Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

Influence Techniques Using Social Media

Anthony Seaboyer
Royal Military College of Canada

Prepared by:
Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4

Contract Number: 123455
Technical Authority: Ritu Gill, PhD
Contractor's date of publication: August 2018

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2018-C177
September 2018

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

Truth, Duty, Valour • Vérité, Devoir, Vaillance

ROYAL MILITARY COLLEGE OF CANADA • COLLÈGE MILITAIRE ROYAL DU CANADA

PO Box 17000, Station Forces • CP 17000, Succursale Forces • Kingston, Ontario • K7K 7B4

Influence Techniques Using Social Media

by:

Anthony Seaboyer
Department of Political Science
Royal Military College of Canada

Prepared by:
Anthony Seaboyer
Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4
(613) 985-6111
Anthony.seaboyer@rmc.ca

RMC Project Manager:
Anthony Seaboyer

Contract Scientific Authority:
Ritu Gill, PhD
DRDC Toronto
Ritu.Gill@forces.gc.ca
416-635-2000 x3002

Introduction

The emergence of social media in the form of Friendster in 2002 and particularly Facebook in 2007, has drastically changed communication within and toward target audiences in form, frequency and reach.[1]Unparalleled influencing opportunities have emerged from social media's low production costs, minimal skill sets required to create content and real-time delivery to platforms audiences voluntarily check 150 times a day.[2] Social media platforms have become so adept in directing content to their user base that younger generations practically live on the sites, communicating with friends (real and virtual), receiving or sharing information, meeting dating partners and hanging out to the extent that they are voluntarily (but often unknowingly) subjecting themselves to near constant influencing activities.[3]

With this infrastructure available to all actors in the information space – human or not[4] – audiences are subjected to an infinite volume of communication that competes for their attention on a scale never seen before in history.[5] This barrage of signals has led to the existence of a level of noise[6] in the information space that significantly impacts the ability to affect reliable desired behavioural change.[7]

Non-state actors, particularly in the form of companies that own the social media services, are increasingly dominating the information space[8] – vastly different from other security domains that are dominated by state actors. The new platforms have clearly broken the barrier between the traditionally few producers that had a considerable information monopoly and the many others that had a mere passive role and just consumed their products. On social media, any person is now simultaneously a consumer and a producer of information as soon as a post is uploaded. What we have witnessed is (seemingly)[9] the democratization of media – though the actual effect of

[1] Watts, Clinton (2018): Messing with the Enemy, Surviving in a Social Media world of Hackers, Terrorists, Russians, and Fake News, Harper Collins, New York.

[2] Brandon, John (2017): The Surprising Reason Millennials Check Their Phones 150 Times a Day, Inc.com; 17 April 2017. https://www.inc.com/john-brandon/science-says-this-is-the-reason-millennials-check-their-phones-150-times-per-day.html.

[3] Gilroy-Ware, Marcus (2017): Filling the Void, Emotion, Capitalism & Social Media, Repeater Books, London.

[4] Greengard, Samuel (2015): The Internet of Things, The MIT Press, Boston.

[5] Vaidhyanathen, Siva (2018): Antisocial Media, How Facebook Disconnects Us and Undermines Democracy, Oxford.

[6] "Noise" refers to signals in the information space that are not of interest to recipients. Actors (for example Russia) have deliberately attempted to overflow the information space with signals to crowd out unwanted information and access to meaningful content to reduce the sharing of undesirable knowledge.

[7] Stieglitz, Stefan/Mirbabaie, Miland/Ross, Bjorn/Neuberger, Christoph (2018): Social media analytics – Challenges in topic discovery, data collection, and data preparation, International Journal of Information Management, Vol. 39, pp. 156-168.

[8] Shaw, Tamsin (2018): Beware the Big Five, The New York Review of Books, 5 April 2018. http://www.nybooks.com/articles/2018/04/05/silicon-valley-beware-big-five/.

[9] Gillespie, Tarleton (2018): Custodians of the Internet, Platforms, Content Moderation and the Hidden Decisions that shape Social Media, Yale University Press, New Haven.

social media on democracies is still very much a matter for debate.[10]Theoretically, anyone can have access to potentially very large audiences.[11]While many advantages for the competition of ideas and policies have emerged through the vast increase of access to information, influencing specific behavioural change in the information space, has become increasingly complicated. Not only because of the exponential increase of actors and “noise” but also due to audiences being increasingly aware of influencing efforts through multiple scandals of data misuse even by actors such as the President of the United States.[12] This is further complicated by countries such as China[13] and Russia[14] that restrict access to Western social media and have implemented their own national alternative to social media such as VKontakte, the Russian version of Facebook, or Weibo, the Chinese equivalent of Twitter, to control domestic access. Access for influencers is becoming even less reliable through the introduction of upload filters where algorithms already censor content during the uploading process before it even reaches any audience members.[15]Leaked documents detail the exact censorship process for example on Weiboo.[16]

The role of information itself has changed both for the consumer and the producer as societies have become increasingly information-based.[17] Societies have generally become far more transparent as never before seen quantities of information – intended and unintended, controlled and uncontrolled – enter the public domain. While social media itself has also created new forms of distraction that can reduce the actual transparency for individual users.[18]In an environment in which any person can have the attention of a large audience at any moment, government authorities need to reconsider their messaging practices to have a desired effect in the information space. The default preference of many in government, specifically in the security community, to stay out of

[10]Lanier, Jaron (2018): Ten Arguments for Deleting Your Social Media Accounts Right Now, MacMillan, New York.

[11] The Economist Staff Report (2016): Free Speech Under Attack, The Economist, 4 June 2016. https://www.economist.com/leaders/2016/06/04/under-attack.

[12]Ineca, Marcello/Vayena, Effy (2018): Cambridge Analytica and Online Manipulation, Scientific American, 30 March 2018. https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/.

[13]Pen America (2018): Forbidden Feeds, Government Controls on Social Media in China, Pen America; 13 March 2018. https://pen.org/wp-content/uploads/2018/03/PENAmerica_Forbidden-Feeds-3.13-3.pdf.

[14]BBC (2018): YouTube and Instagram Face Russian Bans, BBC News, 14 February 2018. https://www.bbc.com/news/technology-43058399.

[15] Ranking, Jennifer (2018): EU Votes for Copyright Law That Would Make Internet a 'Tool for Control', The Guardian, 20 June 2018. https://www.theguardian.com/technology/2018/jun/20/eu-votes-for-copyright-law-that-would-make-internet-a-tool-for-control.

[16] Yang, Yaqiu (2016): The Business of Censorship: Documents Show How Weibo Filters Sensitive News in China, Committee to Protect Journalists, 3 March 2016. https://cpj.org/blog/2016/03/the-business-of-censorship-documents-show-how-weib.php. See also Ng, Jason Q. (2014): Tracing the Path of a Censored Weibo Post and Compiling Keywords That Triggered Automatic Review, The Citizen Lab; 10 November 2014. https://citizenlab.ca/2014/11/tracing-path-censored-weibo-post-compiling-keywords-trigger-automatic-review/.

[17] Quinn, Michael J (2016): Ethics for the Information Age, 7th Edition, New York.

[18]Leetaru, Kalev (2018): Without Transparency, Democracy Dies in the Darkness of Social Media, Forbes, 25 January 2018. https://www.forbes.com/sites/kalevleetaru/2018/01/25/without-transparency-democracy-dies-in-the-darkness-of-social-media/#7269cd817221.

social media to avoid sharing information[19] only creates information vacuums that enable other actors to take over the information space. After the leaks of countless top-secret files – also through social media providers, it has become clear to most that there is no longer a realistic expectation of privacy for anyone in the information space.[20]

In a saturated information environment where information spreads instantaneously and is more uncontrolled than ever before, how can social media be more effectively used as an influence capability? This paper explores using social media as an influence capability by first defining social media, contextualizing how social media is changing the operating environment, and identifying opportunities and challenges associated with employing social media exploitation for influence. Lastly, the most promising forms of social media exploitation for influence are highlighted.

What is Social Media?

While almost everyone uses social media in some shape or form today, there is no agreed upon definition of what it actually is or what services belong to it. Traditionally, social networking services like Facebook, myspace and LinkedIn were primarily seen as social media services. Since the emergence of social media in 2002, the social media domain has drastically expanded to contain over 200 different services – depending on how social media is defined.

When considering social media exploitation for influence in military operations, it is essential to have agreement on what social media actually is and which services are a part of social media in order to effectively operate in the space. Particularly in the influence world, current Canadian Armed Forces (CAF) psychological operations (PSYOPS) doctrine does not define social media, nor does it mention social media.[21] Published in 2004, it does mention methods of dissemination such as "VHS tapes." Furthermore, the only mention of "internet" is as a 'reach back capability'. Specifically, the internet as a reach back capability "may be established in order to provide video, radio and Internet capabilities to TFC [Task Force Commander] in theatre."[22]

The Department of National Defence (DND) and CAF Policy on Joint Information Operations – from April 2018 – does refer to social media as indicated below:

[19] Kosseim, Patricia (2017): Government Information Sharing and Improved Service Delivery: Embracing the Wind of Change without throwing Caution to the Wind, *Remarks at the Government of Canada Data Leads Group*, 27 September 2017. https://www.priv.gc.ca/en/opc-news/speeches/2017/sp-d_20170927_pk/.

[20] O'Connor, Kimberly W./ Schmidt, Gordon B. (2018): Social Media, Data Privacy, and the internet of People, Things and Services in the Workplace, In: Simmers, Claire A./ Anandarajan, Murugan (2018): The Internet of People, Things and Services, New York.

[21] B-GJ-005-313/FP-001 CF JOINT PSYCHOLOGICAL OPERATIONS (15 JAN 2004).

[22] B-GJ-005-313/FP-001 CF JOINT PSYCHOLOGICAL OPERATIONS (15 JAN 2004).

> “Info Ops’ three inter-related activity areas can make use of all or any capabilities or techniques that can influence, affect understanding, or create a counter-command effect. […] These capabilities and activities can be offensive or defensive in nature and the extent of use is only limited by imagination and availability within policy and legal guidelines…this includes activities on social media and SMS platforms. Particular attention is to be to paid to these types of emerging electronic platforms which can be used in the conduct of Info Ops of differing purposes. For example, social media may be used concurrently by Cyber Operations for technical exploitation, PSYOPS for influencing and PA for informing, all of which need coordination.”[23]

Social media is however not defined in this document – nor is there any indication of which services fall under social media and can or even should be considered for influence operations. It appears, at least as far as influencing is concerned, in the realm of information operations and PSYOPS there is not agreed upon working definition of social media for the CAF.

NATO, in its guidelines on social media use within Allied Command Operation’s (ACO) organization, describes social media as “designed for dissemination through social interaction using internet- and web-based technologies to transform broadcast media monologues (one-to-many) into social media dialogues (many-to-many)”.[24]

The European Union (EU) provides further detail when defining social media as “online technologies and practices to share content, opinions and information prompting discussion and building relationships. Social media services and tools involve a combination of technology, telecommunications and social interaction. They can use a variety of formats, including text, pictures, audio and video”.[25]

In academia, there is also no one generally agreed upon definition of social media but instead many quite different perspectives exist. Very helpful is the definition by Thomas Nissen:

> “Social network media refers to internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content, that can influence knowledge and perceptions and thereby directly or indirectly prompt behaviour as a result of social interaction within networks”.[26]

Drew Herrick likely provides the most comprehensive definition of social media regarding security applications: “Social media operations consist of three distinct types: information-gathering, defence, and offense.

[23] DND AND CAF POLICY ON JOINT INFORMATION OPERATIONS (INFO OPS) (3 APR 2018)

[24] NATO (2009): ACO Directive 95-3: Social Media. December 2009. http://www.aco.nato.int/page300303028.aspx.

[25] European Commission (2013): Communicating with the outside world – Guidelines for All Staff on the Use of Social Media. http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf.

[26] Nissen, Thomas (2015): #TheWeaponizationOfSocialMedia @Characteristics_of_Contemporary Conflicts, Royal Danish Defence College, Copenhagen.

A. Information-gathering media operations: Information-gathering media operations (IGMO) focus on passive information-gathering. As demonstrated in the Ukraine, with ISIS, and the Bin Laden raid cases, passive information-gathering can be used for monitoring adversary activities and for targeting. Through IGMO, military and intelligence forces are not interacting with known social media actors but instead are passively monitoring and documenting social media activity. IGMO focuses on two types of data: direct data collection (the content displayed on social media); and metadata collection (technical details related to the characteristics of social media users and the mechanics of their social media use). Direct data collection allows access to the actual content displayed on social media services. Metadata collection is not as qualitatively rich as direct data collection, but can reveal important details regarding a population or target's location, the time of day when the target is active, the target's social graph (network connections), specific applications or services that the target is accessing, whether the target is using a mobile device, and in some cases even the specific hardware and software configuration of the device that the target is using […].

