Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach

A Bergh

Norwegian Defence Research Establishment (FFI)
Kjeller, Norway

Email: Arild.Bergh@ffi.no

Abstract: *Discussions about recent state-run influence operations in social media often focus only on quantitative elements—the number of people interacting with fake news or how many tweets were sent by bots. This article suggests that understanding how influence operations in social media may affect individuals and groups requires a socio-technical approach to examine what is unique about the social media information environment and people's interactions in and through these media. A socio-technical understanding emerges through the development of a model based on the Cyber Kill Chain that conceptualises the influence operation process as interlinked stages seeking alternate actions from a target audience.*

Keywords: *Social Media, Influence Operations, Kill Chain, Conceptual Model*

Introduction

The ubiquity of social media across geographical and demographic boundaries has given actors in inter- or intra-state conflicts new channels to try to affect opinions worldwide—at home, among the enemy, and in countries that might support either side. This can be done at a low cost in terms of time, money, and possible retaliation. At the same time, people increasingly get their news first and foremost from social media (Stelter 2008; Gottfried & Shearer 2016). These factors mean that social media is a desirable new arena for actors seeking to complement and to improve their traditional attempts at influencing people.

From 2014 to 2016, the use of social media as a component of state and terrorist level conflicts can be said to have simultaneously matured in use and entered the public consciousness. In the Middle East, ISIS successfully used videos on YouTube and other social media to spread propaganda and to recruit fighters from around the world to its cause (Fisher 2015; Matejic 2016). Russia annexed Crimea from Ukraine in 2014 and used social media to present narratives such as Crimea being helped by Russia in a crisis (Dougherty 2014; Giles 2015; Iasiello 2017). In the 2016 U.S. presidential election, Russian operatives undertook influence operations that partly sought to support a candidate believed to be more positive for Russia (Howard *et al.* 2018; Chen 2015).

There exists a fair amount of research that examines, rather than just reports on, influence operations in social media (examples include Geers 2015; Bialy 2017; Svetoka 2016). Such work often

ISSN 1445-3312 Print/ISSN 1445-3347 Online

approaches the topic at a fairly high level, and different elements of an influence operation are left as black boxes (for example, Van Niekerk & Maharaj 2013, p.1175). However, the importance of including the human/cognitive aspect when working with or in the cyber domain has occasionally been emphasised (Sartonen*,* Huhtinen & Lehto 2016).

There is thus a (partly acknowledged) need to connect the ways in which people interact with and process information in and through social media, as well as the technical underpinnings of social media, a so-called socio-technical perspective (Bergh 2018; Bergh 2019; Marwick 2018). This perspective, emerging from organisational research, suggests that one has to understand both social interactions from a social sciences perspective and the technology that facilitates and affects these interactions (Trist *et al.* 1990; Tatnall 2003; Akbari & Land 2016). In the case of influence operations in social media, one should examine how individuals and groups work within the structures that are created through technologies, such as search or instant messaging, to achieve different tasks linked to the goal of manipulating social media users (Inglis 2016).

This paper presents an approach to a socio-technical understanding of online influence operations in order to 1) throw some light upon the elements that are often left as black boxes in influence operation discussions; 2) examine social-media-based influence operations as a process that is not wholly controlled by the instigator; and 3) establish a model that has explanatory potential for how these influence operations may have an effect. The model is meant to encourage further work, such as the development of analytical tools. It is not directly concerned with information environment assessment (Paxton 2018), nor is it an analytical framework such as the information influence framework (Hammond-Errey 2019).

Terminology

An influence operation is the concerted effort by an actor, such as a state or a terrorist group, to interfere in the process of meaning making by individuals or groups outside its own legal control through tools and facilities on publicly available social media services. This is done to contribute to the generation of opinions and impressions that are favourable to the actor undertaking the influence operation and/or non-favourable to the other side. This definition is specific to this paper and may not mirror more broadly available definitions of influence operations (Larson *et al.* 2009; Santa Maria 2013). Furthermore, this paper focuses on activities targeting larger groups through public posts. Influence operations that target selected individuals or small groups are outside the scope of this article.

For the purpose of this paper the working definition of ‘social media’ is services that are available through the Internet that allow the posting of content by people who do not operate or control the service; and the facility for other people to access, use and respond to such content. This definition allows one to perceive online interactions around user-created content in other fora than pure social networks—from comment fields in local newspapers via online reviews to Facebook posts.

Finally, technical terms used include ‘algorithms’ (automated software processes that perform certain actions based on rules such as selecting news items for a user) and ‘bots’ (software using a social media profile to automatically post information or interact with others’ posts through likes and retweets, for example).

A Kill Chain Approach to Influence Operations in Social Media

To further the understanding of how influence operations in social media may have some effect, it is useful to break them down into different stages and examine the socio-technical aspects of each stage. This is done by building on an existing attempt to fuse Internet-based attacks with traditional military concepts; see the Cyber Kill Chain (Hutchins, Cloppert & Amin 2011) in **Figure 1**, below. This is an interesting departure point as the purpose of this concept is to "[treat] cyber security holistically, not as a collection of discrete functions" (Croom 2010, pp. 54-55). This is similar to what this article advocates, namely that influence operations need to be examined within the overall context of how people and technology interact in, around, and through social media. Facebook's internal security department has discussed some of these stages in relation to information operations (Weedon, Nuland & Stamos 2017) but does not attempt to account for how such operation may have an effect.

The phases outlined in **Figure 1** describe and analyse cyberattacks, such as hacking into an email account, from the preliminary reconnaissance phase to the final activities, for instance downloading confidential emails. This article 1) will develop a model of influence operations in social media that uses these phases to generate an updated kill chain for social media influence operations and 2) will explore whether this model has some explanatory potential with regard to how influence operations might achieve an effect in social media.

Reconnaissance	→	Research, identification, and selection of targets.
Weaponization	→	Pairing remote access malware with exploit into a deliverable payload (for example, Adobe PDF and Microsoft Office files).
Delivery	→	Transmission of weapon to target (such as via email attachments, websites, or USB drives).
Exploitation	→	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems.
Installation	→	The weapon installs a backdoor on a target's system thus allowing persistent access.
Command and Control	→	Outside server communicates with the weapons providing 'hands on keyboard access' inside the target's network.
Actions on objectives	→	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.

Figure 1: Phases of the "Cyber Kill Chain", based on figure from http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf

The two first phases of the kill chain shown in **Figure 1**, above, map quite easily onto the kill chain as seen in **Figure 2**, below. For example, the Russian influence efforts in the 2016 U.S. election campaign focused on issues that were found to be divisive, such as religion or guns (phase 1), were clearly selected by looking at the public discourses in American politics. The weaponization in phase 2 occurred through the creation of inflammatory images or texts that were published mainly on Twitter or Facebook (Penzenstadler, Heath & Guynn 2018; Timberg *et al.* 2017; Timberg & Romm 2018).

Reconnaissance	→	Find issues to exploit
Weaponization	→	Select social media outlets and create content

Figure 2: Steps 1 & 2 in a social media influence operation mapped onto the Cyber Kill Chain

However, the remaining steps in the chain (delivery, exploitation, installation, command and control, actions on objectives) require a more careful examination to see if a similar mapping approach can illuminate how influence operations function in social media.

Delivery: Using the Affordances of Social Media

In practical terms, the delivery is simply the posting of content, whether automated or manual, to a social media service. One can, therefore, say that this phase also exists in a kill chain for influence operations in social media. However, just as a hacking attack needs to find a suitable delivery mechanism, an influence operation must spread content in relevant fora. Different social media services have different characteristics and properties; these in turn provide certain affordances for actions. The affordance concept suggests that different objects lend themselves more to some actions than others (Gibson 1977; Norman 1999). This will in turn influence the actions of the actor using the object in question. A social media example would suggest that blogs afford longer, in-depth engagement, longer content lifetime, but less sharing of content. Twitter, on the other hand, facilitates rapid spread, single issue posts, less time to engage critically with content, and a short shelf-life for the content. It is of course possible to just read the ingress of a blog or spend a long time thinking about a tweet; thus, affordances are not static; they represent the 'most likely action(s) of many' that an entity can be used for (Bergh 2015).

