National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SOCIAL MEDIA INTELLIGENCE

Lieutenant-Commander Ryan Vince

JCSP 45	PCEMI 45
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
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.	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.
© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2019.	© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2019.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

SOCIAL MEDIA INTELLIGENCE

Lieutenant-Commander Ryan Vince

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

SOCIAL MEDIA INTELLIGENCE

INTRODUCTION

"In a few years, men will be able to communicate more effectively through machine than face to face. This is a rather startling thing to say, but it is our conclusion."[1] This intriguing statement was made by J.C.R. Licklider and Robert W. Taylor, both psychologists who witnessed the emergence of computers in World War II.[2] Subsequently, Licklider and Taylor helped the US military create ARPANET, a technological evolution that would connect people globally like the telegraph and telephone did as well reach society in ways that newspaper, radio and television did.[3]

Today, society lives in the age of rapid transfer of information via Social Media (SM). People rely heavily on SM platforms such as Facebook, Twitter, Google+ and LinkedIn to transfer their lives onto "a new kind of public and private sphere; a vast digital social commons for social connection."[4] The internet and SM has revolutionised communications as we know it, becoming mediums used for both social advocacy and human rights groups, and additionally as an indispensable medium for terrorist activities.[5] In 2017, 71 percent of people using the internet were also using SM, and a majority of

[1] P.W. Singer. *Like War: The Weaponization of Social Media*. (New York: Houghton Mifflin Harcourt, 2018), 34.

[2] *Ibid*., 34-35.

[3] *Ibid*., 46.

[4] David Omand, Jamie Bartlett and Car Miller. "#INTELLIGENCE A balance between security and privacy online must be struck…" *Demos*. April 24, 2012, 15.

[5] Alexander Tsesis. "Terrorist Speech on Social Media." *Vanderbilt Law Review* 70, no. 2 (2017), 659.

society now receive news updates through SM platforms such as Facebook and Twitter, a figure which is expected to grow in the future.[6]

Although many enjoy the interconnectedness that social media offers, there is a dark side stemming from Violent Extremist Organisations (VEO's) exploitation of this resource. VEO's are using SM as a means to distribute propaganda, educate jihadists, and recruit.[7] Their actions on SM are strategically calculated and coordinated. However, what separates VEO's and businesses is that VEO's strategic purpose is to incite people, especially in the West, to conduct terror operations and attacks.[8] P.W. Singer, author of *Like War: The Weaponization of Social Media* explains "this is what the internet has become. It is the most consequential communications development since the advent of the written word. Yet, like its precursors, it is inextricably tied to the age-old human experiences of politics and war."[9] Singer adds that SM "has also become a colossal information battlefield, one that has obliterated centuries worth of conventional wisdom about what is secret and what is known."[10]

SM has become the preeminent means of communication and info sharing. The information collected from SM has been defined as Social Media Intelligence (SOCMINT) by Sir David Omand, a former Director of the Government Communications Headquarters in the United Kingdom. Subsequently, SOCMINT has

[6] Statisa. "Number of social media users worldwide from 2010 to 2021 (in billions)." Last accessed May 5, 2019. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

[7] Levi J West. "#Jihad: Understanding Social Media as a Weapon." *Security Challenges* 12, no.2 (2016), 14,15.

[8] *Ibid*., 9,12.

[9] P.W. Singer. *Like War: The Weaponization of Social Media*. (New York: Houghton Mifflin Harcourt, 2018), 67.

[10] *Ibid*.

been identified by Omand as the new intelligence domain, in concert with signal intelligence (SIGNINT) and imagery intelligence (IMINT) which are included in the intelligence community (IC) functions. The CAF intelligence community has the capacity to collect, analyse and exploit information on SM. Therefore, this paper will argue that SM is merely a revamped means for people, groups, and organisations to interact and communicate and subsequently the Canadian Armed Forces (CAF) does not need to create SOCMINT as a new intelligence function as claimed by Omand.

This paper is divided into four sections. The first section will provide background on how the internet was created and why. Section two will argue that SM is nothing new and is merely a component of the internet. Section three discusses SOCMINT, including why proponents are fond of it as an intelligence function and why the CAF should not adopt it. The final section will look at an alternative method for the CAF to exploit SM, specifically in an integrated Information Warfare (IW) capability, leveraging existing CAF intelligence resources.

BACKGROUND

After the Soviet Union launched Sputnik space satellite, the United States (US) created the Advanced Research Projects Agency (ARPA) in 1957 to maintain parity with the Soviet Union.[11] Both Licklider and Taylor were employees of ARPA, focusing on communications. In 1968 they published The Computer as a Commutation Device. They envisioned the world connected by multiple computers that were not just used for

[11] *Ibid*., 36.

calculations, but more importantly to share information. They called this system the "Intergalactic Computer Network (ICN)".[12] Licklider and Taylor took their foresight even further and saw the ICN as a way to connect people by creating interactive communities, jobs as well as giving people a sense of belonging.[13] The Pentagon saw ICN as a way to prevent the Soviet Union from destroying the command and control structure of the US military, which was subsequently funded into a project in 1969 called ARPANET.[14] The first international network connection was made in 1973 between two mini university networks. However, these networks were not joined until Vint Cerf and Robert Kahn "designed the transmission-control protocol/internet protocol (TCP/IP)", which was an adaptable framework permitting ARPANET to integrate with all the mini university networks.[15] Electronic mail, known today as email was created in 1979, 40 years later Cerf can still recall the time he realised that "the internet would be something more than every other communications technology before it. It was clear we had a social medium on our hands."[16]