B. Defensive social media operations: Defensive social media operations (DeSMO) involve using social media in a more active way than IGMO, but not as active as for offensive operations. Actors can use social media as a broadcasting platform to conduct counter-messaging or counter-propaganda activities. As demonstrated in the Russian Troll and ISIS cases, social media can be used effectively to broadcast content widely to otherwise difficult-to-reach audiences. In fact, US government agencies are already using social media services to counteract known propaganda and radicalization campaigns […].

C. Offensive social media operations (OSMO): Social media operations are commonly viewed as a broadcasting or counter-narrative tools […]. More recently, social media operations are viewed as a passive information-gathering (or IGMO) tool and have received some attention as the conversation surrounding ISIS and online radicalization has subtly shifted from 'shut it down' towards a monitoring mentality. Instead of actively closing known ISIS accounts and websites, intelligence agencies and even non-governmental actors can passively observe and analyze their content."[27]

While this is likely the most comprehensive definition currently existing, the definition Christian Bell developed focuses on social media from a specific influence capability perspective: "Social media refers to internet-based platforms and software used to collect, store, aggregate, share, process, discuss, or deliver user-generated and general

[27] Herrick, Drew (2016): The Social Side of 'Cyber Power'? Social Media and Cyber Operations, paper presented at the 2016 8th International Conference on Cyber Conflict. https://ccdcoe.org/cycon/2016/proceedings/07_herrick.pdf.

media content, that can influence awareness, perception, acceptance and can promote behaviour indirectly as a means of interaction".[28]

This report modifies Christian Bell's definition to include the marketing aspect of social media (for which platforms like Facebook were primarily created, as it is their business model to generate revenue through advertising) to the following working definition of social media for this research report:

Social media are internet-based platforms created for influencing, marketing, collecting, storing, aggregating, sharing, processing, discussing and delivering user-generated content, which can influence awareness, perception, acceptance and actions and promote behaviour as a means of interaction.

Notably, there are at least 200 different forms of social media providers that vary based on where they are primarily used and what services they offer. Examples for each platform are the following:[29]

Platform type	**Providers**
Social networks	Facebook, VKontakte, WeChat, LinkedIn, Xing, QQ, Google+ myspace
Video content	Youtube, Vimeo, Youku, Periscope, Facebook Live
Picture content	Instagram, Tumblr, Flickr, Snapfish, Snapchat, Pinterest
Book content	Goodreads, WeRead, Audible
Training content	Strava, Polar Flow, Garmin Connect[30], KeepFitness
Instant messaging	Facebook messenger, WhatsApp, Telegram, Skype, Signal, Viber
Blogs	WordPress, Blogspot, SquareSpace, LiveJournal
Micro-blogging	Twitter, Friendfeed, Twitpic, Weibo, Qzone
Analytics tools	Klout, Socialmention, Geofeedia, Audiense, TweetReach
Crowd-sourcing	InnoCentive, iStockPhoto, GoFundMe, Kickstarter, IndieGo, Patreon
Location based services	Foursquare, Tripadvisor, Yelp, Tinder, Grindr

The above table only contains a fraction of the existing sites; notably, social media sites generally have short life cycles. The exception is Facebook that has existed – although

[28] Bell, Christian (2016): Use of Social Media as an Effector, Multinational Capability Development Campaign, Zentrum fur Operative Kommunikation der Bundeswehr, Mayen.

[29] This table is inspired by (but adds additional platform types and providers): Bell, Christian (2016): Use of Social Media as an Effector, Multinational Capability Development Campaign, Zentrum fur Operative Kommunikation der Bundeswehr, Mayen.

[30] Both Polar Flow and Garmin Connect have different primary functions (analysis of training data) but offer social media services to connect with other athletes, share pictures and competition or training results or simply to communicate with others through the platform.

in a vastly altered form – since 2004. New forms emerge frequently making it difficult to list all existing sites that are currently of relevance.

How Social Media is Changing the Operating Environment

Even before considering social media exploitation for influence, it is important to be aware of how social media has affected the operating environment – both in the theatre, as well as at home. In fact, this is one of the most relevant concerns to the operating environment, as within social media the delineation between home and the host nation is no longer relevant. While a conventional kinetic weapon can usually be aimed at a very specific location, at a very specific time, there is no guarantee that information does not reach undesired (home) audiences – or even appears weeks later on the front page of the New York Times. Not only are space and time restrictions far less reliable with social media, the battle space has become crowded with countless actors with multiple agendas. Actors in the information space range from the human (e.g., Russian trolls, children, paid influencers), and the non-human (e.g. bots, domestic appliances).[31]

One of the most significant impacts of services such as Twitter and Facebook is that every member of the audience has an effective voice of his or her own that can broadcast to an international audience at no cost to the user.[32] One significant effect this brings for actors in the information space is that within seconds, a member of an audience may not only show approval but disapproval of any message by 'liking' or 'not liking' a post. The feedback can also be instantly re-shared with any number of like-minded people – referring to the original message and adding support for the post or contradicting it, therefore effectively deciding on how members of the target audience should see it. While there are ways to manipulate the distribution, social media is specifically designed to spread engaging content and therefore will always favor and further spread content that users deem to be more emotionally inspired.[33]

Given that when messages are framed so that they align with the goals of the target audience, they can have a significant effect on behaviour change.[34]This creates a need

[31]Soro, Alessandro/Bereton, Margot/Roe, Paul (2018): Social Internet of Things, Springer International Press, Cham.

[32] Mangold, W. Glynn/ Faulds, David J. (2009): Social Media: The New Hybrid Element of the Promotion Mix, Kelley School of Business, Indiana University, *Business Horizons*, No. 52, 2009.https://www.sciencedirect.com/science/article/pii/S0007681309000329.

[33] Vaidhyanathen, Siva (2018): Antisocial Media, How Facebook Disconnects Us and Undermines Democracy, Oxford.

[34] Lindenberg, Siegwart/ Steg, Linda (2007) Normative, Gain and Hedonic Goal Frames Guiding Environmental Behavior, *Journal of Social Issues*, Volume 63, Issue 1, pages 117–137, March 2007.https://www.rug.nl/research/portal/publications/normative-gain-and-hedonic-goal-frames-guiding-environmental-behavior(36809827-091d-4d03-84f5-7205bf464c53).html.

for very high quality[35] and veracity in any messaging designed to influence. Message histories are easily retrievable at any time after they have been sent, creating a transparent track record that can affect behavioral change of a target audience (TA) long after an influence operation has been completed.[36] In addition, words are no longer the primary element to convey messages. Rather, producing video messages, for example, has become so easily accessible that noise[37] easily crowds out content introduced to influence.[38] This widespread availability of major messaging formats comes with the requirement for many more technical skills than were prior needed, especially if the message is intended to stand out in the noise. It is essential to create content with high quality production values, attuned to the specific target audience and completed in a short turnaround as users have come to expect instantaneous responses to events. These require very different skills than drafting messages in conventional media. The increased speed of message distribution creates timing and decision-making challenges which significantly complicate the task of message design and distribution. New skills must be acquired as each new platform emerges, and these skills need to be applied at a much faster pace and with attention to quality and professionalism to project the desired effect and gain traction in the information space among the exponentially higher competition.[39] If an event occurs relating to an organization and it does not react in almost real time to that event, an information vacuum occurs that will be immediately filled by interested third parties.[40] This will rarely lead to a narrative that is desired by the affected organization. Here again, the time factor poses significant challenges if sign offs are required from lengthy chains of command. Given the vastly increased potential spread of messages and possibly emerging consequences, there is a clear conflict between the need for increased message control and a lack of messages impact due to delays that create an information vacuum.

In addition, despite new technologies becoming seemingly easier to master, the skills required on the side of message design and distribution have increased significantly. In

[35] Higher quality refers here to how closely the message is designed to align with the goals and preferences of the target audience. The closer the messaged design is modeled after the very specific preferences of the TA the more effective it will likely be.

[36] McCay, Layla (2012): The Internet Never Forgets: How to Live in the 21st Century, The Huffington Post, 30 June 2012. http://www.huffingtonpost.com/dr-layla-mccay/the-internet-never-forgets_b_1460110.html.

[37] 'Noise' is understood here as any kind of signal that crowds the information space. This can be anything that attracts the attention of the TA or effectively hinders the TA from accessing information it is trying to access.

[38] Hofseth, Anders (2017): Fake News, Propaganda, and Influence Operations – a guide to journalism in a new, and more chaotic media environment, Reuters Institute, 14 March, 2017. https://reutersinstitute.politics.ox.ac.uk/risj-review/fake-news-propaganda-and-influence-operations-guide-journalism-new-and-more-chaotic.

[39] Sunstein, Cass R. (2018): #Republic: Divided Democracy in the Age of Social Media, Princeton University Press, Princeton.

[40] Kruh, Willy (2014): Social media Have Changed How We Communicate Ideas, The Globe and Mail, 29 June 2014. https://www.theglobeandmail.com/report-on-business/careers/careers-leadership/social-media-have-changed-how-we-communicate-ideas/article19385666/.

other words, high skill requirements are necessary to operate the new technologies, otherwise a risk emerges resulting in unintended consequences of messaging.

Social Media Exploitation: Opportunities

Governments around the world have recognized the advantages social media offers for government operations.[41] Apart from the above-mentioned advantages regarding the speed of distribution, reach and low cost per message, social media offers superior advantages for designing messages to captivate the target.[42] Social media user data mining can provide very accurate descriptions of audience preferences that enable highly relevant message design.[43] This highly accurate designing of messages, known as micro-targeting, is based on very detailed analysis of target audience preferences and user activities, enabling powerful influence opportunities which can be employed by governments and other political actors.[44] Tailoring relevant messaging to target audiences allow PSYOPS and InfoOps to reach audiences directly in an efficient, focused manner.[45]

Exceptional influencing opportunities also arise from delivery direct-to-screen – meaning that audiences no longer have to walk by a billboard or receive a leaflet.[46] The audience voluntarily transports the messaging platform, usually a mobile phone, maintaining perpetual contact and therefore, subjecting themselves to constant influencing. On average, across all age groups, Americans check their personal “platform” 46 times a day.[47] Not only do they carry the influencing platform with them at any time but they also willingly customize it by personalizing the platform with their exact personal preferences, voluntarily providing information about how they can best be influenced in an environment that they prefer. As this information can be easily accessed through social media data, it informs influencers how target audience members prefer to be influenced,[48] and as a consequence, how they are most vulnerable to influencing operations.

[41] PEN America (2018): Forbidden Feeds, Government Controls on Social Media in China, PEN America; 13 March 2018. https://pen.org/wp-content/uploads/2018/03/PENAmerica_Forbidden-Feeds-3.13-3.pdf.

[42] Lanier, Jaron (2018): Ten Arguments for Deleting Your Social Media Accounts Right Now, MacMillan, New York.

[43] Schaeffer, Ute (2018): Fake statt Fakt, DTV, München.

[44] Weaver, Matthew (2018): Social media ‘micro-targeting’ of voters on the increase, MP told, The Guardian, 23 January, 2018. https://www.theguardian.com/media/2018/jan/23/social-media-micro-targeting-of-voters-on-the-increase-mps-told

[45] Ventre, Daniel (2016): Information Warfare, John Wiley & Sons, Hoboken.

[46] Coster, Helen, Cellphones: The New Billboards, Forbes, 15 July 2009. https://www.forbes.com/2009/07/15/mobile-marketing-cmo-network-mobilemarketing.html#b00079240753.

[47] Eadicicco, Lisa (2015): Americans Check Their Phones 8 Billion Times a Day, Time, 15 December 2015. http://time.com/4147614/smartphone-usage-us-2015/.

[48] Story, Louise (2008): To Aim Ads, Web Is Keeping Closer Eye on You, New York Times, 10 March 2008. http://www.nytimes.com/2008/03/10/technology/10privacy.html.

