23]

Although the impact of these attacks was relatively small in terms of physical or violent damage, many use the examples of Estonia and Georgia, among others, as proof of the growing dangers of cyber attacks. US presidential cyber security advisor Richard Clarke and his co-author Robert Knake point to "non-kinetic" attacks like DoS as evidence of the need for stronger cyber defences.[24] For Clarke and Knake and others, the attacks in Estonia and Georgia reveal the threat of cyber war for governments. Since the attacks of 2007 and 2008, the US government has increased its preparation for cyber attacks. Public pressure mounted as individuals increasingly warned of the threat of cyber war. Senators Jay Rockefeller and Olympia Snowe published an op-ed in the Wall Street Journal in 2010 warning that "now is the time to prepare for Cyberwar."[25] While the push towards tougher cyber defences is worthwhile, other scholars have questioned whether such low-key attacks could represent a declaration of (cyber)war. Jerry Brito and Tate Watkins questioned the "threat inflation" of cyber security policy, arguing that a "cyber-industrial complex" benefited from the fear mongering surrounding small scale attacks like those in Georgia and Estonia.[26] Thomas Rid offers the bolder argument that "cyber war will not take place." For Rid, "the world has never experienced an act of

cyber war, which would have to be violent, instrumental and—most importantly—politically attributed…Instead, the last decade saw increasingly sophisticated acts of network-enabled sabotage, espionage, and subversion."[27] It is clear that there is a split over the significance of the cyber attacks against Estonia and Georgia. Are they red flags against the dangers of cyber war; or, do they point to the limits and perhaps even the impotence of cyber operations in warfare?

I highlight the incidents in Georgia and Estonia, and the response to them, because they demonstrate how using the historic understanding of information war proposed in this paper makes it easier to distinguish the significance of these small-scale attacks. Scholars like Adam Liff have concluded, "cyberwarfare appears to be a tool for states to pursue political (strategic) and/or military (tactical) objectives at relatively low cost under very limited circumstances."[28] Yet the use of a term like "cyber war" is provocative and implies a level of aggression which is not present in attacks like those against Estonia and Georgia. Such attacks fall under the historical conception of "information war." The operations against the two nations in 2007 and 2008 were more analogous to the manipulation and use of cartography as an information medium that holds strategic or political advantages. Rather than leading to a state of war, or even acting primarily as a function of wartime operations, cartography was a tool that aided or deceived military and political planning. Russia (if it was responsible) did not engage in cyberwar in 2006 and 2007, but rather in information war. Military and government policy should reflect the difference between the two concepts and plan accordingly. A nation preparing for a non-kinetic information war would surely have different approaches than one preparing for a kinetic cyber war. Equally, the defence policy aimed at preventing one or the other must be considered separately as well. The historical examples of information war presented here point to a modern information war that is just as focused on the cyber medium as maps were centuries ago.

5. Conclusion

Differentiating information war from cyber war is a difference we can come to through this historical perspective. The printed book as a means of communicating information in the age of the printing press revolutionized Western society's view of information. This first Information Revolution forced Europeans to adopt news ways of categorizing and absorbing information as they adapted to a new technological era. Cartography, another important vessel of the printed medium, became increasingly important as a means of assuring or denying political and military success. Both printed books and maps help shape two lessons for us here in 2013: first, we must adapt to new ways of transmitting information in the computer age; second, understanding the societal impact of cyberspace is essential to success. Thus as previous generations had to adapt to these new ways of creating, presenting and manipulating information, so too must today's public and specifically those involved with security and defence of the country adapt. In his book, *Wiki at War* James Jay Carafano argues that a successful cyber strategy does not require a particular person or specific technical ability but rather "a set of knowledge, skills and attributes essential to all leaders at all levels of government and in the private sector."[29] Martin Libicki echoes his point, stating we do not simply need "well-educated" individuals, but specially trained ones.[30] Modern armies and state apparatuses operate in a digital society irrevocably linked to cyberspace. We cannot plead ignorance of thumb drives or social media or

