Friending Enemies and Influencing People

Identifying and Examining Issues in the Use of Social Media for CF Influence Activities

Neil O'Reilly
Royal Military College of Canada

DRDC CORA CR 2011-081
June 2011

Defence R&D Canada
Centre for Operational Research & Analysis

Strategic Analysis Section

National Defence Défense nationale

Canada

Friending Enemies and Influencing People

Identifying and Examining Issues in the Use of Social Media for CF Influence Activities

Neil O'Reilly
Royal Military College of Canada

Prepared By:
Neil O'Reilly
Royal Military College of Canada
PO Box 17000
Stn Forces
Kingston Ontario
K7K 7B4
Royal Military College of Canada
Contractor's Document Number: RMCC SLA #2009-0302-SLA-PR10023
Contract Project Manager: Dr. Michael Hennessy, 613-541-6000 x 6845
PWGSC Contract Number:
CSA: Neil Chuka, Defence Scientist Strategic Analyst

Defence R&D Canada – CORA

Contract Report
DRDC CORA CR 2011-081
June 2011

Principal Author

Original signed by Neil O'Reilly

Neil O'Reilly

Royal Military College of Canada

Approved by

Original signed by Gregory Smolynec, PhD

Gregory Smolynec, PhD

Section Head Strategic Analysis

Approved for release by

Original signed by Paul Comeau

Paul Comeau

Chief Scientist

This work was conducted on behalf of applied research project 12QR "Influence Activities Capability Assessment". The research was supervised at RMCC by Dr. Michael Hennessy, Dean of Continuing Studies.

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

This report provides an overview of potential policy, legal, and procedural issues facing the use of social media and social networking tools by the Canadian Forces (CF) for Influence Activities (IA) purposes. What is most important is the nature of the medium as forum, insomuch as it is user driven, widely accessible, instantaneous, and, in order to succeed, popular. With the built in audience as user, these technologies present an opportunity for a user to target an audience simply by being a member of that online community. Thus, for those interested in promoting a particular message, be it marketing firms, political organizations, or common interest groups, social networking and social media cannot be ignored. The aim of this paper is to examine current usage of social networking tools in order to expose any potential procedural, policy, or legal issues that would affect the employment of such tools by the CF. In general, the paper finds that while certain policy, legal, and doctrinal issues do exist, none appear to be severe enough to seriously hinder the use of such tools by the CF for a variety of purposes. In fact, the greatest hindrance may be acceptance of the fact that the use of such tools requires relinquishing control of a message to a certain degree. Findings of the report show that, while more detailed work needs to be done in specific areas touched on by the study, the CF and DND should adopt social media and social networking as a force multiplier for IA, but need to develop streamlined, modern, comprehensive and clearly articulated policies and procedures if these tools are to be used effectively.

Résumé

Ce compte rendu présente un aperçu des questions pouvant être soulevées sur le plan politique, juridique et des procédures en ce qui concerne l'utilisation des médias sociaux et des outils de réseautage social par les Forces canadiennes pour la tenue d'activités d'influence. Ce qui importe le plus, c'est la nature du média utilisé comme tribune, d'autant qu'il est adapté aux utilisateurs, qu'il est largement accessible et instantané et qu'il est, afin d'être fructueux, populaire. Étant donné que les membres de l'auditoire de ces médias en sont aussi les utilisateurs, ces médias permettent à un utilisateur de cibler un auditoire simplement en devenant membre de sa communauté virtuelle. Ainsi, les groupes intéressés à faire passer un message, qu'il s'agisse d'entreprises de marketing, d'organisations politiques ou de groupes d'intérêts communs, ne peuvent pas ignorer les sites de réseautage social et les médias sociaux. Cet article examine donc l'utilisation actuelle des outils de réseautage social afin de mettre en lumière toutes les questions sur le plan politique, juridique et des procédures pouvant nuire à l'utilisation de ces outils par les Forces canadiennes. En gros, cet article conclut que malgré l'existence de certaines questions sur le plan politique, juridique et de la doctrine, aucune de ces questions ne semble suffisamment grave pour nuire sérieusement à l'utilisation de ces outils à diverses fins par les Forces canadiennes. En fait, le plus gros obstacle à contourner pourrait plutôt être l'acceptation du fait que l'utilisation de ces outils exige de renoncer dans une certaine mesure au contrôle exercé sur le message véhiculé. Le compte rendu conclut que même s'il faut étudier plus en profondeur certains des sujets abordés par l'étude, les Forces canadiennes et le ministère de la Défense nationale devraient se servir des médias sociaux et des outils de réseautage social afin de multiplier les effets de leurs activités d'influence; ils devront toutefois élaborer des procédures et

des politiques concises, à jour, exhaustives et clairement structurées pour pouvoir utiliser efficacement ces outils.

Executive summary

Friending Enemies and Influencing People: Identifying and Examining Issues in the Use of Social Media for CF Influence Activities

Neil O'Reilly; DRDC CORA CR 2011-081; Defence R&D Canada – CORA; June 2011.

The emergence of Web 2.0 technologies has opened a new frontier for the free flow of communication and exchange of ideas and opinion. It is not only about reaching a wide audience; it is also about the audience reaching you. Web 2.0 technologies provide a multiple agent communication device between the original creators (or posters) of information, the responders to that information, and the collection of contributors to the overall knowledge base. Singular voices and ideas become intertwined with others in the ether of the internet. Radical or otherwise marginalized individuals can meet like minded people, or, perhaps more insidiously, create like minded people if their ideas, no matter how perverse, can resonate with an audience. The content of communication exchange may not necessarily be well grounded in anything more than opinion, rumour, heresy, or conjecture, with all the biases and misconceptions inherent therein. However, with social networking technologies, the medium of transmission and exchange is as important as the message itself. That is to say, the interactive nature of the medium makes the user/contributor both empowered in having a voice, and included in a community of participants, who, through their discourse, come to define the message.

Contributors to social networking and social media sites are also the audience of those sites. With this, the user base of any particular social media platform can simultaneously be considered the target audience of that site, or social media platform. What is most important is the nature of the medium as forum, insomuch as it is user driven, widely accessible, instantaneous, and, in order to succeed, popular. With the built in audience as user, these technologies present an opportunity for a user to target an audience simply by being a member of that online community. Thus, for those interested in promoting a particular message, be it marketing firms, political organizations, or common interest groups, social networking and social media cannot be ignored.

For these reasons, the Canadian Forces (CF) cannot afford to overlook social media and social networking tools for Influence Activities (IA) purposes during expeditionary operations and for Public Affairs (PA) purposes. IA is defined within the Canadian Forces Land Operations Manual as "An activity designed to affect the character or behaviour of a person or a group as a first order effect."[1] The aim of this paper is to examine current usage of social networking tools in order to expose any potential procedural, policy, or legal issues that would affect the employment of such tools by the CF. In general, the paper finds that while certain policy, legal, and doctrinal issues do exist, none appear to be severe enough to seriously hinder the use of such tools by the CF for a variety of purposes. In fact, the greatest hindrance may be acceptance of the fact that the use of such tools requires relinquishing control of a message to a certain degree.

[1] Department of National Defence Land Operations Manual, B-GL-300-001/FP-001, January 1, 2008, Chapter 5, Section 6 (506).

Sommaire

Friending Enemies and Influencing People: Identifying and Examining Issues in the Use of Social Media for CF Influence Activities

Neil O'Reilly; DRDC CORA CR 2011-081; R & D pour la défense Canada – CORA; juin 2011.