Further advantages for influence operations emerge from the fact that the infrastructure cost for message distribution is very low compared to almost all traditional forms of communication. Once the skill set is acquired to operate the platforms, social media allows for a much higher frequency of message distribution and also for targeting much larger audiences. It does so independently of audience location and physical barriers that may exist between the message sender and the recipient. Furthermore, as no physical borders need to be crossed, the risks for operators are also far less significant.[49]

In addition, accurate feedback on the effectiveness of operations can be obtained through the analysis of social media data. Data analysis enables measuring the exact spread of messages as well as their penetration of an audience, resulting in more precise customization of messages based on the data analyses which cannot be achieved with traditional media monitoring. Social media data analysis offers a new level of precise access to target audiences. Never before have military communications had such close, two-way, access to audiences who may be in an area physically controlled by the enemy.[50]

The ability to message the enemy directly at all levels is also a new capability that provides great potential. Not all enemies may be as ideologically committed or loyal. Combined with tailored messages and direct negotiations, military communicators may be able to increase rates of surrender or convince enemy combatants to refrain from entering the battle.[51]

Social Media Exploitation: Challenges

Interviews with social media operators of NATO member states revealed significant challenges to the use of social media in information operations. The following five challenges were mentioned repeatedly:

- Military Culture: The military culture is described as inherently conservative leading to an organization that is slow to adopt new technologies.[52] Many military

[49] With the exception of locating capabilities that can be used to identify and find operators through social media (meta) data that can lead to serious risks in the field. See: MacAskill, Ewen (2014): Cover-up: Ukraine rebels destroying all links to MH17 air atrocity UN demands full inquiry but armed Russian separatists block access to crash site amid confusion over black boxes, The Guardian (UK), 18 July 2014.https://www.theguardian.com/world/2014/jul/18/separatist-links-malaysia-airlines-mh17-removed.

[50] Watts, Clinton (2018): Messing with the Enemy, Surviving in a Social Media world of Hackers, Terrorists, Russians, and Fake News, Harper Collins, New York.

[51] Cordy, Jane (2017): The Social Media Revolution: Political and Security Implications, NATO Committee on the Civil Dimension of Security, 7 October, 2017. https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20158%20CDSDG%2017%20E%20bis%20-%20SOCIAL%20MEDIA%20REVOLUTION%20-%20CORDY%20REPORT.pdf

[52] Blanken, Leo/Lepore, Jason/Rodriguez, Stephen (2018): America's military is choking on old technology, Foreign Policy, 29 January, 2018. https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/

leaders still see the information environment, and social media as outside of their purview.[53]

- Training: Leveraging advances in machine learning, and data science relating to social media for military applications such as InfoOps or PSYOPS requires advanced knowledge of both conventional PSYOPS and a very high degree of technical savvy that may not be sufficiently available.[54]
- Policy: Only in recent years has the military even adopted social media policy and many are unclear on what is allowed in terms of data collection.[55]
- Culture of Secrecy: Many of the tactics, techniques and procedures used to leverage social media intelligence reside in the communications research and signals intelligence communities. These communities have a culture of over-classification, even in cases that where the data is publicly available. This over-classification results in a situation where operators who could use the intelligence do not have the clearance to access it.[56] This is especially a challenge in social media where postings have to be very timely to have a desired effect.
- Risk Aversion: The ability to access a global audience, and the ability of global audiences to access all out communications with a local population is both high risk and high reward. The risk of doing nothing is often not calculated and the risk of public controversy is weighed extremely carefully.[57] This again raises questions about how timely postings can be achieved sufficiently often to generate desired effects.

There can be no doubt that social media has also brought many unforeseen challenges for message distribution; the cost of mistakes can be much higher, which is not only due to distribution speed and reach. The internet "never forgives" as it remains as a near permanent archive of activities.[58] This archive can be accessed by practically anyone at any time. Therefore, an archive of previous messages sent by an organization is available to interested parties. This has huge implications for message design regarding authenticity, accuracy and possible narratives. With this comes the fact that messages cannot be designed only to have an effect on a certain event. The message which is intended for a specific event can have an effect long after the event as it continues to be available to and shared by interested parties. Due to the archive, messages always have an effect that goes far beyond the current situation. Therefore, the message designer must be mindful of both the short-term reaction and the long-term shelf-life of

[53] Based on interviews with Social Media operators at the NATO seminar "How to operationalize social media? June 18/19 2018, Milan, Italy.
[54] Based on interviews between April 2018 and June 2018 with CAF members working in INFOOP and PSYOPS.
[55] Based on interviews between April 2018 and June 2018 with CAF members working in INFOOP and PSYOPS.
[56] Based on interviews with Social Media operators at the NATO seminar "How to operationalize social media? June 18/19 2018, Milan, Italy.
[57] Based on interviews with Social Media operators at the NATO seminar "How to operationalize social media? June 18/19 2018, Milan, Italy.
[58] Rosen, Jeffrey (2010): The Web Means the End of Forgetting, The New York Times, 21 July 2010. https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

that response. They are speaking to the audience in the moment but also to a future audience that might compare messages sent out by the same sender. In this regard, it is clear that social media can be both the solution and the cause of a crisis.[59]

Social media has also fundamentally changed how audiences consume information, as[60] people increasingly appear to be almost addicted[61] to a news cycle. One has to be aware that there is not just “the” news cycle but a multitude of news cycles, at any given time and place given the democratization of media. There are vast numbers of news sources and therefore, news cycles – many of which provide nothing more than entertainment value with primarily questionable or frivolous newsworthiness. It appears that the primary interest of consumers is being fed by this news cycle, rather than an interest in seeking accurate information. For message design, this means that not only is the amount of information available to the audience much greater but also that there is an expectation to be informed constantly about any issues that are perceived to be of relevance.

At the same time, consumers are more easily able to identify information that is wrong from more trustworthy information after many scandals about inauguration audience sizes, ‘alternative facts’ and lies spread through social media.[62] An almost constant bombardment of false information has trained many users to differentiate more easily truth from false information than in the early days of social media. The constant stream of false information is slowly leading to a more critical observation of sources. However, social media services are at the same time becoming increasingly more effective in presenting individually tailored content to users that is more effective in influencing.[63] False news has been proven to spread six times faster on the internet then actual facts.[64] But particularly, messages from official sources are often met with great skepticism. This is partially the effect of too many official messages containing content that is false.[65] Audiences have practically themselves become part of the competition for attention.

Another challenge associated social media exploitation is that anyone and everyone can be the messenger, or influence the message. The audience, with its own greater

[59] Jacobsson Purewal, Sarah (2010): Facebook Messages: The Worst Thing That Ever Happened, PC World, 16 November 2010.https://www.pcworld.com/article/210758/Facebook_Messages_The_Worst_Thing_That_Ever_Happened.html.
[60] Watts, Clinton (2018): Messing with the Enemy, Surviving in a Social Media world of Hackers, Terrorists, Russians, and Fake News, Harper Collins, New York.
[61] Kleinman, Zoe (2015): Are we addicted to technology? BBC, 31 August 2015.https://www.bbc.com/```news/technology-33976695.

influence in the information space, can spread perceptions of the accuracy or inaccuracy of a message in real time to very significant audiences. At the same time, they can add contrary evidence, fabricated or not, to narratives. The audience becomes both consumer and producer of media, in its own right, at the same time.[66]

For government institutions, there is no question that the efforts to influence effectively have become much greater with social media – despite how the actual process has become less resource intensive per individual message that is being distributed through social media. This refers to multiple aspects: time involved in drafting messages that can spread rapidly not only requires a higher degree of accuracy but also proper planning and preparation long before a message needs to be sent. This requires preparing the audience for message distribution by creating a network of supporters on social media that will spread a message, which is typically based on trust that has to be built up long before it needs to be counted on.

Maintaining the audience's attention has become more complicated than it was in the past, representing another challenge for social media exploitation. Only content that is highly engaging will spread widely, meaning target audience members will bypass content unless it in some way triggers strong emotions.[67] This has led to the radicalization of online dialogue – and to some extent even online culture in general as only content that is drastic or unusual is typically shared.[68] It also drastically raises the bar for the level of emotion a message has to trigger to have a chance at being widely spread by social media and actually reaching many members of an intended target audience. If the audience is not "learning something [really relevant to them], laughing at something or getting a spectacular deal on whatever it is you are selling, one-click and they're gone."[69] The competition for the attention of the audience is so high that almost always there is a more attractive option for the audience.[70] This has significant implications on the possible complexity of messages to which the vast majority of people have become accustomed.

To correspond with the reduction in viewer attention spans, messages must be designed to convey the message as fast and comprehensible as possible.[71] This raises huge challenges for designing messages in the defense and security domain where issues dealt with are often of a complex nature. There can be no doubt that to manage

[67] Lanier, Jaron (2018): Ten Arguments for Deleting Your Social Media Accounts Right Now, MacMillan, New York.
[68]Nagle, Angela (2017): Kill All Normies, Zero Books, Alresford.
[69] Matejic, Nicole (2015): Social Media Rules of Engagement: Why Your Online Narrative is the Best Weapon During a Crisis, Wiley and Sons, Melbourne.
[70] Turkel, Sherry (2015): Reclaiming conversation: the power of talk in the digital age. Penguin, Toronto.
[71]Min, Jinyoung (2017): Effects of the Use of Social Network Sites on Task Performance: Toward a Sustainable Performance in a Distracting Environment, *Sustainability*, 2017, 9.

all of these challenges, significant pre-emptive planning and preparations are necessary. A robust social media policy is an effective first line of defence but a very specific, extensive training and awareness program combined with sufficient resources and staffing is critical.

Social Media Exploitation for Influence

The following section describes eight of the most effective forms of social media exploitation for influence in operations. Based on a review of research publications on social media in the security environment, as well as interviews with operators involved in social media operations, these social media influence capabilities appear to be the most effective:

- Targeting
- Surveillance
- Target discovery
- Social network analysis
- Social trends Analysis
- Measures of effect
- Appeals to surrender
- Influencing public support of adversaries.

Targeting

While traditional intelligence gathering methods have been the primary data source in the past for target influence campaigns, new methods like social network analysis and personality profiling techniques can effectively supplement traditional intelligence data.[72] The data analytics services that became famous through the now-closed Cambridge Analytica[73] (that has continued operations under other names)[74] have highlighted the potential capabilities of data analytics for any kind of investigation of target audiences – while the actual full impact of the campaign by the company is still debated.[75] In a military operation, blue forces could use social media data to identify and – based on accessed social media data – design resonant messages to key target audiences with an extraordinary refinement of detail on many individuals within the target group

[72] Marcellino, William M. / Smith, Meagan L./ Paul, Christopher/ Skrabala, Lauren (2017): Monitoring Social Media, Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations, Santa Monica.

[73] Ballhaus, Rebecca/ Gross, Jenny (2018): Cambrige Analytica Closing Operations Following Facebook Data Controversy, The Wall Street Journal, 2 May 2018. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140.

[74]Siegelman, Wendy (2018): Cambridge Analytica is dead – but its obscure network is alive and well, The Guardian (UK), 5 May 2018.https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-scl-group-new-companies-names.

[75] Wong, Julia Carrie (2018): Cambridge Analytica-linked Academic Spurns Idea Facebook Swayed Election, The Guardian (UK), 20 June 2018. https://www.theguardian.com/technology/2018/jun/19/aleksandr-kogan-facebook-cambridge-analytica-senate-testimony.

simultaneously.[76] The data offered by social media services – voluntarily uploaded by the target audience (or collected by the media platform with or without user permission – raising potential ethical and legal barriers to acquisition of user-data)– allows a degree of customization and therefore, information about personal preferences by the individual user that can hardly be acquired by other means – certainly not with the investment of the comparably minimal resources required to access the already existing data.[77]

Targeting based on this very detailed data enables engagement with the target audience in a way that appears very natural to them, is tuned to how they most likely will want to be addressed and even reaches them directly on the networks they already use – making it more natural to them. This approach has benefits as very specific and accurate data can be gathered through social media about every individual member of the target audience, and each individual can be reached in an environment he or she is likely to visit on a regular basis.

Recent psychological studies demonstrate that surprisingly little social media data is required to identify an individual's gender, sexuality, political beliefs, and key personality traits.[78] This data can be used to identify audiences most amenable to narratives and develop unifying messages to reinforce beliefs and behavioursfurther which enable operational goals. More covertly, the same data can be used to amplify rifts within adversaries and fracture the group's internal cohesion.

The use of social media to support incumbent governments, as well as to discredit jihadists, has already been seen in Russia[79] and China[80] – and is being frequently misused by authoritarian governments.[81] Social media's use to increase the divide between ethnic Russians and other ethnicities has been promoted in Latvia.[82] The same techniques applied in these countries can be adapted to CAF military operations.

All of this is dependent on the production of resonant messages for micro-targeted audiences. Social media platforms lend themselves to the automation of testing of a wide variety of message structures, post layouts as well as differing angles and perspectives on issues. The 2016 US presidential election for example saw approximately 35 to 45 thousand iterations of similar political ads delivered to millions of

[76] Marcellino, William M. (2017): Revisioning Strategic Communication Rough Rhetoric and Discourse Analysis, *Joint Force Quarterly*, No. 76, First Quarter 2015.

