National Defence | Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SOCMINT: FOLLOWING AND LIKING SOCIAL MEDIA INTELLIGENCE

LCol M.E.K. Mahood

JCSP 41

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 41

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

SOCMINT: FOLLOWING AND LIKING SOCIAL MEDIA INTELLIGENCE

LCol M.E.K. Mahood

Word Count: 5435

Compte de mots : 5435

Today's criminal and terrorist organizations include digital natives, young persons who have grown up with the Internet and social media. Consequently they comfortably and habitually use social media to communicate in all their activities. When society adopts a new technology or communication medium, it behooves those charged with protecting society to understand it, employ it and police it where necessary. Social Media Intelligence (SOCMINT) has great potential as a tool to be used against violent non-state actors and intelligence organizations have made great use of SOCMINT. Unfortunately despite acknowledgment of the capability gap, the Canadian Armed Forces has not yet adopted SOCMINT. Through a Canadian lens, and with a general and unclassified approach that does not reveal capabilities, this paper will prove that intelligence from social media is highly effective and best used in combination with other intelligence capabilities. SOCMINT alone is not sufficient to stand as a substitute for other intelligence disciplines, but it certainly adds an incredible capability: "Social media intelligence needs to be paired with other forms of information and intelligence to be effective."[1] First SOCMINT will be defined; then SOCMINT will be examined as an addition to all source intelligence; next, this paper will examine the use of SOCMINT in targeting; fourth, SOCMINT's role in predictive analysis to anticipate future events will be discussed; and last future opportunities for SOCMINT will be examined.

DESCRIBING SOCMINT

According to the Canadian Security Intelligence Service (CSIS), intelligence is: "the product resulting from the collection, collation, evaluation and analysis of information."[2] The Oxford English Dictionary defines social media as "web sites and applications which enable users

---

1 Nina Laven, "Social Media Intelligence" (Key note speaker, Security Industry Conference, Singapore, 28 August 2014), last accessed 24 April 2015, http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

2 Canada, Canadian Security Intelligence Service, "Intelligence Collection and Analysis," last accessed 12 May 2015, https://www.csis.gc.ca/bts/ntllgnc-en.php.

to create and share content or to participate in social networking."[3] Open Source Intelligence, or OSINT, which is defined as "intelligence derived from information collected through publicly available media sources,"[4] including everything from library books to tweets. SOCMINT is an extension of OSINT. Sir David Omand who coined the acronym SOCMINT defined social media intelligence simply as "intelligence derived from social media."[5] In the same paper, he further argued that SOCMINT should be restricted to non-intrusive collection from open sources as opposed to intrusive collection from closed sources.[6] Arguably SOCMINT ends when intrusive means are employed, as activities behind the screen are the realm of Signals Intelligence (SIGINT). Differentiation between platforms however is becoming less of a defining feature. Social networking (Facebook, WeiBo), content communities (Flickr) media sharing (You Tube, Instagram), blogs (Army.ca) and micro blogs (Twitter), social news (Reddit) and instant messaging (Whats App, BBM) are common social media fora. These categories are no longer useful as lines are blurring.[7] A user could, as one example, share media, or write a micro blog, or create a content community all on the same social networking site.

The Canadian Armed Forces (CAF) has no SOCMINT capability at present. Although the CAF has a robust and very useful OSINT capability that at times uses or disseminates SOCMINT based commercial intelligence products, the social media exploitation capability is missing. While analysts realize that SOCMINT is a much-needed tool and a policy has been drafted, the approval process appears mired in bureaucracy.[8] This is not surprising as SOCMINT

---

3 Oxford English Dictionary, "Social media," last accessed 23 April 2015, http://www.oed.com/view/Entry/183739?redirectedFrom=social+media#eid272386371

4 Canada, Department of National Defence, B-GJ-005-200/FP-002, CFJP 2.0 Intelligence, Ottawa: DND Canada, 2011, 2-8.

5 David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence & National Security* 27, no. 6 (2012), 802.

6 David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence & National Security* 27, no. 6 (2012), 820.

7 Nina Laven, "Social Media Intelligence" (Key note speaker, Security Industry Conference, Singapore, 28 August 2014), last accessed 24 April 2015, http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

8 Angela Maxwell, CAF OSINT Specialist, *SOCMINT*, email, 23 April 2015.

is a new and highly analytical field that does not appear to be well understood. Like any other new technology, development of the SOCMINT capability will take time and resources that may not be available in the CAF. One solution might be a comprehensive whole of government effort that draws the best specialists from across the government. In addition to creating a cluster of specialists, this combined effort could provide reporting to all agencies and departments thus centralizing the SOCMINT effort and reducing duplication of work. Age may be a reason social media has not been embraced in the CAF. Today's decision makers are less likely to have grown up with the Internet, never mind social media. Until the digital native generation occupies senior level positions, CAF decision makers will be less comfortable with SOCMINT than their subordinates. Another factor may be cultural reticence; some agencies may be reluctant to engage in social media intelligence due to beliefs about its accuracy and reliability in comparison to more traditional intelligence sources.[9] Education, demonstration of SOCMINT's effectiveness, and growing familiarity with social media will ease the reluctance to accept social media intelligence.

SOCMINT AND ALL SOURCE INTELLIGENCE

The concept of all source intelligence is easily understood but not well defined. The best explanation is found in Rémillard's 2007 article explaining the All Source Intelligence Centre. Essentially, all source intelligence is a joint effort that encompasses the entire intelligence cycle.[10] All source intelligence is multi-disciplinary, sometimes virtual, and encompasses all intelligence sub-disciplines and capabilities notably human intelligence (HUMINT), signals intelligence (SIGINT), counterintelligence (CI), imagery intelligence (IMINT), geomatics (GEOINT) and fusion and analysis. Non-military personnel, allies and liaison officers are both contributors to and beneficiaries of all source intelligence. All source intelligence provides a common,

---

[9] Richard Evans, "Social Media Intelligence: Current Approaches & Emerging Opportunities," IHS White Paper, September 2013, 6. Last accessed 4 April 2015, www.ihs.com/osint.