computers—everyone involved in our nation's cyber strategy must understand the consequences of these technological developments and how to utilize them. Today we do not face a new era of information society or information war. Today we face the pinnacle of it (until the next leap forward!). Kings and generals required knowledge of books and maps as scholars formalized new methods of reading and information management. Likewise, modern strategists must understand computer networks and the internet. The key difference between then and now is that they were using mediums of information such as books and maps to better wage war. In 2013 the medium itself, computer networks, is where war is waged. Cyber is not the fifth domain, but the domain that links all others together.

Governments adapt to cyber war, the 21st century information war. Strategists and scholars should consider cyber war as the culmination of these historic processes behind information war, though on a far larger scale and across a much larger space, not a new form of war entirely. The idea that information war is unique to the 21st century, or that cyber operations are solely the product of unprecedented technological developments, limits our ability to adapt to a digital society. Analysts and scholars ask questions that delineate cyber operations in great detail. They dichotomize cyber operations as kinetic or non-kinetic, or the capability of terrorists versus state actors, or parse legalities of what constitutes a declaration of "cyber war". Yet all of these questions should be asked after we answer the question of how digital societies engage with each other on a political or military level. The history of information society that I have outlined here demonstrates that we can begin to answer that question without waiting for future historians. Those who experienced the rise of print society were not aware of the societal influence of printed books, but we are not restrained by their ignorance. We know cyberspace is fundamentally changing who we are and how we interact with each other as individuals and nation states. We can look to cartography's influence and reflect on the importance of operations in the cyber medium. A forward-looking strategy must incorporate these concepts into our understanding of the medium that computer networks represent and understand how closely that information medium influences our conception of the world. Any successful policy regarding defensive or offensive cyber operations must acknowledge the dominance of digital society. Instead of fitting old ideas and models onto new paradigms, we must create policy and objectives based on the new society in which we find ourselves, not the one we have left behind.

Recommendation 1 –

Notwithstanding the government's 2010 Cyber Security Strategy, the 2012 Auditor General's Fall Report (Chapter 3, Section 3.25) noted that "the lack of action plans since the 2001 commitments for cyber security were announced has contributed to the overall lack of measurable progress. We noted that the 2010 Cyber Security Strategy does not yet have an action plan to guide its implementation." This paper agrees with the Auditor General's recommendation of implementing an action plan and suggests that the Government must accompany an action plan with broader policy acknowledging the "digital society" that exists today.

The whole-of-government approach should be supplemented with a "whole-of-society" initiative focusing on Canada's digital society. The Government should champion its place defending and

nurturing Canada's digital society. It should actively seek to increase "digital literacy" among government employees, military personnel and the Canadian public. It should be able to actively engage with "digitally literate" Canadians about its cyber policy and communicate how it is defending Canada's interests and prepared for attacks. These steps would speed up the implementation of the 2010 Cyber Security Strategy as well as prepare for future initiatives.

Recommendation 2 –

The Canadian Cyber Incident Response Centre (CCIRC) is tasked with advising, protecting and responding to cyber attacks against the Canadian government and its people. To better perform their task, they should strongly differentiate between information war and cyber war. From that, cyber operations that fall under information war will likely be small-scale interactions between nations, like those seen in Estonia and Georgia. Those incidents demonstrate that it will be difficult to clearly identify the nation or organization behind an attack. Not all cyber operations will necessarily be a part of a large-scale military or political conflict. They are a normal result of the interaction between digital societies. In the future, organizations or nation-states may more frequently engage in cyber operations that remain untraceable. Therefore, policy should be able to distinguish between cyber attacks that are national security threats and those that are information disruptions.