[77] Perez, Sarah (2017): Twitter launches lower-cost subscription access to its data through new Premium APIs, Techcrunch, 14 November 2017.https://techcrunch.com/2017/11/14/twitter-launches-lower-cost-subscription-access-to-its-data-through-new-premium-apis/.

[78] Anderson, Berit (2017): The Rise of the Weaponized AI Propaganda Machine, Medium; 12 February 2017. https://medium.com/join-scout/the-rise-of-the-weaponized-ai-propaganda-machine-86dac61668b.

[79] Melia, O. Thomas (2018): Russia and America Aren't Morally Equivalent, The Atlantic, 27 February 2018.https://www.theatlantic.com/international/archive/2018/02/election-meddling-democracy-promotion/554348/.

[80] Luo, Ting (2018): Explaining Incumbent Re-Election in Authoritarian Elections: Evidence from a Chinese County, Democratization, 19 April 2018. https://www.tandfonline.com/doi/full/10.1080/13510347.2018.1462798.

[81] Gunitsky, Seva (2015): Social media helps dictators, not just protestors, The Washington Post, 30 March 2015. https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/30/social-media-helps-dictators-not-just-protesters/?utm_term=.5f008e4842ca.

[82] Blumenthal, Paul (2018): The Techno-Colonialism of Facebook And Cambridge Analytica, Huffington Post; 23 March 2018. https://www.huffingtonpost.ca/entry/facebook-cambridge-analytica-developing-world_us_5ab50bc7e4b0decad04951d1.

people daily.[83]Traditional PSYOPS product pre-tests without social media involve delivering around two or three versions of a message in a small number of focus groups in the field, run over a period of weeks – producing likely much less accurate results.

Surveillance

In recent years, there has been increased interest in event detection using social media data. On social media, the host nationals can post real-time reactions to "real world" events, thereby acting as hundreds of thousands of social sensors. Detecting and categorizing these events, particularly small-scale incidents, before they spill over into violence and escalate to widespread unrest is of high value to military and police in an area of operations (AoO). Recent advances in data science have seen the invention of automated event detection frameworks driven by social media data.[84] These frameworks provide the capability to detect small scale incidents, which threaten social safety and security or could disrupt social order. This technology includes automatically generated summaries and descriptions.[85]

Similarly, intelligence analysts can use social media data to track the movements and relations of local government and other public officials as well as associated topics and narratives.[86] Social media data could be used to supplement other forms of intelligence in determining governmental or public servant relations with criminal or other malignant actors. When attempting to establish a credible government, the host nationals' perceptions of corruption are as important as their actual corruption levels. Using new technology in topic modeling and natural language processing, social media data can be used to assess changes in how the host nationals view government and enemy actors as well as the actions or activities with which they are associated.[87]

Conventional surveillance can also be enabled or supplemented by social media data. Recently, the careless use of social media has allowed coalition aircraft to target members of the ISIS terrorist group because they inadvertently left on their geotagging feature[88] or when posting a selfie with easily identifiable landmarks.[89]

[83] Haines, Ian (2018): The Power of A/B Testing: The US Election, Symposium; 10 February 2018. https://symposeum.com/power-b-testing-us-election/.

[84] Kousiouris, George et. al. (2018): An integrated information lifecycle management framework for exploring social network data to identify dynamic large crowd concentration events in smart cities applications, Surrey Research Insight*, Future Generation Computer Systems*, Volume 78, Part 2; 2018. http://epubs.surrey.ac.uk/841839/.

[85] Alsaedi, Nasser/ Burnap, Pete/ Rana, Omer (2017): Can We Predict A Riot? Disruptive Event Detection Using Twitter, ACM Transactions on Internet Technology (TOIT) - Special Issue on Advances in Social Computing and Regular Papers, Volume 17, Issue 2, Article 18, ACM, New York; May 2017.https://dl.acm.org/citation.cfm?id=2996183.

[86] Vomiero, Jessica/ Do, Eric Marl (2017): Snapchat's New Map Feature Could Be Tracking You All the Time. Global News, 25 June 2017. https://globalnews.ca/news/3554398/snapchats-new-map-feature-could-be-tracking-you-all-the-time/.

[87] Smith, Marc A./ Rainie, Lee/ Shneiderman, Ben/ Himelboim, Itai (2014): Mapping Twitter Topic Networks: From Polarized Crowds to Community Clusters, Pew Research Center; 20 February 2014. http://www.pewinternet.org/2014/02/20/mapping-twitter-topic-networks-from-polarized-crowds-to-community-clusters/.

[88] Nicks, Denver (2015): New Zealander ISIS Fighter Accidentally Tweets Secret Location, Time; 1 January 2015. http://time.com/3651559/new-zealand-isis-twitter/.

[89] Castillo, Walbert (2015): Air Force Intel Uses ISIS 'Moron' Post to Track Fighters, CNN; 5 June 2015.

Target discovery

Social media can assist with target discovery either through social network analysis to determine high value individuals (HVI) or by crowdsourcing imagery of enemy positions and equipment from the frontlines. During the 2016 and 2017 various resistance groups in Mosul, Iraq posted potential targets to social media. Beyond kinetic targeting, these groups coordinated international support for counter ISIS operations. In military operations, social media could be used to reach out to friendly and compatible groups to enable intelligence gathering and targeting efforts, both kinetic and non-kinetic.

For over two years after the June 2014 fall of Mosul to ISIS, Omar Mohammed, operating as “Mosul Eye” documented ISIS atrocities on social media.[90] Despite reportedly having been contacted by intelligence agencies and rebuffing them, using social media, he extensively reported extensively on the state of ISIS battle preparations to the public, the ISIS use of Mosul University and other data useful to targeteers.[91] In at least one case Mohammed was able to reach out directly to coalition forces on Twitter to warn them of large civilian populations in an apartment complex rumored to be garrisoned by ISIS.[92] Other resistance groups known as “Mim Battalions” have provided a large amount of military intelligence that has led to the capture and death of major ISIS commanders.[93] A famous example of how social media can be used for targeting comes from social media service for athletes called Strava. Runners can upload GPS tracks from their runs or bike rides and share them with friends. US soldiers can do the same and did so from various runs on US bases that do not appear on public maps.[94]

During the 2016-2017 battle for Mosul, many Iraqi soldiers were equipped with GoPro cameras, and constantly broadcasted their activities on social media. The combined Iraqi Armed Forces and resistance group constantly uploading battle updates, in part, allowed coalition military planners to prioritize targets dynamically that assisted counter-ISIS groups with whom they were not in direct contact. Social media played an even greater role in enabling coordination between the Western air campaign and the Kurdish-led Syrian Democratic Forces distributed campaign against ISIS in a large area of Northern Syria.[95]

https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html.

[90] Tremonti, Anna Maria (2018): ISIS on Your Doorstep: Meet Mosul Eye, The Man Who Defied The Terrorists To Save His City, CBC Radio ‘The Current’; 6 February 2018. (Transcript and Audio File). http://www.cbc.ca/radio/thecurrent/the-current-for-february-6-2018-1.4522000/isis-on-your-doorstep-meet-mosul-eye-the-man-who-defied-the-terrorists-to-save-his-city-1.4522333.

[91] As an example see, Mosul Eye (2016): What’s happening in Mosul?, Mosul Eye© Report – Oct. 20, 2016; Mosul Eye Blog; 20 October 2016. https://mosul-eye.org/2016/10/21/whats-happening-in-mosul-mosul-eye-report-oct-20-2016/.

[92] Mosul Eye Twitter Post (2016): Twitter Post: To the Liberation Ops Command in Gugjali, @Mosul Eye Twitter Feed; 2 November 2016. https://twitter.com/MosulEye/status/793936900931387393.

[93] Kossov, Ivan (2017): Meet the men who fought ISIS from inside Mosul, USA Today; 2 May 2017.https://www.usatoday.com/story/news/world/2017/05/02/islamic-state-isis-militants-iraq-civilians-resistance/101131176/.

[94] Hern, Alex (2018): Fitness Tracking App Strava Gives Away Location of Secret US Army Bases, The Guardian (UK), 28 January 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[95] Based on interviews with CAF members deployed at CJTF-OIR.

In addition, the convergence of online speech and physical violence creates new targeting priorities such as the case of Junaid Hussain. Hussain was a British Muslim radicalized to ISIS who traveled to Syria and began working as a social media propagandist for the group. By August 2015, Hussain had reportedly become the third-most-important name on the anti-ISIS coalition's priority target list. Rather than any battlefield skills or strategic insight, it was his social media marketing skills that led targeteers to prioritize his killing. Ironically, it was also his non-stop internet use that led to his capture and execution. Hussain was reportedly tricked into clicking a link in a compromised messaging app, allowing him to be geo-located and killed by a Hellfire missile.[96]

Social Network Analysis

By mapping out the social networks of various groups it is possible to determine key nodes in the network such as people who bridge different communities together or influential members of a community.[97]In military operations this social network could be used as a map of the information domain enabling the identification of actors who may be credible within a target audience as hostile or skeptical of blue forces. Blue forces could reach out to these actors to act as intermediary messengers for audiences who do not trust the delivered information.

A recent study of counter insurgency (COIN) efforts in the Philippines investigated the spread of information through civilian social networks, and explains why counterinsurgency efforts were successful in some villages but not others. Civilians in villages with family members in neighbouring villages influenced by the insurgents received information through their social networks that gave the impression that the insurgents had staying power in the area and would be able to retaliate. Other villages, despite being geographically close to the same insurgent-held villages, predominantly had family ties to other government-controlled villages, making government forces look more powerful. Moreover, civilians in villages that had family ties to surrounding government-held areas that recently received stabilization projects formed beliefs that the government was providing sustained economic development.[98] While this study employed traditional research methods, the use of social media data could assist in mapping the trusted sources of information and how the COIN narrative may be disseminated best to civilians.

Similarly, Social Network Analysis of ISIS on social media has revealed the accounts and topics that get the most engagement both by supporters of ISIS and by the broader

[96] Brooking, Emerson T./ Singer, Peter W. (2016): War Goes Viral, The Atlantic; November 2016. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.
[97] Del Vicario, Michaela/ Zollo, Fabiana/ Calarelli, Guido/ Scala, Antonio/ Quattrociocchi, Walter (2017): Mapping social dynamics on Facebook: The Brexit Debate, *Social Networks*, Volume 50. http://eprints.imtlucca.it/3684/.
[98] Haim, Dotan A. (2017): Civilian Social Networks and Counter Insurgency, Department of Political Science, University of California, San Diego; 2017. http://dotanhaim.com/wp-content/uploads/2017/10/Haim_WS1.pdf.

community.[99] The use of this kind of social media data in social network analysis could facilitate the expansion of Attack the Network (AtN) doctrine, currently used in defeating improvised explosive devices (IED) production networks, to defeating insurgent information networks.[100] In this way, it is also possible to identify the grievances or issues that an insurgent or terrorist group is exploiting to garner support from the broader population.

Social Trends Analysis

Social media is also effective to compartmentalize target audiences to determine the sentiments within the audience, to learn about relevant topics discussed and what actions are being taken.[101] Who will protest a given action? Where? Are they dangerous? Are there calls for violence? In addition to reaching out to potentially hostile groups directly, using social network analysis and social trends analysis, adversaries could reach out to friendly or compatible actors at the right time to request assistance in spreading our messages and/or to diffuse potentially tense situations. These techniques can also be used to understand better which narratives hostile groups are spreading and whether these narratives are resonating with the target audience in order to develop more effective counter messaging strategies.

Data from protest movements in the United States, Spain, Turkey, and Ukraine shows that social media facilitates the exchange of information vital to the coordination of protest activities, such as event timing and assembly location, transportation, turnout, police presence, violence, medical services, and legal support. Additionally, social media makes possible the dissemination of emotional and motivational content that enables support of and opposition to protest activity.[102] These messages often contain content that is created to rally support, provoke anger, promote a sense of social identification, group efficacy, and may highlight concerns about fairness, justice, and deprivation as well as ideological themes.[103] Similar data for 16 Middle Eastern countries during the Arab Spring shows that traditional actors such as the media and members of the political establishment are not driving these anti-government trends. The data indicates large-scale decentralized coordination of protests such as flash

[99] Yarlagadda, Rithvik/Felmlee, Diane/Verma, Dinesh/Gartner, Scott (2018): Implicit Terrorist Networks: A Two-Mode Social Network Analysis of Terrorism in India. In: Thomson R., Dancy C., Hyder A., Bisgin H. (eds) Social, Cultural, and Behavioral Modeling. Lecture Notes in Computer Science, vol 10899. Springer, Cham.

[100] CAF does not have formal AtN doctrine however it is well known in the C-IED and intelligence communities and adopted by most of NATO and 5EYES militaries.