[10] The intelligence cycle comprises direction, collection, processing and dissemination.

fused/analyzed, intelligence picture. All source intelligence is found at the tactical, operational and strategic level.[11] Social media was too young in 2007 to be discussed, but the article missed OSINT. Today a complete intelligence picture is not possible without OSINT and SOCMINT in particular.

The nature of SOCMINT means that it cuts across all source intelligence. A single social media item could contain information useful to multiple intelligence disciplines. For example, a mobile Facebook post from a known international user might contain some text, a tagged photograph, and geo-referenced metadata. The communication means used to post the data might be analyzed by a SIGINT capability;[12] the user's online activity pattern and sentiment could be used to add to a HUMINT profile; the text translated and analyzed holistically; the tagged image used to establish connections to the tagged subjects, a possible CI nexus, and perhaps analyzed as part of IMINT; and the geolocation plotted against the user's pattern or other known data. SOCMINT does not supplant other forms of intelligence, but given the nature of the technology involved there is something for everyone.

One of the advantages of the all source system is the ability to use SOCMINT to focus or cross cue other collection activities.[13] Cross cueing is the sharing of useable information to focus or reorient another sensor. To use the Facebook example above, the geolocation data could be used to reassign an Unmanned Aerial Vehicle (UAV) to *look* in the general area for the online poster. Cross cueing saves time and creates efficiencies. Most beneficially, cross cueing can provide a clue to focus a sensor to collect from a specific area in a vast area of operations. SOCMINT originated cross cueing could be used to quickly provide feedback into the all source

---

11 L. H. Rémillard, "The "All-Source" Way Of Doing Business – The Evolution Of Intelligence In Modern Military Operations" *Canadian Military Journal,* Autumn 2007.

12 Canada, Communications Security Establishment, "Frequently Asked Questions," last accessed 20 May 2015, https://www.cse-cst.gc.ca/en/about-apropos/faq.

13 Richard Evans, "Social Media Intelligence: Current Approaches & Emerging Opportunities," IHS White Paper, September 2013, 4. Last accessed 4 April 2015, www.ihs.com/osint.

process and even create additional cross cueing opportunities. Effective SOCMINT cross cueing is only possible in an all source environment.

Analysis is a key function of all source intelligence. SOCMINT can add value be used to corroborate or deny other reporting. The strength of all source intelligence is the consolidation and analysis of multiple intelligence streams. Analysis is used to gauge threats, identify gaps, evaluate impact, determine battle damage (in the military context), and determine source reliability and information credibility.[14] SOCMINT can support the intelligence function in all these areas. To help assess threat intelligence, social media can be examined for intention, as threat is determined as the sum of the adversary's capability and intent. Information collected from social media can be cross referenced against other reporting to help build a picture; a blog comment could be checked against an online news report and a signals intercept to develop the context and add to the verification of the blog information. SOCMINT often provides fragmentary information that point to gaps in the intelligence picture. These gaps would normally feed into an intelligence collection plan. Physical Battle Damage Assessment (BDA) on infrastructure targets can be assessed by imagery, but when the target is a leader, or a group, imagery is not as useful. Here SOCMINT can provide useful signs of grief, remorse or discussion of a replacement for the leader. Source reliability in the HUMINT context is based on a history of reporting and activity. Data rich SOCMINT reporting could support reliability assessments. In terms of information credibility, social media products could provide information in relation to other reporting. When cross-referenced, if the SOCMINT corroborates the other reporting, it strengthens the assessment that the original reporting is correct. If it contradicts the original reporting, then it would add to the body of reporting that increases the likelihood that the original report is false. Although SOCMINT adds great value to all source analysis, evaluation

---

[14] L. H. Rémillard, "The "All-Source" Way Of Doing Business – The Evolution Of Intelligence In Modern Military Operations" *Canadian Military Journal*, Autumn 2007.

based solely on social media, or even on two pieces of corroborating information is no guarantee of certainty.

As useful as SOCMINT is to all source intelligence, it does have drawbacks. It produces a vast amount of data and analysis can be very challenging. There are no cold war templates or doctrinal models to predict today's adversary actions.[15] One problem with social media is excessive volume. Consider that "Facebook ingests approximately 500 times more data each day than the New York Stock Exchange (NYSE) [and] Twitter is storing at least 12 times more data each day than the NYSE."[16] The vast amount of data produced on the Internet and collected as part of SOCMINT is a stark contradiction to the relative intelligence desert of the Cold War era. In the aftermath of the failed 2009 Christmas Day underwear bombing, US President Barack Obama identified the problem not as "a lack of information but, in fact, an overabundance of it."[17] Excessive volume of reporting leads to wasted time and effort, and likely to missed indicators. Automation could be a solution,[18] but despite the advance in Neuro linguistic language and sentiment analysis, the best analyst is still the human one. Mathematically, the more social media nodes producing social media postings, the more noise that analysts have to scrutinize. As in the Christmas Day underwear bomb plot, increased volume of reporting does not equate to truth, however it can make it difficult for the analyst to find it.

---

15 L. H. Rémillard, "The "All-Source" Way Of Doing Business – The Evolution Of Intelligence In Modern Military Operations" *Canadian Military Journal,* Autumn 2007, 21.