L'arrivée des technologies Web 2.0 a éliminé de nouvelles frontières en faveur de la libre transmission des communications et des échanges libres d'idées et d'opinions. Ces technologies ne permettent pas seulement de rejoindre un vaste auditoire : elles permettent aussi à l'auditoire de nous rejoindre. Les technologies Web 2.0 offrent en effet une plateforme de communication à agents multiples entre les créateurs de l'information (ou ceux qui publient l'information), les personnes qui répondent à l'information publiée et l'ensemble des personnes qui contribuent à la base de connaissances globale. Les opinions et idées singulières s'entremêlent ainsi aux autres opinions et idées véhiculées dans Internet. Cela permet aux individus radicaux, sinon marginalisés, de communiquer avec des gens qui partagent leurs opinions ou, peut-être de façon plus insidieuse, de convaincre d'autres personnes d'adopter leurs idées, qu'importe combien perverses elles puissent être, si ces idées interpellent l'auditoire. Le contenu des communications échangées ne repose pas nécessairement sur des bases solides. Il peut en effet se fonder sur de simples opinions, sur des rumeurs, sur des idées hérétiques ou sur des conjectures et ainsi s'accompagner de points de vue tendancieux et de fausses idées. Cependant, grâce à la technologie du réseautage social, le média de transmission et d'échange d'information devient aussi important que le message lui-même. En d'autres termes, la nature interactive du média permet aux utilisateurs et aux contributeurs de s'exprimer et de faire partie d'une communauté de participants qui, par le biais de leurs discussions, en viennent à définir un message.

Les contributeurs aux sites de réseautage social et aux sites des médias sociaux forment également l'auditoire de ces sites. De ce fait, les utilisateurs de tous les sites des médias sociaux peuvent être simultanément considérés comme l'auditoire de ces mêmes sites. Ce qui importe le plus, c'est la nature du média utilisé comme tribune, d'autant qu'il est adapté aux utilisateurs, qu'il est largement accessible et instantané et qu'il est, afin d'être fructueux, populaire. Étant donné que les membres de l'auditoire de ces médias en sont aussi les utilisateurs, ces médias permettent à un utilisateur de cibler un auditoire simplement en devenant membre de sa communauté virtuelle. Ainsi, les groupes intéressés à faire passer un message, qu'il s'agisse d'entreprises de marketing, d'organisations politiques ou de groupes d'intérêts communs, ne peuvent pas ignorer les sites de réseautage social et les médias sociaux.

Pour ces raisons, les Forces canadiennes ne peuvent pas se permettre de passer outre les médias sociaux et les outils de réseautage social pour la tenue de leurs activités d'influence durant les opérations expéditionnaires ainsi que pour les besoins des Affaires publiques. Le manuel *Opérations terrestres* des Forces canadiennes définit ainsi les activités d'influence : « Activité conçue pour influer sur le caractère ou le comportement d'une personne ou d'un groupe à titre

d'effet de premier ordre. »[2] Cet article examine l'utilisation actuelle des outils de réseautage social afin de mettre en lumière toutes les questions sur le plan politique, juridique et des procédures pouvant nuire à l'utilisation de ces outils par les Forces canadiennes. En gros, cet article conclut que malgré l'existence de certaines questions sur le plan politique, juridique et de la doctrine, aucune de ces questions ne semble suffisamment grave pour nuire sérieusement à l'utilisation de ces outils à diverses fins par les Forces canadiennes. En fait, le plus gros obstacle à contourner pourrait plutôt être l'acceptation du fait que l'utilisation de ces outils exige de renoncer dans une certaine mesure au contrôle exercé sur le message véhiculé.

[2] Ministère de la Défense nationale, *Opérations terrestres* , B-GL-300-001/FP-002, 1er janvier 2008, chapitre 5, section 6 (506).

This page intentionally left blank.

Table of contents

This page intentionally left blank.

1 Preface

What exactly is meant by social media? The term itself is new, contentious, fluid, and organic and lacks either a formal or standardized definition. However, for the purposes of this brief a working definition is required. According to Wikipedia, itself an archetype of social media, it is "the use of web based and mobile technologies to turn communication into interactive dialogue."[3] The Wikipedia entry on social media also cites a definition put forth by Andreas Kaplan and Michael Haenlein, which defines social media as "a group of internet based applications that build on the ideological and technological foundations of Web 2.0, which allows the creation and exchange of user generated content."[4] In addition to these there are literally millions of alternative but similar definitions of social media.[5] Despite the variations, there are consistent commonalities in most working definitions. For the purposes of this paper, the author will define social media as internet based applications which: are publicly accessible; where information is user generated and elicits user feedback; function as on-line communities; collapses hierarchical concepts of information exchange; rely on the interaction between its individual users.[6] However, as social media is an evolving concept, so too must be its definition.

The proliferation of social media has been made possible by the evolution of internet technologies and applications. In the wake of the internet Dot Com boom, and beginning shortly after the turn of the century, a new type of internet emerged. No longer was content simply delivered in a one way exchange from a transmitter to a receiver. Information exchange became a two- way, three - way, and multi-participant process. The new, user based information system utilized the World Wide Web as a platform where services and applications were open sourced and shared between individuals. This became known as Web 2.0.[7] Within this loosely defined paradigm of internet usage, the new power of the web became its use as a forum "to harness collective intelligence".[8]

The emergence of social media, and social networking made possible by Web 2.0 technologies has allowed a heretofore unknown capability for individuals to exchange information instantaneously, across the globe, and to virtually any other party that has access to the necessary

[3] "Social Media", Wikipedia, www.wikipedia.org, March 11, 2011. Although the author is loathe to cite Wikipedia as a source, it is, given the nature of this discussion, perhaps one of the most relevant sources of information for disambiguating this matter.

[4] "Social Media", Wikipedia, www.wikipedia.org, citing Kaplan, A, Haelein, H., "Users of the World, Unit! The Challenges and Opportunities of Social Media", *Business Horizons*, Volume 53, Issue 1, January- February 2010, pp.59-68.

[5] A Google search of the question "What is social media?" returned 207, 000, 000 results.

[6] This is a rough amalgamation of various definitions proposed on innumerable websites visited throughout the course of this research. Other definitions may be more exhaustive, and each individual may have their own preferences of precise definitions, which is perfectly fitting with the nature of the concept. The author is not averse to modifying this definition with the addition or availability of new information that would necessitate revisions.

[7] O'Reilly, Tim, "What is Web 2.0: Design patterns and Business Models for the Next Generation of Software", September 30, 2005, p.1. Available at http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1 .

[8] O'Reilly, Tim, "What is Web 2.0: Design patterns and Business Models for the Next Generation of Software", September 30, 2005, p. 2. Available at http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=2 .

technology. The material hardware necessary to engage in social media/social networking information exchange is nearly ubiquitous in developed areas, and not uncommon in less developed areas. Any household or public library computer, personal mobile phone, or any number of recently available digital gadgets will allow an individual to both send and receive information instantly. In environments where the technology is available, information dissemination is literally as easy as clicking buttons. Within this environment, virtually anybody can add to the glut of information that fills the digital world. This allows individuals, regardless of qualifications, to participate in the discourse of real world issues and events by contributing opinion and/or information, factual or otherwise. This information, in turn, has the potential to influence those who access the information, and guide, albeit by varying degrees, the collective understanding of events that are shaping an environment or situation. In this environment participation is the key to influence.

2 Introduction

The emergence of Web 2.0 technologies has opened a new frontier for the free flow of communication and exchange of ideas and opinion. It is not only about reaching a wide audience; it is also about the audience reaching you. Web 2.0 technologies provide a multiple agent communication device between the original creators (or posters) of information, the responders to that information, and the collection of contributors to the overall knowledge base. Singular voices and ideas become intertwined with others in the ether of the internet. Radical or otherwise marginalized individuals can meet like minded people, or, perhaps more insidiously, create like minded people if their ideas, no matter how perverse, can resonate with an audience. The content of communication exchange may not necessarily be well grounded in anything more than opinion, rumour, heresy, or conjecture, with all the biases and misconceptions inherent therein. However, with social networking technologies, the medium of transmission and exchange is as important as the message itself. That is to say, the interactive nature of the medium makes the user/contributor both empowered in having a voice, and included in a community of participants, who, through their discourse, come to define the message.