Recommendation 3 –

Resources must be used to protect critical infrastructure, but there should also be policy aimed at circumventing Denial of Service attacks on websites or Canadian network access. This can be accomplished by, as the Auditor General also suggests, by increasing CCIRC hours of operation, but also expanding their ability to appropriately respond to network or website failures by understanding them as more than attacks against network infrastructure, but as attacks against digital society and its psychological consequences on Canadians. The Government of Canada should actively distribute information helping Canadians to know generally how security will be ensured if cell phone or internet services were interrupted, or if government websites were inoperative for extended periods. Panic can be avoided if proper plans are in place and the public is informed in advance.

Recommendation 4 –

Most nations are currently considering the expansion of military operations into cyberspace as another "battlespace," which is a mistake. Cyber should be classified as a domain that links all others together and not its own fifth domain.

The Canadian Forces/Department of National Defence, which has a Director General Cyber and a Director General, Information Management Operations, is moving in a similar direction. They should continue operating within a "whole-of-government" approach and maintain their strong relationship with Communications Security Establishment Canada. To continue being successful in a digital society, CF/DND should expand the digital literacy of their personnel so that the CF can continue to expand their cyber capabilities beyond the realm of cyber operations to integrating all levels of the armed forces with technological advancements. Further integration could improve their performance and also attract "digitally literate" Canadians.

Endnotes

McAuley's "Canada's Tactical Fixation? Rethinking the IED Phenomenon"

1 General Stanley McChrystal, Commander, NATO International Security Assistance Force, Afghanistan, "Commander's Initial Assessment, 30 Aug 2009, p. 1-2. http://media.washingtonpost.com/wp-srv/politics/documents/Assessment_Redacted_092109.pdf?sid=ST2009092003140 (accessed 18 Jan 2013).

2 Ibid.

3 The Canadian Key Villages Approach (KVA) commencing in the village of Deh-e Bagh south of Kandahar City has been hailed as a template for effective COIN operations; however, it is critical to note that such efforts were only possible once the Canadians handed off responsibility for much of Kandahar province in 2009 to elements of the US 4th Infantry Division. Carl Forsberg, *Afghanistan Report 3: The Taliban's Campaign for Kandahar* (Washington: Institute for the Study of War, 2009), p. 52.

4 Olivier Grouille, "Bird and Fairweather in Context: Assessing the IED Threat", *The RUSI Journal*, 154: 4 (2009), 40-45. Canadian casualty statistics for the Afghanistan mission to January 2011. Canadian Forces' Casualty Statistics (Afghanistan), FS 11.001 - January 12, 2011, http://www.forces.gc.ca/site/news-nouvelles/news-nouvelles-eng.asp?cat=00&id=3695 (accessed 30 Jan 2011).

5 See General Stanley McChrystal, Commander, NATO International Security Assistance Force, Afghanistan, "Commander's Initial Assessment, 30 Aug 2009. http://media.washingtonpost.com/wp-srv/politics/documents/Assessment_Redacted_092109.pdf?sid=ST2009092003140 (accessed 18 Jan 2013).

6 Considerable military efforts have been made by Coalition members to develop and implement effective counter-IED strategies. In response to the growing impact of IEDs in October 2003 in Iraq and Afghanistan, the U.S. Army Chief of Staff established an Army IED Task Force. This organization was subsequently transformed into the Joint IED Task Force (JIEDTF) and then into the Joint IED Defeat Organization (JIEDDO) in February 2006. Allocated an annual budget of approximately $3.5 billion per year since 2006, the JIEDDO's mission is to lead, advocate, and coordinate all U.S. DoD actions in support of Combatant Commanders' and their respective Joint Task Forces' efforts to "defeat IEDs as weapons of strategic influence". The JIEDDO focuses on three lines of operation: defeat the device, attack the network, and train the force. https://www.jieddo.dod.mil/about.aspx (accessed 22 April 2011); http://www.defense.gov/Releases/Release.aspx?ReleaseID=15063 (accessed 12 November 2012). The same lines of operation have been adopted by the much smaller Canadian Forces Counter-IED Task Force established in 2007 to "coordinate efforts to attack the IED network, develop CF capabilities to defeat IEDs, and provide advice on preparing the force to operate in an IED environment." http://www.army.forces.gc.ca/land-terre/ciedtf-focdec/au-ns-eng.asp (accessed 12 Nov 2012).