16 Marcello Ballve, "Mobile, Social, And Big Data — The Intersection Of The Internet's Three Defining Trends," *Business Insider,* last accessed 11 May 2015, http://www.businessinsider.com/mobile-and-social-drive-big-datas-potential-2014-5.

17 Heather Maher, "Analysts Say U.S. Intelligence System Overloaded, Out Of Date," Radio Free Europe Radio Liberty, last accessed 5 April 2015, http://www.rferl.org/content/Analysts_Say_US_Intelligence_System_Overloaded_Out_Of_Date/1930418.html.

18 Richard Evans, "Social Media Intelligence: Current Approaches & Emerging Opportunities," IHS White Paper, September 2013, 3. Last accessed 4 April 2015, www.ihs.com/osint.

Like volume, context is another feature of SOCMINT that can cause a significant negative impact in all source intelligence if it is not correctly addressed. Analysts must understand the full context, including social, political, economic, cultural and religious aspects to name but a few, surrounding the material being analysed. As any email user knows, written tone is important, and used without care, can lead to misinterpretation. An analyst must also seek to understand the reason for which the communication was sent; it could be intended as humour, sarcasm, venting, mocking, or seriousness. Furthermore, a writer could send a message simply with the intent to gauge its reception with a larger or different audience. The intended audience is also important to understand. A social media user could have multiple identities: son, husband, worker, rebel, criminal, activist, or terrorist.[19] A user will write to their family differently than they would to their peer group or adversaries. One growing cross-cultural phenomenon that can lead to contextual difficulty is the extensive use of emojis in social media. These icons, which originated in Japan, have migrated around the world via the Internet and form a new multilingual hybrid language. Although widespread, they are not universal in meaning and their use in social media, particularly gun emojis, which when associated with school or police officer emojis others, has led to trouble.[20] While there are efforts underway to create an emoji translation tool, this too points to the importance of context. Metadata also provides contextual clues. It can show the time and location of the message even when time zone settings have been modified or mobile device locational services disabled. Last in terms of context, access to the user's posting history on various forms of media will allow the analyst to determine a baseline pattern of social media use. Some users who might be considered as hardcore supporters of violent non-state actors on Twitter have been seen to post in radically different ways with their school age peer group thus calling into question their motivation: jihad enthusiast or internet thrill seeker. Although there are

---

[19] Alexander Klimburg, "Mobilizing Cyber Power," *Survival* 53, no 1, (Feb-Mar 2011): 47-48.

[20] Emma Bowman, "As Emoji Spread Beyond Texts, Many Remain [Confounded Face] [Interrobang]," NPR, 4 May 2015, last accessed 4 May 2015, http://www.npr.org/blogs/alltechconsidered/2015/05/04/404209790/as-emoji-spread-beyond-texts-many-remain-confounded-face-interrobang.

notable limitations in using SOCMINT for all source analysis, these drawbacks can be mitigated with training and experience. Overall the value of SOCMINT for all source intelligence greatly outweighs the negatives.

SOCMINT AND TARGETING

SOCMINT is a discipline that lends itself readily to targeting. Targeting intelligence is "intelligence that concerns the analysis of a target, target complex or target system in order to determine how its functional characteristics and vulnerabilities may be exploited in a systematic manner to achieve a desired effect."[21] Targeting intelligence supports both kinetic targeting and influence operations. Regardless, the key is having complete and current information about the target be it a person, place or facility. SOCMINT is applicable to targeting development particularly in its compatibility with social network analysis, source identification, cultivation and recruitment, and the exploitation of hastily formed networks.

Social network analysis (SNA) is at the heart of locating adversary High Value Targets (HVT). SNA, sometimes called link analysis or association analysis evaluates linkages and relationships amongst its subjects. It is concerned with the nature of the relationship, not just the fact that a relationship exists.[22] SNA requires good qualitative, not just quantitative, data for detailed analysis; Social media can help provide this. If the subjects of the network analysis, or their family, friends or even associates use social media, then SOCMINT can provide information to help support the analytical effort. The nature of information posted on social media ranges from the superficial to the profound, trivial to momentous. All of it can be useful, especially when analyzed alongside other sources.

---

[21] Canada, Department of National Defence, B-GJ-005-200/FP-002, CFJP 2.0 Intelligence, Ottawa: DND Canada, 2011, GL-12.

[22] David W. Pendall and Julieann Mazak, "Effective Network Targeting," *Military Intelligence Professional Bulletin* 38, no. 2 (Apr-Jun 2012, 2012): 26.

SOCMINT has changed source identification, cultivation and recruitment operations. It remains to be seen if SOCMINT is simply another tool for Human Intelligence (HUMINT) operatives, or potentially a replacement for some HUMINT operations. Cyber war expert Thomas Rid notes that cyber-espionage may be less risky and even more ethical than traditional forms of HUMINT.[23] Now sources within adversary networks can be contacted using Twitter and tasked to collect or report without risk to the operative. In addition, source reporting, audio, visual, or text, can be quickly conveyed via social media.[24] Another advantage that SOCMINT offers over traditional HUMINT is the ability to use geolocation to confirm from where a social media post was made. Adversary groups can be infiltrated using SOCMINT too. Although professional criminal gangs would not likely be fooled with a simple online posting history, following or liking members, violent non-state actors and other non-traditional groups could be. Using social media tools intelligence analysts can penetrate open networks and identify potential sources for HUMINT operations. In addition to the simply identifying the source, well-analyzed social media can give the operator clues to other potential sources' character, habits, and traits for consideration in their cultivation and recruitment. A potential source may even reveal financial issues or character flaws that could in turn be used as motivation to encourage cooperation. Although technically not a HUMINT organization, IHS, formerly Information Handling Services, which now own Jane's Information Group, identifies sources for its online research using social media. Like HUMINT agencies, IHS assesses their online sources by evaluating the source's value by examining their location, cultural proximity, access and timing from event to posting. The source's reliability is based on their track record of previous postings and any endorsement in