The US military came to the realisation that the use of ARPANET had grown larger than its budget could handle with 70,000 institutions and 5000 people using it.[17] After an unsuccessful adventure to find a commercial buyer for ARPANET, the US military split the internet into two, ARPANET and MILNET, which paved the way for the commercialization of the internet.[18] By 1990, the internet was privatised and

[12] *Ibid.*, 35.
[13] *Ibid.*
[14] *Ibid.*, 36.
[15] *Ibid.*, 47.
[16] *Ibid.*, 48.
[17] *Ibid.*, 49.
[18] *Ibid.*

entrepreneurs were able to create a network of networks called the World Wide Web, creating wealth for the owners of the internet infrastructure as those businesses that were born from it.[19]

Two of the more significant companies that influenced society's use of the internet were Google and Facebook. Google was launched in 1996 by Larry Page and Sergey Brin, entrepreneurs who wanted a way to catalogue the internet's endless data. Google became their "idea to organise a seemingly infinite amount of information on the web."[20]

The interesting fact for Mark Zuckerberg, the creator of Facebook, is that he was part of the first generation born into the mass availability of the internet. Similar to ARPANET, Facebook was designed for universities, however its popularity soared and it was expanded across the globe.[21] Zuckerberg further transformed Facebook from a "static web service into a living, breathing world," by adding news feeds, dynamic status updates, delivering everything from international news to member's personal life.[22] In summary, the internet was created to connect people, society, and organisations globally in a way that would enable them to communicate, foster a sense of belonging and share ideas. Therefore, the internet was designed as, and remains, a social connection device.

[19] *Ibid*., 51.
[20] *Ibid*., 52.
[21] *Ibid*., 56.
[22] *Ibid*., 59.

SOCIAL MEDIA IS THE INTERNET

This section will argue that SM is not a new information medium, it is simply a communication and sharing platform which is a system to connect people globally. Toni Ahqlivst, a Research Director at Finland Futures Research Centre, defines SM as "the interaction of people and also to creating, sharing, exchanging and commenting contents in virtual communities and networks."[23] Facebook, Twitter and YouTube had been heralded as the start of the SM era. However, as discussed in the background, these platforms are not the first social networks. There have been many social platforms such as electronic mail, bulletin boards and chat groups launched throughout the 1980s and 1990s.[24] Therefore, an argument can be made that the internet is SM and SM must then be the internet.

There has been no other technology that has developed as fast and is as far reaching as the internet. The internet has supported social change since its evolution from ARPANET to the internet 40 years ago. Consider Iran's use of Twitter during the Green Movement, Burma's use of YouTube during the Saffron Revolution, and the dark side of social change by VEO and criminal organisations incitement of society.[25] As stated by political scientist Ronald Diebert and Rafal Rohozinski, former Director of the Advanced Network Research Group of Cambridge Security Programme, "cyber-technologies

[23] Levi J West. "#Jihad: Understanding Social Media as a Weapon." *Security Challenges* 12, no.2 (2016), 12.

[24] P.W. Singer. *Like War: The Weaponization of Social Media*. (New York: Houghton Mifflin Harcourt, 2018), 56.

[25] Ronald Deibert, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010), 43,48.

possess a special power, that they are technologies of liberations," deducing that SM is part of information and communication technology, thus, the internet.[26]

Many argue that SM is a new information domain because of its supremacy as a communication, sharing and collaboration tools. However, the internet was created to connect people, to share ideas and communicate in groups. The SM of today uses more technologically evolved platforms to connect people, but in essence is no different than society's intended use of the internet 30 to 40 years ago. For instance, in 1994 a group of marginalised workers in southern Mexico, the Zapatista National Liberation Army (EZLN), rose up to challenge the Mexican government.[27] The Mexican government took ruthless military action against the ELZN and drove them to the jungle. Cut off from traditional communication means, the ELZN leveraged the internet to connect with the world and share their story. The ELZN gained solidarity with international labour movements, foreign like-minded leftist movements, the international Red Cross and international journalists to capture the atrocities of the Mexican military.[28] The Mexican government was forced to cease military action as a result of the global pressure that came from all directions and all at once.

The ELNZ's use of the internet, Iranian use of Twitter, Burma's use of YouTube, and VEO and criminal organisations' incitement of society, all demonstrate how the internet is the platform for connection and social change. Soon after the ELZN revolt, one of the most recognised sociologists, Manuel Castells, stated that "the internet's

[26] *Ibid*., 43.

[27] P.W. Singer. *Like War: The Weaponization of Social Media*. (New York: Houghton Mifflin Harcourt, 2018), 53.

[28] *Ibid*.

integration of print, radio, and audiovisual modalities into a single system promises an impact on society comparable to that of the alphabet."[29] Castells' statement is even more accurate today as it was in 1996, given how individuals and business have used social platforms to connect easier and with greater information sharing. Meaning that the internet is what connects society globally and therefore SM is simply the internet.