[101] Maurya Chandra Gupta / Gore, Sandeep/ Rajput, Dharmendra Singh (2018) A Use of Social Media for Opinion Mining: An Overview With the Use of Hybrid Textual and Visual Sentiment Ontology, In: Tiwari, B./ Tiwari, V./ Das K./ Mishra, D./ Bansal, J. (eds) *Proceedings of International Conference on Recent Advancement on Computer and Communication - Lecture Notes in Networks and Systems*, Volume 34, Singapore. https://link.springer.com/chapter/10.1007/978-981-10-8198-9_33.

[102] Jost, John T. et. al. (2018): How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks, *Political Psychology*, Volume 39, Issue 51; February 2018.https://onlinelibrary.wiley.com/doi/abs/10.1111/pops.12478.

[103] Jost, John T. et. al. (2018): How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks, *Political Psychology*, Volume 39, Issue 51; February 2018.https://onlinelibrary.wiley.com/doi/abs/10.1111/pops.12478.

mobbing where demonstrators converge on an assembly location with a planned idea of what might occur and spreads as “online word of mouth”.[104] A good example of mass mobilization of protesters via social media are the Yellow Duck anti-corruption rallies held in Brazil,[105] Serbia[106]and Russia.[107]Analysis of this kind of data was used to disrupt protests in Russia[108] and can likely be used for early warning that a protest may turn violent.

In 2013-14 social media trends analysis clearly showed thousands of foreign fighters moving into Syria and Iraq in support of ISIS. This data provided a loud and public warning that a local, small, insurgency was quickly becoming global in nature. Social media trends analysis data further helped quantify ISIS’ growth at that time by providing data on the surprising number of women and westerners joining the movement. Analysis of trends in gender, ethnicity, ideology and other factors relating to these foreign fighters, help allied forces develop messages to stem the flow of supporters to the ISIS insurgency. Allied countries were also able to reach out to disenfranchised Muslims most vulnerable to radicalization through more moderate Mullahs and Imams to address flaws in the ISIS view of Islam and how better to address common grievances among Muslims susceptible to ISIS radicalization efforts.[109]

Measures of Effectiveness

Influence-related measures of effectiveness (MOE) are of key importance as they provide insight into which activities are producing results and which are not. This in turn forms the basis for improving the quality and focus of influence activities as well as the proper allocation of resources. Social media data directly lends itself to this effort particularly because it is being used by so many actors as a key part of their influence campaigns.[110]

[104]Steinert-Threlkeld, Zachary C./ Mocanu, Delia/ Vespignani, Alessandro/ Fowler, James (2015): Online Social Networks and Offline Protest, *EPJ Data Science*, Volume 4, Issue 19; December 2015. https://link.springer.com/article/10.1140/epjds/s13688-015-0056-y.

[105] Doce, Nacho (2016): Brazil’s Restive Rich Draft a Duck to Protest President, Reuters; 20 March 2016. https://www.reuters.com/article/us-brazil-politics-duck-idUSKCN0WM0F1?utm_source=Facebook.

[106] Dragojlo, Sasa (2015): Giant Duck Becomes Belgrade Resistance Symbol, Balkan Insight.com; 26 September 2015. http://www.balkaninsight.com/en/article/giant-duck-becomes-belgrade-resistance-symbol-09-25-2015.

[107] Robson, John (2017): Beware the Yellow Ducks – Russia’s Humorous Anti-Corruption Protests Have Teeth, National Post; 30 March 2017. http://nationalpost.com/opinion/john-robson-beware-the-yellow-ducks-russias-humorous-anti-corruption-protests-have-teeth. See also: Bershidsky, Leonid (2017): The Yellow Rubber Duck is a Potent Protest Symbol, Bloomberg; 28 March 2017. https://www.bloomberg.com/.../the-yellow-rubber-duck-is-a-potent-protest-symbol. And: Eremenko, Alexey (2017): Russia's Protests Explained: Why Rubber Ducks, Sneakers Are at Demonstrations, NBC News; 27 March 2017. https://www.nbcnews.com/news/world/russia-s-protests-explained-why-rubber-ducks-sneakers-are-demonstrations-n738891.

[108] Enikolopova, Ruben/ Makarine, Alexey/ Petrova, Maria (2016): Social Media and Protest Participation: Evidence from Russia, *CEPR Discussion Papers* , Number 11254; 2016.https://www.tcd.ie/Economics/assets/pdf/Seminars/20172018/Social_Media_Protests_17-04-12.pdf.

[109] Based on interviews with members supporting OP IMPACT, CJTF-OIR and other counter ISIS efforts.

[110]Bradshaw, Samantha/Howard, Philip N. (2018): Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project University of Oxford. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Content analysis, or media monitoring can be used to assess influence campaign exposure, influence, and associated changes in attitudes and sentiments. Content analysis involves the systemic observation of traditional press as well as social media sources to quantify programs and messages to determine how narratives are spreading through target audiences. Messages disseminated on social media reflect both the exposure to a message and reactions to it, as well as baseline sentiments on a topic from before an influence campaign has begun. Cumulatively, social media analysis can be used to measure campaign exposure as well as changes in knowledge, attitudes, and, to some extent, behaviour.[111]

A recent RAND study to determine the amount of Turkish speaking ISIS supporters online found a significant decrease in the ISIS support base and Twitter activity. The findings indicate this is due to the effectiveness of Twitter's suspension campaigns. Overall data can be examined in a way which calculates the 'radicalization score'. This score is based on algorithms that have been created for machine learning. The score ranges from 1 to 100, indicating how well new discoveries match the online behaviours of known violent extremists online. While the number itself matters, what are more important are any significant shifts in large groups of individuals.[112]

Automated sentiment analysis, also known as "tonality scoring", and "opinion mining" associated with a particular topic or audience from a variety of content can be used to measure several important constructs along the hierarchy of behavioural change. These include awareness, attitudes toward and perceptions of friendly forces, perceptions and resonance of adversaries and adversary institutions.[113]

No doubt, there is reason to question the validity of some claims regarding the actual capability of some tools. But discussions with NATO SMEs reveal that there are a broad variety of tools in use, mostly provided by external contractors that offer many different capabilities. Nonetheless, both the NATO workshop and RAND report agree that, despite these challenges, social media data will continue to play a key role in influence related MOE.

Appeals to Surrender

Since social media micro-targeting can be employed to influence the individual recipient, it is likely one of the most effective tools for appeals to surrender of insurgency forces. Not only can the message be most effectively designed for reaching a target audience even if it contains only one target, but it also reaches individuals in a

[111]Paul, Christopher/ Yeats, Jessica/ Clarke, Colin P./ Matthews, Miriam (2015): Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade, RAND Corporation, Santa Monica; 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z1/RAND_RR809z1.pdf.

[110] Paul, Christopher/ Yeats, Jessica/ Clarke, Colin P./ Matthews, Miriam (2015): Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade, RAND Corporation, Santa Monica; 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z1/RAND_RR809z1.pdf.

[113] Paul, Christopher/ Yeats, Jessica/ Clarke, Colin P./ Matthews, Miriam (2015): Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade, RAND Corporation, Santa Monica; 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z1/RAND_RR809z1.pdf.

way that is not suspicious to them as the appeal reaches them in their natural environment and is therefore more likely to be plausible.[114] For instance, after months of surrender appeals to the remaining pockets of territory controlled by ISIS terrorists in Iraq and Syria, the Pentagon used social media to broadcast that if enemy forces did not surrender they would be "shot in the face or beaten to death with an entrenching tool."[115] While this message was not well received within many coalition countries, it may have helped to solidify how dire the situation was for ISIS fighters within these pockets. In preceding posts, the US army senior enlisted member made assurances that if these fighters did surrender they would be well treated, fed and given due process.[116]

Similarly, Turkey's president, Recep Tayyip Erdogan, used social media to appeal to his followers to resist the 2016 attempted military coup as well as to broadcast images of troops turning over their weapons, stripping off their uniforms and surrendering.[117] This content was created in order to promote an image of control and to convince the faction of the military attempting the coup that their cause was hopeless.

Surrender appeals in any type of conflict are primarily focused on convincing the enemy of the hopelessness of his or her situation and that he or she will be treated fairly if detained by coalition forces. Conventional surrender appeals are typically conveyed via leaflet drop or loud speaker messaging. Directly messaging soldiers on social media is effective if the surrender messages are also linked to locally credible sources of information detailing how futile the military situation has become for the target audience. Additionally, non-governmental organizations such as the International Committee of the Red Cross (ICRC) could simultaneously broadcast that their members are in place to monitor detention facilities and ensure that blue forces will act in accordance with international law. Moreover, families and friends of the enemy soldiers may also see these messages and urge their loved ones to stop fighting. While loudspeakers and leaflets may be effective in having the message delivered, direct messages on social media are much more personally targeted and will be seen not just by the soldier but their network. Conversely, individually targeted surrender messages may also induce fear in these soldiers based on the fact that coalition forces are tracking them as a specific people rather than as anonymous soldiers. This fear can also be used to convince the enemy of the pointlessness of their situation.

[114] Fisher, Nicole (2018): Your Brain On Drama: What Social Media Means For Your Personal Growth, *Forbes*, 10 August 2018. https://www.forbes.com/sites/nicolefisher/2018/08/10/your-brain-on-drama-what-your-social-media-means-for-personal-growth/#93e0f77e91dd.

[115] Lamothe, Dan (2018): Senior Pentagon Soldier Warns ISIS: Quit or Be Shot in The Face, Beaten with Entrenching Tools, The Washington Post, 11 January 2018. https://www.washingtonpost.com/news/checkpoint/wp/2018/01/10/senior-pentagon-soldier-warns-isis-quit-or-be-shot-in-the-face-beaten-with-entrenching-tools/?utm_term=.2c46454be2bf.

[116] Lamothe, Dan (2018): Senior Pentagon Soldier Warns ISIS: Quit or Be Shot in The Face, Beaten with Entrenching Tools, The Washington Post, 11 January 2018.https://www.washingtonpost.com/news/checkpoint/wp/2018/01/10/senior-pentagon-soldier-warns-isis-quit-or-be-shot-in-the-face-beaten-with-entrenching-tools/?utm_term=.2c46454be2bf.

[117] Financial Times Staff Report (2016): How Erdogan Turned to Social Media to Help Foil Coup, Financial Times; 16 July 2016. https://www.ft.com/content/3ab2a66c-4b59-11e6-88c5-db83e98a590a.

Influencing public support for adversaries

Social media can be used to target members of a host nation in their natural environment directly and introduce them to information that might lead to the reconsideration of their support for the insurgency. The US has for example has successfully tried to weaken support for ISIS by spreading images of ISIS atrocities on social media.[118] The effect of social media for influencing public support of the adversary is twofold. First, the target audience becomes aware of adversary activities from an angle it might not otherwise have, which can lead to doubts about the legitimacy of an insurgency,[119] potentially weakening public support of an opponent.[120] Second, by signaling to the host nation public that the information space is not owned by the adversary (in this case, ISIS). Therefore, it gives members of the public resisting ISIS hope in their own activities against ISIS. As crucial as the actual message content is, it is simply not enough to leave the information space to the adversary, but to make available an alternative interpretation of the events.

Another example of the use of social media to influence public support is Russia's worldwide propaganda campaign to undermine support of governments the Kremlin would like to see replaced.[121] As part of this campaign, Russia disseminates propaganda to Russian speakers – among many other countries -in the Baltics, Ukraine, and other nearby states through a variety of means, including social media. It has used this outreach to sow dissent against host and neighbouring governments, as well as against NATO and the EU.[122] Russia has also used social media to promote a narrative throughout the global Russian diaspora that the insurgency it supports in Eastern Ukraine is a response to an all-out war against the Russian population of Eastern Ukraine.[123] Russian bot networks have also used social media to undermine public support in the West for interventions against the Assad government in Syria.[124]

[118] Helmus, Todd C./ Bodine-Baron, Elizabeth/ Magnuson, Madeline/ Mendelsohn, Joshua/ Marcellino, William/ Bega, Andriy/ Winkelman, Zev (2016): Examining ISIS Support and Opposition Networks on Twitter, RAND Corporation, Santa Monica; 2018.https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

[119] Zeitzoff, Thomas (2018): Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict, *Journal of Conflict Resolution*, Volume 62, Issue 1. http://journals.sagepub.com/doi/abs/10.1177/0022002716650925.

[120] Bodine-Baron, Elizabeth (2016): U.S. Social Media Strategy Can Weaken ISIS Influence on Twitter, Rand, 16 August 2016. https://www.rand.org/news/press/2016/08/16.html.

[121] The Economist (2018): Russian disinformation distorts American and European democracy, The Economist, 22 February 2018. https://www.economist.com/briefing/2018/02/22/russian-disinformation-distorts-american-and-european-democracy.