Contributors to social networking and social media sites are also the audience of those sites. With this, the user base of any particular social media platform can simultaneously be considered the target audience of that site, or social media platform. For the sake of this paper the particular technologies, such as Facebook, Twitter, or Linkedin, are not as important as the way these technologies work. What is most important is the nature of the medium as forum, insomuch as it is user driven, widely accessible, instantaneous, and, in order to succeed, popular. With the built in audience as user, these technologies present an opportunity for a user to target an audience simply by being a member of that online community. Thus, for those interested in promoting a particular message, be it marketing firms, political organizations, or common interest groups, social networking and social media cannot be ignored.

For these reasons, the Canadian Forces (CF) cannot afford to overlook social media and social networking tools for Influence Activities (IA) purposes during expeditionary operations and for Public Affairs (PA) purposes. IA is defined within the Canadian Forces Land Operations Manual as "An activity designed to affect the character or behaviour of a person or a group as a first order effect."[9] The aim of this paper is to examine current usage of social networking tools in order to expose any potential procedural, policy, or legal issues that would affect the employment of such tools by the CF. In general, the paper finds that while certain policy, legal, and doctrinal issues do exist, none appear to be severe enough to seriously hinder the use of such tools by the CF for a variety of purposes. In fact, the greatest hindrance may be acceptance of the fact that the use of such tools requires relinquishing control of a message to a certain degree.

[9] Department of National Defence Land Operations Manual, B-GL-300-001/FP-001, January 1, 2008, Chapter 5, Section 6 (506).

3 Current Military Use of Social Media

The use of social media by military organizations is not an entirely new phenomenon. The Canadian Army, via the Canadian Army News, has been active in utilizing social media to disseminate its messages. The United States (US) military has recognized the potential of new forms of communication and is currently undertaking pro-active measures to incorporate social media into its overall chest of core capabilities. For example, blogging is mandatory for all students of the US Army Command and General Staff College.[10] US Northern Command, which is responsible for the American continental military response in the event of crisis, is anticipating the use of Twitter as an avenue to direct a domestic target group toward relief facilities during times of emergency.[11] The U.S. Army also has a presence on "Second Life", which serves as a public outreach center, and allows visiting guests, or "avatars", to partake in virtual activities, including skydiving and commanding an Apache helicopter.[12] This usage is geared toward both a domestic and friendly audience. It is, however, clearly designed to promote the interests and a positive image and of the U.S. military. It functions as both a recruitment and information office for any interested party inhabiting the virtual realm, through virtual social interactions.

The use of social media for military/strategic purposes is not exclusive to the traditional purveyors of information control. The power of nation states as the primary proprietors of the control mechanisms of information dissemination "was rapidly lost as technology improved and the means to transmit that information became smaller, faster, cheaper and, consequently, ubiquitous".[13] This is evidenced by recent confrontations between Israel and both Hamas and Hezbollah, respectively. The power of social media came into play most notably in the Israeli-Hezbollah war of 2006 and the incursion into Gaza in December of 2009/January 2010. In both instances social media was utilized by the belligerents, traditional media sources, and civilians who documented their experiences with real time updates to a global audience. Despite enjoying an overwhelming military superiority over its adversaries in both instances, Israel "snatched defeat from the jaws of victory by abrogating the information battlespace."[14] In losing control of the information war, Israel failed to gain support from the international community and, more importantly, allowed its adversaries to turn a crushing military defeat into a moral victory. The information war ultimately strengthened the positions of both Hamas and Hezbollah. Given the types of engagements the CF has been involved in, such as operations in regions of the former Yugoslavia, the current mission in Afghanistan, and most foreseeable engagements, this is a

[10] "Lieutenant General William B. Caldwell IV on New Media in Military Operations", *IO Sphere*, Summer, 2009, p. 26. Available at http://www.au.af.mil/info-ops/iosphere/09summer/iosphere_summer09_caldwell.pdf

[11] Macavoy, Audrey, "Military Uses Social Networking to Reach Public", *The Associate Press,* February 13, 2009.

[12] "Army Debuts Second Life Island, Virtually", www. Army.Mil., December, 2008, Available at http://www.army.mil/-newsreleases/2008/12/10/14966-army-debuts-second-life-island-virtually/.

[13] Murphy, D., "Fighting Back: New Media and Military Operations", U.S. Army War College: Carlisle, PA., November 2008. p.4

[14] Murphy, D., "Fighting Back: New Media and Military Operations", U.S. Army War College: Carlisle, PA., November 2008. p.4 For a more in depth discussion of the use of social media in the Gaza conflict see Ward, Will, "Social Media and the Gaza Conflict", *Arab Media and Society,* www.arabmedianadsociety.com , Issue 7, Winter 2009, Available at http://www.arabmediasociety.com/?article=701

lesson that must be understood and learned. Though Canada and the CF does not face the same challenges as the Israeli Defence Force (IDF), contemporary mission requirements dictate that the CF must be aware of and deal with those parties that are hostile to the Canadian and international presence in an area of operations, communicate effectively the intent of the CF and Canadian Government to an indigenous population, and offer a forum for feedback from and discourse with that population. While none of these problems are new, effective use of social media has the potential to mitigate the attendant problems of such missions.

3.1 The Canadian Forces

The CF and Department of National Defence (DND) have begun to dabble in social media in a domestic context, albeit to a significantly lesser degree than the US or United Kingdom (UK). While there is a vibrant community of personnel within the CF who use social networking for personal use, via sites such as Facebook, Myforces.ca, and the Canadian Forces Social Media Group (GFSMA), the military itself seems to be lagging in exploiting the technologies for official or operational use. There is an active investigation into the use of social networking for the CF.[15] In order to explore the viability of such networks the DND sought outside assistance via Defence and Research Development Canada (DRDC).

DRDC commissioned a study by CAE Professional Services entitled "Virtual Social Networking and Interoperability in the Canadian Forces Netcentric Environment" in 2009.[16] This report suggests that information sharing through social networks would be beneficial in "distributed network environments, such as joint force and multi agency operations where component members are physically dispersed".[17] A large portion of this report is an exhaustive taxonomy of the various social media and social networking tools that are available on the internet, but it is short on recommendations or analysis of how specifically these tools might be used. More importantly, for the aims of this brief, the report centers on the use of social media within the CF, amongst friendly forces, and in conjunction with elements who are co-operating with the CF and its allies.[18] This is anticipated to be a system designed for soldiers, to be used by soldiers communicating with other soldiers and friendly agents. However, networking exclusively amongst friends and allies is not the work of IA practitioners. There is a much greater requirement for, and emphasis on, reaching out to the "other", i.e., those who are not necessarily in agreement with the ends and means of the CF and its associated agencies, as dictated by Canadian government policy. The proposed system is, for all intents and purposes, for those who

[15] Bascaramurty, D., "Forces Eyes Its Own Social Network", *The Globe and Mail*, July 7, 2009, Available at http://www.theglobeandmail.com/news/technology/forces-eyes-its-own-social-network/article1210151/

[16] Pronovost, S., Lai, G., "Virtual Social Networking and Interoperability in the Canadian Forces Netcentric Environment", Defence Research and Development Canada, DRDC Atlantic CR Report 2009-09, July 2009 Available at http://pubs.drdc.gc.ca/PDFS/unc92/p532606.pdf

[17] Pronovost, S., Lai, G., "Virtual Social Networking and Interoperability in the Canadian Forces Netcentric Environment", Defence Research and Development Canada, DRDC Atlantic CR Report 2009-09, July 2009

[18] The report specifically states that it is the first in a series of explorations, yet as of this report, there is no follow up.

are already "in", and excludes those who are "out." It is not useful for getting messages out to target audiences, or for receiving feedback from target audiences for whom information campaigns are directed. Thus, the nature of a system recommended by this report is not adequate to address the needs of IA by the CF, DND, or any associated agency or department.

