THE ROLE OF SOCIAL MEDIA IN THE MILITARY

Namosha Veerasamy
*Council for Scientific and Industrial Research (CSIR)**
*Pretoria, South Africa **

William Aubrey Labuschagne
*Council for Scientific and Industrial Research (CSIR)**
*Pretoria, South Africa **

ABSTRACT

We now live in a digital, interconnected world. Social media has emerged as a pervasive component of this digital age in which having an online presence dominates. Facebook, Twitter and LinkedIn all provide modern forms of engagement for organisations including the military. However, the dangers of these brisk and innovative forms of communication should not be overlooked. Social media can capture a wealth of information regarding an organisation's operations, functions, roles, responsibilities, projects and related details about the Information and Communication Technology (ICT). In the wrong hands, this information can be leveraged into intelligence that can be further utilised to profile individuals or launch cyber attacks.

This paper discusses the role that social media can play in the military- both beneficial and detrimental. It does so by presenting the arguments for its positive uses, as well as how it can be manipulated for malicious purposes. Social media can be utilised by individual and leaders in the military as an effective form of modern communication that serves as a helpful and dynamic tool for interaction. However, social media can also be utilised for malevolent uses like malware propagation and terrorist propaganda . In this paper, the beneficial and adverse functionality of social media is explored so as to discuss its useful contributions to the military, as well as create awareness of how it can be negatively exploited.

KEYWORDS

Communication, digital, military, propaganda ,social media.

1. INTRODUCTION

Social media has brought about a global transformation in personnel and professional exchanges. The penetration of social media is unprecedented and its reach is far spread. We are living in an era dominated by cyber devices- smart phones, tablets, laptops, social media, Youtube and blogs are the all predominant tools employed by the masses. Life has become digital and users are engaged in a myriad of online activities- shopping, music download, communication and job hunting are just some of the activities users digitally absorb themselves in. On-line communities are growing as users can pursue interests and skills through these forums. Online forms of media encourage group activities, interactions and social behaviour through ease, convenience and appeal of its features. Users are continuously communicating and interacting on social media. Facebook Messenger and Whatapp handle 60 billion messages a day (Smith (a) 2016).

Users have embraced social media adoption and usage. However, social media can serve as both an opportunity and threat in the military. While it provides tremendous transparency and interaction, it can also present a threat through uninformed and malicious use. Social media has affected not only peaceful human interaction but affected extremist, irregular warfare and terrorism in such an inexplicable way that is just being understood by militaries of the world (Sethi 2013).

This paper discusses the role that social media can play in the military- both beneficial and detrimental. It does so by presenting the arguments for its positive uses, as well as how it can be manipulated for malicious purposes. The positive uses of social media for the military is initially discussed. Thereafter the challenges of social media are discussed.

2. OPPORTUNITIES

Military users need to tap into the full potential of social media to realise its possibilities for information exchange, awareness creation and communication capabilities. Embracing social media could provide a vital medium for functional uses like influence, knowledge generation, networking and information dissemination. The medium can be used to instantly share data and stories and operational lessons that can help develop better strategies for future campaigns. "Speech and reach" is a powerful capability of social media that pales in comparison to conventional forms of communication like postal services and printed media.

Social media has provided a perfect global medium through which military professionals can engage in discourse and debate (Ryan and Thompson 2016). Military dialog can be facilitated through the medium of social media that encourages discussion, interchange and deliberation of ideas and critical topics.

Networking and extending professional connections are added benefits of social media.Development sessions can be carried out through videos demonstration of leadership techniques, awareness and strategies. Social media networks built in peacetime might be mobilized during war to help gain situational awareness, advance messaging, and aid in collaboration with our partners and allies (Byerly 2015).

Social media can help bridge the generational gap between older work forces and younger military members (Ryan and Thompson 2016). Embracing this newer form of communication will help older generations keep in touch with more modern methods of interaction and information exchange.

Strategic communication and public affairs can be supported by social media. The open forum helps foster transparency and can be usefully employed in the daily operations of the military. Through the publication of key objectives and programs, the aims of military organisations can be better understood.

An added benefit of social media is the support it can provided to military families. Through social media broadcasts, military families can grasp the difficulties and view the accomplishments of relatives. In this way, family members and the public can support each other and gain an awareness and understanding of difficult assignments and exercises.