SOCMINT VS. CAF INTELLIGENCE COMMUNITY

"The opportunities that the explosion of social media offer are remarkable. SOCMINT must become a full member of the intelligence and law enforcement family."[30] Sir David Omand, made the above statement, publishing several journals on SM and the need for law enforcement and security services to create a SOCMINT function which should be joined with IMINT, Human Intelligence (HUMINT) and SIGINT.[31] SOCMINT from an academic perspective is important as academics see SM as a method for providing insight into people and social groups, improved situational understanding of the operational environment, identifying the intent of criminal organisations.[32]A majority of the research into SM surround supporting law enforcement, and not the larger IC. The purpose of this section is to argue that the CAF has the capability to collect, analyse and exploit SM and a separate SOCMINT function is therefore not required.

[29] *Ibid*., 54.

[30] David Omand, Jamie Bartlett and Car Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (2012), 822.

[31] *Ibid*., 801.

[32] Simon Andrews, Ben Brewster and Tony Day. "Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online." *Security Informatics* 7, no. 3 (2018), 2.

Omand and fellow academics argue that SM requires a SOCMINT function since people transfer more of their personal lives to open spaces like SM, and law enforcement agencies have the responsibility to react and adapt.[33] Omand iterates that SOCMINT follows the same approach for the IC regarding process, collection, analysis and dissemination of intelligence products.[34] Further adding that a significant difficulty is social sciences have not established a methodology for analysing the information that evolves in the SM space. He believes a SOCMINT function would provide the required structure to properly access social contextual cues, behaviour and intent infused in the messaging of the person.[35] Omand and his colleagues argue for the need to respect privacy, particularly in the exploitation of closed source, or private SM information. In this case, he argues that a SOCMINT function would create the legal and ethical framework to protect society's private space against intrusive SOCMINT.[36] In his book *Securing the State*, Omand offers five principles from the HUMINT and SIGINT community the SOCMINT community should follow. These include sufficient, sustainable cause, integrity, necessity and proportionate methods, authority and oversight and intrusive intelligence should be a last resort and must be prospect of success.[37] Omand's recommendations center around the growing criminal and VEO use of SM from a law enforcement view and not from an IC view point.

[33] David Omand, Jamie Bartlett and Car Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (2012), 804.

[34] *Ibid*., 808.

[35] *Ibid*., 808,810.

[36] David Omand, Jamie Bartlett and Car Miller. "#INTELLIGENCE A balance between security and privacy online must be struck…" *Demos*. April 24, 2012, 37.

[37] *Ibid*., 41-46.

Omand applies his model to the domestic environment, however the CAF IC and law enforcement operate in a much different environment. For several reasons, SOCMINT could be ineffective in combating VEO and criminal organisations. Firstly, these groups operate in the shadows, always maneuvering to stay ahead of authorities, continually adapting and innovating to exploit the internet.[38] Secondly, many of these groups operate outside of western influence and in states that have far more relaxed regulations regarding privacy settings for personal accounts. This is compounded by the fact that some governments can go so far as to render services such as ISP's and mobile phone networks inoperative to prevent their exploitation.[39] Thirdly and probably more importantly, these groups are now undertaking more sophisticated procedures to protect their operational security by using encrypted platforms such as Telegram, Surespot or Kik and applying cyber security procedures.[40] A dedicated SOCMINT capability would not defeat the precautions taken by VEO and criminal organisations. Additional support from HUMINT, SIGINT and Cyber capabilities would be required to counter them. Private sector and law enforcement do not have access to other classified intelligence functions such as cyber or SIGINT and therefore rely solely on SOCMINT. For example, shipping companies have been monitoring the SM sites used by pirates to gain situational understanding of these criminals to increase the company's security awareness.[41] Unlike

[38] Ronald Deibert, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010), 48.

[39] *Ibid*., 51.

[40] Levi J West. "#Jihad: Understanding Social Media as a Weapon." *Security Challenges* 12, no.2 (2016), 22,23. Telegram, Surespot and Kik are communication platforms for people and groups who want to communicate in secrecy. These sites use end to end encryption software that make it impossible to read communication messages between individuals or groups who are not part of the chat session/group.

[41] William Marcellino, Meagan Smith, Christopher Paul and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. (Santa Monica, CA: *RAND Corporation,* 2017), 11.

law enforcement and the private sector, the CAF has further intelligence enablers at its disposal to analyse and exploit SM in greater detail.

The RAND corporation identified several limitations of SM in their report for the US Department of Defence on SOCMINT. Key limitations addressed were that the content on SM only represent a limited percentage of the population, and SM's global audience is varied. Data collected by SOCMINT is skewed by the participants and dependant on where the SM data is located, and there can be legal restrictions to its collection.[42] Furthermore, because SM is both public and private, intelligence services are operating in a grey space when collecting information from SM.[43] The CAF IC, on the other hand, is empowered to manage and operate in this grey space, through pre-existing intelligence capabilities such as HUMINT, SIGINT and Cyber. SOCMINT advocates' main argument is that analysts are not trained to understand SM or how to navigate these platforms. Without crossing into classified areas, the CAF analysts are trained in Open Source Intelligence (OSINT) collection methods and Cyber operators can operate and navigate the internet. This demonstrates that SM spans more intelligence functions than just SOCMINT, and that there is a multi-disciplinary requirement. The CAF has an All Source Intelligence Centre (ASIC) which includes geomatics (GEOINT), SIGINT, Cyber, HUMINT and IMINT functions. An advantage of the ASIC system used by the CAF is that it can use SM to focus and prompt the collection efforts of the other intelligence enablers.[44]

[42] *Ibid*., x.