---

[23] Thomas Rid, "Cyberwar and Peace," *Foreign Affairs*, 92, no 6 (Nov/Dec 2013, 2013), last accessed 11 May 2015, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

[24] Richard Evans, "Social Media Intelligence: Current Approaches & Emerging Opportunities," IHS White Paper, September 2013, 9. Last accessed 4 April 2015, www.ihs.com/osint.

the form of followers or links.[25] This allows IHS to track their most valuable and reliable sources in a region using off the shelf software. IHS notes one potential legal problem with HUMINT operations on social media is that the nationality of the subject cannot be easily ascertained. For some agencies this could be problematic.[26]

Hastily formed networks are a feature of social media. The fluid nature of social media and the requirement to adapt to external pressures make hasty networks a reality. Twitter's efforts, alongside those of cyber vigilantes who post facts about Islamic Extremist social media users, including their IP addresses and related account information with a view to shutting down users have led to a climate where hasty networks are not just common they are accepted. For this reason, networks are vulnerable to exploitation by new joiners. 5elphabook, or CaliphateBook, was launched by ISIS supporters just days after ISIS Twitter and Facebook bans were enacted, however it was short lived as it too was shut down after one day. It is not clear who shut down 5elphabook, but online supporters appeared to be wary of posting information there, as they believed that servers were not secure.[27] Furthermore, some ISIS supporters value their shut-down account status as they consider it adds to their credibility. Frequently within hours of being kicked off Twitter these supporters are back online re-establishing contacts often using previously established but inactive accounts.[28] In these cases, they may use their new accounts to reach out to old account followers. Overall social media users, especially those supporting ISIS show online resiliency and readily form hasty networks.

---

[25] Nina Laven, "Social Media Intelligence" (Key note speaker, Security Industry Conference, Singapore, 28 August 2014), last accessed 24 April 2015, http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

[26] Richard Evans, "Social Media Intelligence: Current Approaches & Emerging Opportunities," IHS White Paper, September 2013, 6. Last accessed 4 April 2015, www.ihs.com/osint.

[27] Noah Browning, "Blocked online, Islamic State supporters launch CaliphateBook," *Reuters*, 10 March 2015, Last accessed 15 April 2015, http://www.reuters.com/article/2015/03/10/us-mideast-crisis-socialmedia-idUSKBN0M60F720150310

[28] Laura Huey, "#IS_Fangirl: The Creation of a New (Old) Role for Women in Terrorism (and a New Set of Headaches for Security Professionals)" (panellist, Social Media and Cyber-Influence Workshop, Canadian Forces College, Toronto, ON, 9 April 2015), with permission.

However, social media targeting applications are not without hazard. As suggested social media users are comfortable with the technology. Those with nefarious intent, such as violent non-state actors, can easily engage in counter-socmint. Whilst no real definition of counter-socmint exists, counterintelligence is defined as: "activities concerned with identifying and counteracting threats…"[29] Accordingly counter-socmint is defined here as activities concerned with identifying and counteracting online and social media threats. Adversary social media users may seek to identify and counter threats, deny information, deceive, and self-sensor. Any counter-socmint activity can have an adverse impact on intelligence collection and analysis. Accordingly, analysts need to be aware of and watch for this activity. Other inaccuracies in SOCMINT can result from "false positives" that is the result of unintentional collection on other collectors, and overestimating poster "investment." Omand noted that because of the "online disinhibition effect" people communicate differently online than face to face.[30] In fact, profanity, threats and dabbling in pornography, or following a violent non-state actor are facilitated by a sense of anonymity, invisibility, and other factors that encourage riskier behaviour than seen in person.[31] For this reason, it would be wrong to assess the nature of social media users who follow or like pro-ISIS material based on SOCMINT alone. Regardless, used properly by well-trained analysts, SOCMINT is a powerful tool to support targeting. Another area in which SOCMINT can play a significant role is predictive analysis.

SOCMINT AND PREDICTIVE ANALYSIS

Predictive analysis is another area where SOCMINT can really prove its worth. Accurately determining what may happen in the future presents a serious challenge. However, by using

---

29 Canada, Department of National Defence, B-GJ-005-200/FP-002, CFJP 2.0 Intelligence, Ottawa: DND Canada, 2011, GL-3.

30 David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence & National Security* 27, no. 6 (2012), 812.

31 John Suler, "The Online Disinhibition Effect," *Cyberpsychology & Behavior*, Volume 7, no 3 (2004), 321-322.

analytical tools, extant patterns and tracking developing ones, social media can provide clues to identify future potential events. The future can be deduced through the use of SOCMINT. Pattern analysis, crowd sourcing, and semantic analysis are SOCMINT assessment tools.