7 Renowned college basketball coach John Wooden has been credited with the remark that it is always important never to mistake activity for achievement.

8 Howard Coombs and Lieutenant-General (retired) Michel Gauthier, "Campaigning in Afghanistan: A Uniquely Canadian Approach", in Colonel Bernd Horn and Emily Spencer, ed. *No Easy Task: Fighting in Afghanistan* (Toronto: Dundurn, 2012), pp. 101-121.
9 US Embassy Kabul staff US Embassy Kabul (Afghanistan) Cable 09KABUL2335, *Canada's Revised COIN Strategy in Kandahar*, 12 Aug 2009. http://wikileaks.org/cables/2009/08/09KABUL2335.html (accessed 1 Oct 2012).

10 The 2008 Manley Report observed that "stronger strategy, and more cohesive strategic direction, [were] essential" and that "Canada should press diplomatically, at the highest level, for a comprehensive political-military strategy". Beyond simply observing the need for renewed interest in strategy, the report did not explicitly discuss Canada's obligations and responsibilities in terms of developing a coherent national strategy or contributing to coalition strategy formulation. Defining such obligations and responsibilities is arguably the domain of the government-of-the-day rather than an Independent Panel and would therefore not be expected in such a report. The level of responsible that the Government of Canada perceived it held in relation to Afghanistan strategy is unclear and perhaps requires further scrutiny. See *Independent Panel on Canada's Future Role in Afghanistan* (Ottawa: Minister of Public Works and Government Services, 2008).

11 Howard Coombs and Lieutenant-General (retired) Michel Gauthier, "Campaigning in Afghanistan: A Uniquely Canadian Approach", in Colonel Bernd Horn and Emily Spencer, ed. *No Easy Task: Fighting in Afghanistan* (Toronto: Dundurn, 2012), p. 120.

12 US Embassy Kabul staff reported that Representative of Canada in Kandahar (RoCK) Ken Lewis acknowledged to Kandahar Provincial Reconstruction Staff (KPRT) on 8 Aug 2009: "We've been playing whack-a-mole for years"; US Embassy Kabul (Afghanistan) Cable 09KABUL2335, *Canada's Revised COIN Strategy in Kandahar*, 12 Aug 2009. http://wikileaks.org/cables/2009/08/09KABUL2335.html (accessed 20 Oct 2012).

13 Note that at least two distinct bombing campaigns, one perpetrated by the Taliban in Afghanistan and parts of Balochistan and another by Baloch separatists in Pakistan, have been observed in this conflict region. Alec D. Barker, *Improvised Explosive Devices in Southern Afghanistan and Western Pakistan*, 2002-2009, Counterterrorism Strategy Initiative Policy Paper (Washington, DC: New America Foundation, April 2010), p. 16.

14 Commander John Moulton, US Navy, "Rethinking IED Strategies: From Iraq to Afghanistan", Military Review (July-August 2009) 26-33, p. 28. Colonel John Boyd, a retired US Air Force pilot, developed the theory of the OODA loop after observing that certain pilots excelled in aerial dogfights and questioned why the US kill ratio over Korea was 10:1 when North Korean and Chinese aircraft where often superior in capability. See Major C.S. Oliviero, "Manoeuvre Warfare - Our Chance to Adopt a Winning Style", *Armour Bulletin* 20 (September 1987).

15 Colonel John R Boyd, "Patterns of Conflict", Unpublished Briefing Slides, December 1986.

16 Carl von Clausewitz relates the conduct of war to the workings of an intricate machine which generates tremendous friction. Clausewitz equates activity in war to movement in a resistant medium; such as walking in water. He observed that activities easily planned on paper are not so easily executed as a result of friction. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), p. 119.