The Canadian Army, through its Public Affairs office, has taken steps to be more interactive through the use of social media tools. This is in keeping with the principles of IA, as PA is described in the Land Operations Manual as an IA activity that "facilitates the flow of information to various audiences through the media" to enhance understanding.[19] In effect, PA performs an 'inform' vice 'influence' function. The Army, through the *Army News*, has a presence on Youtube, Flickr, Facebook, Twitter, a podcast and Rich Site Summary (RSS) feed, as well as a presence on cable television in certain Canadian areas.[20] The presence of the Canadian Army on Youtube exemplifies the way in which social media is currently being used by the CF. The Canadian Army News Channel provides compilation videos available on the Canadian Army website, with the added feature of allowing commentary from Youtube viewers. Though this is a legitimate attempt at conducting public outreach by the CF, numbers belie the efficacy of this endeavour. There are approximately 2 billion videos watched on Youtube each day.[21] Since the premiere of its presence on Youtube in June of 2008, the Canadian Army News Channel has had 94, 207 views, while clips from the channel have been watched approximately 1, 755, 763 times.[22] However, despite the relatively low numbers of viewership it must be noted that even a quiet presence is better than no presence at all. Additionally, the content available on Youtube is accessible to a global audience that would perhaps not readily investigate the official DND Website. The Canadian Army News channel promotes videos that show the CF in a positive light. As a data mining tool for any potential enemies, they will see the professionalism, and in some cases the firepower of the CF. Any person who views the videos will see, in addition to professionalism and firepower, the CF participating in everything from humanitarian relief operations to the training of Afghan women as Air Force pilots, and even hockey clinics conducted by CF personnel.

The CF presence on Youtube displays many aspects of its capabilities and functions in a positive light. The move from relegating the videos from the official DND website to Youtube has opened the messaging up from a predominantly domestic audience, specifically interested in the work of DND and the Forces, to potentially an international audience who might happen upon the videos in a variety of ways. The Canadian Army Channel on Youtube, and the content it delivers, therefore, depending on who the audience might be, fulfills several functions of IA. For domestic and non-Canadian friendly audiences, it provides an illustration of CF capabilities while for real

---

[19] Department of National Defence Land Operations Manual, B-GL-300-001/FP-001, January 1, 2008, Chapter 5, Section 6, (506-6a).

[20] *Army News*, www.army.forces.gc.ca, Available at http://www.army.forces.gc.ca/land-terre/news-nouvelles/stories-reportages-eng.asp

[21] "Internet 2010 in Numbers", royal.pingdom.com, January 12, 2011, Available at http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/ also consider the Canadian Army News Twitter feed. As of September, 2010, there were 175 million people signed up with Twitter. Of these, the Canadian Army has 966 followers.

[22] Canadian Army News Channel, www.youtube.com, Available at http://www.youtube.com/user/CanadianArmyNews . Figures taken at time of writing, and subject to change.

or potential enemies it may have some type of influence on their thinking.[23] The Canadian Army Channel is a PA tool for friendly and domestic audiences, and may act as an influence tool if it dissuades potential enemies from confronting the CF or taking up arms. In effect, the content is designed to inform and, implicitly, persuade viewers of the power, professionalism and meritorious work of the Canadian Army. As such, it can affect understanding and perceptions and hopefully, under certain circumstances, the will of the recipient of the message, to affect "behaviour in the desired manner."[24] The presence of the CF on Youtube does in some ways fit the definition laid out in the CF Land Forces Operations Manual regarding IA, in so much as it can "persuade, convince, deter, disrupt, compel or coerce" an audience.[25] However, it lacks the necessary condition of being targeted or designed with the specific intention of seeking to "create a direct, first order effect of influencing a target audience".[26]

The Army news is a product of PA, designed to inform a domestic audience and other members of the Forces, and vetted for content to ensure security.[27] Ultimately, what distinguishes the Army News from being an explicit IA operation is the specific targeting of an audience. Though it meets the mandate of PA, and provides a forum to disseminate messages of, for, and about the Canadian Army, it is a generic form that, while using the tools of social media in a context that could easily fit IA requirements, is not designed to target a specific audience in support of any particular operation or overall mission.

3.2 Issues to Consider

The purpose of this paper is to consider various aspects of the use of social media and social networking in IA operations by the CF and potential legal issues surrounding social media/social networking are the first that need to be considered. Because social media is so new, many questions regarding the nature of legalities relating to this issue remain unanswered. In fact, many of the questions regarding the legalities surrounding social media have yet to be asked. Within the context of IA there are even more variables that must be entertained than would be the case of social media in a unorganized, domestic or civilian setting. Within a military context, social media must be considered according to its own rules of engagement because of the unique virtues of the technologies and their applications. What are the legal considerations of using social media as a tool of IA? Under what jurisdiction would IA operations using social media fall? Are there existing legal constraints? Is there consensus on what is appropriate? How do the rules apply, and to whom? Up to this point there is a dynamic discussion taking place over the legal implications of social media. Many of these are questions of tort and procedural law.

[23] DND/CF Public Affairs Headquarters has denied that there is any IA objective, intent or connection to the Canadian Army News. This would be consistent with the mandate of CF PA. E-mail exchange with LCol. Sarto LeBlanc, DA Public Affairs, March 24, 2011.
[24] Department of National Defence, "Counter Insurgency Operations", B-GL-323-004/FP-003, December 13, 2008, Chapter 8, Section 1(2).
[25] Department of National Defence, "Land Operations Manual", B-GL-300-001/FP-001, January 1, 2008Chapter 5, Section 2(506-2).
[26] Department of National Defence, "Land Operations Manual", B-GL-300-001/FP-001, January 1, 2008Chapter 5, Section 2(506-3).
[27] E-mail exchange with LCol. Sarto LeBlanc, DA Public Affairs, March 24, 2011.

Rules concerning the use of social media tend to be ad hoc, but following guidelines previously set down in both criminal and civil courts that deal with anything from defamation to the use of individual network accounts as evidence.[28] Essentially, the legal community is playing catch up, though there is now a small but growing field in the study of legal considerations when dealing with social media.

Within the public domain, issues regarding individual privacy remain the most prominent legal dilemma. In 2009, at the behest of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), Canada's federal Office of the Privacy Commissioner (OPC) launched an investigation into the practices of Facebook.[29] The OPC's interest in the matter stemmed from allegations by the CIPPIC that Facebook was in violation of Canadian law under the Personal Information Protection and Electronic Documents Act (PIPEDA).[30] The result of the investigation was a compromised agreement between the OPC and Facebook concerning the establishment of new protocols for privacy settings. As result of the process, the OPC concluded that the case illustrated "how PIPEDA privacy protections are flexible enough to be easily applied to new technologies" and strike a balance between the rights of users and the interests of business.[31] This case is important because it involved the Government of Canada acting against an internet service provider to reconcile Canadian legal statutes with a social media forum. It set the precedent for future considerations of the application of Canadian law to social media. If the CF is going to engage in social media and more importantly if it is going to use social media for specific ends, then it is necessary to consider how the technologies have, can, and do conform to and/or deviate from Canadian law. More particularly, it is necessary to consider the terms and use of each particular technology, and to cross reference that with existing laws and the particular requirements of the Forces.