One of the drawbacks of social media, the vast oceans of data that must be sifted through, can be an advantage here. Pattern analysis is only possible when there is a sufficient data set to compare. The computing power of modern computers and the retrievability of data, even that which has been deleted, provides analysts a sufficient data set. In fact IHS uses a sample of only 10% of the daily worldwide Twitter feed for its analysis.[32] Comparison of pre-event social media activity can also lead to the identification of patterns. Once a pattern is identified, social media analysts can create a model and search for similar patterns to identify future events. Given the metadata available with much social media communication, patterns could be temporal, geographical, hierarchical, or a combination of patterns. The patterns however, may not be universal as different groups, organized criminal and violent non-state actors for example, may operate differently in the lead up to a similar event. In addition, groups are dynamic; they may change tactics to increase success opportunities or prevent failure. Looking at terror attacks as an example, Stratfor argues that: "Individuals planning a terrorist attack follow a discernible cycle — and that cycle and the behaviours associated with it can be observed if they are being looked for."[33] Furthermore, despite differences in groups, according to Stratfor, once they decide on an attack, there is "remarkable similarity in the planning process:" target selection, surveillance, planning - which often includes a "dry run" or rehearsal, deployment and the attack.[34] In this example, the groups are most vulnerable when they communicate and during surveillance. The

---

[32] Nina Laven, "Social Media Intelligence" (Key note speaker, Security Industry Conference, Singapore, 28 August 2014), last accessed 24 April 2015, http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

[33] Stratfor, "Detection Points in the Terrorist Attack Cycle," *Security Weekly*, 1 March 2012, last accessed 21 April 2015, https://www.stratfor.com/weekly/detection-points-terrorist-attack-cycle.

[34] Stratfor, "Detection Points in the Terrorist Attack Cycle," *Security Weekly*, 1 March 2012, last accessed 21 April 2015, https://www.stratfor.com/weekly/detection-points-terrorist-attack-cycle.

use of social media, especially when imagery and geolocation of both vulnerabilities are exploited, gives opportunities to defending analysts.

Omand notes that crowd sourced intelligence can provide genuine value to analysis. During the London Riots, bystanders used social media to provide reporting to police. The police in turn used social media and provided information back to observers; citizens were able to assist in the identification of suspects.[35] Similarly during a 2012 Ohio school shooting incident, students were able to tweet information to the wider world.[36] Although in this case it does not seem that the students were able to provide information unavailable elsewhere, the potential still exists for crowd sourced intelligence via social media in similar situations. In addition to direct reporting, crowd sourced analysis can benefit SOCMINT. The Intelligence Advanced Research Projects Activity (IARPA) is a US Director of National Intelligence organization that is assessing the effectiveness of crowdsourcing intelligence. Unlike the London Riots and the school shooter example, IARPA is interested in crowd sourced analysis and assessment vice raw data.[37] Reportedly crowd sourced assessments in trials by Wikistrat, a crowd sourcing consultancy firm working with IARPA, were 25% more accurate than those of the control group.[38] Wikistrat, following in the collaborative model of Wikipedia argues that its strength is being able to focus the efforts of "hundreds of topic experts."[39] Although the future of open source analysis may lie in outsourcing crowd sourcing, its weaknesses are that those experts are limited to open source

---

[35] David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence & National Security* 27, no. 6 (2012), 804-5.

[36] Lauren Dugan, 'Twitter Used as an Impromptu Broadcast System During Ohio School Shooting', *Media Bistro*, 28 February 2012, last accessed 21 April 2105, http://www.adweek.com/socialtimes/twitter-used-as-impromptu-emergency-broadcast-system-during-ohio-school-shooting/460514?red=at.

[37] Sharon Weinberger, "Intelligence agencies turn to crowdsourcing," BBC Future, last accessed 21 April 2015, http://www.bbc.com/future/story/20121009-for-all-of-our-eyes-only.

[38] Sharon Weinberger, "Intelligence agencies turn to crowdsourcing," BBC Future, last accessed 21 April 2015, http://www.bbc.com/future/story/20121009-for-all-of-our-eyes-only.

[39] Wikistrat Crowdsourced Consulting, "What is Crowdsourced consulting?," last accessed 21 April 2015, http://www.wikistrat.com/about/.

material only and the nature of collaboration makes members subject to the fallacy of group think.

Like crowdsourcing and pattern analysis, SOCMINT augments predictive analysis in research and understanding through semantic analysis. Semantic analysis, part of the field of linguistics, is the process by which meaning is derived from words, phrases and sentences. Semantic analysis goes well beyond the simple and limited key word analysis as frequently seen on morning television news. Key word analysis in which the presence of certain words is detected and tracked can lead to false interpretations. For example the tweets about a hockey team's poor playoff performance being a 'bomb,' could if analyzed for key word frequency, might lead analysts to assess a greater threat than really exists. Still, the application of semantic analysis to social media may be problematic. Social media users have their own language modifications and microblogging platforms such as Twitter further restrict users causing abbreviations and abridged messages. On top of that, social media is a global phenomenon in which users are not restricted to the English language, or even Latin characters. Given its utility and potential, semantic analysis will likely continue to develop as a social media analytical tool.

Advancement in automated Natural Language Process (NLP) systems have kept pace with the social media revolution. Nowadays automated NLP processors can separate fact from opinion, analyze opinion to determine and classify its value (positive, neutral or negative), and using the context, make sense of words with multiple meanings.[40] Although these tools were developed for business, NLP has great potential for use in SOCMINT. The differentiation between fact and opinion is one that is critical in intelligence. Knowing the difference between what a source understands as a truth and what a source thinks is a critical intelligence capability that has strong parallels in HUMINT. That differentiation nevertheless is lacking at present in basic automated

---

[40] "Step 3 Systems, Inc.; Patent Issued for System and Method for Automatically Predicting the Outcome of Expert Forecasts," *Robotics & Machine Learning* (14 January 2013): 1144.