17 A representation of John Boyd's concept of imbedded Observe-Orientate-Decide-Act Loops representing the idealized synergy between decision making at the political, strategic, operational, and tactical levels. Friction is experienced at the tactical interface between imbedded OODA Loops as both cycles attempting to run in the clockwise direction come into contact with each other. The Adversary seeks to induce sufficient friction at the tactical interface in order to cause the Friendly decision cycle to run in reverse, thereby causing tactical reactions to drive decisions, which predetermine orientation, and in turn influence observations. The reversal of the tactical cycle may subsequently transfer into the imbedded operational, strategy, and political OODA Loops if these cycles are weak or out of sync with the outer levels.

18 Lieutenant Colonel David Kilcullen, "Twenty-Eight Articles: Fundamentals of Company-level Counterinsurgency," Military Review (May-June 2006) 103-108, p. 105.

19 Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Penguin Group, 2007), pp 135-6.
20 Ibid, p. 137.

21 Sawyer, *The Seven Military Classics*, translator's introduction to Sun-Tzu's Art of War, p.155. For further description of the 'classical dilemma of operational art' see Eric Ouellet, "Ambushes, IEDs and COIN: The French Experience", *Canadian Army Journal* 11.1 (Spring 2008), 7-24, p. 20.

22 In August 2005 Canada assumed leadership of the Kandahar Provincial Reconstruction Team (KPRT) and command over the Kandahar province with just 2,500 soldiers. Kandahar province is 54,000 km2, comparable in area to Nova Scotia.

23 Department of National Defence, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Defence*. NDID A-JS-005-000/AG-001. 2005.

24 Ibid, p. 1.

25 Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Penguin Canada, 2007), p. 289.

26 Robert Murray and John McCoy, "From Middle Power to Peacebuilder: The Use of the Canadian Forces in Modern Canadian Foreign Policy", *American Review of Canadian Studies Vol.*40.2 (2010), p.178.

27 See Douglas Bland, *Chiefs of Defence: Government and the Unified Command of the Canadian Armed Forces* (Toronto: Canadian Institute of Strategic Studies, 1995).

28 Douglas Bland, "Everything Military Officers Need to Know About Defence Policy-Making in Canada", David Rudd, Jim Hanson, Jessica Blitt, ed. *Advance or Retreat: Canadian Defence in the 21st Century* (Toronto: Canadian Institute of Strategic Studies, 2000), pp. 15-29.

29 Lieutenant-Colonel J.H. Vance, "Canada's Departure from the Classic Doctrine of Operational Art", Canadian Forces College AMSC-7 Paper, October 2004, p. 6.

30 Sandy Gall, *War Against the Taliban: Why it all went wrong in Afghanistan* (London: Bloomsbury Publishing Plc, 2012); Rajiv Chandrasekaran, *Little America: The War Within the War For Afghanistan* (New York: Alfred A. Knoff, 2012); Sherard Cowper-Coles, *Cables from Kabul: The Inside Story of the West's Afghanistan Campaign* (London: Harper Press, 2011).

31 Carl Forsberg, *Afghanistan Report 3: The Taliban's Campaign for Kandahar* (Washington, DC: Institute for the Study of War, 2009), p. 29.

32 Forsberg, *Afghanistan Report 3*, p. 49.=

33 Colonel Bernd Horn, "Full Spectrum Leadership Challenges in Afghanistan" in Colonel Bernd Horn ed. *In Harms Way*, "The Buck Stops Here": *Senior Military Commanders on Operations* (Kingston: Canadian Defence Academy Press, 2007), p. 196.

34 David J. Bercuson and J.L. Granatstein, Lessons Learned? What Canada Should Learn from Afghanistan (Canadian Defence & Foreign Affairs Institute, October 2011), pp. 20-26. http://www.cdfai.org/PDF/Lessons%20Learned.pdf (accessed 3 Feb 2013).