Foremost among the affordances of relevance to influence operations is the instantaneous and non-geographical nature of the Internet, and by extension, social media. Its potential for free, immediate, worldwide dissemination of content from influence operations is unique. This lack of geographical boundaries is further augmented by the lack of any realistic oversight and control by national authorities. Internet services, such as YouTube, have generally focused on removing intermediaries to lower costs and to provide individuals or small groups with opportunities previously in the domain of large or national entities, for instance video distribution. Furthermore, efforts by social media services to manually moderate content tend to use centrally located staff (Fisher 2018; Hopkins 2017). Thus, posts are examined by people who often are in a different physical location with dissimilar tacit knowledge, who lack language skills (Safi 2018), and who have different cultural understandings than the intended audience. This all makes moderation difficult, resulting in fewer barriers for the influence operation.

This reach is further augmented with the affordances for sharing built into social media. These can be manual, such as users retweeting Twitter messages or linking to a news story. They may also be automated. Algorithms are an important dimension of social media affordances. Most news and social media sites rely on these algorithms to automatically select content deemed relevant/desirable by the person (Bucher 2012; Dias 2014). These can be manipulated to create the impression that a story is important, that it is accepted by many users (and so on) to target particular audiences for adverts, fake news stories, shocking images, etc. (Giesea 2015; Levin 2017; McKay 2017). So-called 'bots' are also important here. This is software that controls social media profiles and automatically performs certain actions, such as generating fake engagement data by retweeting messages to boost their visibility in trending topics (Stella, Ferrara & De Domenico 2018; Arnaudo 2017; Mezzofiore 2018). It is also possible to pay commercial services to inflate social media statistics such as the number of clicks or followers, often done through poorly paid staff in low income countries (Deahl 2017; Reinstein 2018; Cresci *et al.* 2015; Fredheim 2019).

Another important affordance is the fuzziness of 1) sender identity and 2) the context of the content. The ability to anonymise who is behind an influence operation from the target audience makes it difficult for users and moderators to simply block a user to avoid fake news, for instance. More importantly, pseudonymity (Tsikerdekis 2012) allows those posting content to claim expertise/knowledge that they do not possess on certain topics, or, by using multiple falsified online identities, they can make supporting statements to enhance the believability of information presented. Regarding content, the lack of context in social media means that content posted by other users can be reframed. This can be done through outright dishonesty, subtle sarcasm, or by not referencing the real-world context to make it seem as if this content supports the influence operator's goals.

The media formats—such as short text, video, image, and mixed content—that the social media service uses provide various affordances. For example, the rise of visual information means that the attacking side can sidestep the need for language skills and can create content that appeals directly to emotions and thus bypass any cognitive work/analysis (see, for example, Joffe 2008; Richardson & Wodak 2009; Seo 2014), such as images of children dying (Jolicoeur & Seaboyer 2014). The content format may also affect the ability to detect influence operations. Smaller actors with less IT resources who are trying to defend against influence operations may struggle to analyse a large number of videos that require both audio/language and image processing in real time, whereas plain text analysis is much less resource intensive.

Beyond social media affordances but supported by these affordances is the notion of viral content, a phenomenon that greatly enhances delivery. 'Viral content', a term first used in 1996 in connection with marketing, is 'word of mouth' (people sharing with friends) + 'exponential growth' (social media facilitating faster/wider distribution) (Kaplan & Haenlein 2011).

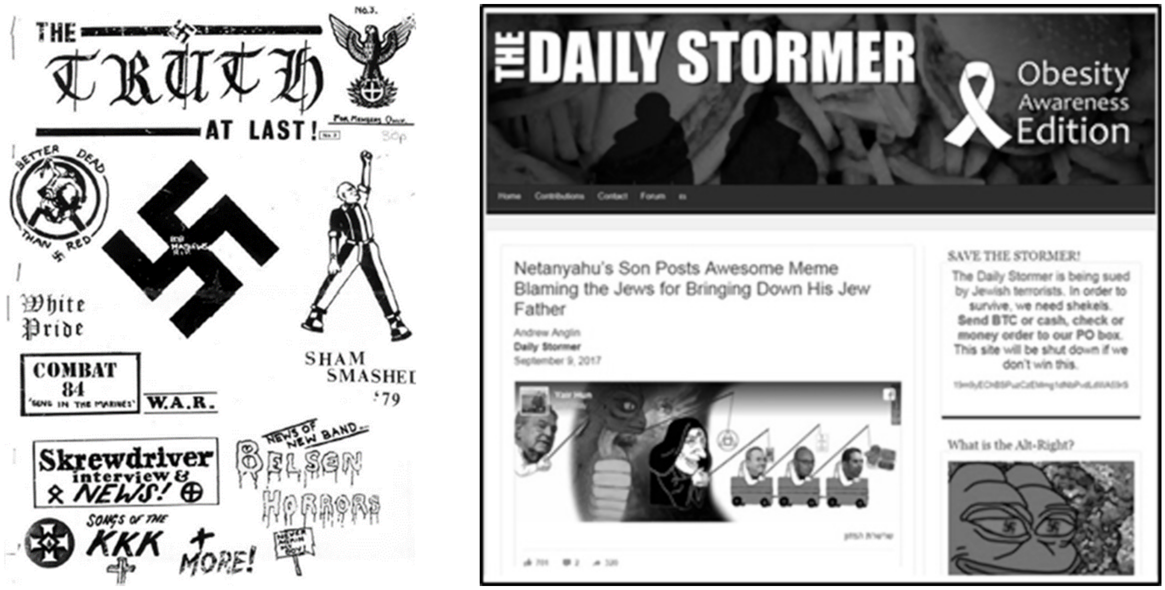
The key here is the exponential growth. Viral exposure, and any effects from it, are free to the content creator through a combination of social media infrastructure (storage, sharing mechanisms, for example) and the free labour that social media users engage in (Terranova 2000). Virality is thus highly desirable for the type of influence operations discussed here. There is also a qualitative dimension to this. As virality is a digital form of word of mouth, those exposed to the viral message may trust the content more, as it was shared by someone they know.

Virality can be encouraged through targeting, perception of importance, and content. Targeting to achieve virality is rudimentary; one wants large audiences, not small pinpointed ones. Examples have been found of targeting based on geographical location or membership of online groups (Keating, Schaul & Shapiro 2017). The content from influence operations that has been found in social media recently is usually aimed at sowing distrust, often appealing to existing conflicts in the society targeted (Brooks 2017; Morgan 2017; Shapiro 2017). The manipulation of algorithms and use of bots or low paid manual workers to make content seem important or popular was discussed above; these strategies are also used to boost the chances of virality.

Finally, emotional reactions to content can be manipulated to encourage virality. Research suggest that "emotionally charged Twitter messages tend to be retweeted more often and more quickly compared to neutral ones" (Stieglitz & Dang-Xuan 2013, p.217), findings supported by research that shows how users expressing moral emotion around topics like abortion rights are more likely to share content that they deem morally important (Brady *et al.* 2017). A review of research on sharing and emotions also supported this idea, suggesting that sharing information can also be about sharing emotions (Dafonte-Gómez 2018, p. 2142). In terms of influence operations, in an Italian sample, consumers of fake news were found to have more online interactions with the posts they read (Bessi *et al.* 2014). The fact that users often pass on information without reading it themselves also aids virality. One study estimated that some 59% of links are shared without the user sharing it having read the linked page him or herself (Gabielkov *et al.* 2016).

Exploitation: Fighting for Attention

In this paper's take on the cyber kill chain, exploitation is aimed at people and not applications or systems. Whereas the delivery phase is concerned with getting the message into users' social media streams, the core aim of the exploitation phase is to facilitate a move from a screen to the social media users' mind. The first step here is that the message must not be rejected outright. The fact that one social media flattens all content to have the same look and feel, so news items from a reputable news organisation are indistinguishable from postings from a fake news operation, is an important affordance for influence operations in this regard. Additionally, there is little cost involved in creating a well-designed website, or even in cloning an existing website to make falsified information seem legitimate (Ruddick 2017). This contrasts with pre-Internet communications as exemplified in the images in **Figure 3**. Thus, the platforms remove cues that could help readers differentiate between the validity of sources.