Acknowledgement and appreciation for achievement can also be provided by social media (Ryan and Thompson 2016). While military organisation recognise achievement through ceremonies that award medals, ribbons and commendations, social media can also be used to publicise these accomplishments. Posts acknowledging achievement show appreciation for outstanding acts, deeds, successes and triumphs.

Educational and training initiatives can also be explored through social media. Information can be captured in a digital medium which can be quite engaging for the user. This can stimulate greater learning in an enriched and appealing experience. Quizzes, games, tutorials, video segments, broadcasts, lectures, webinars and podcasts are just some of the educational forums that social media can be used to provide learning and training. The US Department of Defense offers various educational training on social media (Available at http://dodcio.defense.gov/Social-Media/Social-Media-Education-and-Training/).

Social media can be utilised as a cognitive weapon and exploited for perception management. Influence, speed and accessibility all enable social media to be an effective tool in swaying opinion and shaping views. Due to the interactive nature of social media, the effect of a marketing, recruitment or informational campaign can be gauged. Users post opinion, engage in the medium, make enquiries and can react to messages posted. Feedback from social media can help determine the effect of the ideas publicised.

Through social media, people can also organise themselves to protest against the government. The Arab Spring uprising demonstrated the ability to organise the public to engage in anti-government protests. Twitter emerged as a key source for real-time logistical coordination, information, and discussion among people, both within the Middle East and North Africa (MENA) and across the globe (Lotan et al. 2015). Social movements can be promoted through the capabilities of digital communications. The interconnectedness and span of social networks has resulted in a powerful recourse for influencing the public. Social networks can be an effective unifying tool and help coordinate the activities of the masses (Fridman 2013). This social revolution has led to individuals unifying together for a common cause as was the case for Arab Spring uprising. One of the force multipliers of social media is the ease of use of mobile devices. At the swipe of a finger, prominent members in the group co-ordinate activities and provide instructions to be carried out.

A further use of social media for the military is sentiment analysis whereby a profile is built to determine how an individual feels about a particular topic (Albright 2015). Marketing companies could use sentiment analysis to determine how the public feels about a particular product and so too the military could use

sentiment analysis to gauge users' feelings and reactions to certain subject matters. Sentiment analysis could then be utilised as part of publicity campaigns, diplomacy projects, recruitment and intelligence gathering.

Narratives can also be controlled through social media. Cross-Media Narratives are stories projected through social media and are, in essence, characterized by being centred on social media characteristics and supporting stories that are self-contained and smaller in scale (Nissen 2015). Furthermore, the narrative's supporting stories are told through multiple sites or platforms and from different angles. Through the use of "sock puppets", accounts can be created to automatically take part in conversations and respond on social media. Responses from sock puppets are generated to appear and the tone and direction of the responses can be programmed in various ways. It could appear that a similar opinion is felt or on the other spectrum opposing comments can be posted. Already in 2013, China had been using an army of sock puppets known as the 50 Cent Party to control public opinion (Elsner 2013).

Social media can aid in the location of persons of interest based on the information in the geotags of tweets or Facebook updates. It could also be used to identify locations of interest like areas that crimes are being carried out or storage facilities for weapons of mass destruction. Protection of critical sites to prevent them falling into the hands of terrorist groups can be aided by geotag identification and analysis.

From an offensive point of view, the military could utilise social media to plant malware into an enemy group. This could be used as a cyber attack or to gather intelligence. This form of social engineering would aptly serve military objectives in the case of an offensive or information gathering mission.

3. CHALLENGES

Social media has influenced not only normal forms of communication but also opened up a new battlefield for militaries, terrorists, extremists and governments. Irregular warfare is now being carried out in this new battlefield whereby socio-technical transformations are taking place.

Terrorist organisations actively use social network for recruiting new members, influencing opinions and communicating about operations. Extremists of all kinds are increasingly using social media to recruit, radicalise and raise funds (Telegraph 2014). The Internet has become a playground for arms and drugs deals which all fund extremist activities. Terrorist groups use the net to communicate with potential recruits and sympathisers in order to gain support for their actions. Social media have played an essential role in the *jihadists'* operational strategy in Syria and Iraq, and beyond with Twitter in particular being used to drive communications over other social media platforms (Klausen 2014). Powerful messages are distributed in order to condone their activities and elicit the message of jihad. American companies like Twitter, Facebook, Google, Apple, Microsoft, Yahoo and other popular services, including YouTube, WhatsApp, Skype, Tumblr and Instagram, are facilitating global jihad (Carmon and Stalinsky 2015). These new forms of media have helped increase and maintain support for extremist organisations. Unfortunately, social media has also become a playground for propaganda campaigns which spread anti-national messages. Some websites allow users to download an "e-jihad" application through which users can launch a low-level denial-of-service cyberattack on a specified target (Theohary 2015).