[122] Helmus, Todd C./ Bodine-Baron, Elizabeth/ Magnuson, Madeline/ Mendelsohn, Joshua/ Marcellino, William/ Bega, Andriy/ Winkelman, Zev (2016): Examining ISIS Support and Opposition Networks on Twitter, RAND Corporation, Santa Monica; 2018. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

[123] Makhortykh, Mykola/ Sydorova, Maryna (2017): Social media and visual framing of the conflict in Eastern Ukraine, *Media, War & Conflict*, Volume 10, Issue 3; 9 April 2017.http://journals.sagepub.com/doi/full/10.1177/1750635217702539.

[124] Middle East Eye Staff Report (2018): Russia driving huge online 'disinformation' campaign on Syria gas attack, says UK PM Theresa May, Middle East Eye; 20 April 2018. http://www.middleeasteye.net/news/salisbury-syria-russia-social-media-theresa-may-528921594.

Specifically, the Kremlin uses social media to achieve policy paralysis by creating chaos and eroding trust in governments and its institutions by spreading false narratives.[125] Russia employs a synchronized mix of media that varies from attributed television and news website content to far-right blogs with unclear attribution, as well as non-attributed social media accounts in the form of bots and trolls. Recent reports show that since 2014, Facebook has been the platform of choice to sow discord within the US, not only over foreign policy, but to exploit internal divisions on issues such as religion, race and immigration.[126] However, Facebook has recently deleted mass numbers of fake accounts created by Russian troll farms[127] as well as content uploaded by them.[128] This has drastically reduced Russian influence through these channels – at least for the time being. Other social media services like Tumblr have taken similar measures further reducing Russia's impact on public support through social media in Western countries.[129]

ISIS also used social media, among many other forms, not only to promote itself as a legitimate state, but also to broadcast its success as they swept through much of Syria and then pushed into Iraq in 2014.[130] A key message on social media was the "End of Sykes Picot", as ISIS tweeted photographs of a bulldozer demolishing the earthen barrier that had long marked the border between Syria and Iraq.[131] This message was a reference to the 1916 agreement between the UK and France that led to the current borders in that area. While it was likely primarily intended to rally global Muslim audiences to their cause, it was also intended to dissuade public support in the West for military intervention to re-establish the perceived false borders which had caused the conflict in the first place. ISIS has very effectively succeeded in influencing public support for campaigns against them through social media.[132]

Finally, in Afghanistan, Taliban insurgents also use social media to influence public opinion. They promote themselves as a government in exile or state within a state whose legitimacy is visible through al-Emarah, the Islamic Emirate of Afghanistan which still exists online. The Taliban's limited but targeted broadcasts to audiences in the Muslim and Western worlds are intended to help it achieve its long-held goal of

[125] Helmus, Todd C./Bodine-Baron, Elizabeth/Radin, Andrew/Magnuson, Madeline/Mendelsohn, Joshua/Marcellino, William/Bega, Andriy/Winkelman, Zev (2018): Russian Social Media Influence, Rand Corporation, Santa Monica. https://www.rand.org/pubs/research_reports/RR2237.html.

[126] Frenkel, Sheera/ Benner, Katie (2018): To Stir Discord in 2016, Russians Turned Most Often to Facebook, The New York Times; 17 February 2018. https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html.

[127] Meixler, Eli (2018): Facebook Has Removed Hundreds of Accounts Linked to a Russian Troll Farm, Time, 4 April 2018. http://time.com/5227225/facebook-russia-troll-accounts/.

[128] Menn, Joseph, Ingram, David (2018): Facebook Deletes Posts Linked To Russian 'Troll Factory': CEO Zuckerberg, Reuters, 3 April 2018. https://www.reuters.com/article/us-facebook-ceo-fakenews/facebook-deletes-posts-linked-to-russian-troll-factory-ceo-zuckerberg-idUSKCN1HA2LV.

[129] BBC (2018): Tumblr Deletes 'Russian Troll' Accounts, BBC News, 26 March 2018.https://www.bbc.com/news/technology-43539886.

[130] Diresta, Renee (2018): How ISIS and Russia won friends and manufactured crowds, Wired, 3 March 2018. https://www.wired.com/story/isis-russia-manufacture-crowds/.

[131] Geltzer, Joshua A. (2018): Bad Actors Are Using Social Media Exactly as Designed, Wired; 11 March 2018. https://www.wired.com/story/bad-actors-are-using-social-media-exactly-as-designed/.

[132] Prier, Jarred (2017): Commanding the Trend: Social Media as Information Warfare*, Strategic Studies Quarterly*, Volume 11, Issue 4, Winter 2017. www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

expelling foreign soldiers from Afghanistan by accenting weak support for more operations in the country, thereby achieving a reduced presence of international forces.[133] The Taliban has also used social media to undermine the credibility of the Afghan Government and in some cases to join in on conversations mocking the government for its perceived incompetence.[134]

[133] Bodetti, Austin (2016): The Taliban's Latest Battlefield: Social Media, The Diplomat; 8 September 2016. https://thediplomat.com/2016/09/the-talibans-latest-battlefield-social-media/.

[134] First Post Staff Report (2015): Taliban Joins Social Media to Mock Afghan Leaders Delaying Decision on New Cabinet, The First Post; 6 January 2015. https://www.firstpost.com/world/taliban-joins-social-media-to-mock-afghan-leaders-delaying-decision-on-new-cabinet-2033101.html.

Conclusion

In reviewing social media exploitation forms it is evident that using social media for influence targeting promises the most operational benefits compared to traditional forms of influence operations. Actively introducing information into the information space in any operation is likely to have the largest effect on mission success for example in COIN operations as it can reduce the impact of enemy messaging, give those hope that are resisting adversaries, motivate others to support the counter insurgency, and reduce the impression of ownership of the information space by adversaries.

While most other forms of social media exploitation have considerable value in military operations, the potential for direct impact is the largest with influence targeting. Notably, the most impactful effect is likely achieved with a combination of the eight forms of social media exploitation we discussed above. Many of the other forms are necessary to be able to design a message for influence targeting that is likely to have the largest effect. Without very detailed social network analysis, target discovery, and surveillance of a target audience, influence targeting will not have a reliable, desired behavioral change effect.

Further research is needed on how to best achieve a reliable influence capability through social media. At this point, there is very little empirical research on how to best exploit social media in operational environments to achieve very specific effects.

Bibliography

BOOKS

Bell, Christian (2016): Use of Social Media as an Effector, Multinational Capability Development Campaign, Zentrum für Operative Kommunikation der Bundeswehr, Mayen.

Bodine-Baron, Elizabeth/Helmus C. Todd/Magnuson, Madeline/Winkelman, Zev (2016): Examining ISIS Support and Opposition Networks on Twitter, Rand, Santa Monica.

Gillespie, Tarleton (2018): Custodians of the Internet, Platforms, Content Moderation and the Hidden Decisions that shape Social Media, Yale University Press, New Haven.

Gilroy-Ware, Marcus (2017): Filling the Void, Emotion, Capitalism & Social Media, Repeater Books, London.

Greengard, Samuel (2015): The Internet of Things, The MIT Press, Boston.

Hayden, Michael V. (2018): The Assault on Intelligence, Penguin Press, New York.

Lanier, Jaron (2018): Ten Arguments for Deleting Your Social Media Accounts Right Now, MacMillan, New York.

Marcellino, William M. / Smith, Meagan L./ Paul, Christopher/ Skrabala, Lauren (2017): Monitoring Social Media, Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations, Rand, Santa Monica.

Matejic, Nicole (2015): Social Media Rules of Engagement: Why Your Online Narrative is the Best Weapon During a Crisis, Wiley and Sons, Melbourne; 2015.

Murthy, Dhiraj (2013): Twitter Digital Media and Society Series, Polity Press, Cambridge.

Nagle, Angela (2017): Kill All Normies, Zero Books, Alresford.

Newmann, Nic (2018): Journalism, Media, and Technology Trends and Predictions. Reuters, Oxford.

Nissen, Thomas (2015): #TheWeaponizationOfSocialMedia @Characteristics_of_Contemporary Conflicts, Royal Danish Defence College, Copenhagen.

O'Connor, Kimberly W./ Schmidt, Gordon B. (2018): Social Media, Data Privacy, and the internet of People, Things and Services in the Workplace, In: Simmers, Claire A./ Anandarajan, Murugan (2018): The Internet of People, Things and Services, New York.

Quinn, Michael J (2016): Ethics for the Information Age, New York.

Schaeffer, Ute (2018): Fake statt Fakt, DTV, München.

Silberstein, Schlecky (2018): Das Internet muss weg, Knaus, München.

Soro, Alessandro/Bereton, Margot/Roe, Paul (eds.) (2018): Social Internet of Things, Springer International Publishing, New York.

Sunstein, Cass R. (2018): #Republic: Divided Democracy in the Age of Social Media, Princeton University Press, Princeton.

Taplin, Jonathan (2018): Move Fast and Break Things, Pan Books, London.

Turkel, Sherry (2015): Reclaiming Conversation: The Power of Talk in The Digital Age, Penguin, Toronto.

Vaidhyanathen, Siva (2018): Antisocial Media, How Facebook Disconnects Us and Undermines Democracy, Oxford.

Ventre, Daniel (2016): Information Warfare, John Wiley & Sons, Hoboken.

Watts, Clinton (2018): Messing with the Enemy, Surviving in a Social Media world of Hackers, Terrorists, Russians, and Fake News, Harper Collins, New York.

Yarlagadda, Rithvik/Felmlee, Diane/Verma, Dinesh/Gartner, Scott (2018): Implicit Terrorist Networks: A Two-Mode Social Network Analysis of Terrorism in India. In: Thomson R., Dancy C., Hyder A., Bisgin H. (eds) Social, Cultural, and Behavioral Modeling. Lecture Notes in Computer Science, vol 10899. Springer, Cham.

JOURNAL ARTICLES

Alencer, Amanda (2017): Refugee integration and social media: a local and experimental perspective, Information Communication and Society, June 2017. https://www.researchgate.net/publication/317728781_Refugee_integration_and_social_media_a_local_and_experiential_perspective

Constantinides, Efthymios, et al. (2008): Social Media: A New Frontier for Retailers?, *European Retail Research*, Volume 22, 2008.

Del Vicario, Michaela/ Zollo, Fabiana/ Calarelli, Guido/ Scala, Antonio/ Quattrociocchi, Walter (2017): Mapping social dynamics on Facebook: The Brexit Debate, *Social Networks*, Vol. 50. http://eprints.imtlucca.it/3684/.

Gawthorpe, Andrew J. (2017): All Counterinsurgency is Local: Counterinsurgency and Rebel Legitimacy, Small Wars & Insurgencies, Volume 28, Issue 4-5, 26 July 2017. https://www.tandfonline.com/doi/full/10.1080/09592318.2017.1322330.

Jost, John T. et. al. (2018): How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks, *Political Psychology*, Volume 39, Issue 51; February 2018. https://onlinelibrary.wiley.com/doi/abs/10.1111/pops.12478.

Kousiouris, George et. al. (2018): An integrated information lifecycle management framework for exploring social network data to identify dynamic large crowd concentration events in smart cities applications, Surrey Research Insight, *Future Generation Computer Systems*, Volume 78, Part 2; 2018. http://epubs.surrey.ac.uk/841839/.

Lindenberg, Siegwart/ Steg, Linda (2007) Normative, Gain and Hedonic Goal Frames Guiding Environmental Behavior, *Journal of Social Issues*, Volume 63, Issue 1, pages 117–137, March 2007. https://www.rug.nl/research/portal/publications/normative-gain-and-hedonic-goal-frames-guiding-environmental-behavior(36809827-091d-4d03-84f5-7205bf464c53).html.

Makhortykh, Mykola/ Sydorova, Maryna (2017): Social media and visual framing of the conflict in Eastern Ukraine, *Media, War & Conflict*, Volume 10, Issue 3; 9 April 2017. http://journals.sagepub.com/doi/full/10.1177/1750635217702539.

Mangold, W. Glynn/ Faulds, David J. (2009): Social Media: The New Hybrid Element of the Promotion Mix, Kelley School of Business, Indiana University, *Business Horizons*, No. 52, 2009. https://www.sciencedirect.com/science/article/pii/S0007681309000329.

Marcellino, William M. (2017): Revisioning Strategic Communication rough Rhetoric and Discourse Analysis, *Joint Force Quarterly*, No. 76, First Quarter 2015.

Min, Jinyoung (2017): Effects of the Use of Social Network Sites on Task Performance: Toward a Sustainable Performance in a Distracting Environment, *Sustainability*, Number 9-2017.