Netanyahu's Son Posts Awesome Meme Blaming the Jews for Bringing Down His Jew Father

Andrew Anglin
Daily Stormer
September 9, 2017

The Daily Stormer is being sued by Jewish terrorists. In order to survive, we need shekels. **Send BTC or cash, check or money order to our PO box.** This site will be shut down if we don't win this.

Figure 3: Photocopied 1970s neo-Nazi pamphlet (Worley & Copsey 2016) and current neo-Nazi website

When the danger of outright rejection is avoided, it is important to gain the attention of social media users. The attention economy theory is useful in this discussion; it is in part based on insights by Herbert Simon a quarter of a century before social media emerged. Discussing organisations and the increase in available information, he stated that "What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention" (Simon 1971, pp. 40-41). The need to compete for attention, as a scarce resource (Goldhaber 2006), is not only driven by the vast amount of information generated online. It is also a result of the underlying business model of most social media, namely advertising. What social media services are selling is their users' attention, or as the adage goes: "If you are not paying for it, you're not the customer; you're the product being sold" (Andrew Lewis qtd. in <<garson>> [username] 2017). Many of the social media affordances discussed above are there with the aim of getting more users' attention through engagement tactics, such as 'Like' buttons or tools for easily sharing content.

The strategies that have been used in recent influence operations are based on the same approaches that advertisers and newspapers have deployed for some time. Goldhaber, who developed the idea of the attention economy, suggested that "this new economy is based on endless originality, or at least attempts at originality" (Goldhaber 1997). What can be seen is not exactly originality; rather it is a continuous increase in exaggerations and hyperbole in language and imagery used to elicit emotional reactions to grab someone's attention. So-called clickbait tactics are used by news websites to get more readers for a regular story (Tangen 2017) perhaps by using an exaggerated headline leading to a more mundane story. Another tactic is used by 'content farms' where stories are created in response to market opportunities —what do Facebook users discuss (Dewey 2015), what search terms are popular, or what are expensive advertising keywords (Napoli 2014). Such tactics are copied and made more extreme by, for example, outfits that make money from fake news stories (Tynan 2016; Kirby 2016; Bergsaker, Karlsen & Bakken 2018).

Another approach is to gain the attention of gatekeepers and content curators, that is well-known social media users, whether celebrities, so-called influencers, or others who have many followers. As mass media makes way for social media, these users act as filters for their followers by selecting what news receives attention. As a researcher on social movements online explained: "[the] fracturing of publics, somewhat ironically, increases the importance of 'focusers' of attention, which can be institutions (media outlets), individual mediators of attention […] journalist-curators […], celebrities" (Tufekci 2013, p. 851).

Installation: Adding to Information Sediments

Before discussing how an influence operation can install its payload, the next step in the cyber kill chain, there is a need to conceptualise online content to account for its constant flow and accumulation of information. There are many metaphors used to describe and discuss Internet related phenomenon, arising from people's need to reify the abstractness of the Internet in everyday life (Jamet 2010; Tomaszewski 2002). This may be marketing terms like 'the cloud' for online services or the somewhat forced description 'the information superhighway' from the 1990s. Such metaphors are not merely a matter of making it easier to understand how the vast, interconnected set of technologies, protocols, and content link together. Markham has pointed out that "our discursive choices in talking about Internet and Communication technologies have actual and meaningful consequences on the shape and perception of these technologies" (Markham 2003, p.1).

On social media, nothing disappears; it merely fades from view. Social media services may delete content that breaches internal guidelines, or that authorities demand be deleted, but the default is to keep everything available. For example, on Flickr, one can still see the first ever image uploaded in 2003 (https://www.flickr.com/photos/caterina/88). From the perspective of influence operations, this is a key issue in terms of executing or defending against influence operations. The use of algorithms by social media services to find relevant material for users and the ease with which existing content is accessed instantly and world-wide can be manipulated to bolster influence operations.

Given this environment, this paper suggests that the content of social media is best thought of as 'online information sediments'. In the world of big data, the term 'data lakes' is used to describe raw, unstructured data in large quantities, emphasizing the vastness of the data (Walker & Alrehamy 2015). If one imagines the social media infrastructure as an always-flowing 'river' that carries 'particles' of content that eventually arrive in a vast delta where they are stored, layer upon layer as they age, then using the metaphor of 'sediments' provides several perspectives to better understand, and act upon, influence operations in social media.

> 1) It emphasises the long term, cumulative workings of social media. The incessant accumulation and aggregation of information with easy access is a differentiator between social and traditional media.
> 2) The metaphor highlights the fact that, despite information never disappearing, it will quickly fade from view. Recent posts, stories, and narratives in the top layer will soon be covered by new layers.
> 3) Furthermore, how narratives emerge in social media can both affect and are affected by existing information. Many new posts that twist existing information in a particular

way may change an established narrative. However, previous social media posts provide a frame that can influence how new posts are perceived.

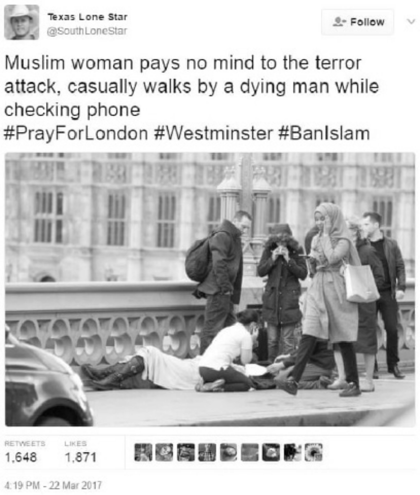
4) Finally, influence operations do not start from scratch; they connect with existing posts that may already have influenced those reading the new posts. For example, research on online hate-speech suggests that "despite the relatively short 'half-life' of antagonistic content towards Jews, once this temporary increase in online hate speech receded it left behind a new, higher baseline of online hate" (Williams & Burnap 2018, p. 6).

Thus, the installation step in the present kill chain concerns itself with how the content that has been delivered blends in with the general social media information flow and, through this flow, becomes part of the online information sediment. From here, it can have long term effects. For example, it may be used to make influence operations more believable by referencing existing material to make it seem like a mainstream opinion. Furthermore, algorithms that work on content selection will also be trained on content from the information sediment, which will help skew it so that content relevant to an influence operation may be selected.

Command and Control: Influencing Meaning Making

Unlike hacking attacks that target hardware or software, the command and control phase in the influence operation kill chain cannot execute commands that the subjects it seeks to manipulate will automatically follow. Instead it must enter into the social media users' cognitive processes (Sartonen, Huhtinen & Lehto 2016). This is a person's own 'command and control' process; this paper suggests that this would be individuals' and groups' meaning-making processes. The term 'meaning making' is from social science (Krauss 2005) and highlights the fact that different actors' reactions to information is neither pre-determined nor predictable. Individuals and groups will generally seek to interpret information so it fits into their world view. This is the key link in the model that this paper develops: people may perform actions beneficial to the entity behind an influence operation, but only when the information from the campaign is incorporated into and supporting their understanding of the world. An influence operation that achieves some measure of success does not attempt to challenge someone's world view head on. The approaches that have been found in the influence operations discussed here are generally about making existing convictions stronger or sowing some doubts about common, existing discourses (Morgan 2017; Richter 2017). Neither does the shift need to be permanent. A short, even a few seconds, response can be enough to fulfil the objectives of the influence operation.

An example of such content was found in an account controlled by Russian operatives. It was posted in the aftermath of a terrorist attack in London in 2017 (see **Figure 4**, below). This post attempts to amplify existing divisions between the majority population and the minority Muslim population. This is done by reframing a photo and claiming it shows a Muslim woman ignoring a terrorist victim, whereas other photos from the same series show this is not the case (Evon & Mikkelson 2017).