35 Ibid, p. 19.

36 Boyd, "Patterns of Conflict", p. 7. Author's emphasis.

37 Ibid, pp. 134 & 141.

38 Forsberg, Afghanistan Report 3, p. 21.

39 Ibid, 31.

40 David Charters, "From Post-Cold War to Hot War: Canadian Military Intelligence in Transition", paper presented at the annual meeting of the International Studies Association Annual Conference "Global Governance: Political Authority in Transition", Montreal, QC, 16 Mar 2011, p. 42. http://www.allacademic.com/meta/p499372_index.html (accessed 19 Jan 2013).

41 Ibid, p. 42.

42 Kilcullen, "Twenty-Eight Articles", p. 105.

43 Norman Dixon, *On the Psychology of Military Incompetence* (London: Random House, 1976), p. 293.

44 Sherard Cowper-Coles, *Cables from Kabul*: *The Inside Story of the West's Afghanistan Campaign* (London: Harper Press, 2011), p. 142.

45 Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for New American Society, January 2010), p. 8.

46 DND, Land Force, B-GL-323-004/FP-003, *Counter-Insurgency Operations*, 13 Dec 2008.

47 "CF HUMINT experts praised by allied forces", *The Maple Leaf* (19 January 2011), p. 6; Major Gordon Ohlke, "Army News – The All Source Intelligence Centre", *The Canadian Army Journal*, Vol.10.3 (January 2007), 5-9.

48 An organization chart of the Expeditionary-in-Theatre Generic All Source Intelligence Centre (ASIC) suggests that the number of actual operators actually engaged in field HUMINT collection activities could be as low as six. Ohlke, "Army News–The All Source Intelligence Centre" *Canadian Army Journal* Vol.10.3 (Fall 2007), p. 6.

49 Stability Operations Information Centre Kabul, *Kandahar City Municipality & Dand District: District Narrative Analysis*, 30 March 2010, p. 58-9. http://info.publicintelligence.net/SOICKandaharAssessment.pdf (accessed 31 Dec 2012).

50 DND, Land Force, B-GL-323-004/FP-003, *Counter-Insurgency Operations*, 13 Dec 2008.

51 Richard Livingstone, ed. *Thucydides: The History of the Peloponnesian War* (New York: Oxford University Press, 1960), p. xxi.

52 Dixon, *On the Psychology of Military Incompetence*, p. 293.

53 The Canadian approach commencing in the village of Deh-e Bagh has been hailed as a template for effective COIN operations; however, it is critical to note that such efforts were only possible once the Canadians handed off responsibility for much of Kandahar province in 2009 to elements of the US 4th Infantry Division. Carl Forsberg, *Afghanistan Report 3: The Taliban's Campaign for Kandahar* (Washington: Institute for the Study of War, 2009), p. 52.

Williams' "Hell on Heels: the Intersection of Women, Terror, & Insurgency"

1 Bobby Ghosh, "The Mind of a Female Suicide Bomber," *TIME,* Sunday, June 22, 2008, http://www.time.com/time/world/article/0,8599,1817158,00.html (accessed 21 Dec 2012).

2 David Kilcullen, *Counterinsurgency*, (New York: Oxford University Press, 2000), p. 1.

3 Mia Bloom, "Death Becomes Her: Women, Occupation, and Terrorist Mobilization," Symposium Presentation (July 2010), p. 6.

4 Bruce Hoffman, "Holy Terror: The Implications of Terrorism Motivated by a Religious Imperative," *Studies in Conflict and Terrorism Vol.18 (1995)* p. 272.