Pechenkina,Anna/ Bennett, D. Scott (2017): Violent and Non-Violent Strategies of Counterinsurgency, *Journal of Artificial Societies and Social Simulation*, Volume 20, Issue 4. https://jasss.soc.surrey.ac.uk/20/4/11.html.

Prier, Jarred (2017): Commanding the Trend: Social Media as Information Warfare*, Strategic Studies Quarterly*, Volume 11, Issue 4, Winter 2017.www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

Steinert-Threlkeld, Zachary C./ Mocanu, Delia/ Vespignani, Alessandro/ Fowler, James (2015): Online Social Networks and Offline Protest, *EPJ Data Science*, Volume 4, Issue 19; December 2015. https://link.springer.com/article/10.1140/epjds/s13688-015-0056-y.

Stieglitz, Stefan/Mirbabaie, Miland/Ross, Bjorn/Neuberger, Christoph (2018): Social media analytics – Challenges in topic discovery, data collection, and data preparation, International Journal of Information Management, Vol. 39.https://www.sciencedirect.com/science/article/pii/S0268401217308526

Ucko, David H. (2018): Violence in context: Mapping the Strategies and Operational Art of Irregular Warfare, Contemporary Security Policy, Volume 39, Issue 2; 9 February 2018. https://www.tandfonline.com/doi/abs/10.1080/13523260.2018.1432922.

Vousoughi, Soroushi/ Roy, Deb/ Aral, Sinan (2018): The Spread of Truth and False News Online, *Science*, Volume 359, Issue 6380, 9 March 2018.http://science.sciencemag.org/content/359/6380/1146.full.

Zeitzoff, Thomas (2018): Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict, *Journal of Conflict Resolution*, Volume 62, Issue 1. http://journals.sagepub.com/doi/abs/10.1177/0022002716650925.

OTHER SOURCES

Alsaedi, Nasser/ Burnap, Pete/ Rana, Omer (2017): Can We Predict A Riot? Disruptive Event Detection Using Twitter, ACM Transactions on Internet Technology (TOIT) - Special Issue on Advances in Social Computing and Regular Papers, Volume 17, Issue 2, Article 18, ACM, New York; May 2017. https://dl.acm.org/citation.cfm?id=2996183.

Anderson, Berit (2017): The Rise of the Weaponized AI Propaganda Machine, Medium; 12 February 2017. https://medium.com/join-scout/the-rise-of-the-weaponized-ai-propaganda-machine-86dac61668b.

Anderson, Janna/ Rainie, Lee (2012): Millennials Will Benefit and Suffer Due to Their Hyper Connected Lives, Pew Research Center, *Pew Internet/Elon University Survey*, 29 February 2012. http://www.pewinternet.org/2012/02/29/millennials-will-benefit-and-suffer-due-to-their-hyperconnected-lives-2/.

Ballhaus, Rebecca/ Gross, Jenny (2018): Cambrige Analytica Closing Operations Following Facebook Data Controversy, The Wall Street Journal, 2 May 2018. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140.

Barret, Victoria (2012): CEOs Afraid of Going Social Are Doing Shareholders a Massive Disservice, Forbes, 12 July 2012. http://www.forbes.com/sites/victoriabarret/2012/07/12/ceos-afraid-of-going-social-are-doing-shareholders-a-massive-disservice/#5498eb0659b7.

BBC (2018): YouTube and Instagram Face Russian Bans, BBC News, 14 February 2018. https://www.bbc.com/news/technology-43058399.

BBC (2018): Tumblr Deletes 'Russian Troll' Accounts, BBC News, 26 March 2018. https://www.bbc.com/news/technology-43539886.

Berger, J.M./ Morgan, Jonathan (2015): The ISIS Twitter Census, *Project on U.S. Relations with the Islamic World,* Number 20, Brookings Institution; March 2015. https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

Bershidsky, Leonid (2017): The Yellow Rubber Duck is a Potent Protest Symbol, Bloomberg; 28 March 2017.https://www.bloomberg.com/.../the-yellow-rubber-duck-is-a-potent-protest-symbol.

Blanken, Leo/Lepore, Jason/Rodriguez, Stephen (2018): America's military is choking on old technology, Foreign Policy, 29 January, 2018. https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/

Blumenthal, Paul (2018): The Techno-Colonialism of Facebook And Cambridge Analytica, Huffington Post; 23 March 2018. https://www.huffingtonpost.ca/entry/facebook-cambridge-analytica-developing-world_us_5ab50bc7e4b0decad04951d1.

Bodetti, Austin (2016): The Taliban's Latest Battlefield: Social Media, The Diplomat; 8 September 2016. https://thediplomat.com/2016/09/the-talibans-latest-battlefield-social-media/.

Bodine-Baron, Elizabeth (2016): U.S. Social Media Strategy Can Weaken ISIS Influence on Twitter, RAND Corporation, 16 August 2016. https://www.rand.org/news/press/2016/08/16.html.

Bradshaw, Samantha/Howard, Philip N. (2018): Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project University of Oxford. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Brandon, John (2017): The Surprising Reason Millennials Check Their Phones 150 Times a Day, Inc.com; 17 April 2017. https://www.inc.com/john-brandon/science-says-this-is-the-reason-millennials-check-their-phones-150-times-per-day.html.

Brooking, Emerson T./ Singer, Peter W. (2016): War Goes Viral, The Atlantic; November 2016. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

Canadian Land Forces Command and Staff College (undated): Mission and Task Verbs, Retain CAF Staff College; Undated. http://armyapp.forces.gc.ca/SOH/SOH_Content/Retain/Retain.htm.

Castillo, Walbert (2015): Air Force Intel Uses ISIS 'Moron' Post to Track Fighters, CNN; 5 June 2015. https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html.

Chadwick, Paul (2018): Why fake news on social media travels faster than the truth, The Guardian, 19 March 2018. https://www.theguardian.com/commentisfree/2018/mar/19/fake-news-social-media-twitter-mit-journalism.

Cordy, Jane (2017): The Social Media Revolution: Political and Security Implications, NATO Committee on the Civil Dimension of Security, 7 October, 2017. https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20158%20CDSDG%2017%20E%20bis%20-%20SOCIAL%20MEDIA%20REVOLUTION%20-%20CORDY%20REPORT.pdf.

Coster, Helen (2009): Cellphones: The New Billboards, Forbes, 15 July 2009. https://www.forbes.com/2009/07/15/mobile-marketing-cmo-network-mobilemarketing.html#b00079240753.

Diresta, Renee (2018): How ISIS and Russia won friends and manufactured crowds, Wired, 3 March 2018. https://www.wired.com/story/isis-russia-manufacture-crowds/.

Doce, Nacho (2016): Brazil’s Restive Rich Draft a Duck to Protest President, Reuters; 20 March 2016.
https://www.reuters.com/article/us-brazil-politics-duck-idUSKCN0WM0F1?utm_source=Facebook.

Dragojlo, Sasa (2015): Giant Duck Becomes Belgrade Resistance Symbol, Balkan Insight.com; 26 September 2015.
http://www.balkaninsight.com/en/article/giant-duck-becomes-belgrade-resistance-symbol-09-25-2015.

Eadicicco, Lisa (2015): Americans Check Their Phones 8 Billion Times a Day, Time, 15 December 2015. http://time.com/4147614/smartphone-usage-us-2015/.

Eikenberry, Karl W. (2013): The Limits of Counterinsurgency Doctrine in Afghanistan: The Other Side of the COIN, Foreign Affairs; September/October 2013. https://www.foreignaffairs.com/articles/afghanistan/2013-08-12/limits-counterinsurgency-doctrine-afghanistan.

Enikolopova, Ruben/ Makarine, Alexey/ Petrova, Maria (2016): Social Media and Protest Participation: Evidence from Russia, *CEPR Discussion Papers*, Number 11254; 2016. https://www.tcd.ie/Economics/assets/pdf/Seminars/20172018/Social_Media_Protests_17-04-12.pdf.

Eremenko, Alexey (2017): Russia's Protests Explained: Why Rubber Ducks, Sneakers Are at Demonstrations, NBC News; 27 March 2017. https://www.nbcnews.com/news/world/russia-s-protests-explained-why-rubber-ducks-sneakers-are-demonstrations-n738891.

European Commission (2013): Communicating with the outside world – Guidelines for All Staff on the Use of Social Media. http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf

Fasteneau, Jelle (2018): Under the Influence: The Power of Social Media Influencers, Medium; 6 March 2018. https://medium.com/crobox/under-the-influence-the-power-of-social-media-influencers-5192571083c3.

Fisher, Nicole (2018): Your Brain On Drama: What Social Media Means For Your Personal Growth, *Forbes*, 10 August 2018. https://www.forbes.com/sites/nicolefisher/2018/08/10/your-brain-on-drama-what-your-social-media-means-for-personal-growth/#93e0f77e91dd.

Financial Times Staff Report (2016): How Erdogan Turned to Social Media to Help Foil Coup, Financial Times; 16 July 2016. https://www.ft.com/content/3ab2a66c-4b59-11e6-88c5-db83e98a590a.

First Post Staff Report (2015): Taliban Joins Social Media to Mock Afghan Leaders Delaying Decision on New Cabinet, The First Post; 6 January 2015. https://www.firstpost.com/world/taliban-joins-social-media-to-mock-afghan-leaders-delaying-decision-on-new-cabinet-2033101.html.

Frenkel, Sheera/ Benner, Katie (2018): To Stir Discord in 2016, Russians Turned Most Often to Facebook, The New York Times; 17 February 2018. https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html.

Geltzer, Joshua A. (2018): Bad Actors Are Using Social Media Exactly as Designed, Wired; 11 March 2018. https://www.wired.com/story/bad-actors-are-using-social-media-exactly-as-designed/.

Griffiths, Mark/Kuss, Daria (2018): 6 questions help reveal if you’re addicted to social media, The Washington Post, 25 April, 2018. https://www.washingtonpost.com/news/theworldpost/wp/2018/04/25/social-media-addiction/?utm_term=.bf65d01f0138.

Gunitsky, Seva (2015): Social media helps dictators, not just protestors, The Washington Post, 30 March 2015. https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/30/social-media-helps-dictators-not-just-protesters/?utm_term=.5f008e4842ca.

Haim, Dotan A. (2017): Civilian Social Networks and Counter Insurgency, Department of Political Science, University of California, San Diego; 2017. http://dotanhaim.com/wp-content/uploads/2017/10/Haim_WS1.pdf.

Haines, Ian (2018): The Power of A/B Testing: The US Election, Symposium; 10 February 2018. https://symposeum.com/power-b-testing-us-election/.

Helmus, Todd C./ Bodine-Baron, Elizabeth/ Magnuson, Madeline/ Mendelsohn, Joshua/ Marcellino, William/ Bega, Andriy/ Winkelman, Zev (2016): Examining ISIS Support and Opposition Networks on Twitter, RAND Corporation, Santa Monica; 2018. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

Helmus, Todd C./Bodine-Baron, Elizabeth/Radin, Andrew/Magnuson, Madeline/Mendelsohn, Joshua/Marcellino, William/Bega, Andriy/Winkelman, Zev (2018): Russian Social Media Influence, RAND Corporation, Santa Monica. https://www.rand.org/pubs/research_reports/RR2237.html.
Herrick, Drew (2016): The Social Side of 'Cyber Power'? Social Media and Cyber Operations, paper presented at the 2016 8th International Conference on Cyber Conflict. https://ccdcoe.org/cycon/2016/proceedings/07_herrick.pdf.

Hern, Alex (2018): Fitness Tracking App Strava Gives Away Location of Secret US Army Bases, The Guardian (UK), 28 January 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

Hofseth, Anders (2017): Fake News, Propaganda, and Influence Operations – a Guide to Journalism in a New, and More Chaotic Media Environment, Reuters Institute, 14 March 2017. https://reutersinstitute.politics.ox.ac.uk/risj-review/fake-news-propaganda-and-influence-operations-guide-journalism-new-and-more-chaotic.

Ineca, Marcello/ Vayena, Effy (2018): Cambridge Analytica and Online Manipulation, Scientific American, 30 March 2018. https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/.

Jacobsson Purewal, Sarah (2010): Facebook Messages: The Worst Thing That Ever Happened, PC World, 16 November 2010. https://www.pcworld.com/article/210758/Facebook_Messages_The_Worst_Thing_That_Ever_Happened.html.

Kandemir, Berfin, Brand, Alexander (2017): Social Media in Operations: A Counter Terrorism Perspective, *NATO Stratcom COE-DAT*, Ankara; September 2017. https://www.stratcomcoe.org/download/file/fid/77718.