Texas Lone Star
@SouthLoneStar

Muslim woman pays no mind to the terror attack, casually walks by a dying man while checking phone
#PrayForLondon #Westminster #BanIslam

RETWEETS 1,648
LIKES 1,871

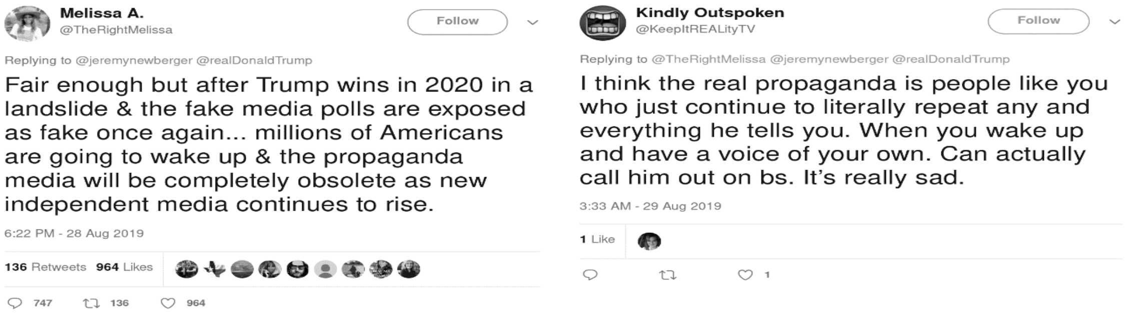
4:19 PM - 22 Mar 2017

Figure 4: Tweet from Russian account after London terror attack (Hern 2017)

When information such as this gets the attention of a social media user, he or she becomes part of that person's meaning-making processes, the practices people engage in when trying to make sense of the world. Such meaning making is often a collective creation, where categorisation helps people make sense of the world (Dobbin 2009), to "produce identification, commonality, connectedness and groupness" (in other words, different forms of 'togetherness') in social media (Leppänen *et al.* 2013, p.1).

There are numerous mechanisms involved in meaning making; two that are particularly helpful to influence operations in social media are filtering and categorisation. The filtering of information is a form of confirmation bias; new information is incorporated into meaning making when it confirms existing beliefs. Filtering is often linked to the algorithmic selection of information (Dias 2014; Treré 2016). This is the automated display of content that social media services deem relevant based on, for instance, posts or news items that the user has written or looked at before. Such filtering often leads to echo chambers where everyone is in agreement (Krasodomski-Jones 2017; Williams *et al.* 2015). However, a study on how users react to news that does not match their ideological background found that "compared with algorithmic ranking, individuals' choices played a stronger role in limiting exposure to cross-cutting content" (Bakshy*,* Messing & Adamic 2015, p.1130). Filtering in social media is therefore an interplay between personal and algorithmic selections.

Categorisation of individuals or groups is a key element of meaning making. There is considerable research on the concept of in- and out-groups, the dividing up of people into those who are like one's self and those who are not (Barth 1969; Allport 1954; Bergh 2010). Often the in-group will discriminate against, or make negative judgements about, the out-group and its members through stereotyping (Alexander, Brewer & Hermann 1999; Alexander 2005; Macrae, Milne & Bodenhausen 1994). Online, these tendencies are exaggerated since it is much easier to form an in-group (that also becomes an echo-chamber) given the worldwide and instant reach to others like one'self without the need to invest a lot of time and, in great measures, helped by algorithms and social media affordances. These born online in-groups can be *ad-hoc*, for instance people who self-identify with certain viewpoints in a Twitter conversation as seen in the two opposing tweets in **Figure 5**, below. Or it can be long lasting and formal, such as the membership of a closed Facebook group.



Melissa A.
@TheRightMelissa

Follow

Replying to @jeremynewberger @realDonaldTrump

Fair enough but after Trump wins in 2020 in a landslide & the fake media polls are exposed as fake once again... millions of Americans are going to wake up & the propaganda media will be completely obsolete as new independent media continues to rise.

6:22 PM - 28 Aug 2019

136 Retweets 964 Likes

747 136 964

Kindly Outspoken
@KeepItREALityTV

Follow

Replying to @TheRightMelissa @jeremynewberger @realDonaldTrump

I think the real propaganda is people like you who just continue to literally repeat any and everything he tells you. When you wake up and have a voice of your own. Can actually call him out on bs. It's really sad.

3:33 AM - 29 Aug 2019

1 Like

1

Figure 5: *Two responses to a Trump tweet, each accusing 'the out-group' of propaganda*

For information to enter someone's meaning making processes, the information must be believable. Research examining how people accept content suggests that the number of times something is shared plays an important role (Kim 2018; Lee & Oh 2017; Morris *et al.* 2012; Oh, Agrawal & Rao 2013) as does information that claims some form of evidence and has the appearance of being objective (Paul & Matthews 2016). Repetition of information, even when fake or implausible (Paul & Matthews 2016; Pennycook, Cannon & Rand 2018) also makes users see it as true more frequently when encountering the repeated information. These findings also highlight the importance that online information sediments play in influence operations. The more supporting information a user can find in the aggregated and accumulated content of social media, the more believable, popular, or important a narrative may seem. This means that the techniques used in influence operations to increase the reach of content that is created, as discussed in the section on 'Delivery: Using the Affordances of Social Media', also play an important role in making the messages acceptable.

To conclude, directly controlling a target population through influence operations in social media is not possible. Any effects would be indirect; information from an operation receives attention from an individual or a group and may influence meaning making if the information is believed and deemed important or useful. However, even if a social media user's opinion is changed or strengthened, actors behind an influence operation only gain when someone swayed by online content engages in activities of benefit to the actor. This step will be explored next.

Actions on Objectives: Causing Alternate Actions

Whereas a hacking attack at this stage may seek to obtain or destroy data, an influence operation would want to see a change in actions undertaken by the targeted population, or by people influenced by the target population. Sartonen, Huhtinen and Lehto (2016) have suggested that a person's cognition is the ultimate target of influence operations. The present model separates meaning making and acting upon views that emerge from meaning making into two phases. A particular attitude does not necessarily result in predictable behaviour (Tatham 2015), and changing someone's views is not itself useful to an attacker. The final phase in the kill chain, and the goal of the attacker, is to cause alternate actions to occur.

In terms of the attention economy discussed above, it has been suggested that turning attention into actions may be a goal of attention seeking and that this "comes with the territory. That is part of the power that goes with having attention" (Goldhaber 1997). However, is this possible through influence operations in social media?

The first question would be whether people initiate actions based on information distributed through social media? The answer here is a clear yes. Examples include the killing of 25 people in mob attacks in India in response to fake news about child abductions spread through WhatsApp (Allana 2017; Biswas 2018). This problem caused WhatsApp to restrict sharing (as opposed to writing new) messages (Cellan-Jones 2019), a move that highlights how social media specific affordances such as easy sharing of information plays a role in users' behaviour. Another example can be found in the communal riots that broke out in Sri Lanka after incitements to violence were spread via Facebook posts (Safi & Perera 2018).

These examples show that influencing people to perform actions through attention given to (untrue) information spread online is, in principle, possible. To believe otherwise would be to fall for the fallacy that participation in the digital space is somehow separated from every day, offline life, what has been termed "digital dualism" (Jurgenson 2011). The interlinking between social media and real life is clearly evidenced in the so-called 'self-radicalisation' process that has occurred in recent times and has resulted in terror-related activities (Kardaş & Özdemir 2018; Picart 2015).

There is debate about whether it is possible to persuade someone to change his or her mind through social media; these debates are often related to elections and politics (see, for example, Guess, Nyhan & Reifler 2018; Broockman & Green 2014; Kalla & Broockman 2018; Kaplan, Gimbel & Harris 2016). This paper would argue that this debate is missing the point; known social media influence operations have tended to focus on enhancing existing beliefs or divisions among target audiences, not trying to change people's attitudes or opinions. This is not very different from many political campaigns; an 'us and them' discourse is aimed at getting voters to turn up and vote in an election, and at the same time trying to discourage supporters of other parties from voting.