In order to determine if the use of a particular tool for the purposes of IA is feasible, practical, and does not come at the expense of other requirements, it is imperative to understand the legal responsibilities of the administrators of a social media and/or social networking forum, and the rights of the user. If the CF wishes to use social media through conventional, pre-established networks such as Facebook, Twitter, or any other number of internet applications, it must be assumed that any information given, whether for registration to the site, or that which is posted, is no longer controlled or protected by the CF/DND or any of its affiliates. Information cannot be removed once it has been posted. For example, according to Facebook's Privacy Policy, it may collect information from users from their electronic devices such as "browser type, location, and

[28] Ossian, K., "Legal Issues in Social Networking", *Miller, Canfield, Paddock and Stone PLC,* April 2009, available at http://www.millercanfield.com/media/article/200120_LEGAL%20ISSUES%20IN%20SOCIA%20NETWORKING.pdf

[29] Stoddart, J., "Remarks at a Press Conference on the Facebook Investigation", Officer of the Privacy Commissioner of Canada, August 27, 2009, Available at http://www.priv.gc.ca/speech/2009/sp-d_20090827_e.cfm

[30] Davies, A., "Social Media: 3. Privacy and the Facebook Example", Parliament of Canada, Publication No. 2010-06E, February 8, 2010, Available at http://www2.parl.gc.ca/Content/LOP/ResearchPublications/2010-06-e.html

[31] Davies, A., "Social Media: 3. Privacy and the Facebook Example", Parliament of Canada, Publication No. 2010-06E, February 8, 2010.

IP address", as well as a record of web pages visited.[32] Facebook is just one example, albeit the most prominent, of the abdication of certain rights by users when utilizing the medium. Linkedin, in its user agreement, states explicitly that any content posted may be used by Linkedin for any purposes that it decides.[33] Obviously the use of such networks by the CF in an official capacity must be well considered, taking into account not only such things as operational security, but its own images, logos and trademarks. In this case, legal authority for information provided by users falls with the provider of the service. If the poster of the information can be both digitally tracked and observed, and relinquishes control over content posted, then questions of privacy and dissemination of information and content, at least in the user- server relationship, are moot. Law is on the side of the server in such relationships.

Copyright is one of the leading issues of contention when considering the use of social media. Here the waters are murky at best, and for the most part opaque. First of all, is this a matter for consideration in the use of social media for IA? Generally speaking, the users of social media are responsible for content disseminated through their personal accounts. Use of third party content, such as photos or songs, or posting photos or videos of people without their permission can result in liability based on breach of individual privacy rights.[34] The rules governing usage and copyright are, however, subject to the statutes of independent nations. While there are certain bi-lateral and multi-lateral agreements on copyright law between nations, "no international copyright law exists".[35] As such, any content posted is subject to the copyright laws of each individual nation. This may be a consideration for the Forces, depending on the targeted area or group of an IA operation. It must be conceded that many current and foreseeable deployments by the CF, and attendant IA operations, occur in areas where the rule of law is either lacking or non-existent. In these areas copyright issues are the least of a plethora worries for affected individuals. However, in such environments, false reproductions of material, images or information disseminated by the CF or DND can proliferate with little consequence. This is an important issue to consider in image management. If an individual agent or group uses the voice and/or likeness of the CF in such environs, it can undermine the Forces, the message being conveyed, and the overall mission. Conversely, the CF must be aware of the images and likenesses of other individuals, groups, or organizations it uses in any disseminated material.

Due to the heightened sensitivity of military applications for social media, there is need for a stricter awareness of what exactly is being published in the public sphere. For example, the Canadian Army News has posted video of the International Sniper Competition, which included personnel from allied and partnering nations, on both the Canadian Army website, and subsequently on You Tube.[36] In this case, it was not as simple as ensuring rights to intellectual properties. In order to broadcast the piece to a public audience, DND had to secure agreement from the governments and armed forces responsible for those soldiers from other nations involved

[32] "Facebook's Privacy Policy", www.facebook.com, December 22, 2010, Available at http://www.facebook.com/policy.php
[33] "Linkedin User Agreement", www.linkedin.com, Section 2(B), March 24, 2010, Available at http://www.linkedin.com/static?key=user_agreement
[34] Ossian, K., "Legal Issues in Social Networking", *Miller, Canfield, Paddock and Stone PLC,* April 2009.
[35] "International Copyright Law", University of Washington Copyright Connection, depts.washington.edu, 2011, Available at http://depts.washington.edu/uwcopy/Copyright_Law/International_Copyright_Law/
[36] Canadian Army News Channel, www.youtube.com

in the competition and appearing in the video to ensure the broadcast respected their operational security (OPSEC) requirements.[37]

This report can only begin the conversation regarding the legal implications of using social media and social networking in IA activities by the CF. There is, as of the time of this writing, seemingly no codified system explicitly concerning social media/social networking in Canadian Juris Prudence, though cases that do arise tend to be built upon existing laws and precedence.[38] Any consideration of the legalities of using social media or social networking by the CF in operations must be referred, ultimately, to DND's Directorate of Law/ Intelligence and Information Operations.[39] This directorate is responsible for the analysis and interpretation of Canadian domestic, foreign, and international law, and the provision of the development of legal policies "in relation to Intelligence and Information Operations" at the tactical, operational and strategic levels.[40] Thus, they are responsible for vetting the legal requirements of any potential IA activity, using social media or otherwise, undertaken by the CF.

3.3 Current Policy

Canadian government policies on the usage of the internet, and especially those regarding DND and the CF, are labyrinthine. DND has outlined its policy on internet usage as both an order for members of the CF and a directive for civilian employees. The DND policy on internet usage reads as such: "The Internet shall be used only in support of legitimate operational and business requirements".[41] There are several levels of administration tasked with implementing this policy. The Assistant Deputy Minister of Information Management (ADM (IM)) is responsible for providing "direction, military operations support, and products and services to manage information".[42] Chief Review Services (CRS), Office of the Judge Advocate General (JAG) and the Assistant Deputy Minister of Public Affairs (ADM(PA)) are tasked with providing legal, technical and other advice, as per each respective departments area of responsibility.[43] Level 1 advisors and/or commanding officers can then appoint a member of the Internet Office of Primary Interests (I(OPI) to publish information on the internet.[44]

---

[37] E-mail exchange with LCol. Sarto LeBlanc, DA Public Affairs, March 24, 2011.

[38] Extensive (though not exhaustive) research has shown that the legal world cannot keep apace of the technology, but must react to the resulting issues. See the Canadian Internet Policy and Public Interest Clinic at www.cippic.ca , Dr. Michael Geist's blog at www.michaelgeist.ca, Office of the Privacy Commissioner of Canada at www.priv.gc.ca, or innumerable sites owned by private law firms.

[39] Department of National Defence, "Directorate of Law/ Intelligence and Information Operations", www.forces.gc.ca, July 28, 2010, Available at http://www.forces.gc.ca/jag/oplaw-loiop/dlawiio-djroi-eng.asp

[40] Department of National Defence, "Directorate of Law/ Intelligence and Information Operations", www.forces.gc.ca, July 28, 2010, Available at http://www.forces.gc.ca/jag/oplaw-loiop/dlawiio-djroi-eng.asp

[41] Department of National Defence, "DAOD 6001-0, Internet", www.forces.gc.ca , February 12, 1999. Available at http://www.admfincs.forces.gc.ca/dao-doa/6000/6001-0-eng.asp .