SOCMINT analysis. As with semantic analysis, NLP requires a known lexicon against which to compare its subject words and phrases. All languages are dynamic, but social media has the potential to change even faster than traditional communication. Accordingly, analysts would need to constantly update and validate the lexicon by testing; this effort however would be well worth the increased social media analytical potential. As indicated, communication is complex enough without having a fluid Internet language and social media restrictions placed upon it. As non-native language learners know, metaphors can cause unique challenges to understanding. For that reason IARPA has developed a metaphor program to understand cultural nuances on the Internet.[41] Most interestingly, hidden meanings in language may be unintentionally added by social media users with intimate, background or exclusive knowledge of events, policies or adversary intentions. Pairing the metaphor program with targeted SOCMINT collection could yield even greater results. Like with NLP, new metaphors need to be collected, given value and added to the database. Clearly metaphor, or opinion sentiment collected from a few pro-ISIS Facebook posts would not amount to results of intelligence value. The value in NLP and metaphor analysis would come over longer periods and larger datasets when it would be possible to temporally and spatially track the spread of an idea or the changing of opinion.

Like the other areas in which SOCMINT contributes, there are pitfalls to predictive analysis. SOCMINT enabled predictive analysis operates in a new cultural milieu. The new language and culture of social media needs to be properly understood to be exploited by SOCMINT analysts. Facebook, the flagship of Western social media, has been open to the public for less than nine years.[42] Similarly, social media users can be disingenuous. Truth in social media is not binary, it is more of a continuum, and the use of automation to winnow through the greyness is problematic. It has been assessed that in the aftermath of the Boston Marathon bombing, only

---

[41] Alexis C. Madrigal, "Why Are Spy Researchers Building a 'Metaphor Program'?" *The Atlantic*, 25 May 2011, last accessed 23 April 2015, http://www.theatlantic.com/technology/archive/2011/05/why-are-spy-researchers-building-a-metaphor-program/239402/.

[42] Wikipedia, "Facebook," last accessed 23 March 2015, https://en.wikipedia.org/wiki/Facebook.

20% of tweets contained true information. This doesn't mean that the 80% posters were lying; 29% contained rumours and erroneous information and 51% were opinion based or contained comments.[43] To look at the data from another view, 20% of the tweets contained information that was useful. The trick is in the quick identification of which 20% contains useful information. At present, the nuances of truth are best discerned through culturally mindful human analysis in an all source environment, as Artificial Intelligence has not yet developed to the point at which it is a reliable substitute. Motivation, intent and audience, as alluded to above, also need to be considered. While these pitfalls may cast a shadow over the usefulness of SOCMINT as a predictive analysis adjunct, they are articulated here simply as potential hazards to overcome and not as significant obstacles to SOCMINT.

FUTURE OPPORTUNITIES FOR SOCMINT

This paper has articulated a numbers of ways in which SOCMINT significantly augments present intelligence capabilities. There are opportunities for SOCMINT exploitation and expansion as there will likely be new opportunities in the near future. Canada's cyber capability, local social networks, and new media exploitation are some areas for growth and expansion.

The term cyber is often bandied about when talking about social media and intelligence. The word cyber however is "chronically contested," misunderstood, and has a "certain buffet quality" to it.[44] In essence the term is misapplied often and not well understood. The Oxford English Dictionary provides a very broad definition of cyber: "In predicative use. Of, relating to, or

---

[43] Nina Laven, "Social Media Intelligence" (Key note speaker, Security Industry Conference, Singapore, 28 August 2014), last accessed 24 April 2015, http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

[44] David J. Betz, review of *On Domains: Cyber and the Practice of Warfare*, by Chris McGuffin and Paul Mitchell, The International Security Studies Forum, last accessed 23 April 2015, https://issforum.org/articlereviews/article-review-32-on-domains-cyber-and-the-practice-of-warfare.

involving (the culture of) computers, virtual reality, or the Internet; futuristic."[45] For the purposes of clouding the adversary's understanding of one's own capabilities, vague definitions are useful. For coordination of effort and defence activities, specific delineation of tasks is advantageous. In June 2011 the Canadian Armed Forces (CAF) announced the creation of its Cyber Command.[46] In 2012 it was staffed with 20 positions.[47] It is unclear if the CAF possesses any real offensive cyber capability at all. It seems that the CAF, unlike other militaries plays a secondary role to the Communications Security Establishment (CSE) whose role it is to "detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems."[48] Regardless of the lead, the CAF contribution seems woefully inadequate when compared to other nations. The United States Cyber Command has five subordinate cyber commands: the Navy, Air Force, Army, Marines and Coast Guard all have their own Cyber Commands.[49] China has integrated cyber-warfare units into the PLA since 2003.[50] According to the Rand Corporation, China has significantly grown its cyber capability (to an unknown size) over the last 20 years. They assess that it could deploy its cyber warfare capabilities offensively or to collect intelligence.[51] The United Kingdom recently announced a cyber capability that takes a wide view of cyber operations. Brigade 77 a joint cyber brigade which will monitor social media, collect intelligence, and conduct psychological and

---

45 Oxford English Dictionary, "Cyber, adj.," last accessed 23 April 2015, http://www.oed.com/view/Entry/250878?rskey=v0gTq2&result=1#eid.

46 Canada, The Maple Leaf, 22 June 2011, Vol. 14, No. 22, p.3

47 Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal* 69, no. 3 (2014): 395.

48 Canada, Public Safety, "Canada's Cyber Security Strategy," last accessed 11 May 2015, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

49 United States. U.S. Cyber Command Fact Sheet, last accessed 23 April 2015, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

50 Alexander Klimburg, "Mobilizing Cyber Power," *Survival* 53, no 1, (Feb-Mar 2011): 45.

51 Michael S. Chase, et al., "China's Incomplete Military Transformation," Rand Corporation, February 2015, last accessed 23 April 2015 http://www.uscc.gov/sites/default/files/Research/China's%20Incomplete%20Military%20Transformation_2.11.15.pdf, 18, 115.

deception operations.[52] As social media collectors often engage with their subjects, liking or following them at a minimum, to facilitate collection it makes sense that the brigade's cyber engagement strategy is linked. A middle power like Canada would do well to define and properly invest funds and personnel in its CAF Cyber Command. Additionally, the CAF might see fit to bring its cyber capability under the Canadian Forces Intelligence Command to take advantage of efficiencies and like other nations join its SOCMINT collection and cyber offensive action capabilities.

