National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SOCIAL MEDIA: OPERATIONAL USES

MAJOR HANS LA PIERRE

JCSP 46

Service Paper

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 46

Étude militaire

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 46 – PCEMI 46
2019 – 2020

SERVICE PAPER - ÉTUDE MILITAIRE

SOCIAL MEDIA: OPERATIONAL USES

Major Hans La Pierre

Word Count: 2,356

Nombre de mots : 2.356

SOCIAL MEDIA: OPERATIONAL USES

AIM

1. The aim of this service paper is to inform the Chief of the Defence Staff (CDS) on how, in terms of uses and requirements, social media can be employed to support Canadian Armed Forces (CAF) operations. It should be noted that although not addressed herein, how we defend against the use of social media by adversaries merits further study in order to provide a holistic answer to the question.

INTRODUCTION

2. The Internet has brought about an age of instant access to information. Social media, the collection of "websites and applications that enable users to create and share content or to participate in social networking"[1], have further expanded on that reality by making information creation and dissemination instantaneous. As of 2019, Facebook & Twitter, perhaps the most well known social media platforms, respectively boast over 2.41 billion[2] and 330 million[3] monthly active users. More than ever, Millennial & Generation Z individuals employ these platforms to inform and entertain themselves, as well as to socialize.[4] It was therefore only a matter of time before various nefarious actors took to manipulating and spreading information through these platforms in order to avoid or influence the outcome of a kinetic conflict.[5] To these adversaries, the Internet "has become a battlefield where information itself is weaponized."[6] Given this new reality, the CAF must learn to employ social media to its own advantage in order to ensure the success of its current and future operations.

3. Two uses of social media will be explored. The first, winning the narrative battle, will be looked at through a short case study. The second consists of using social media to enable cyber and Signals Intelligence (SIGINT) operations. In both cases, a short analysis will be conducted in order to identify key enabling factors and requirements.

DISCUSSION

4. In early summer 2014, the terrorist group known as Daesh entered northern Iraq expanding an existing ground invasion that Iraq, the Middle-East and much of the West would fight for years to come.[7] A force of 1,500 Daesh fighters, armed with pickup trucks and small arms, rapidly made its way toward the city of Mosul.[8] There, they faced a population of 1.8 million inhabitants protected by police forces and the Iraqi army,

---

[1] (Oxford English Dictionary n.d.)
[2] (Clement, Number of monthly active Facebook users worldwide as of 2nd quarter 2019 (in millions) 2019)
[3] (Clement, Number of monthly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions) 2019)
[4] (Singer and Brooking, LikeWar: The Weaponization of Social Media 2018), 261.
[5] Ibid, 11.
[6] Ibid, 19.
[7] Ibid, 4.
[8] Ibid, 5-6.

numbering 10,000 strong, who were comparatively much better equipped.[9] Against all odds, Daesh was nevertheless able to capture Mosul surprisingly swiftly and without much of a fight.[10] How was this possible? The answer to that question lies in the Daesh social media campaign that preluded the fight for Mosul.

5. Representative of its time, a hashtag initiated the drive toward Mosul.[11] A heavy social media campaign highlighting carefully edited daily Daesh actions and successes followed.[12] Furthermore, sectarian and religious divides existing amongst Mosul inhabitants were leveraged in order to create highly targeted and divisive messages.[13] A network of worldwide supporters, as well as the use of bots, amplified this propaganda by spreading it across multiple social media platforms (Twitter, Instagram, WhatsApp, etc.) and by exploiting their underlying algorithms.[14] This intense propaganda barrage, which described in no uncertain terms and in gruesome detail what awaited the defenders of Mosul, instilled terror and disunion in Iraqi ranks even before the fighting started.[15] The defenders effectively bought into the idea that their defeat was a foregone conclusion and consequently defected heavily, leaving the city of Mosul defenceless and ready for the taking.[16]

6. Three key factors of success concerning the use of social media in support of operations can be extrapolated from this particular case study. Namely the relevancy of the message (emphasis on recent successes and atrocities, manipulation of sectarian and religious cleavages), the speed of its delivery (onslaught of daily social media posts), and its amplification (multiplicity of social media platforms, use of bot networks and large fan base, exploitation of social media algorithms). In order for the CAF to successfully integrate the use of social media into its array of influence operations options and impose its meaning on its adversaries, all three of these factors must be addressed.