In sum, when the goal of influence operations is triggering alternate actions, 'alternate' does not imply actions that are counter to what the person believes in. Rather, the alternate acts refer to actions that would not be done without the influence operation's nudging through adverts, viral messages, videos, and so on. Furthermore, alternate action and alternate inaction (from different audiences) can both be of benefit to those running an influence operation. For example, in a conflict over a geographical space, the attacking side could create fake news, falsify Wikipedia entries, generate deep fake images of archaeological artefacts that 'show' the attacking side has a historical claim to that space. An influence operation through social media based on this narrative could encourage citizens of one's own country to join the conflict (action) while making the citizens of the country being attacked less supportive of going to war to reclaim the land (inaction).

Conclusion

This article has examined the phases of the so-called cyber kill chain to explore if and how they may be applied to influence operations in social media. Using the depiction of the original kill chain in **Figure 1** as the starting point and amending it for the purposes of this paper, the model in **Figure 6** emerges.

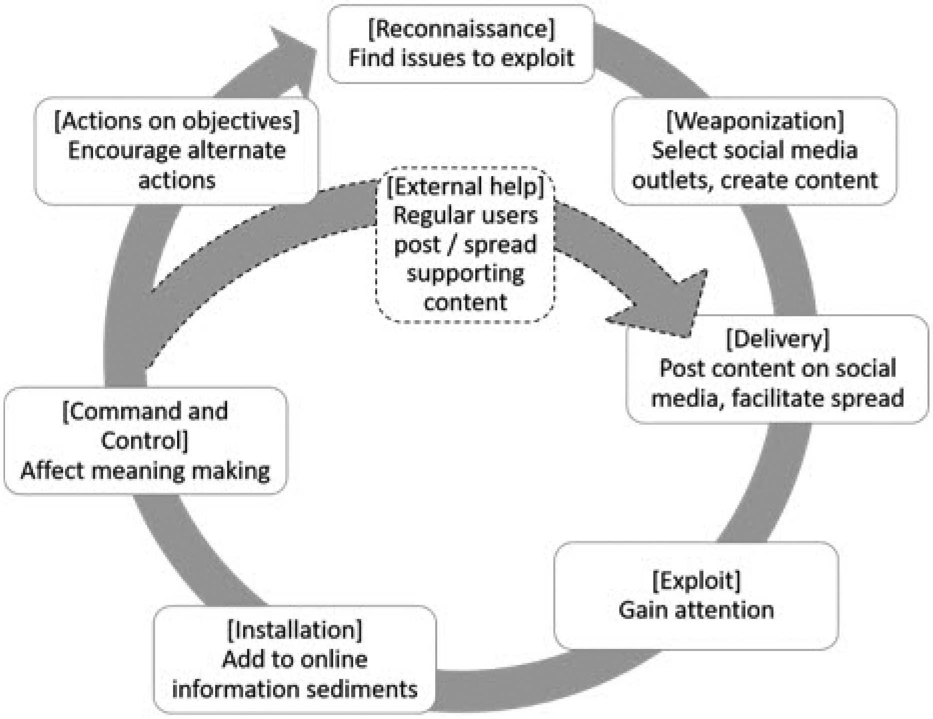

[Reconnaissance]
Find issues to exploit
[Weaponization]
Select social media outlets, create content
[Delivery]
Post content on social media, facilitate spread
[Exploit]
Gain attention
[Installation]
Add to online information sediments
[Command and Control]
Affect meaning making
[Actions on objectives]
Encourage alternate actions
[External help]
Regular users post / spread supporting content

Figure 6: Updated kill chain for social media influence operations. This shows how content from influence operations becomes part of general online content, thus creating a circular effect beyond the influence operation.

An important difference from the original cyber chain in **Figure 1** is the circular nature of influence operations in social media. This is caused by the triggering of external involvement, such as sharing, commenting on, and creating new content, in response to original content from influence operation operators. This can in turn create more external involvement. The first two steps in the kill chain are not relevant to such third-party involvement; users typically engage with topics that interest them, through the social media arenas they already are a part of. The visualization in **Figure 6** integrates and illustrates these issues.

What benefits can this model provide? It seems clear that using a socio-technical perspective and introducing the concept of online information sediments to describe social media's approach to data, furnish this kill-chain-based model with explanatory and analytical potential. The key contributions of this conceptualisation are that one can clearly perceive that a) such attacks rely on social media affordances; b) the notion of information sediments show that influence operations are a long-term issue due to aggregation and algorithms that also support narratives through selection of similar content; c) the attention grabbing techniques are not a means in themselves, but a way to surreptitiously enter the meaning-making processes of individuals and groups; and finally d) these attacks seek to encourage alternate actions where a conversion of people's opinions or beliefs is not required; spurring a short term (in)action may be enough. These points can help analysts and others concerned with information warfare generally, and influence operations in particular, to structure information environment assessment efforts, and to provide pointers to how effects of such operations can be mitigated.

Thus, the kill chain in this article provides a ‘cognitive mental model’ for those who need to, in some capacity, deal with social media influence operations—in the same way that the original cyber kill chain did for cyber security experts (Khan, Siddiqui & Ferens 2018). However, Lockheed Martin’s original cyber kill chain was developed to help stop cyberattacks and was perhaps too narrowly focused on perimeter protection (Hospelhorn 2016; Engel 2014). In social media, there are no perimeters; its openness is its defining characteristic. To put a complete stop to a campaign is thus impossible. However, each step in the model developed here has affordances that may aid certain actions to reduce the impact of influence operations—a natural next step to extend this initial work on a kill chain for influence operations in social media.

The model developed here needs to be verified through further research. This could be achieved through distinct investigations of the different steps that apply quantitative or qualitative approaches. For instance, if one were to examine the usefulness of the information sediments in an influence operation, then a quantitative study of how many posts referred to existing online information could be a useful method. On the other hand, to learn more about how attention is manipulated, in-depth interviews with social media users could provide valuable insights.

References

Akbari, H & Land, F 2016, *Socio-technical theory – IS theory*, *Theories used in IS Research Wiki*, viewed 16 January 2018, < https://is.theorizeit.org/wiki/Socio-technical_theory>.

Alexander, MG 2005, ‘Putting stereotype content in context: Image theory and interethnic stereotypes’, *Personality and Social Psychology Bulletin*, vol. 31, no. 6, pp. 781-94.

Alexander, MG, Brewer, MB & Hermann, RK 1999, ‘Images and affect: A functional analysis of out-group stereotypes.’, *Journal of Personality and Social Psychology*, vol. 77, pp. 78-93.

Allana, A 2017, *WhatsApp, Crowds and Power in India, New York Times*, viewed 26 June 2017, <https://www.nytimes.com/2017/06/21/opinion/whatsapp-crowds-and-power-in-india.html>.

Allport, GW 1954, *The nature of prejudice*, Addison-Wesley Publishing Company, Cambridge, MA, US.

Arnaudo, D 2017, *Computational propaganda in Brazil: Social bots during elections*, *Working paper no. 2017.8*, Project on Computational Propaganda, Oxford Internet Institute, Oxford, UK, viewed 20 June 2020, <https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf>.

Bakshy, E, Messing, S & Adamic, LA 2015, ‘Exposure to ideologically diverse news and opinion on Facebook’, *Science*, vol. 348, no. 6239, pp. 1130-2.

Barth, F 1969, *Ethnic groups and boundaries: The social organization of cultural difference*, *Universitetsforlaget*, Bergen, NO.

Bergh, A 2010, ‘I’d like to teach the world to sing: Music and conflict transformation’, PhD thesis, University of Exeter, Exeter, UK.

——2015, ‘Seeing is believing; Hearing is understanding: Building real trust through virtual tools’, *ICCRTS*, *Proceedings of the 20th International Command and Control Research and Tech-*

nology Symposium, ICCRTS 2015, CCRP, Annapolis, US, viewed 1 August 2016, <http://www.dodccrp-test.org/s/071.pdf>.