[42] Department of National Defence, "National Defence and the Canadian Forces: About Us", www.forces.gc.ca, August 15, 2006, Available at http://www.img.forces.gc.ca/au-ns/index-eng.asp .

[43] Department of National Defence, "DAOD 6001-0, Internet", www.forces.gc.ca, February 12, 1999

[44] Department of National Defence, "DAOD 6001-0, Internet", www.forces.gc.ca, February 12, 1999

Information that is to be published must adhere to the guidelines laid out in a set of directives and orders specific to internet publishing. *Defence Administration Orders and Directives (DAOD) 2008-6: Internet Publishing* stipulates that information disseminated on the internet by members of the CF in an official capacity must adhere to a slew of official government policies and procedures, including: the M*anagement of Government Information Holdings (*MGIH) *Policy; Copyright Act; Treasury Board Policy on Using The Official Languages on Electronic Networks; Internet Corporate Standards of the Department of National Defence and the Canadian Forces;* the aforementioned DND and CF *Internet Policy Use; DAOD 6000-0 Information Management; DAOD 6003-3 Records Management and Disposition Policy; Privacy Act; Canada Evidence Act; National Defence Act; Official Secrets Act; Information Systems Security Internet Connections Guidelines; Interim Internet Acceptable Use Policy;* and the *DND Internet Web Publishing Standards (IMS 513.10).*[45] Additionally, any official publication on the internet by a Canadian governmental agency must conform to the Treasury Board's *Common Look and Feel for the Internet 2.0* policy guidelines.[46] The *Internet Publishing* guidelines apply to information dissemination on "policies, programs, services, operations, activities and or initiatives" for an "external or internal audience" by DND and the CF.[47] These policy guidelines are accompanied by a nine step procedure to be followed by managers and commanders, Public Affairs Officers (PAO), web administrators, and the IOPI.[48] As such, the policy guidelines for any IA activity utilizing social media are laid out (albeit not so clearly) in official Canadian Government and DND/CF policies concerning the use of the internet and internet publishing. Though the only subset IA capability referred to in the documents is PA, an inference can be made that rules governing the use of social media for other IA activities in official applications would subscribe to similar guidelines. It must also be noted that DAOD 2008-6 was issued in January of 1998. While this order and directive was modified in 2008, its applicability to the most up to date and forthcoming technologies must be considered.

Another set of general orders applies primarily to the use of social networking and social media by soldiers, seamen and airmen of the CF. Canadian Forces General Order (CANFORGEN) 136-06. Stipulates that CF members must check with the chain of command before "publishing CF related information and imagery on the internet".[49] While this general order is ostensibly directed at individuals using social media in an unofficial capacity, it does reference potential uses of the medium in an IA capacity by members of the Forces. For example, Articles 5 and 6 of the order refer to the sharing of information with third parties and the media.[50] Article 6, specifically,

---

[45] Department of National Defence, "DAOD 2008-06: Internet Publishing", www.forces.gc.ca, December 18, 2008, Available at http://www.admfincs.forces.gc.ca/dao-doa/2000/2008-6-eng.asp .

[46] Treasury Board of Canada Secretariat, "Common Look and Feel for the Internet 2.0", www.tbs-sct.gc.ca, February 8, 2010, Available at http://www.tbs-sct.gc.ca/clf2-nsi2/index-eng.asp .

[47] Department of National Defence, "DAOD 2008-06: Internet Publishing", www.forces.gc.ca, December 18, 2008, Available at http://www.admfincs.forces.gc.ca/dao-doa/2000/2008-6-eng.asp .

[48] Department of National Defence, "DAOD 2008-06: Internet Publishing", www.forces.gc.ca, December 18, 2008.

[49] "Canadian Military Blogging", Army.ca, posted September 20, 2006, Available at http://forums.army.ca/forums/index.php/topic,50598.msg447866.html#msg447866

This blog on the Army .ca forum posted CANFORGEN 136-06 in its entirety for use by members of the military.

[50] "Canadian Military Blogging", Army.ca, posted September 20, 2006.

states that PA will "ensure the appropriate management and release of information".[51] While this directive was issued primarily for OPSEC considerations, it also has consequences for the "branding" of the CF. Brand can here be described as "perceptions people have of [a] product".[52] Any use of social media by a member of the Forces, who can be identified as such, will reflect on the CF as a whole. In such a case, the unintentional use of information can affect the "brand", which in turn can affect the perceptions, attitudes, and potential behaviours of those who receive the information.

As the aim of IA is to "focus on promoting perceptions, attitudes and understanding that influence will", management of the image of the CF is paramount to IA activities.[53] In this regard, the OPSEC considerations of CANFORGEN 136-06 also serve to help control the image of the CF. The policy of having information vetted by a superior and/or filtered through PA ensures quality control of information release. More importantly, for the purposes of IA, this can serve to control what particular image of the CF is released. Usage in this manner may represent an alternative form of the traditional application of demonstrative fires. For example, and as per Chapter 5, Section 506(11b) of the Land Operations Manual, displays of "fires", or Canadian firepower on sites such as Youtube, or even individual soldiers Facebook or home pages, may dissuade individuals who view these sites from becoming belligerents, or belligerents from taking action, in areas where the CF is known to be operating.[54] Soldiers, who recount their personal experiences of helping earthquake victims in Haiti, or Civil Military Cooperation (CIMIC) activities in Afghanistan, can help support an image of the CF as a benevolent force, thereby ingratiating itself to communities who may initially be wary of foreign forces. These stories will have a greater impact if they are not seen to be "official" accounts, or sound bites, but actual human stories told from individual perspectives.

If the CF chooses to use social media/social networking as a tool of IA, the information released through unofficial forums can fully support the ends and aims of an operation. Equally important, information released by members of the CF in an unofficial capacity on social networking sites, blogs, or through other internet forums, must not be in contradiction to the message being promoted by the CF through IA activities. In this regard, CANFORGEN 136-06, when properly adhered to and enforced, helps to ensure that all parties and components of the CF are releasing information in support of, or at least not in contradiction to, the same desired ends.

[51] "Canadian Military Blogging", Army.ca, posted September 20, 2006.

[52] Helmus, T., Paul, C., Glenn, R., "Enlisting Madison Avenue: The marketing Approach to Earning Popular Support in Theatres of Operation", RAND Corporation, 2007, p. 70.

[53] Department of National Defence, "Land Operations Manual", B-GL-300-001/FP-001, Chapter 5, Section 2(506-7).

[54] Department of National Defence, "Land Operations Manual", B-GL-300-001/FP-001, Chapter 5, Section 2(506-11b). Such displays are in abundance on Youtube and Liveleak. Though there is much more material posted exhibiting US capabilities, there is no lack of Canadian content.

3.4 Current Procedures

Contained within the policy documents concerning internet use and publication discussed above are certain vague descriptions of procedures to be followed by members of DND, the Forces, employees of agencies falling under the auspices of DND, and contractual employees of these organizations. For instance, and as has previously been mentioned, PA has a nine step procedure to follow before information can be posted to a site, and to ensure quality control and maintenance of a site.[55] However, with the exception of CANFORGEN 136-06, there are no guidelines detailing content, or the presentation of content. Even with this, it must be conceded that the procedure outlined in CANFORGEN 136-06 simply amounts to checking for permission or clearance from higher ups before posting anything.