Kleinman, Zoe (2015): Are we addicted to technology? BBC, August 31, 2015. https://www.bbc.com/news/technology-33976695.

Kosseim, Patricia (2017): Government Information Sharing and Improved Service Delivery: Embracing the Wind of Change without throwing Caution to the Wind, *Remarks at the Government of Canada Data Leads Group*, 27 September 2017. https://www.priv.gc.ca/en/opc-news/speeches/2017/sp-d_20170927_pk/.

Kossov, Ivan (2017): Meet the men who fought ISIS from inside Mosul, USA Today; 2 May 2017. https://www.usatoday.com/story/news/world/2017/05/02/islamic-state-isis-militants-iraq-civilians-resistance/101131176/.

Kruh, Willy (2014): Social media Have Changed How We Communicate Ideas, The Globe and Mail, 29 June 2014. https://www.theglobeandmail.com/report-on-business/careers/careers-leadership/social-media-have-changed-how-we-communicate-ideas/article19385666/.

Lamothe, Dan (2018): Senior Pentagon Soldier Warns ISIS: Quit or Be Shot in The Face, Beaten with Entrenching Tools, The Washington Post, 11 January 2018. https://www.washingtonpost.com/news/checkpoint/wp/2018/01/10/senior-pentagon-soldier-warns-isis-quit-or-be-shot-in-the-face-beaten-with-entrenching-tools/?utm_term=.2c46454be2bf.

Leetaru, Kalev (2018): Without Transparency, Democracy Dies in the Darkness of Social Media, Forbes, 25 January 2018. https://www.forbes.com/sites/kalevleetaru/2018/01/25/without-transparency-democracy-dies-in-the-darkness-of-social-media/#7269cd817221.

Luo, Ting (2018): Explaining Incumbent Re-Election in Authoritarian Elections: Evidence from a Chinese County, Democratization, 19 April 2018. https://www.tandfonline.com/doi/full/10.1080/13510347.2018.1462798.

MacAskill, Ewen (2014): Cover-up: Ukraine Rebels Destroying All Links to MH17 Air Atrocity UN Demands Full Inquiry But Armed Russian Separatists Block Access To Crash Site Amid Confusion Over Black Boxes, The Guardian (UK), 18 July 2014. https://www.theguardian.com/world/2014/jul/18/separatist-links-malaysia-airlines-mh17-removed.
Maurya Chandra Gupta / Gore, Sandeep/ Rajput, Dharmendra Singh (2018) A Use of Social Media for Opinion Mining: An Overview With the Use of Hybrid Textual and Visual Sentiment Ontology, In: Tiwari, B./ Tiwari, V./ Das K./ Mishra, D./ Bansal, J. (eds.) *Proceedings of International Conference on Recent Advancement on Computer and Communication - Lecture Notes in Networks and Systems*, Volume 34, Singapore. https://link.springer.com/chapter/10.1007/978-981-10-8198-9_33.

McCay, Layla (2012): The Internet Never Forgets: How to Live in the 21st Century, Huffington Post, 30 June 2012. http://www.huffingtonpost.com/dr-layla-mccay/the-internet-never-forgets_b_1460110.html.

Meixler, Eli (2018): Facebook Has Removed Hundreds of Accounts Linked to a Russian Troll Farm, Time, 4 April 2018. http://time.com/5227225/facebook-russia-troll-accounts/.

Melia, O. Thomas (2018): Russia and America Aren't Morally Equivalent, The Atlantic, 27 February 2018. https://www.theatlantic.com/international/archive/2018/02/election-meddling-democracy-promotion/554348/.

Menn, Joseph, Ingram, David (2018): Facebook Deletes Posts Linked to Russian 'Troll Factory': CEO Zuckerberg, Reuters, 3 April 2018. https://www.reuters.com/article/us-facebook-ceo-fakenews/facebook-deletes-posts-linked-to-russian-troll-factory-ceo-zuckerberg-idUSKCN1HA2LV.

Middle East Eye Staff Report (2018): Russia Driving Huge Online 'Disinformation' Campaign on Syria Gas Attack, says UK PM Theresa May, Middle East Eye; 20 April 2018. http://www.middleeasteye.net/news/salisbury-syria-russia-social-media-theresa-may-528921594.

Mosul Eye (2016): What's happening in Mosul?, Mosul Eye© Report – Oct. 20, 2016; Mosul Eye Blog; 20 October 2016. https://mosul-eye.org/2016/10/21/whats-happening-in-mosul-mosul-eye-report-oct-20-2016/.

Mosul Eye Twitter Post (2016): Twitter Post: To the Liberation Ops Command in Gugjali, @Mosul Eye Twitter Feed; 2 November 2016. https://twitter.com/MosulEye/status/793936900931387393.

NATO (2009): ACO Directive 95-3: Social Media. December 2009. http://www.aco.nato.int/page300303028.aspx.
Ng, Jason Q. (2014): Tracing the Path of a Censored Weibo Post and Compiling Keywords That Triggered Automatic Review, The Citizen Lab; 10 November 2014. https://citizenlab.ca/2014/11/tracing-path-censored-weibo-post-compiling-keywords-trigger-automatic-review/.

Nicks, Denver (2015): New Zealander ISIS Fighter Accidentally Tweets Secret Location, Time; 1 January 2015. http://time.com/3651559/new-zealand-isis-twitter/.

Paul, Christopher/ Yeats, Jessica/ Clarke, Colin P./ Matthews, Miriam (2015): Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade, RAND Corporation, Santa Monica; 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z1/RAND_RR809z1.pdf.

PEN America (2018): Forbidden Feeds, Government Controls on Social Media in China, PEN America; 13 March 2018. https://pen.org/wp-content/uploads/2018/03/PENAmerica_Forbidden-Feeds-3.13-3.pdf.

Perez, Sarah (2017): Twitter Launches Lower-Cost Subscription Access to its Data Through New Premium APIs, Techcrunch, 14 November 2017. https://techcrunch.com/2017/11/14/twitter-launches-lower-cost-subscription-access-to-its-data-through-new-premium-apis/.

Raleigh Bousquet, Christopher (2018): Why Police Should Monitor Social Media to Prevent Crime, Wired; 20 April 2018. https://www.wired.com/story/why-police-should-monitor-social-media-to-prevent-crime/.

Ranking, Jennifer (2018): EU Votes for Copyright Law That Would Make Internet a 'Tool for Control', The Guardian (UK), 20 June 2018. https://www.theguardian.com/technology/2018/jun/20/eu-votes-for-copyright-law-that-would-make-internet-a-tool-for-control.

Robson, John (2017): Beware the Yellow Ducks – Russia's Humorous Anti-Corruption Protests Have Teeth, National Post; 30 March 2017.

http://nationalpost.com/opinion/john-robson-beware-the-yellow-ducks-russias-humorous-anti-corruption-protests-have-teeth.

Rosen, Jeffrey (2010): The Web Means the End of Forgetting, The New York Times, 21 July 2010. https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

Shaw, Tamsin (2018): Beware the Big Five, The New York Review of Books, 5 April 2018. http://www.nybooks.com/articles/2018/04/05/silicon-valley-beware-big-five/.

Siegelman, Wendy (2018): Cambridge Analytica is dead – but its obscure network is alive and well, The Guardian (UK), 5 May 2018. https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-scl-group-new-companies-names.

Smith, Marc A./ Rainie, Lee/ Shneiderman, Ben/ Himelboim, Itai (2014): Mapping Twitter Topic Networks: From Polarized Crowds to Community Clusters, Pew Research Center; 20 February 2014. http://www.pewinternet.org/2014/02/20/mapping-twitter-topic-networks-from-polarized-crowds-to-community-clusters/.

Story, Louise (2008): To Aim Ads, Web Is Keeping Closer Eye on You, The New York Times, 10 March 2008. http://www.nytimes.com/2008/03/10/technology/10privacy.html.

The Economist (2016): Free Speech Under Attack, The Economist, 4 June 2016. https://www.economist.com/leaders/2016/06/04/under-attack.

The Economist (2018): Russian disinformation distorts American and European democracy, The Economist, 22 February 2018. https://www.economist.com/briefing/2018/02/22/russian-disinformation-distorts-american-and-european-democracy.

Tremonti, Anna Maria (2018): ISIS on Your Doorstep: Meet Mosul Eye, The Man Who Defied The Terrorists To Save His City, CBC Radio 'The Current'; 6 February 2018. (Transcript and Audio File). http://www.cbc.ca/radio/thecurrent/the-current-for-february-6-2018-1.4522000/isis-on-your-doorstep-meet-mosul-eye-the-man-who-defied-the-terrorists-to-save-his-city-1.4522333.

Vomiero, Jessica/ Do, Eric Marl (2017): Snapchat's New Map Feature Could Be Tracking You All the Time. Global News, 25 June 2017. https://globalnews.ca/news/3554398/snapchats-new-map-feature-could-be-tracking-you-all-the-time/.

Weaver, Matthew (2018): Social media 'micro-targeting' of voters on the increase, MP told, The Guardian (UK), 23 January, 2018. https://www.theguardian.com/media/2018/jan/23/social-media-micro-targeting-of-voters-on-the-increase-mps-told.

Wong, Julia Carrie (2018): Cambridge Analytica-linked Academic Spurns Idea Facebook Swayed Election, The Guardian (UK), 20 June 2018. https://www.theguardian.com/technology/2018/jun/19/aleksandr-kogan-facebook-cambridge-analytica-senate-testimony.

Yang, Yaqiu (2016): The Business of Censorship: Documents Show How Weibo Filters Sensitive News in China, Committee to Protect Journalists, 3 March 2016.https://cpj.org/blog/2016/03/the-business-of-censorship-documents-show-how-weib.php.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Influence Techniques Using Social Media

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

Seaboyer, A.

5. DATE OF PUBLICATION (Month and year of publication of document.)

August 2018

6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)

37

6b. NO. OF REFS (Total references cited.)

125

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

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

DRDC – Toronto Research Centre
Defence Research and Development Canada
1133 Sheppard Avenue West
Toronto, Ontario M3K 2C9
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2018-C177

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

123455

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

influence; Intelligence; social media

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Social media has drastically changed communication within and toward target audiences in form, frequency and reach. Unparalleled influencing opportunities have emerged from social media's low production costs, minimal skill sets required and real-time message delivery to platforms audiences voluntarily check constantly - subjecting themselves to near constant influencing activities. The role of information itself has changed both for the consumer and the producer as societies are increasingly information-based. Leaks of top-secret files through social media have proven that there is no longer a realistic expectation of privacy for anyone. In a saturated environment where information is less controlled than ever before, how can social media be more effectively used as an influence capability? This paper explores aspects of social media as an influence capability by contextualizing how it is changing the operating environment, by identifying opportunities and challenges associated with social media exploitation for influence, and by discussing some promising forms of social media exploitation for influence. Social media exploitation for influence targeting promises the greatest operational benefits. Introducing information into the information space is likely to have the largest impact on mission success, for example, in COIN operations as it can reduce the impact of enemy messaging, give those hope that are resisting adversaries, motivate others to support the counter insurgency, and reduce the impression of ownership of the information space by adversaries.

Les médias sociaux ont radicalement changé les communications au sein et vers les publics cibles tant dans leur forme, leur fréquence et leur portée. Des opportunités d'influence inégalées découlent du fait des faibles coûts de production des médias sociaux, des compétences minimales requises pour les exploiter et de la diffusion en temps réel des messages sur les plateformes que les utilisateurs consultent volontairement - se soumettant ainsi presque constamment aux activités d'influence des organisations gouvernementales et non gouvernementales. Les fuites d'innombrables fichiers top-secrets par le biais de fournisseurs de médias sociaux ont prouvé qu'il n'y a plus d'attentes réalistes en matière de confidentialité pour quiconque dans l'espace de l'information. Cependant, dans un environnement saturé où les informations sont moins contrôlées que jamais, comment les médias sociaux peuvent-ils être utilisés plus efficacement comme capacité d'influence? Cet article explore les caractéristiques des médias sociaux en tant que capacité d'influence en contextualisant l'évolution de l'environnement d'exploitation, en identifiant les opportunités et les défis associés à l'exploitation des médias sociaux et en abordant certaines des formes les plus prometteuses d'exploitation des médias sociaux. Il conclut que l'utilisation des médias sociaux pour le ciblage d'influence a le potentiel d'offrir d'importants avantages opérationnels. L'introduction d'informations dans une opération est susceptible d'avoir un grand impact sur le succès de la mission, par exemple dans les opérations de contre-insurrection, car elle peut réduire l'impact des messages ennemis, donner de l'espoir à ceux qui résistent à l'adversaire, en inciter d'autres à soutenir la contre-insurrection et réduire l'impression de propriété de l'espace d'information par les adversaires.