——2018, 'Rebel with a temporary cause: The asymmetrical access to distrust, hipness and intensity as resources in cyber-conflicts', viewed on 5 January 2020, <https://isaconf.confex.com/isaconf/wc2018/webprogram/Paper104220.html>.

——2019, *Social network centric warfare: Understanding influence operations in social media*, FFI, Kjeller, NO.

Bergsaker, T & Karlsen, ML & Bakken, J 2018, *Smirnoff-is, flaggbot og hai i Stavanger – løgnfabrikker laget Norges mest delte saker i mai*, *Faktisk*, viewed on 24 February 2019, <https://www.faktisk.no/artikler/bA/lognfabrikker-laget-norges-mest-delte-saker-i-mai>.

Bessi, A, Scala, A, Rossi, L, Zhang, Q & Quattrociocchi, W 2014, 'The economy of attention in the age of (mis)information', *Journal of Trust Management*, vol. 1, p. 12.

Bialy, B 2017, *New trends in social media*, NATO Strategic Communications Centre of Excellence.

Biswas, S 2018, 'Fighting India's WhatsApp fake news war', viewed 8 February 2019, <https://www.bbc.com/news/world-asia-india-45140158>.

Brady, WJ, Wills, JA, Jost, JT, Tucker, JA & Bavel, JJV 2017, 'Emotion shapes the diffusion of moralized content in social networks', *Proceedings of the National Academy of Sciences*, vol. 114, no. 28, pp. 7313–8.

Broockman, DE & Green, DP 2014, 'Do online advertisements increase political candidates' name recognition or favorability? Evidence from randomized field experiments', *Political Behavior*, vol. 36, no. 2, pp. 263-89.

Brooks, RC 2017, *How Russians attempted to use Instagram to influence Native Americans*, *BuzzFeed News*, viewed 7 March 2018, <https://www.buzzfeed.com/ryancbrooks/russian-troll-efforts-extended-to-standing-rock>.

Bucher, T 2012, 'Want to be on the top? Algorithmic power and the threat of invisibility on Facebook', *New media & society*, vol. 14, no. 7, pp. 1164–80.

Cellan-Jones, R 2019, 'WhatsApp restricts message-sharing', viewed 25 January 2019, <https://www.bbc.com/news/technology-46945642>.

Chen, A 2015, 'The agency', *The New York Times*, viewed 21 March 2016, <http://www.nytimes.com/2015/06/07/magazine/the-agency.html>.

Cresci, S, Di Pietro, R, Petrocchi, M, Spognardi, A & Tesconi, M 2015, 'Fame for sale: Efficient detection of fake Twitter followers', *Decision Support Systems*, vol. 80, pp. 56-71.

Croom, C 2010, 'The Cyber Kill Chain: A foundation for a new cyber security strategy', *High Frontier*, vol. 6, no. 4, pp. 52-6.

Dafonte-Gómez, A 2018, 'Audiences as medium: Motivations and emotions in news sharing', *International Journal of Communication*, vol. 12, p. 20.

Deahl, D 2017, *Three men in Thailand reportedly ran a clickfarm with over 300,000 SIM cards and 400 iPhones*, *The Verge*, viewed 26 June 2017, <https://www.theverge.com /2017/6/12/15786402/thai-clickfarm-bust-iphones>.

Dewey, C 2015, 'The fastest-growing 'news' site of 2015 was an obscure content farm for moms', *Washington Post*, viewed 4 February 2019, <https://www.washingtonpost. com/news/the-intersect/wp/2015/07/16/how-moms-won-the-internet-and-what-that-means-for-the-rest-of-us/>.

Dias, P 2014, 'From "infoxication" to "infosaturation": A theoretical overview of the cognitive and social effects of digital immersion', *Ámbitos. Revista Internacional de Comunicación, n. 24, año 2014, primer trimestre (primavera)*.

Dobbin, F 2009, *How Durkheim's Theory of Meaning-Making influenced organizational sociology*, Oxford University Press, Oxford, UK, viewed 6 February 2019, <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199535231.001.0001/oxfordhb-9780199535231-e-009>.

Dougherty, J 2014, *Everyone lies: The Ukraine conflict and Russia's media transformation,* Discussion paper series #D-88, July 2014, Shorenstein Center on Media, Politics and Public Policy, John F. Kennedy School of Government, Harvard University, Cambridge, MA, US, viewed 17 June 2020, <http://shorensteincenter.org/everyone-lies-ukraine-conflict-russias-media-transformation/>.

Engel, G 2014, *Deconstructing the Cyber Kill Chain*, *dark reading*, viewed 4 April 2019, <https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542>.

Evon, D & Mikkelson, D 2017, *Muslim woman ignores dying victim of London terror attack?*, *Snopes.com*, viewed 6 February 2019, <https://www.snopes.com/news/ 2017/03/24/muslim-woman-london-attack/>.

Fisher, A 2015, 'Swarmcast: How *jihadist* networks maintain a persistent online presence', *Perspectives on Terrorism*, vol. 9, no. 3, p. 18.

Fisher, M 2018, 'Inside Facebook's secret rulebook for global political speech', *The New York Times*, viewed 28 January 2019, <https://www.nytimes.com/2018/12/27/world /facebook-moderators.html>.

Fredheim, R 2019, *Robotrolling 2019/2*, NATO Strategic Communications, Centre of Excellence, Riga, LV.

Gabielkov, M, Ramachandran, A, Chaintreau, A & Legout, A 2016, 'Social clicks: What and who gets read on Twitter?', ACM SIGMETRICS / IFIP Performance 2016, viewed 4 February 2019, <https://hal.inria.fr/hal-01281190/document>.

<<garson>> (username) 2017, 'You're not the customer; You're the product', *Quote Investigator*, viewed 3 February 2019, <https://quoteinvestigator.com/2017/07/16/product/>.

Geers, K 2015, *Cyber war in perspective: Russian aggression against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Gibson, JJ 1977, 'The theory of affordances', eds. R Shaw & J Bransford, *Perceiving, acting, and knowing*, Lawrence Erlbaum Associates, Hillsdale, NJ, US.

Giesea, J 2015, 'It's time to embrace memetic warfare', *Defence Strategic Communications*, vol. 1, no. 1.

Giles, K 2015, 'Russia's hybrid warfare: A success in propaganda', *Bundesakademie für Sicherheitspolitik,* Working paper, no. 1, p. 2015.

Goldhaber, MH 1997, 'The attention economy and the net', *First Monday*, vol. 2, no. 4.

——2006, 'The value of openness in an attention economy', *First Monday*, vol. 11, no. 6.

Gottfried, J & Shearer, E 2016, 'News use across social media platforms 2016', *Pew Research Center's Journalism Project*, viewed 18 May 2017, <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>.

Guess, A, Nyhan, B & Reifler, J 2018, 'Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign', *European Research Council*.

Hammond-Errey, M 2019, 'Understanding and assessing information influence and foreign interference', *Journal of Information Warfare*, vol. 18, no. 1, pp. 1-22.

Hern, A 2017, 'How a Russian "troll soldier" stirred anger after the Westminster attack', *The Guardian*, viewed 28 March 2019, <https://www.theguardian.com/uk-news/2017/nov/14/ how-a-russian-troll-soldier-stirred-anger-after-the-westminster-attack>.

Hopkins, N 2017, 'Revealed: Facebook's internal rulebook on sex, terrorism and violence', *The Guardian*, viewed 22 May 2017, <https://www.theguardian.com/news/2017/may/21/ revealed-facebook-internal-rulebook-sex-terrorism-violence>.

Hospelhorn, S 2016, *What is the Cyber Kill Chain and how to use it effectively,* viewed 13 September 2019, <https://www.varonis.com/blog/cyber-kill-chain/>.

Howard, PN, Ganesh, B, Liotsiou, D, Kelly, J & François, C 2018, *The IRA, social media and political polarization in the United States, 2012-2018*, Oxford Internet Institute, Oxford, UK.

Hutchins, EM, Cloppert, MJ & Amin, RM 2011, 'Intelligence-Driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains', *Leading Issues in Information Warfare and Security Research*, vol. 1, no. 1, p. 80.