7. The creation of a relevant message, one that will displace the enemy's unfavourable narrative and effectively replace it with a desired one is of paramount importance.[17] It requires extensive analysis of the target's population and its various communities based on their interests, culture and concerns in order to determine the social dynamics of communication and flow of ideas relevant in developing compatible messages.[18] Communication specialists, cultural advisors and linguists are therefore required in order to create a strong narrative, one that will be implicitly understood and accepted by the target audience. While the CAF possesses this expertise, it is dispersed amongst its many organizations; any attempt to generate the required messages is prone to failure due to diverging priorities and the absence of concerted efforts. For instance,

[9] Ibid.
[10] Ibid, 6.
[11] Ibid, 4.
[12] Ibid.
[13] Ibid, 5.
[14] Ibid, 4-5.
[15] Ibid, 6.
[16] Ibid.
[17] (Waltzman 2017), 6.
[18] Ibid, 6.

communication specialists can be found within Director Military Strategic Communications (DMSC) and the Canadian Army's Influence Activities (IA) group, while cultural advisors and linguists are present within Director General Information Management Operations (DGIMO) and the various CAF component commands. Hence, the creation of a dedicated social media operations capability, or of an ad hoc structure into which personnel can be pulled when necessary, is required. This requirement could likely be tackled by the Chief Force Development (CFD) through the Force Management and Structure Design (FMSD) analysis currently underway.[19]

8. The rapid and iterative delivery of messages to their target audience is key for two reasons.[20] First, the nature of a given message is unlikely to be invariable in time. As the target reacts, or its mindset and view of a given situation changes, so too will the message need to change or be re-emphasized. Second, the enemy is unlikely to abandon his own efforts to win the narrative battle. As with any other type of operation, it is essential to maintain the shortest decision-action cycle in order to retain the initiative. Therefore, messages need to be delivered quickly to their target audience in order to maximize their effects.[21] Within the CAF context, this means that the current targeting process needs to be further refined to allow the Canadian Joint Operations Command (CJOC) Joint Targeting Intelligence Center (JTIC) to collaborate with the aforementioned and proposed social media operations capability in order to prioritize, develop and nominate targets, while the later also concurrently conducts weaponeering of messages in order to impose the desired narrative on the chosen targets. Finally, whenever feasible the authorities related to target validation and target engagement must be delegated to the lowest level possible (e.g. down to the Task Force commander) in order to push power, and speed, to the edge.[22]

9. Once an effective narrative has been designed and pushed to its target audience, it must be amplified. Amplification is a crucial aspect of the use of social media as a conduit for influence operations.[23] Its goal is to ensure the message gets shared to increase its exposure therefore preventing it from fizzling out or being overtaken by a contrary one. By flooding the information sphere with the same message, individuals will tend to accept the common discourse that they are being exposed to.[24] Amplification can be achieved through the exploitation of the social media algorithms (how social media platforms prioritize and present content to users), by leveraging influence networks, or by employing bot networks to spread the message as widely as possible and across as many social media platforms as feasible.[25] Defining the amplification strategy of a given message must be part of the weaponeering stage of the targeting process, and should call upon the communication expertise of DMSC and the CA's IA group, as well as the cyber expertise of DGIMO.

---

[19] (Rouleau 2019), 1.
[20] (Department of National Defence 2008), 5-58.
[21] Ibid, 5-66.
[22] (Rouleau 2019), 7.
[23] (Bodine-Baron, et al. 2018), 10.
[24] (Singer and Brooking, LikeWar: The Weaponization of Social Media 2018), 137.
[25] (Bodine-Baron, et al. 2018), 10.

10. Social media allows for the rapid creation and dissemination of messages to a vast audience. Consequently, they can be an important force multiplier to the success of CAF operations by winning the narrative battle. To do so, however, requires that a joint capability drawing on a wide variety of expertise from within the CAF be established, and that the authorities required to create and disseminate a strong CAF narrative be delegated to the lowest level possible.

11. The second way in which social media can support CAF operations is in their ability to enable cyber and SIGINT operations. In and of themselves, social media platforms and accounts are inherently valuable targets to gather intelligence on an enemy or, in some cases, to degrade his ability to effectively command and control. The exploitation of social media accounts can provide such information as a user's cellphone text messages, as well as detailed time stamped coordinates of his location.[26] There is, however, another way to advantageously use social media in support of SIGINT and cyber operations; through social engineering, specifically phishing and spear phishing operations.

12. Still to this day, the weakest link in any computer network layered defense architecture remains the user.[27] By using social media to create and deliver content or messages that look and feel trustworthy to users, individuals can be led to unknowingly compromise the computers they are using.[28] This method, known as phishing, allows the attacker to avoid several perimeter defense mechanisms and effectively create a beachhead within the network. Assuming the users were accessing social media through their workplace information system, further and more traditional cyber exploitation of the computer network can occur in order to gather intelligence, or deny or degrade its use. While phishing is ultimately enabled by its victims, its reliance on system vulnerabilities and cyber exploits to compromise computer networks effectively categorizes it as an offensive cyber activity. Consequently, to enable phishing operations using social media, the use of cyber operations must be authorized by the CDS and brought to bear in all CAF expeditionary operations under CJOC direction and prioritization.