[43] Kira Vrist Ronn and Sille Obelitz Soe. "Is social media intelligence private? Privacy in public and the nature of social media intelligence." *Intelligence and National Security* 34, no. 3 (2019), 363.

[44] Richard Evans. "Social Media Intelligence: Current Approaches & Emerging Opportunities." HIS White Paper, September 2013, 4.

Two major capabilities that the CAF ASIC has to analyse and exploit SM outside of the SOCMINT concept are Cyber and HUMINT. First, a critical vulnerability that SOCMINT does not address is cyber exploitation, nor have academics proposed any solutions to the manipulation of SM. US National Security Agency (NSA) Director, Michael Rogers stated "at the moment most of the cyber hacks have been theft, but what if someone gets into the system and starts manipulating and changing data to the point where now as an operator, you no longer believe what you are seeing in your system."[45] The Director of National Intelligence (DNI), James Clapper, added further that "I believe we'll see more cyber operations that will change or manipulate electronic information to compromise integrity."[46] These statements from the NSA Director and DNI came after a Syrian hacker gained access to the Associated Press's SM account. The Syrian hacker sent a tweet that stated there was an explosion at the White House and that the President was injured in the attack which caused the DOW to drop $136 billion.[47] SOCMINT analysis alone would not be proficient enough to detect manipulation to this extent. The CAF ASIC, on the other hand, would have operators trained in cyber exploitation who could potentially detect this breach and respond with messages to counter the attack.

In addition to cyber exploitation, one of the main flaws noted for SOCMINT analysis is the lack of social and behavioural sciences, as well as anthropological and social psychology perspectives of information gathered from SM. Understanding the messaging from the author, and or, interacting with people is not an easy skill to master.

[45] Gregory Treverton, Andrew Thvedt, Alicia Chen, Kathy Lee and Madeline McCue. "Addressing Hybrid Threats." *Swedish Defence University*, (2018), 56.

[46] *Ibid*.

[47] *Ibid*.

Omand emphasizes understanding human dynamics and social interaction of humans is a science and skill in itself. Thus, delivering social human interaction training to SOCMINT analysts would only scratch the surface, especially if it was only a one-time course with limited continuation training. Fortunately, the CAF has an intelligence function that specialises in human interaction. The HUMINT capability would be able to leverage and exploit SM to the fullest extent. HUMINT training, tactics and procedures (TTPs) are designed and tested to understand and exploit people to gain situational understanding. Therefore, CAF HUMINT TTPs could be easily adapted to conduct source operating on SM.

Finally, SOCMINT supporters argue that a SOCMINT function would legitimize the collection and exploitation of SM. This statement may hold true for law enforcement and other domestic security service, but for the CAF, there are rules, regulations and national oversight guiding HUMINT and Cyber/SIGINT functions. The HUMINT function does extensive training pertaining to the regulations and laws on sensitivities to recruit, manage, task and exploit human sources. HUMINT also has mandated national oversight of all recruitment, source operations and file management. Cyber/SIGINT follow similar rules and regulations to exploit signal and cyber platforms. These powers are being expanded by the Canadian Government in Bill C-59 which will allow the Canadian Security Establishment the "mandates to include both active (offensive) and defensive cyber operations" as well as improved accountability, review, and oversight.[48]

[48] Canadian Civil Liberties Association. "Ten Things You Need to Know About Bill C-59." September 12, 2017. https://ccla.org/ten-things-need-know-bill-c-59.

Therefore, the CAF Cyber/SIGINT and HUMINT capabilities already have the required legitimacy which Omand is a shortfall.

There is no denying that SM with its diverse range of human perspectives can provide the CAF situational understanding of the operational environment.[49] The CAF IC and law enforcement have differing operating environments and a SOCMINT function would be a waste of resources for the CAF to invest in. SOCMINT spans all domains of intelligence, and therefore should not be considered a standalone function. SOCMINT must be paired with other intelligence enablers and capabilities to be effective and exploited. The CAF ASIC embodies all the constraints and restraints that SOCMINT proponents argue it must have. Therefore, the CAF ASIC is more than capable of collecting, analyzing, monitoring and exploiting SM, compared to the SOCMINT function recommended by Omand.

INFORMATION WARFARE: THE WEAPONIZATION OF SOCIAL MEDIA

This section highlights the most critical function the SOCMINT model does not address: the exploitation of SM to support operations. P.W. Singer explored how business, States, criminal organisations and VEOs leveraged SM platforms to exploit society, governments and international organisations to achieve their goals. Weaponization of SM is simply IW, a significant hybrid tool used to remain in the grey zone of conflict. CAF adversaries use hybrid threats to achieve objectives without war,

[49] William Marcellino, Meagan Smith, Christopher Paul and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. (Santa Monica, CA: *RAND Corporation,* 2017), 7.

by opposing societies not militaries. If CAF adopts SOCMINT as its own IC function, the CAF will lose the IW against state and non-state actors who have perfected the weaponization of SM. The CAF has very capable resources that would give the CAF excellent IW capability, predominantly within Information Operations (IO) and Information Activity (IA). IO includes collection, analytics, cueing and Public Affairs (PA). IA incorporates the exploitation, manipulation and transformation of SM by Cyber/SIGINT and HUMINT. As discussed in section three, the CAF Cyber/SIGINT and HUMINT functions are positioned legally and ethically within federal legislation, regulations and oversight to conduct intrusive operations for IA.