Iasiello, EJ 2017, 'Russia's improved information operations: From Georgia to Crimea', *Parameters*, vol. 47, no. 2.

Inglis, C 2016, 'Cyberspace: Making some sense of it all', *Journal of Information Warfare*, vol. 15, no. 2, pp. 17-26.

Jamet, DL 2010, ‘What do Internet metaphors reveal about the perception of the Internet?’, Metaphorik, no. 18, pp. 7-32, viewed 20 June 2020, <https://www.metaphorik.de/sites/www.metaphorik.de/files/journal-pdf/18_2010_jamet.pdf>.

Joffe, H 2008, ‘The power of visual material: Persuasion, emotion and identification’, *Diogenes*, vol. 55, no. 1, pp. 84-93.

Jolicoeur, P & Seaboyer, A 2014, *140 character defence and security in the cyber age: The case of the IDF-Hamas Twitter war*, Defence Research & Defence Canada, Toronto Research Centre, Toronto, CA, viewed 4 April 2019, <https://www.researchgate.net/publication/263769060_140_Character_Defence_and_Security_in_the_Cyber_Age_The_Case_of_the_IDF-Hamas_Twitter_War>.

Jurgenson, N 2011, ‘Digital dualism versus augmented reality’, *The Society Pages, Cyborgology*, 24 February, viewed 20 June 2020, <https://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/>.

Kalla, JL & Broockman, DE 2018, ‘The minimal persuasive effects of campaign contact in general elections: Evidence from 49 field experiments’, *American Political Science Review*, vol. 112, no. 1, pp. 148-66.

Kaplan, AM & Haenlein, M 2011, ‘Two hearts in three-quarter time: How to waltz the social media/viral marketing dance’, *Business Horizons*, vol. 54, no. 3, pp. 253-63.

Kaplan, JT, Gimbel, SI & Harris, S 2016, ‘Neural correlates of maintaining one’s political beliefs in the face of counterevidence’, *Scientific Reports*, vol. 6, 39589.

Kardaş, T & Özdemir, ÖB 2018, ‘The making of European foreign fighters: Identity, social media and virtual radicalization’, eds. M Yeşiltaş & T Kardaş, *Non-State armed actors in the Middle East*, Springer International Publishing, Cham, CH, pp. 213-35, viewed 12 September 2019, <http://link.springer.com/10.1007/978-3-319-55287-3_10>.

Keating, D, Schaul, K & Shapiro, L 2017, ‘The Facebook ads Russians targeted at different groups’, *Washington Post*, viewed 5 February 2019, <https://www.washingtonpost.com/ graphics/2017/business/russian-ads-facebook-targeting/>.

Khan, MS, Siddiqui, S & Ferens, K 2018, ‘A cognitive and concurrent Cyber Kill Chain model’, *Computer and Network Security Essentials*, ed. K Daimi, Springer International Publishing, Cham, CH, pp. 585-602, viewed 4 April 2019, <https://doi.org/10.1007/978-3-319-58424-9_34>.

Kim, JW 2018, ‘Rumor has it: The effects of virality metrics on rumor believability and transmission on Twitter’, *New Media & Society*, vol. 20, no. 12, pp. 4807–25, <https://doi.org/10.1177/1461444818784945p. 1461444818784945>.

Kirby, EJ 2016, ‘The city getting rich from fake news’, *BBC News*, viewed 31 July 2018, <https://www.bbc.co.uk/news/magazine-38168281>.

Krasodomski-Jones, A 2017, *Talking to ourselves: Political debate online and the echo chamber effect*, viewed 4 February 2019, <https://demosuk.wpengine.com/wp-content/uploads/2017/02/Echo-Chambers-final-version.pdf>.

Krauss, SE 2005, ‘Research paradigms and meaning making: A primer’, *The Qualitative Report*, vol. 10, no. 4, pp. 758-70.

Larson, EV, Darilek, RE, Gibran, D, Nichiporuk, B, Richardson, A, Schwartz, LH & Thurston, CQ 2009, *Foundations of effective influence operations: A framework for enhancing army capabilities*, Rand Arroyo Center, Santa Monica, CA, US.

Lee, H & Oh, HJ 2017, ‘Normative mechanism of rumor dissemination on Twitter’, *Cyberpsychology, Behavior, and Social Networking*, vol. 20, no. 3, pp. 164-71.

Leppänen, S, Kytölä, S, Jousmäki, H, Peuronen, S & Westinen, E 2013, *Entextualization and resemiotization as resources for (dis)identification in social media*, viewed 7 February 2019, <https://www.tilburguniversity.edu/upload/a3d5524e-4413-4772-9f96-9fe0ee714c6f_ TPCS _57_Leppanen-etal.pdf>.

Levin, S 2017, ‘Facebook and Google promote politicized fake news about Las Vegas shooter’, *The Guardian*, viewed 6 October 2017, <https://www.theguardian.com/us-news /2017/oct/02/las-vegas-shooting-facebook-google-fake-news-shooter>.

Macrae, CN, Milne, AB & Bodenhausen, GV 1994, ‘Stereotypes as energy-saving devices: A peek inside the cognitive toolbox’, *Journal of Personality and Social Psychology*, vol. 66, no. 1, pp. 37-47.

Markham, AN 2003, ‘Metaphors reflecting and shaping the reality of the Internet: Tool, place, way of being’, Unpublished manuscript, *4th Annual Conference of the International Association of Internet Researchers,* viewed 3 April 2019, <https://pure.au.dk/portal/files/69632404/MarkhamTPW.pdf>.

Marwick, AE 2018, ‘Why do people share fake news? A sociotechnical model of media effects’, *Georgetown Law Technology Review*, vol. 2, no. 2, pp. 474-512.

Matejic, N 2016, *Content Wars: Daesh’s sophisticated use of communications*, *NATO Review*, 16 November, viewed 25 November 2016, <https://2016/wars-media-daesh-communications-solis/EN/index.htm>.

McKay, T 2017, ‘Once again, Google promoted disinformation and propaganda after a mass shooting’ [Updated], *Gizmodo*, viewed 7 March 2018, <https://gizmodo.com/once-again-google-promoted-disinformation-and-propagan-1820166979/amp>.

Mezzofiore, G 2018, *Russian bots promote guns after Florida shooting*, *CNN*, viewed 7 March 2018, <https://www.cnn.com/2018/02/16/us/russian-bots-florida-shooting-intl/index.html>.

Morgan, J 2017, ‘How to fool Americans on Twitter’, *Data for Democracy*, viewed 30 January 2019, <https://medium.com/data-for-democracy/how-to-fool-americans-on-twitter-2a1da10724a2>.

Morris, MR, Counts, S, Roseway, A, Hoff, A & Schwarz, J 2012, ‘Tweeting is believing?: Understanding microblog credibility perceptions’, *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, pp.441-50.

Napoli, PM 2014, ‘On automation in media industries: Integrating algorithmic media production into media industries scholarship’, *Media Industries Journal*, vol. 1, no. 1.

Norman, DA 1999, ‘Affordance, conventions, and design’, *Interactions*, vol. 6, no. 3, pp. 38-43.

Oh, O, Agrawal, M & Rao, HR 2013, ‘Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises’, *MIS Quarterly*, vol. 37, no. 2, pp. 407-26.

Paul, C & Matthews, M 2016, *The Russian ‘Firehose of Falsehood’ Propaganda Model: Why it might work and options to counter it*, RAND Corporation, Santa Monica, CA, US, viewed 19 March 2018, <http://www.rand.org/pubs/perspectives/PE198.html>.

Paxton, J 2018, ‘Trident Juncture and the information environment’, *NATO Review*. viewed 23 October 2019, <http://www.nato.int/docu/review/2018/Also-in-2018/trident-juncture-and-the-information-environment/EN/index.htm>.

Pennycook, G, Cannon, T & Rand, DG 2018, ‘Prior exposure increases perceived accuracy of fake news.’, *Journal of Experimental Psychology: General*, vol. 147, no. 12, p. 1865.