Digital platforms are now a battleground for a "war of ideas, words and images" whereby influence is being used to convince the public to support causes and draw the enemy into being a follower of the promoted cause. Extremist groups are using social media as a strategic weapon to shape the narrative and influence opinion so as to engage in conflict. Social media processes and practices accelerate terrorism incident consequences, acting as multipliers, enabling short- and longer-term follow-through (Lohrmann 2016). Social media is used to spread violent videos and photos, publish biographies of martyrs and promote other ideological texts. Isis has proved fluent in YouTube, Twitter, Instagram, Tumblr, Internet memes and other social media (Telegraph 2014).

Social media now plays a prominent role in the recruitment and radicalisation of new warriors to carry out terrorist activities. Training, fund raising, propaganda and publicity are all carried out through social media as it is directed at a persuasive audience who are easily swayed by videos, graphics and online messages.

Just as social media can be used to identify persons of interest in the geotags of tweets and Facebook images, the reverse is also true about personal information disclosure related to military personnel, family and associates. If multiple data sources are correlated, intelligence could be gathered that disclosed personal information about military personnel, family members, friends and locations. Details like the location,

equipment, types of troops, times and leaders could be identified through inappropriate posts. Seemingly innocent posts could actually contain sensitive information that endangers soldiers by revealing locations, security measures, mission operations, or troop movements, (Ferdinando 2014). A member's interests and activities could be deferred when users "like" posts on Facebook or retweet.

The sharing of information on social media has its associated risks in that it can reveal tactics, techniques, procedures, locations and training details to the adversary. Family and friend information could also potentially be disclosed. A proper social media policy can address some of the issues related to the safe sharing of information on social media.

Another risk emanating from social media is malware cyber attacks. Phishing and malicious links in drive-by-downloads can infect users with malware. Social engineering is primarily used to entice users to click on links with appealing headlines like "OMG!" "Amazing!" and "Shocking!".

A major flaw of social media is the potential to publish fake news. Fake tweets could be published in a political campaign like that of Donald Trump. When somebody clicks on something just based on the headline and shares it without even reading an article, let alone checking it, they are the not just the victims but they become the perpetrators because they spread it to a lot of people who more likely believe the story is true as they receive it from a friend (Zamudio-Suarez 2016).

Fake profiles can also be spoofed and used to trick users on social media. Unquestioning users can easily trust a friend request and begin interacting with an unknown contact. These may be bots or scammers that try to elicit information or money from unsuspecting users. Other issues related to spoofed accounts are the spread of scams, fraud, phishing attempts and even malicious software (IdtheftCentre 2017). Cyber safety awareness is important to prevent falling prey to scam artists and criminals on the web. In the next section, a few guidelines are proposed to help prevent users from making critical mistakes while using social media.

4. GUIDELINES

Social media has been widely adopted and its use will continue to grow. Therefore, it is essential that when engaging in social media that users be aware of inherent risks and safe practices to follow. Brigadier Mick Ryan and Brigadier Marcus Thompson provide the following guidelines for military members using social media (2016):

- Arranging privacy settings to protect a personal social media profile, noting that individual account settings can affect anyone that has links to that account.
- Speaking to family and friends about what they post and 'tag' to their social media accounts.
- Considering what is uploaded, whether it is an image or information, and who may access it.
- Awareness of geo-data attached to uploaded content.
- Considering whether there is a need to identify as a military member, and what other personal and sensitive information is attached to a member's social media profile.

Readers also need to be educated about their vulnerability and literacy in making as assessment of what they look at online (Zamudio-Suarez 2016). This could help prevent the spreading of fake news. Social media best practices needs to form part of awareness training for home and organisational users. Users need to be made aware of the good and malicious users of the cyberspace and trained appropriately on the topic so that they can be aware of influence campaigns, phishing, malware and malicious links.

Staff Sgt. Dale Sweetnam, with the Online and Social Media Division, Office of the Chief of Public Affairs compiled the Army's Social Media Handbook and conducts training for Soldiers about the dos and don'ts of posting on social media (Ferdinando 2014). The dos include using social media to get out the message of your command, inform the public of Army activities or stay connected with loved ones. The don'ts, include revealing sensitive information about missions, units or soldiers.