13. Phishing attacks are remarkably effective and low cost.[29] However, they lack accuracy, i.e. you need to cast a wide net in order to catch a few good fish. In order to increase the accuracy and therefore maximize the return on investment of such an operation, the spear phishing method can be employed. This method, while similar to phishing, relies heavily on intelligence and is best suited to target high value individuals and hardened enemy networks.[30] It requires an intimate knowledge of the specific target and its environment in order to exploit weaknesses and opportunities. In the context of a conflict below the threshold of war, this method could be applied to compromise an enemy high level military official in order to gain access to military information present on his system or to compromise the Internet facing military network he is using. For example, by virtue of knowing the target is a father, and through sustained monitoring, an

[26] (Deibert 2013), 58-59.
[27] (Singer and Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know 2016), 64-65.
[28] Ibid, 40-41.
[29] Ibid, 40.
[30] Ibid, 41.

emerging situation involving his children's school, such as an unexpected snowstorm, could be leveraged to send him a social media update (carefully curated in order to look like it originated from his children's school) with an updated school bus schedule attached. Opening the attached file would trigger the execution of embedded malicious code allowing remote access to his computer and network, while he remained none the wiser. For such a method to be relevant to CAF operations, the convergence of intelligence and cyber operations must continue at all stages of the targeting process involving CJOC, DGIMO and the Canadian Forces Intelligence Command (CFINTCOM), to include the delivery of cyber effects.

14. The recent royal ascent of the Communications Security Establishment (CSE) Act updated CSE's foreign intelligence collection mandate from "from the global information infrastructure"[31] to "through the global information infrastructure"[32] effectively enabling the collection of SIGINT via social engineering methods. Furthermore, since August 1st 2019, CSE is now legally mandated to conduct offensive cyber operations, and to provide assistance to the CAF upon request.[33] Given the finite reality of CFINTCOM SIGINT and DGIMO cyber resources, a robust assistance framework should be developed with CSE in order for authorities, relationships and coordination channels to be in place when called upon to assist CAF in the conduct of SIGINT and cyber operations.

15. By leveraging social media to conduct social engineering, the CAF could enable both the production of foreign intelligence (SIGINT) and the delivery of cyber effects on a given enemy target. However, doing so requires cyber operations to be authorized within the scope of CAF expeditionary operations. In addition, relationships between CAF intelligence and cyber forces, as well as between CAF and CSE, need to be nurtured.

CONCLUSION

16. Propaganda is not new, however at no other time in the history of mankind has it been easier to craft or faster to deliver. The speed at which messages can be created and launched through social media lends them an important force multiplier potential over more traditional influence operation mediums. Combined with the fact that Millennial and Generation Z individuals rely almost exclusively on social media for their entertainment, social, and information needs, they present the CAF with great opportunities in its pursuit of narrative supremacy in support of its operations. Their ubiquity also makes them an ideal conduit to enable SIGINT and cyber operations through social engineering. However, the successful use of social media in support of CAF operations requires issues related to authority, relationships, and synergy of efforts be addressed.

[31] (House of Commons of Canada 2019), s.273.64.
[32] (House of Commons of Canada 2019), s.16.
[33] Ibid, s.19.

RECOMMENDATION

17. On the use of social media to conduct influence operations it is recommended that:

a. the CDS direct CFD to further analyze this problem space, as part of the ongoing FMSD analysis, in order to institutionalize a capability that combines communications, influence activities, cyber and cultural expertise; and

b. the CDS, and Commander CJOC, delegate authorities for target approval, weaponeering of the narrative message, and effect delivery to the lowest level possible.

18. Finally, on the use of social media to enable SIGINT and cyber operations it is recommended that:

a. the CDS authorize the employment of cyber operations in support of all future CAF expeditionary missions;

b. CJOC, CFINTCOM and DGIMO continue to collaborate in order to deliver opportunistic, timely and precise intelligence enabled cyber operations; and

c. CFINTCOM and DGIMO, in collaboration with CSE, develop a robust cyber/SIGINT assistance framework in order to allow CSE to rapidly and seamlessly lend support to CAF operations when requested.

BIBLIOGRAPHY

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. 2018. *Countering Russian Social Media Influence.* Santa Monica: RAND Corporation.

Clement, J. 2019. *Number of monthly active Facebook users worldwide as of 2nd quarter 2019 (in millions).* August 14. Accessed October 27, 2019. https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

—. 2019. *Number of monthly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions).* August 9. Accessed October 27, 2019. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Deibert, Ronald J. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Penguin Random House Company.

Department of National Defence. 2008. *B-GL-300-001/FP-001: Land Operations.* Kingston, Ontario: Army Publishing Office.

House of Commons of Canada. 2019. "Communications Security Establishment Act." *Bill C-59: An Act Respecting National Security Matters.* Ottawa, June 19.

—. 2019. "National Defence Act." Ottawa: Minister of Justice, July 29.

Oxford English Dictionary. n.d. *Lexico.* Accessed October 27, 2019. https://www.lexico.com/en/definition/social_media.

Rouleau, Mike. 2019. *How we Fight: Commander CJOC's Thoughts.* Ottawa, Ontario, February 10.

Singer, P.W., and Allan Friedman. 2016. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Singer, P.W., and Emerson T. Brooking. 2018. *LikeWar: The Weaponization of Social Media.* New York: Houghton Mifflin Harcourt Publishing Company.

Waltzman, Rand, interview by Subcommittee on Cybersecurity, United States Senate Committee on Armed Services. 2017. *The Weaponization of Information: The Need for Cognitive Security* (April 27).