Penzenstadler, N, Heath, B & Guynn, J 2018, ‘What we found in Facebook ads by Russians accused of election meddling’, *USA Today*, viewed 31 July 2018, <http://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/>.

Picart, C 2015, ‘“*Jihad* cool/jihad chic”: The roles of the Internet and imagined relations in the self-radicalization of Colleen LaRose (*Jihad* Jane)’, *Societies*, vol. 5, no. 2, pp. 354-83.

Reinstein, J 2018, ‘“Tweetdecking” is taking over Twitter. Here’s everything you need to know’, *BuzzFeed*, viewed 12 March 2018, <https://www.buzzfeed.com/juliareinstein/ exclusive-networks-of-teens-are-making-thousands-of-dollars>.

Richardson, JE & Wodak, R 2009, ‘The impact of visual racism: Visual arguments in political leaflets of Austrian and British far-right parties.’, *Controversia*, vol. 6, no. 2.

Richter, ML 2017, *The Kremlin’s platform for ‘useful idiots’ in the West: An overview of RT’s editorial strategy and evidence of impact*, European Values, Praha, CZ.

Ruddick, G 2017, ‘Experts sound alarm over news websites’ fake news twins’, *The Guardian*, viewed 7 March 2018, <http://www.theguardian.com/technology/2017/aug/18/ experts-sound-alarm-over-news-websites-fake-news-twins>.

Safi, M 2018, ‘Sri Lanka accuses Facebook over hate speech after deadly riots’, *The Guardian*, viewed 25 March 2018, <http://www.theguardian.com/world/2018/mar/14/ facebook-accused-by-sri-lanka-of-failing-to-control-hate-speech>.

—& Perera, A 2018, ‘Sri Lanka blocks social media as deadly violence continues’, *The Guardian*, viewed 9 March 2018, <http://www.theguardian.com/world/2018/mar/07/sri-lanka-blocks-social-media-as-deadly-violence-continues-buddhist-temple-anti-muslim-riots-kandy>.

Santa Maria, SD 2013, *Improving influence operations by defining influence and influence operations*, Defense Technical Information Center, Fort Belvoir, VA, US, viewed 22 March 2018, <http://www.dtic.mil/docs/citations/ADA606282>.

Sartonen, M, Huhtinen, A-M & Lehto, M 2016, 'Rhizomatic target audiences of the cyber domain', *Journal of Information Warfare*, vol. 15, no. 4, pp. 1-13.

Seo, H 2014, 'Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict', *Visual Communication Quarterly*, vol. 21, no. 3, pp. 150-61.

Shapiro, L 2017, 'Anatomy of a Russian Facebook ad', *Washington Post*, viewed 7 March 2018, <https://www.washingtonpost.com/graphics/2017/business/russian-ads-facebook-anatomy/>.

Simon, H 1971, 'Designing organizations for an information-rich world', ed. M Greenberger, *Computers, communications, and the public interest*, Johns Hopkins Press, Baltimore, MD, US, pp. 37-72.

Stella, M, Ferrara, E & De Domenico, M 2018, 'Bots sustain and inflate striking opposition in online social systems', arXiv preprint arXiv:1802.07292.

Stelter, B 2008, 'Finding political news online, the young pass it on', *The New York Times*, viewed 30 August 2016, <http://www.nytimes.com/2008/03/27/us/politics/27voters.html>.

Stieglitz, S & Dang-Xuan, L 2013, 'Emotions and information diffusion in social media—Sentiment of microblogs and sharing behavior', *Journal of Management Information Systems*, vol. 29, no. 4, pp. 217-48.

Svetoka, S 2016, *Social media as a tool of hybrid warfare*, NATO Strategic Communications Centre of Excellence.

Tangen, HB 2017, *Du vil ikke tro hvordan titlene i sportsjournalistikk varierer fra nettutgaven til papiravisa-En studie av sportsjournalistikkens titler i nett-og papiraviser,* B.S. thesis, *Høgskolen i Oslo og Akershus*.

Tatham, S 2015, *The solution to Russian propaganda is not EU or NATO propaganda but advanced social science to understand and mitigate its effect in targeted populations,* National Defence Academy of Latvia Center for Security and Strategic Research, viewed 22 May 2017, <http://www.stratcomcoe.org/download/file/fid/658>.

Tatnall, A 2003, 'Actor-network theory as a socio-technical approach to information systems research', eds. S Clarke, E Coakes, M G Hunter, and A Wenn, *Socio-technical and human cognition elements of information systems*, IGI Global, Hershey, PA, US, pp.266-83.

Terranova, T 2000, 'Free labor: Producing culture for the digital economy', *Social Text*, vol. 18, no. 2, pp. 33-58.

Timberg, C, Dwoskin, E, Entous, A & Demirjian, K 2017, 'Russian ads, now publicly released, show sophistication of influence campaign', *Washington Post*, viewed 7 March 2018, <https://www.washingtonpost.com/business/technology/russian-ads-now-publicly-released-show-sophistication-of-influence-campaign/2017/11/01/d26aead2-bf1b-11e7-8444-a0d4f04b89eb_story.html>.

Timberg, C & Romm, T 2018, 'These provocative images show Russian trolls sought to inflame debate over climate change, fracking and Dakota pipeline', *Washington Post*, viewed 9 March 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/congress-russians-trolls-sought-to-inflame-u-s-debate-on-climate-change-fracking-and-dakota-pipeline/>.

Tomaszewski, Z 2002, *Conceptual metaphors of the World Wide Web*, viewed 3 April 2019, <http://zach.tomaszewski.name/uh/ling440/webmetaphors.html>.

Treré, E 2016, 'The dark side of digital politics: Understanding the algorithmic manufacturing of consent and the hindering of online dissidence', *IDS Bulletin*, vol. 47, no. 1, viewed 2 August 2016, <http://bulletin.ids.ac.uk/idsbo/article/view/41/html>.

Trist, E, Murray, H, Emery, FE & Trist, B 1990, *The social engagement of social science, volume 2: A Tavistock anthology–The socio-technical perspective*, University of Pennsylvania Press, Philadelphia, PA, US.

Tsikerdekis, M 2012, 'The choice of complete anonymity versus pseudonymity for aggression online', *eMinds: International Journal on Human-Computer Interaction*, vol. 2, no. 8, pp. 35-57.

Tufekci, Z 2013, '"Not this one": Social movements, the attention economy, and microcelebrity networked activism', *American Behavioral Scientist*, vol. 57, no. 7, pp. 848-70.

Tynan, D 2016, 'How Facebook powers money machines for obscure political "news" sites', *The Guardian*, viewed 29 August 2016, <https://www.theguardian.com/technology/2016/ aug/24/facebook-clickbait-political-news-sites-us-election-trump>.

Van Niekerk, B & Maharaj, M 2013, 'Social media and information conflict', *International Journal of Communication*, vol. 7, p. 23.

Walker, C & Alrehamy, H 2015, 'Personal data lake with data gravity pull', *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, pp.160-7.

Weedon, J, Nuland, W & Stamos, A 2017, *Information Operations and Facebook*, Facebook, Menlo Park, CA, USA, viewed 22 March 2018, <https://fbnewsroomus.files.wordpress.com /2017/04/facebook-and-information-operations-v1.pdf>.

Williams, HTP, McMurray, JR, Kurz, T & Lambert, FH 2015, 'Network analysis reveals open forums and echo chambers in social media discussions of climate change', *Global Environmental Change*, vol. 32, pp. 126-38, <https://doi.org/10.1016/j.gloenvcha.2015.03.006>.

Williams, M & Burnap, P 2018, *Antisemitic content on Twitter*, Community Security Trust, London, UK, viewed 13 June 2018, <https://cst.org.uk/public/data/file/ 4/2/Antisemitic%20 Content%20on%20Twitter.pdf>.

Worley, M & Copsey, N 2016, 'White youth: The far right, punk and British youth culture, 1977-87', *Journalism, Media and Cultural Studies Journal*, no. 9, p. 27.