Local social networks are another area in which social media has an encouraging future. New social media applications such as Firechat and Yik Yak create collection opportunities and challenges. Yik Yak is an anonymous social media tool that restricts participation to users inside a 10 mile radius.[53] Yik Yak has the potential to offer SOCMINT opportunities to local collectors particularly due to its anonymity and spatial restrictions. Nowcasting, as opposed to forecasting, is an evolving term used to describe the posting of current situational awareness content. Reporters covering a US Senator's presidential bid gained access to real time crowd sentiment restricted largely to attendees by accessing Yik Yak.[54] Firechat provides a similar service but using mesh networking technology. It establishes a peer hopping network using Wi Fi or Bluetooth connections and is free from mobile network service providers. Firechat is even more geographically restricted than Yik Yak; it is limited to 100 feet from the nearest user on the

---

[52] Larisa Brown, "The Army's latest weapon to defeat jihadis? Twitter! New brigade inspired by WWII Chindits aims to beat terror organisations with digital warfare," *Mail Online*, 31 January 2015, last accessed 24 April 2015, http://www.dailymail.co.uk/news/article-2933907/The-Army-s-latest-weapon-defeat-jihadis-Twitter.html.

[53] Wikipedia, "Yik Yak," last accessed 23 April 2015 http://en.wikipedia.org/wiki/Yik_Yak.

[54] David Weigel, "Ted Cruz Has Skeptics at Liberty, and They Use Yik Yak Last," *Bloomberg Politics*, last accessed 29 March 2015, http://www.bloomberg.com/politics/articles/2015-03-23/ted-cruz-has-skeptics-at-liberty-and-they-use-yik-yak.

network.[55] Like Yik Yak, it is an open area platform that may provide interesting data during or after an event.

SOCMINT will always need to stay close to the leading edge of new media development. Not only do social media technologies develop quickly, but some fail just as fast. The new media that do stick around are adopted quickly by the social media users. This presents a gap between adoption and exploitation if SOCMINT agencies are not prepared to quickly adapt and refocus their collection efforts. For example, Periscope, a Twitter based live video broadcast launched recently. Users immediately identified the possibility of its use for whistleblowers and advocacy groups.[56] The intelligence potential too is readily apparent especially when combined with other intelligence disciplines; a SOCMINT agency could collect live feed geolocated video data of an event, or its immediate aftermath. This data could be used to cross cue other collection, or support analysis. New technologies like Periscope developed by social media users in the post-Snowden era in which citizens are more aware of privacy concerns have greater emphasis on privacy settings. As a result, Periscope like other new media allows users to broadcast to a specific and restricted audience.[57] While this will not likely present problems for cyber warriors, closed networks are outside the realm of SOCMINT. This presents another opportunity for harmonized future SOCMINT and cyber activity.

---

55 Tom Simonite, "The Latest Chat App for iPhone Needs No Internet Connection," *MIT Technology Review*, last accessed 29 March 2015, http://www.technologyreview.com/news/525921/the-latest-chat-app-for-iphone-needs-no-internet-connection/.

56 John Bowman, "Twitter launches Periscope live video app to rival Meerkat," CBC News, last accessed 23 April 2015, http://www.cbc.ca/news/trending/twitter-launches-periscope-live-video-app-to-rival-meerkat-1.3010367.

57 John Bowman, "Twitter launches Periscope live video app to rival Meerkat," CBC News, last accessed 23 April 2015, http://www.cbc.ca/news/trending/twitter-launches-periscope-live-video-app-to-rival-meerkat-1.3010367.

CONCLUSION

Through discussion and examination of social media intelligence, this essay has clearly demonstrated that SOCMINT is a powerful tool especially when combined with other intelligence specialities. In the first section SOCMINT was defined, its limits were articulated and the Canadian Armed Forces' lack of social media capability was discussed. Next the benefit of SOCMINT to all source intelligence as a key enabler was proven. Subsequently, SOCMINT was shown to be of great value in targeting, and in the fourth section SOCMINT's value and role in predictive analysis was shown. The last section discussed areas where social media intelligence has opportunity to grow. The greatest concern is that the CAF has neither SOCMINT nor cyber capability of which to speak. Herein lies a problem (a collection competency gap) and a challenge (to build a capability). The CAF should adopt SOCMINT now, ideally in concert with other intelligence disciplines and its cyber capability. In sum, it is clear that although SOCMINT is a powerful intelligence tool; its value is in the added capacity it brings to the other intelligence disciplines especially targeting, all source intelligence and analysis.

BIBLIOGRAPHY

Ballve, Marcello. “Mobile, Social, And Big Data — The Intersection Of The Internet's Three Defining Trends.” *Business Insider*. Last accessed 11 May 2015. http://www.businessinsider.com/mobile-and-social-drive-big-datas-potential-2014-5.

Betz, David J. Review of *On Domains: Cyber and the Practice of Warfare*, by Chris McGuffin and Paul Mitchell, *The International Security Studies Forum.* Last accessed 23 April 2015, https://issforum.org/articlereviews/article-review-32-on-domains-cyber-and-the-practice-of-warfare.

Bowman, Emma. “As Emoji Spread Beyond Texts, Many Remain [Confounded Face] [Interrobang].” NPR. 4 May 2015. Last accessed 4 May 2015, http://www.npr.org/blogs/alltechconsidered/2015/05/04/404209790/as-emoji-spread-beyond-texts-many-remain-confounded-face-interrobang.