Essentially, while there is an internet policy (albeit based on pre-Web 2.0 applications, technologies and uses) for the Forces, there is no developed procedure for the use of social media by the CF, except that which is loosely outlined for PA. This should be seen in contrast to the social media/social networking policies of the United States military and its separate branches. The US Marines have released a highly detailed and comprehensive procedural manual for the use of social media by Marines that includes such things as a focus on "building credibility/public trust", acceptance of negative feedback and engagement of dissenting views in support of the Marine position, and to "admit mistakes" when engaged in online exchanges.[56] The US Navy has no less than four official manuals and handbooks guiding the use of social media/social networking and Web 2.0 technologies.[57] The US Department of Defence (DOD) has issued a memorandum entitled "Responsible and Effective use of Internet-Based Capabilities" which acknowledges that internet based capabilities, including social networking, are "integral to operations".[58] The British Ministry of Defence (MOD) has released policy and procedural manuals for both commanders and media/communications staff.[59] The MOD also has an online "Defence Social Media Hub", which includes both social media/social networking applications, and contains documents on policy and procedure for members of the UK forces specifically

---

[55] Department of National Defence, "DAOD 2008-06: Internet Publishing", www.forces.gc.ca, December 18, 2008.

[56] United States Marine Corps, "Social Media Standard Operating Procedures", www.usmc.mil, Available at http://www.usmc.mil/usmc/Pages/SocialMediaGuidance.aspx . The USMC has an official presence on 262 different social media and social networking websites.

[57] Boudreaux, C., "Policy Database", *Social Media Governance*, socialmediagovernance.com, 2009, Available at http://socialmediagovernance.com/policies.php . This is a large database of social media/social networking policy and procedural guidelines and manuals from government agencies (municipal, provincial state and federal), private businesses and corporations, IGO's and NGO's. It is very effective for both finding and cross referencing procedures for the currently 164 organizations listed.

[58] Department of Defence, "Responsible and Effective Use of internet Capabilities", Directive Type Memorandum (DTM) 09-026, February 25, 2010, updated February 25, 2011. Available at http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf

[59] Ministry of Defence, "The Defence Online Engagement Guidelines", DMC-PR-05-07-02, August 5, 2009, Available at http://www.mod.uk/NR/rdonlyres/D2AC8314-3B15-4DEBA769-6C85AF4BDA80/0/20090805UMODOnlineEngagementGuidelinesVersion10.pdf

regarding social media/social networking. The Americans and the British have concluded that social media/social networking is a tool that should be harnessed and utilized in the overall arsenal of capabilities. Although the DOD, and to the a lesser extent the MOD, enjoy enormous personnel, material and financial advantage over DND and the CF, this is one area where lack of resources does not justify a failure to develop at least a general procedural framework for the use social media, if for no other reason than to maintain operational standards consistent with those of our closest allies.

While it is far beyond the scope of this paper to develop a procedural manual for the incorporation of social media/social networking into an IA doctrine for the CF, there are a few points worthy of consideration for such work by others. Two parallel issues must be considered. The first is the aforementioned development of a CF policy and development of procedure for the use of social media/social networking. Without a formalized policy and procedural framework for this any tasks undertaken will tend to be ad hoc, and borrow from best practices that have been used in application to technologies which are now outdated. What is needed most, and what Canada's allies have recognized, is that the issues regarding social media/ social networking likely require specific investigation and potentially concept development. Secondly, there may be a requirement for some form of TTP-level doctrine for the use of social media for IA purposes.

3.5 Further Issues

This paper has taken a mere glimpse at the legal, policy and procedural issues for the possible use social media/social networking as an IA activity by the CF. There is much more work that can be done in any one of these areas, though that is a project best left to individuals with specialized knowledge and professional expertise in the relevant fields. Though not within the scope of this particular exploration, there are additional points worth mentioning for future consideration.

Social media and social networking does not occupy geographic space. The servers and physical machinery that allow digital communication can be locked down or destroyed, but they can also be bypassed.[60] Social networking/social media does not exist in, or as, a particular machine, program or technology, but in how people choose to use the concepts to exchange information and ideas. While people may be drawn to a site or forum which addresses issues of race, culture, religion or ethnicity, the people who partake in these sites and discussions cannot necessarily be discerned as belonging to any particular group. It is ideas that unite people on social networking sites, and it is ideas, whether shared, discussed or contested, that binds them together. However, while participants in social networks may be ideologically connected, they may also be adversarial to the dominant thinking of a network, or merely interested and passing observers. This may complicate the targeting of audiences for IA activities. Within such a loose organization of individuals, in an abstract space, the targeting of groups, individuals, leaders, and influencers is more complicated than would be the case in a specific, bounded area of operations, or against a clearly defined and articulated adversary, group or population.

[60] This is currently seen in North Africa and the Middle East, as protesters manage to circumvent government lockdowns and controls over communications technologies, from cell phones to the internet. On March 28th, 2011, a Google query of "How to bypass Internet blocks" returned 5, 770, 000 results.

Much of the relevant and recent research into social media/social networking suggests that people lend more credibility to information received from people they know, be it friends or acquaintances.[61] Those wishing to present information online, have this information judged as credible, and thereby influence others, must develop relationships and create rapport in the same manner as would be the case in the physical realm. If this trust is broken, then the information presented, or more importantly the presenter, will lose credibility, the information will not be deemed accurate, and the ability to influence the conversation, or steer attitudes and opinions, may be lost. Misrepresentation, if discovered, undermines the credibility of the poster. In the case of IA, it could undermine the credibility of the mission in particular, and the CF in general. The US military has recently been exposed as having launched a "sock puppet" program, which will allow individual operators to control up to ten online identities, each of which promotes a pro- American viewpoint in online forums.[62] Repercussions from the exposure of this program has not only undermined the potential efficacy of the program or its intended message, but, as one commentator so eloquently stated, also makes the US government appear as if it has "stoop[ed] to the morals of a clumsy Nigerian spammer".[63] The CF would do well to avoid such embarrassments if it is to employ a program of social media/social networking for IA purposes.

One of the problems faced in the development of this brief was finding knowledgeable, credible sources and relevant, accurate information on the concepts and ideas related to social media. A search of various terms and ideas soon betrayed the reality that, though there is an abundance of information available, most of it is based on opinion, self- marketing (aggrandizement) of those selling their social media services, and the preferred practices of private and public organizations as they are consistent with internal policies.[64] "Experts" on the subject of social media/social networking range from the Platonically self-aware of their own ignorance to the delusional messianic, who believe theirs, is the one true path.[65] In considering the use of social media by the

---

[61] Lewis, Rob, "Canadian Social Media Survey- The Results Are In", www.techvibes.com, March 24, 2009, Available at http://www.techvibes.com/blog/social-media-survey-the-results-are-in And Lin, C.Y., Ehlrich, K., Griffiths Fisher, V, Desforges, C., "Small Blue, People Mining for Expertise Search", *Multi Media IEEE*, Vol. 15, issue 1, Jan- March, 2008, p. 78.

[62] Fielding, N, Cobain, I., "Revealed: US Spy Operation That Manipulates Social Media", *The Guardian*, guardian.co.uk., March 17, 2011, Available at http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks Sudan's ruling National Congress Party also claims to have a "cyber battalion", ready to crush dissent and warn people on social networking sites against acts of defiance against the government. See "Sudan to Release Cyber Jihadists", bbc.co.uk, March 23, 2011, Available at http://www.bbc.co.uk/news/technology-12829808

[63] Jarvis,J., "America's Absurd Stab at Systematizing Sock Puppetry", *The Guardian,* guardian.co.uk., March 17, 2011, Available at http://www.guardian.co.uk/commentisfree/cifamerica/2011/mar/17/us-internet-morals-clumsy-spammer .

[64] The author has learned to read most information concerning social media/social networking with a grain of salt and a degree of scepticism. In contrast to time tested and true "best practices" as a basis for doctrine in any number of disciplines, the newness of social media, and the lack of consensus on concepts, norms and terminology, relegate any supposed doctrinal recommendations to "preferred practices", based on the requirements and likes of the individual or organization asserting the position, borrowed from other professions such as marketing or communications, or according to the requirements of the user.