5 Scott Atran, "The Moral Logic and Growth of Suicide Terrorism," *The Washington Quarterly* Vol 29.2 (2006) p. 129.

6 Karla J. Cunningham, "Countering Female Terrorism," *Studies in Conflict and Terrorism* Vol.30.2 (2008) p. 116.

7 Ibid, p. 116.

8 Anne Speckhard, "The Emergence of Female Suicide Terrorists," *Studies in Conflict and Terrorism* Vol.31 (2008) p. 1025.

9 Ibid, p. 1032.

10 Karla J. Cunningham, "Countering Female Terrorism," p. 115.

11 Anne Speckhard, "The Emergence of Female Suicide Terrorists," p. 1029.

12 There are two elements of the strategic desirability imagined in the insurgent context. First, it may simply be that the use of women has an operational value from the standpoint of being less suspect of undertaking an attack and thus, women are able to access individuals and locales otherwise inaccessible to men. Second, there is a definite strategic desirability for the use of women in the insurgency's media campaign.

Barbara Friedman, "Unlikely Warriors: How Four U.S. News Sources Explained Female Suicide Bombers," *Journalism and Mass Communications* Quarterly Vol 85.4 (2008) p. 845.

13 Karla J. Cunningham, "Cross-Regional Trends in Female Terrorism," *Studies in Conflict and Terrorism* Vol.26 (2003) p. 185.

14 Deborah M. Galvin, "The Female Terrorist: A Socio-Psychological Perspective," *Behavioural Sciences and the Law* Vol.1.2 (1983) p. 30.

15 Ibid, p. 23.

16 David Kilcullen, *Counterinsurgency*, p. 156.

Keelan's "Information War: the Historical Precedents of Cyber Operations"

1 United States' Department of Defense, *Quadrennial Defense Review Report*, February 2010.

2 Information society refers to a society that relies on recorded knowledge rather than inherited wisdom passed down between individuals. The history of information society is relatively new. The last decade has seen many valuable additions to the study of how information has been disseminated and used in the past and, as a recent literature review notes, has finally developed a comprehensive and academic discourse between historians, see Toni Weller, "An Information History Decade: A Review of the Literature and Concepts, 2000-2009," *Library & Information History*, 26 1 (March 2010) p. 83-97. The examples provided below are drawn but from a few examples of scholarly work on the history of "information society," but those curious have a wealth of texts available. A good introductory text for historians is W. Boyd Rayward ed., *European Modernism and the Information Society: Informing the Present, Understanding the Past, (Burlington, VT: Ashgate, 2008)*. For those seeking a more detailed work, they may wish to consult Peter Burke's works, *A Social History of Knowledge: From Gutenberg to Diderot*, (Cambridge: Polity Press, 2000) and *A Social History of Knowledge II: From the Encyclopédie to Wikipedia*, (Cambridge: Polity Press, 2012).

3 The plural form of medium – not media as it is popularly understood today in reference to the agencies of mass communication common since the advent of television.

4 In dealing with this term "information war" as described above, we must specifically avoid discussing the second tier effects cyber operations may have, which include potential kinetic effects.

5 Ann M. Blair, *Too Much to Know: Managing Scholarly Information before the Modern Age*, (New Haven: Yale University Press, 2010) p. 6. See also Richard Yeo, *Encyclopaedic Visions: Scientific Dictionaries and Enlightenment Culture* (Cambridge, 2001).

6 Ibid, p. 11-12, 47.

7 Ibid, p. 205-206.

8 Erasmus, *The Adages of Erasmus*, tr. Margaret Mann Phillips, ed. Williarm Barker, (Toronto: University of Toronto Press, 2001) p. 145, as quoted in Blair, Too Much to Know, p. 55, ft 198.

9 Ann Blair, "Reading Strategies for Coping with Information Overload ca.1550-1700," *Journal of the History of Ideas*, (64.1 January 2003) p. 11-28; and Reinhard Wittman, "Was There a Reading Revolution at the End of the Eighteenth Century?" in *A History of Reading in the West*, ed. Cavallo and Chartier (2003), p. 284-312.