By following these guidelines, it can help balance out the risks associated with the use of social media. Social media can still be utilised for personal and professional practices when used appropriately not to disclose sensitive information, cause a malware infection or be influenced by propaganda campaign.

5. CONCLUSION

New operational realties has emerged and it imperative that the military develop new methods of response in the digital age. Social media provides an apt forum through which communication, perception management, intelligence, organisational capabilities and education can be carried out. The compelling use of social media is derived from its ability to easily share information as a rapid pace. However, social media can also be used in a negative manner in the military. Social media has its inherent risks like information disclosure, malware infection, propaganda campaigns, negative perception management, counter-intelligence and spoofing. Users need to exercise care to minimise their risk of exposure. Due to the rapid adoption of social media, its use will continue to grow. There arises a strong need for education and guidance on the safe use of social media in the military. This paper discusses both the beneficial uses of social media in the military, as well as the challenges of this digital medium.

REFERENCES

Albright D, 19 February 2015, How Social Media is the Newest Military Battleground, Makeuseof, [Online] Available at: http://www.makeuseof.com/tag/social-media-newest-military-battleground/ [Accessed 6 December 2016].

Byerly J, Harnessing Social Media for Military Power, 20 August 2015, Warontherocks, [Online] Available at : https://warontherocks.com/2015/08/harnessing-social-media-for-military-power/ [Accessed 6 December 2016].

Carmon Y and Stalinsky S, Terrorist Use of US Social Media is a National Security Threat, 30 January 2015, Forbes, [Online], Available at : https://www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/#5199d9447619 [Accessed 21 June 2017].

Elsman K. China Uses an Army of Sockpuppet to Control Public Opinion- and the US will too, 27 November 2013, Guardian, [Online] Avilable at : http://guardianlv.com/2013/11/china-uses-an-army-of-sockpuppets-to-control-public-opinion-and-the-us-will-too/ [Accessed 12 December 2016].

Ferdinando L, Maintaining Operational Security with Social Media, 2014, Military.com, [Online], Available at : http://www.military.com/deployment/maintaining-operational-security-with-social-media.html [Accessed 21 June 2017].

Fridman O, The Power of Social Media: Analyzing Challenges and Opportunities for Future Military Operations, *SEDTC Politics Postgraduate Conference*, 20 March 2013, London.

IdtheftCentre, Fake Socia Media Profiles, Watch What You Click, 2017, [Online], Available at: http://www.idtheftcenter.org/Cybersecurity/fake-social-media-profiles-watch-what-you-click.html [Accessed 24 June 2017].

Lohrmann D, How Terrorists Use of Social Media Points to the Future, 20 June 2016, Govtech,com, [Online], Available at : http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html [Accessed 21 June 2017].

Lotan G, Graeff E, Ananny M, Gaffney D, Pearce I and Boyd D, The Revolutions Were Tweeted: Information Flows During the 2011 Tunisian and Egyptian Revolutions, International Journal of Communications, 2011, 5.

Klausen J, 2014, Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq, Studies in Conflict and Terrorism, 2015, 38 (1), pp. 1-22.

Ryan M and Thompson M, Social Media in the Military " Opportunities, Perils and a Safe Middle Path, 21 August 2016, Grounded Curiosity, [online] Availabe at : http://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/ [Accessed 13 December 2016].

Sethi U, " Social Media- A Tool for the Military", *Scholarly Warrior*, Spring 2013, pp. 125-129.

Available at : https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[Accessed 16 January 2017].

Smith K (a), 2016 Social media statistics, Brandwatch.com [online] Available at : https://www.brandwatch.com/blog/96-amazing-social-media-statistics-and-facts-for-2016/ [Accessed 16 January 2016].

Theohary CA, The Role of Social Media in Conflict, 4 March 2015, CRS Insights, [Online] Available at : https://fas.org/sgp/crs/misc/IN10240.pdf.

Telegraph, How Terrorists are Using Social Media, 4 November 2014, [Online] Available at : http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html [Accessed 12 January 2016].

Zamudio-Suarez F, A Profession Once Targeted by Fake News Now is Helping to Visualise it, 22 December 2016, Chronicle, [Online] Available at : http://www.chronicle.com/article/A-Professor-Once-Targeted-by/238742 [Accessed 14 January 2016].