Between national and deployed intelligence teams, the CAF has extremely good coverage of the world. That being said, one of the largest threats to Canada are hybrid threats. Russia is very good at operating in this grey space and have built an effective propaganda machine that they use to convey doubt in truths and policies on a host of information platforms.[50] The Russians use state sponsored news stations such as RT and Sputnik to propagate the Russian narrative in conjunction with SM to maximise the effect and reach of their operations.[51] The importance of hybrid/IW is critical for CAF adversaries for three reasons. First, the instruments used are not easily visible, especially in the cyber domain, making it difficult for the opponent to respond adequately.[52] Second, they are non-linear, making the information attacks very unpredictable, and therefore potentially more lethal than conventional attacks.[53] This unpredictability can be

[50] Gregory Treverton, Andrew Thvedt, Alicia Chen, Kathy Lee and Madeline McCue. "Addressing Hybrid Threats." *Swedish Defence University*, (2018), 48.

[51] *Ibid*., 37.

[52] *Ibid*., 60.

[53] *Ibid*.

accredited to SM and IW in the virtual domain. Third, targets, objectives and the medium for the attack can be changed quickly to maintain the information campaign.[54] Two of CAF adversaries that successfully use information and SM as a weapon are Russia and VEOs.

During Russia's annexation of Crimea in 2014, IW was used extensively to shape the environment and support covert operations and the conventional military invasion. The Crimea annexation is outside the scope of this paper to discuss, but the relevance of Russia's reliance on IW to spread propaganda and create unrest in Eastern Ukraine and Crimea led to the Russian military intervention. The Russian IW campaign in Crimea and future technological advances, including artificial intelligence, will continue to improve Russia's ability to dominate in the information spectrum. Technological advances in the information domain will only make it harder to identify and respond to fake news and disinformation. One scenario discussed in *Addressing Hybrid Threats* builds on the Ukraine conflict to describe what a future hybrid attack from Russia could look like:

> Targeted soldiers will receive demoralising message, like those spammed to Ukrainian soldiers. Ten minutes later, the soldiers compromised phone will access recent contacts and send "killed in action" messages to their families. Shortly after, the families will keep calling the soldiers distracting them from duty. Another demoralising message is sent "retreat and live." The cyber operation then shifts to kinetic action as the compromised phones reveal the soldiers' location and they are targeted by a massive artillery strike. Not long after, there is an infantry and tank attack.[55]

Another example is how VEOs control the "production, direction, editing, and dissemination of their messages" to the global community, which is a far contrast from

[54] *Ibid*.
[55] *Ibid*., 74.

traditional media such as newspapers.[56] VEO leaders understand the importance of SM as a communication platform for "terrorizing populations, indoctrinating recruits, consolidating power, and spreading propaganda."[57] What makes this a concern to the IC is how sophisticated and savvy VEOs have become, specifically in their use of and applying security precautions to their messaging. Hamas uses SM to communicate and coordinate between their operatives to plan attacks in the West Bank, Lebanon and Gaza.[58] ISIS added new social platforms to their SM accounts in the event their accounts were disabled, or security services started to monitor their accounts. Hezbollah has used IW against Israel extensively to influence international public opinion against the Israel Defence Force. In 2006, during the Lebanon war, Hezbollah edited photos of victims and first responders after an Israeli air strike to make the attack seem more as a war crime then military intervention.[59] Deceased AQ leader Anwar al-Awlaki leveraged the power of the internet and exploited SM through his own Facebook page and blog to support violent conflict, and recruit and train terrorist operatives.[60] What causes an even larger problem for the IC is that unlike newspapers, these VEOs do not need to be present in the region to pass their messages. Individuals are able to upload their message from home, internet cafes, mobile devices or Wi-Fi areas, which can be accessed from anywhere at any time adding to the complexity of monitoring and surveillance.

[56] Alexander Tsesis. "Terrorist Speech on Social Media." *Vanderbilt Law Review* 70, no. 2 (2017), 658.

[57] *Ibid*., 659.

[58] *Ibid*.

[59] William Marcellino, Meagan Smith, Christopher Paul and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. (Santa Monica, CA: *RAND Corporation,* 2017), 15.

[60] Alexander Tsesis. "Terrorist Speech on Social Media." *Vanderbilt Law Review* 70, no. 2 (2017), 661.

In *Addressing Hybrid Threats*, Gregory Treverton and his colleagues state "it is important to respond quickly to particular information operations, once discovered, both to minimize their impact and to deter other states or groups that might want to emulate attack."[61] Julian Assange, the Wikileaks founder, admitted that "releasing of secret documents are not random but are always timed to achieve specific political objectives."[62] The future of warfare is IW, and Treverton and Assange confirm information attacks are planned and coordinated. Without a capability to respond or counter the attack, the adversary will prevail in the information age. Therefore, it is critical the CAF adopt an IO and IA capability to weaponize SM to support CAF IW operations.