10 Blair, Too Much to Know, p. 60.

11 Ibid, p. 263.

12 Arthur Jay Klinghoffer, *The Power of Projections: How maps reflect global politics and history*, (Westport, Conn.: Praeger, 2006) p. 30.

13 Jeremy Black, "A Revolution in Military Cartography?: Europe 1650-1815," The *Journal of Military History*, Vol.73.1 (January 2009) 61-62. Black correctly relates his argument to the history of "information society" referred to above, citing M. Poovey, *A History of the Modern Fact: Problems of Knowledge in the Sciences of Wealth and Society* (Chicago: University of Chicago Press, 1998); D.R. Headrick, *When Information Came of Age: Technologies of Knowledge in the Age of Reason and Revolution, 1700-1850* (Oxford: Oxford University Press, 2000); E. Higgs, *The Information State in England* (Basingstoke, U.K.: Palgrave Macmillan, 2004).

14 Black, "A Revolution in Military Cartography, p. 61.

15 Klinghoffer, *The Power of Projections*, p. 12-13.

16 Ibid, p. 76-78, p. 120-122.

17 See G. Henrik Herb, *Under the Map of Germany: Nationalism and Propaganda, 1918-1945*, (London: Routledge, 1996). Those interested in further examples may wish to consult Peter Barber and Tim Harper, *Magnificent Maps: Power, Propaganda and Art*, (London: British Library, 2010).

18 For a brief but informative list of definitions, see Daniel T. Kuehl, "From Cyberpsace to Cyberpower: Defining the Problem," in Franklin Kramer et al. eds., *Cyberpower and National Security*, (Washington D.C.: National Defense University Press, 2009) p. 26-27.

19 Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, (Cambridge, MA: Cambridge University Press, 2007) p. 8-9.

20 Kuehl, "From Cyberspace to Cyberpower," 29. Kuehl adds in a footnote that the crucial element of this definition is interconnectivity, a point which he expands in more detail in relation to Information Operations in Dan Kuehl, "Introduction: "Brother, Can You Spare Me a DIME?," in Leigh Armistead ed., *Information Warfare: Separating Hype from Reality*, (Washington, DC: Potomac Books, 2007) p. 1-4.

21 US Department of Defense, *Quadrennial Defence Review*, February 2010, p. 37

22 For an overview of who might be responsible, see Gadi Evron, 'Authoritatively, Who was Behind the Estonian Attacks?' Darkreading, 17 March 2009. See also, Gadi Evron, 'Battling Botnets and Online Mobs', *Science & Technology* (Winter/Spring 2008), p. 121–8.

23 See Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm and Liis Vihul, *Cyber Attacks against Georgia* (Tallinn: CCDCOE 2008) 12. For more information on the Georgian attacks, see Jose Nazario, 'Georgia DDoS Attacks – A Quick Summary of Observations', Security to the Core (Arbor Networks), 12 Aug. 2008.

24 Additionally, the authors profile an attack on U.S. and NATO websites in 1999 after the accidental bombing of the Chinese Embassy in Belgrade, a July 4, 2009 attack on U.S. and South Korean websites.
Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to do about it*, (New York: Harper Collins, 2010) p. 13-20.

25 Jay Rockfeller and Olympia Snowe, "Now is the time to prepare for Cyberwar," *Wall Street Journal*, April 2, 2010.

26 Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Working Paper Mercatus Centre*, George Mason University (April 2011), p. 1.

27 Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol.35.1, p. 29.

28 Adam P. Liff, "Cyberwar: A new 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol.35.3, p. 429.

29 James Jay Carafano, *Wiki at War: Conflict in a Socially Networked World*, (College Station, TX: Texas A&M University Press, 2012) p. 20.

30 Martin C. Libicki, "Cyberspace is not a Warfighting Domain," *Journal of Law and Policy for the Information* Society, Vol.8.2 (2012) p. 326.