[65] There seems to be a general consensus, though not unanimous, that given the variance in social media/social networking technologies, the quick pace of change, and the newness of the technologies and

CF, it would be best to bare in mind that there are no experts as such, and it is an ongoing experiment being conducted simultaneously, independently and collectively, by hundreds of millions of users. If the CF wants to use social media for the purposes of IA, there is a pool of talent from within the ranks who have been raised with the concepts and spent their formative years utilizing the technologies of social media/social networking. These are the experts.

As has been mentioned at the beginning of this brief, there are as many definitions of social media as there are individuals with the temerity to suggest their own, albeit with regard to certain standards and norms. What this suggests is that the sphere of social media/social networking has not been charted, and it is a world that has only begun to be explored. With this come great opportunities for exploration and development. The CF cannot and should not miss the opportunity to both explore uses for and pioneer innovations in social media and social networking as an IA capability.

concepts, it is impossible to claim expertise in the field as a whole. A Google enquiry of the terms "social media expert" will reveal an impassioned, though mostly one sided, debate.

4 Conclusion

Social Media is a tool to broadcast messages, update previously released information, and perhaps most importantly, respond to queries and criticisms in a timely manner in forums that are seen as non-threatening and comprehensible by the users of those forums. For the purposes of CF activities the use of social media allows a presenter of information to avoid creating pedagogical perceptions that accompany standing behind a podium in a uniform, disconnected from the audience and with suspect intentions. It allows the presenter to be a member of the audience, expressing a common view or concern. As one business executive succinctly stated, use of social media technologies simultaneously "provides a point of contact with the media, a point of contact with the public, and [allows one] to engage in conversation with citizens".[66] Due to limitations in technology, it might not be a practicable or available tool to use. Even where modern technologies are available, more rudimentary means of communication may have a greater significance and impact on a target population.[67] Context matters and the approach to IA operations and activities will be dependent upon each individual mission. However, as far as social media/social networking is concerned, if you are not there, you are not part of the conversation, and have absolutely no influence over the discourse whatsoever. In this case, having a presence is a part of the message.

By the nature of the subject, this brief is designed to, and invariably resigned to, begging more questions than the author claims to be able to answer. It is hoped that some of the ideas presented will spur more thinking, discussion and discourse on the issue. This is simply an introduction to a dynamic and ever changing topic that has come to play an instrumental role in current public and political discourse. Social media and social networking have exploded in usage and prominence within the relatively short time frame of the past several years. The utility of social media as a tool for the empowerment of individuals and groups is not yet entirely understood, and despite its role in toppling entrenched regimes, has not yet shown its full potential of use. It is an avenue through which possible uses cannot and should not be ignored by the CF or practitioners of IA.

[66] "The Fourth Annual Social Media Conference", *The Canadian Business Journal*, www.canadianbusinesssjournal.ca December 10, 2010, Available at http://www.canadianbusinessjournal.ca/features/december_10_features/the_4th_annual_social_media_conference.html

[67] Despite a rate of cell phone ownership in Afghanistan of over 50%, and an increasing access to newer technologies, the CF has been distributing "Night Letters" in Kandahar province as part of its IA campaign. See Broughtigam, Tara, "Canada Delivers Night Letters of It's Own to Counter Taliban Threats", *The Canadian Press*, February 24, 2011. Samarajiva, Rohan, "52% of Afghan Homes Have Mobiles, More Than 41% Than Have T.V.'s", LirneAsia.Net, January 5, 2011. Available at http://lirneasia.net/2011/01/52-percent-of-afghan-homes-have-mobiles-more-than-the-41-percent-that-have-tvs/ Ali,Nad, "Afghan Media in 2010", Altai Consulting, USAID, October 13, 2010. Available at http://www.altaiconsulting.com/docs/media/2010/04.%20Helmand%20-%20Nad%20Ali.pdf Trofimov Yaroslav, "Cell Carriers Bow to Taliban Threat", *Wall Street Journal,*March 10, 2010. Available at http://online.wsj.com/article/SB10001424052748704117304575137541465235972.html

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Neil O'Reilly
Royal Military College of Canada
PO Box 17000
Stn Forces
Kingston Ontario
K7K 7B4

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC December 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Friending Enemies and Influencing People: Identifying and Examining Issues in the Use of Social Media for CF Influence Activities

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Neil O'Reilly

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
June 2011	34	0

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
ARP 12QR	RMC SLA 2009-0297 PR10023

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
RMCC SLA #2009-0302-SLA-PR10023	DRDC CORA CR 2011-081

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report provides an overview of potential policy, legal, and procedural issues facing the use of social media and social networking tools by the Canadian Forces (CF) for Influence Activities (IA) purposes. What is most important is the nature of the medium as forum, insomuch as it is user driven, widely accessible, instantaneous, and, in order to succeed, popular. With the built in audience as user, these technologies present an opportunity for a user to target an audience simply by being a member of that online community. Thus, for those interested in promoting a particular message, be it marketing firms, political organizations, or common interest groups, social networking and social media cannot be ignored. The aim of this paper is to examine current usage of social networking tools in order to expose any potential procedural, policy, or legal issues that would affect the employment of such tools by the CF. In general, the paper finds that while certain policy, legal, and doctrinal issues do exist, none appear to be severe enough to seriously hinder the use of such tools by the CF for a variety of purposes. In fact, the greatest hindrance may be acceptance of the fact that the use of such tools requires relinquishing control of a message to a certain degree. Findings of the report show that, while more detailed work needs to be done in specific areas touched on by the study, the CF and DND should adopt social media and social networking as a force multiplier for IA, but need to develop streamlined, modern, comprehensive and clearly articulated policies and procedures if these tools are to be used effectively.

Ce compte rendu présente un aperçu des questions pouvant être soulevées sur le plan politique, juridique et des procédures en ce qui concerne l'utilisation des médias sociaux et des outils de réseautage social par les Forces canadiennes pour la tenue d'activités d'influence. Ce qui importe le plus, c'est la nature du média utilisé comme tribune, d'autant qu'il est adapté aux utilisateurs, qu'il est largement accessible et instantané et qu'il est, afin d'être fructueux, populaire. Étant donné que les membres de l'auditoire de ces médias en sont aussi les utilisateurs, ces médias permettent à un utilisateur de cibler un auditoire simplement en devenant membre de sa communauté virtuelle. Ainsi, les groupes intéressés à faire passer un message, qu'il s'agisse d'entreprises de marketing, d'organisations politiques ou de groupes d'intérêts communs, ne peuvent pas ignorer les sites de réseautage social et les médias sociaux. Cet article examine donc l'utilisation actuelle des outils de réseautage social afin de mettre en lumière toutes les questions sur le plan politique, juridique et des procédures pouvant nuire à l'utilisation de ces outils par les Forces canadiennes. En gros, cet article conclut que malgré l'existence de certaines questions sur le plan politique, juridique et de la doctrine, aucune de ces questions ne semble suffisamment grave pour nuire sérieusement à l'utilisation de ces outils à diverses fins par les Forces canadiennes. En fait, le plus gros obstacle à contourner pourrait plutôt être l'acceptation du fait que l'utilisation de ces outils exige de renoncer dans une certaine mesure au contrôle exercé sur le message véhiculé. Le compte rendu conclut que même s'il faut étudier plus en profondeur certains des sujets abordés par l'étude, les Forces canadiennes et le ministère de la Défense nationale devraient se servir des médias sociaux et des outils de réseautage social afin de multiplier les effets de leurs activités d'influence; ils devront toutefois élaborer des procédures et

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

influence activities; IA; PsyOps; social media; social networking; web 2.0;

www.drdc-rddc.gc.ca