Information Operations

Effective IO starts with choosing the right message to send on SM and subsequent information mediums.[63] The CAF PA must be heavily involved with the CAF IC to deliver coordinated messaging. linked into the grand IO campaign as well as IA. This integrated messaging is critical in phase 0 in order to properly shape the environment by delivering early narratives that will anchor the message with the population to support additional messages as the operation evolves.[64] The US State Department has stated that an IO organisation is critical to counter VEOs messaging on SM:

[61] Gregory Treverton, Andrew Thvedt, Alicia Chen, Kathy Lee and Madeline McCue. "Addressing Hybrid Threats." *Swedish Defence University*, (2018), 6.

[62] *Ibid*., 36.

[63] Mats Erickson. "Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice." *International Journal of Strategic Communication* 12, no. 5 (2018), 531.

[64] Mica R. Endsley. "Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering." *Human Factors* 60, no. 8 (December 2018), 1084-1085.

> Responding to and quickly debunking misinformation, conspiracy theories, and urban legends is crucial to mission success in the war of ideas. The State Department maintains a public ‘Identifying Misinformation’ website in English and Arabic, which is devoted to countering false stories that appear in extremist websites and other web sources. The site focuses on disinformation likely to end up in mainstream media.[65]

In order to perfect the IO message, the CAF should further leverage the US’s work in IO by following their lead and organising forums, working groups with journalists and communication experts. This would give the CAF IO a competitive advantage in understanding how to determine source reliability and media accuracy as well as common misinformation techniques in countering adversary IO.[66]

Secondly, it is critical to “make friends before you need them.” The CAF HUMINT, PA and liaisons will need to leverage a diverse group of people who can support CAF messaging when called upon.[67] The PA and OSINT function of the CAF IC are required to disseminate the narrative on SM and all other information mediums. Relying on SM as the information platform is not good enough, because once people receive the initial story on SM they will tend to conduct confirmation bias and search other information sources to confirm their pre-existing expectations or beliefs.[68]

Lastly, SM complements other avenues to deliver information and should be used in conjunction with a more comprehensive information campaign that integrates both

[65] Time Aistrope. “Social media and counterterrorism strategy.” *Australian Journal of International Affairs* 70, no. 2 (2016), 127.

[66] *Ibid*., 128.

[67] Mats Erickson. “Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice.” *International Journal of Strategic Communication* 12, no. 5 (2018), 533.

[68] Mica R. Endsley. “Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering.” *Human Factors* 60, no. 8 (December 2018), 1085.

traditional media content within SM and centrally governed.[69] Since confidence in the information people receive needs to be from trustworthy sources, follow-up messaging on traditional platforms is critical to anchor the CAF narrative.[70] Cyber is an additional resource to support IO, particularly in cyber exploitation, which is a non-destructive method used to search and obtain information from networks or computers.[71] This information collection can be used to assist the IO team to develop the right message to target an identified audience.

Information Activity

A CAF IA function is critical to executing a successful IW campaign. IA can work singlehandedly or compliment the IO in shaping the environment. Unlike IO which would typically operate in the open source environment, IA could be more clandestine or secret in nature, a tactic Cyber/SIGINT and HUMINT are traditionally known for. The CAF Cyber/SIGINT and HUMINT have been tremendously successful in their individual traditional collection roles.

There is tremendous protentional for the CAF IC to exploit SM and the virtual world in support of CAF operations. The NSA and Defence HUMINT Service for example has been exploring and exploiting virtual gaming worlds because VEOs have started to use these virtual gaming worlds for “collaborative planning, communication

[69] Mats Erickson. “Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice.” *International Journal of Strategic Communication* 12, no. 5 (2018), 537.

[70] Mica R. Endsley. “Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering.” *Human Factors* 60, no. 8 (December 2018), 1085.

[71] Herbert S Lin. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4, no. 63 (2010), 63.

and training grounds" which are "private meeting places."[72] VEOs have been heavily relying on the virtual gaming world to perfect their planning, training and execution of missions due to the "fact that the terrorist mission is expensive, risky and dangerous" and because of the significant impacts they desire, it is better to practice in a simulated environment then for real.[73] The US defence agencies have been successful at gaining intelligence from a combined effort to exploit VEOs on virtual gaming networks. An integrated Cyber/SIGINT HUMINT team could leverage each speciality to exploit SM and the virtual world, similar to the US Defence IC in order to combat its adversaries.

Targeted surveillance and social-malware attacks are becoming more and more common in the cyber world and exploding on the dark side of the internet.[74] Considering CAF adversaries will be using similar tactics, HUMINT and Cyber/SIGINT would be well positioned to counter these threats in two ways. First, with the recruitment of sources who have access to adversary dark web platforms and second, in the application of source protection training to keep CAF intelligence sources from being identified as spies. The recruitment of HUMINT sources in SM platforms would enable the CAF IC to penetrate adversary cells to monitor communications, networks, learn their TTP's and understand their intentions. In order to exploit adversary SM from a Cyber/SIGINT perspective the delivery of a payload would need to be inserted into an adversary's network.[75] A payload will enable a Cyber/SIGINT Operator to exploit vulnerabilities and weaknesses in an

[72] Tim Stevens. "Security and Surveillance in Virtual Worlds: Who is Watching the Warlocks and Why?" *International Political Sociology* 9, (2015), 238.