Bowman, John “Twitter launches Periscope live video app to rival Meerkat.” CBC News. Last accessed 23 April 2015. http://www.cbc.ca/news/trending/twitter-launches-periscope-live-video-app-to-rival-meerkat-1.3010367.

Brown, Larisa. “The Army's latest weapon to defeat jihadis? Twitter! New brigade inspired by WWII Chindits aims to beat terror organisations with digital warfare.” *Mail Online*, 31 January 2015. Last accessed 24 April 2015. http://www.dailymail.co.uk/news/article-2933907/The-Army-s-latest-weapon-defeat-jihadis-Twitter.html.

Canada. Canadian Security Intelligence Service. “Intelligence Collection and Analysis.” Last accessed 12 May 2015. https://www.csis.gc.ca/bts/ntllgnc-en.php.

Canada. Communications Security Establishment. “Frequently Asked Questions.” Last accessed 1 April 2015. https://www.cse-cst.gc.ca/en/about-apropos/faq.

Canada. Department of National Defence. B-GJ-005-200/FP-002, CFJP 2.0 Intelligence. Ottawa: DND Canada, 2011.

Canada. Public Safety. “Canada's Cyber Security Strategy.” Last accessed 11 May 2015. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

Chase, Michael S. et al. “China’s Incomplete Military Transformation” *Rand Corporation.* February 2015. Last accessed 23 April 2015 http://www.uscc.gov/sites/default/files/Research/China's%20Incomplete%20Military%20Transformation_2.11.15.pdf.

Dugan, Lauren. “Twitter Used as an Impromptu Broadcast System During Ohio School Shooting.” *Media Bistro.* 28 February 2012, Last accessed 21 April 2105. http://www.adweek.com/socialtimes/twitter-used-as-impromptu-emergency-broadcast-system-during-ohio-school-shooting/460514?red=at.

Evans, Richard "Social Media Intelligence: Current Approaches & Emerging Opportunities." IHS White Paper. September 2013. Last accessed 4 April 2015. www.ihs.com/osint.

Huey, Laura. "#IS_Fangirl: The Creation of a New (Old) Role for Women in Terrorism (and a New Set of Headaches for Security Professionals)." Panellist, Social Media and Cyber-Influence Workshop, Canadian Forces College, Toronto, ON, 9 April 2015, with permission.

Klimburg, Alexander. "Mobilizing Cyber Power." *Survival* 53, no 1, (Feb-Mar 2011), 41-60. http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555595

Laven, Nina. "Social Media Intelligence." (Key note speaker, Security Industry Conference, Singapore, 28 August 2014). Last accessed 24 April 2015 http://www.sic.sg/attachments/Day2%20-%201%20Nina%20Laven.pptx.

Madrigal, Alexis C. "Why Are Spy Researchers Building a 'Metaphor Program'?" *The Atlantic*, 25 May 2011. Last accessed 23 April 2015, http://www.theatlantic.com/technology/archive/2011/05/why-are-spy-researchers-building-a-metaphor-program/239402/.

Maher, Heather "Analysts Say U.S. Intelligence System Overloaded, Out Of Date." Radio Free Europe Radio Liberty. Last accessed 5 April 2015. http://www.rferl.org/content/Analysts_Say_US_Intelligence_System_Overloaded_Out_Of_Date/1930418.html.

Maxwell, Angela. CAF OSINT Specialist. *SOCMINT*. Email, 23 April 2015.

McGuffin, Chris and Paul Mitchell. "On Domains: Cyber and the Practice of Warfare." *International Journal* 69, no. 3 (2014): 394-412.

Omand, David, Jamie Bartlett, and Carl Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence & National Security* 27, no. 6 (2012): 801-823.

Simonite, Tom. "The Latest Chat App for iPhone Needs No Internet Connection." *MIT Technology Review*. Last accessed 29 March 2015. http://www.technologyreview.com/news/525921/the-latest-chat-app-for-iphone-needs-no-internet-connection/.

"Step 3 Systems, Inc.; Patent Issued for System and Method for Automatically Predicting the Outcome of Expert Forecasts." *Robotics & Machine Learning* (14 January 2013): 1144.

Suler, John. "The Online Disinhibition Effect." *Cyberpsychology & Behavior*, Volume 7, no. 3 (2004): 321-326.

Rémillard, L. H. "The "All-Source" Way Of Doing Business – The Evolution Of Intelligence In Modern Military Operations" *Canadian Military Journal* (Autumn 2007): 19-26.

Rid, Thomas. "Cyberwar and Peace." *Foreign Affairs,* 92, no 6 (Nov/Dec 2013, 2013). Last accessed 11 May 2015. https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

United States. U.S. Cyber Command Fact Sheet. Last accessed 23 April 2015. http://www.stratcom.mil/factsheets/2/Cyber_Command/.

Weigel, David. "Ted Cruz Has Skeptics at Liberty, and They Use Yik Yak Last." *Bloomberg Politics*. Last accessed 29 March 2015. http://www.bloomberg.com/politics/articles/2015-03-23/ted-cruz-has-skeptics-at liberty-and-they-use-yik-yak.

Wikistrat. "What is Crowdsourced consulting?" Crowdsourced Consulting. Last accessed 21 April 2015, http://www.wikistrat.com/about/.

Wikipedia. "Facebook." Last accessed 23 April 2015. https://en.wikipedia.org/wiki/Facebook.

Wikipedia. "Yik Yak." Last accessed 23 April 2015. http://en.wikipedia.org/wiki/Yik_Yak.