[73] *Ibid*.

[74] Ronald Deibert, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010), 54.

[75] Herbert S Lin. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4, no. 63 (2010), 67.

adversary's network. The best way to deliver a payload is by loading the payload onto a network or acceptance through an online virus. HUMINT sources with access to adversary SM would be able to assist in delivering payloads in support of IA. These sources with the right training could also create secret back doors in SM platforms that would allow CAF IC to further collect valuable information on adversary social groups, communication networks and intent.[76] In conducting source operations, source security is paramount and for SM sources, HUMINT operators would be able to teach on-line source security tactics to protect themselves with the assistance of Cyber/SIGINT. Additionally, Cyber/SIGINT could be used in an offensive manner, to push adversaries to use other SM platforms or communication means as well as deny them the use of them all together in order to support pre-planned CAF IA operations.

The CAF can no longer afford to ignore the benefits of SM to support the IW campaign, specifically with considering SM's power to transform a crisis into a favourable advantage.[77] The only question now is how to integrate it into the information campaign. In such a complex hybrid information environment, SOCMINT alone will not combat CAF adversaries now and into the future. As demonstrated IW is an effective solution. The CAF will require a fulsome IW capability that can deliver coordinated IO and IA effects. To achieve this, the IO must be integrated within a robust PA and ASIC function to ensure the CAF information campaign is credible and able to reach all aspects of society. Cyber/SIGINT and HUMINT must integrate their specialties to exploit SM and the virtual worlds where CAF adversaries are now operating. Finally, the IW

[76] *Ibid*., 66.

[77] Mats Erickson. "Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice." *International Journal of Strategic Communication* 12, no. 5 (2018), 538.

campaign must have a feedback loop to understand if the message has had the desired effect. The IO and IA capabilities must coordinate their resources to confirm that the message is achieving the aim. Integrating these capabilities under one organisation will ensure that the required synchronisation will take place to support the mission.[78]

CONCLUSION

Many academics have argued that SOCMINT is a new information domain and that it needs to be stood up as a new intelligence function. Except, SM is not new, it is the internet which simply uses more technologically inclined software to connect people. The SOCMINT concept could potentially work well for law enforcement in combating a less sophisticate adversary. However, for the CAF, who faces state adversaries with more capability and less stringent rules as well as VEOs who have global reach, SOCMINT will not suffice. SM spans all domains of intelligence and to completely exploit SM it must be paired with other CAF intelligence capabilities which are part of the ASIC. The CAF IC has the capacity to collect, analyse and exploit information on SM and subsequently the CAF does not need to create a SOCMINT function as argued by Sir David Omand. More importantly, as discussed, a robust IW capacity that comprises IO and IA capabilities will be required by the CAF to combat the likes of Russia, China, Iran and the various VEOs that continue to operate and advance in the information domain.

Instead of SOCMINT becoming a separate intelligence function, a more intelligent approach would see it evolved into a new academic discipline as part of the

[78] Mica R. Endsley. "Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering." *Human Factors* 60, no. 8 (December 2018), 1088.

social science umbrella. An academic discipline would give it the theoretical rigour required, in addition to educating the public on the vulnerabilities that come with SM. Furthermore, the SOCMINT idea can evolve a step further and become part of national education strategy to socialize society on the weaponization of information, partially from SM. This strategy could partner with business as well as academia to deliver educational programs that could demonstrate how to apply critical thinking towards SM, specially taking into account fake news, disinformation, and the protection of private data. A national counter IW approach would benefit Canada, particularly as evidence has proven the meddling of state actors in national elections, economies and social movements. Finally, SM is only the enemy if you do not understand its limitations and vulnerabilities. As emphasized in section four, SM has the power to transform a crisis into a favourable advantage.

BIBLIOGRAPHY

Aistrope, Tim. "Social media and counterterrorism strategy." *Australian Journal of International Affairs* 70, no. 2 (2016), 121-138.

Andrews, Simon, Brewster, Ben and Day, Tony. "Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online." *Security Informatics* 7, no. 3 (2018), 1-21.

Business and Economics, "What is Business Intelligence." *Progressive Digital Media Technology News*, last accessed 13 January 2019, https://search.proquest.com/docview/1794545.

Canadian Civil Liberties Association. "Ten Things You Need to Know About Bill C-59." September 12, 2017. Last accessed 30 April 2019, https://ccla.org/ten-things-need-know-bill-c-59.

Cogan, Charles. "Hunters not Gatherers: Intelligence in the Twenty-First Century." *Intelligence & National Security* 19, no. 2 (2004), 304-321.

Davies, Philip H.J. "Information Warfare and the Future of the Spy." *Information, Communication & Society* 2, no. 2 (1999), 957-969.

Deibert, Ronald and Rohozinski, Rafal. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010), 43-57.

Endsley, Mica R. "Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering." *Human Factors* 60, no. 8 (December 2018), 1081-1094.

Erickson, Mats. "Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice." *International Journal of Strategic Communication* 12, no. 5 (2018), 526-551.

Evans, Richard. "Social Media Intelligence: Current Approaches & Emerging Opportunities." IHS White Paper, September 2013. Last accessed 25 April 2019, www.ihs.com/osint.

Fournier, Susan, Quelch, John and Rietveld, Bob. "To Get More Out of Social Media, Think Like an Anthropologist." 2016. Last accessed March 20, 2019, https://hbr.org/2016/08/to-get-more-out-of-social-media-think-like-an-anthropologist.

Grove, Nicole Sunday. "Weapons of mass destruction: Social media, violence entrepreneurs, and the politics of crowdfunding for war." *European Journal of International Relations* 25, no. 1 (2017), 86-107.

Ivan, Adrian, Iov, Claudia, Lutai, Raluca and Grad Marius. “Social Media Intelligence: Opportunities and Limitation.” *CES Working Papers* 7, no. 2A (2013), 1-6.

Landon-Murray, Michael. “Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate.” *Journal of Strategic Security* 8, no. 3 (2015), 67-79.

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4, no. 63 (2010), 63-86.

Lyon, David. “Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity.” *International Journal of Communication* 11, (2017), 824-842.

Mahadevan, Prem. “A Wilderness of Shifting Mirrors.” *The RUSI Journal* 155, no. 5 (2010), 38-43.

Marcellino, William, Smith, Meagan, Paul, Christopher and Skrabala, Lauren. “Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations.” Santa Monica, CA: *RAND Corporation,* 2017. https://www.rand.org/pubs/research_reports/RR1742.html.

O’Brien, Kevin A. “Managing national security and law enforcement in a globalised world.” *Review of International Studies* 35, (2009), 903-915.

Omand, David, Bartlett, Jamie and Miller, Carl. “#INTELLIGENCE A balance between security and privacy online must be struck…” *Demos*. April 24, 2012. Accessed April 8, 2019. https://demos.co.uk/project/managers-too.

Ohmand, Sir David, Bartlett, Jamie and Miller, Carl. “Introducing Social Media Intelligence (SOCMINT).” *Intelligence and National Security* 27, no. 6 (*2012), 801-823*.

Perez, Beatrice, Musolesi, Mirco and Stringhini, Gianluca. “You are your Metadata: Identification and Obfuscation Social Media Users using Metadata Information.” *Association for the Advancement of Artificial Intelligence,* (2018). www.aaai.org

Pun, Darien. “Rethinking Espionage in the Modern Era.” *Chicago Journal of International Law* 18, no. 1 (Summer 2017), 353-391.

Reid, Ian D., Gonza, Lynsey F., and Boon, Julian CW. “From Tactical to Strategic Deception Detection: Application of Psychological Synthesis.” *Journal of Strategic Security* 10, no. 1 (2016), 81-101.

Richey, Melonie K. and Binz, Mathias. "Open Source Collection Methods for Identifying Radical Extremists Using Social Media." *International Journal of Intelligence and CounterIntelligence* 28, no. 2 (2015), 347-364.

Ronn, Kira Vrist and Soe, Sille Obelitz. "Is social media intelligence private? Privacy in public and the nature of social media intelligence." *Intelligence and National Security* 34, no. 3 (2019), 362-378.

Sano, John. "The Changing Shape of HUMINT." *Intelligencer: Journal of U.S. Intelligence Studies* 21, no. 3 (Fall/Winter 2015), 77-80.

Saugmann, Rune. "The civilians visual security paradox: how open source intelligence practices create insecurity for civilians in warzones." *Intelligence and National Security* 34, no. 3 (2019), 344-361.

Singer, P.W. *Like War: The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt, 2018.

Statisa. "Number of social media users worldwide from 2010 to 2021 (in billions)." Last accessed May 5, 2019. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Stevens, Tim. "Security and Surveillance in Virtual Worlds: Who is Watching the Warlocks and Why?" *International Political Sociology* 9, (2015), 230-247.

Sun, Qindong, Cao, Han, Qi, Wenjing and Zhang, Jingpeng. "Improving the security and quality of real-time multimedia transmission in cyber-physical-social system." *International Journal of Distributed Sensor Networks* 14, no. 11 (2018), 1-10.

The Cove. "The Tactical Application of Open Source Intelligence (OSINT)." January 16, 2019. Last accessed March 20, 2019. https://www.cove.org.au/war-room/article-the-tactical-application-of-open-source-intelligence-osint

Treverton, Gregory, Thvedt, Andrew, Chen, Alicia, Lee, Kathy and McCue Madeline. "Addressing Hybrid Threats." *Swedish Defence University*, (2018), 1-92. Accessed 8 April 2019. www.fhs.se

Trottier, Daniel. "Open source intelligence, social media and law enforcement Visions, constraints and critiques." *European Journal of Cultural Studies* 18, no. 4-5 (2015), 530-547.

Tsesis, Alexander. "Terrorist Speech on Social Media." *Vanderbilt Law Review* 70, no. 2 (2017), 651-708.

Uldam, Julie. "Social Media Visibility: Challenges to Activism." *Media, Culture & Society* 40, no. 1 (2008): 41-58.

West, Levi J. "#Jihad: Understanding Social Media as a Weapon." *Security Challenges* 12, no.2 (2016), 9-26.

Zhou, Pan, Wang, Kehao and Wu, Dapeng. "Differentially-Private and Trustworthy Online Social Multimedia Big Data Retrieval in Edge Computing." *IEE Transactions on Multimedia* 21, no. 3 (March 2019), 539-554.