2020

Computational Propaganda: Targeted Advertising and the Perception of Truth

Julie Murphy

Anthony Keane

Aurelia Power

Computational Propaganda: Targeted Advertising and the Perception of Truth

Julie Murphy, Anthony Keane and Aurelia Power
School of Informatics and Engineering, Technological University Dublin, Ireland
Julie.murphy@mytudublin.ie
Anthony.keane@tudublin.ie
Aurelia.power@tudublin.ie
DOI: 10.34190/EWS.20.503

Abstract: Social media has become an effective medium for the execution of cyberpsychological threats by adopting language to influence perceptions based on personal interests and behaviours. Targeted messages can be refined for maximum effect and have been implicated in changing the outcome of democratic elections and the decreasing uptake of vaccinations. However, computational propaganda and cyberpsychological threats are not well understood within the cybersecurity community. To address this, we adopt the theoretical model of *the illusory truth effect* to posit that how information is presented online, may solidify views in an 'undecided' group with 'some' knowledge of an argument. We test this hypothesis by employing an explanatory sequential design. We first analyse a dataset containing adverts related to Brexit to determine influential terms using the corpus linguistics method. Analysing term frequencies, collocational and concordance information, the results of our quantitative analysis indicate that function words such as the personal pronouns 'we' or the definite article 'the' play a significant role in the construction of computational propaganda language. We then conduct a qualitative analysis of a Facebook ad related to Brexit to further understand how the 'who' and the 'what' elements are realised in computational propaganda language, that is, who is targeted and what is the underlying message. We found that understanding these, one can gain insights into a threat actor's motivation, opportunity and capability and, thus, allows a defensive response to be put into place. In turn, how an audience responds, may provide insight on the impact of the threat.

Keywords: computational propaganda, illusion of truth, cyberpsychology, critical discourse analysis, threat intelligence

1. Introduction

Influence comes under many guises, with terms such as propaganda or advertising used interchangeably to describe what is determined by the motivation of the influencer. Their enduring prevalence verifies the effectiveness of these techniques. This study considers the significance of influential techniques for the cybersecurity community by investigating why these tactics are effective and their amplified risk when propagated online. A sociocognitive critical discourse study is applied to determine what intelligence can be derived from these indicators as part of a broader framework.

Targeted advertising can create a direct communication with an audience predisposed to a certain view. Social media platform providers are perfectly situated to facilitate such communication based on pre-determined information surrounding interests and behaviours. Therefore if the message is designed for a specific target, it is feasible to reverse engineer the communication to determine what the underlying message is, who is being targeted and why. If traction and perception surrounding the message are also monitored; a threat actors capability, opportunity and motivation may be determined.

This study addresses the construct and delivery of a message text as an example for the cybersecurity community to highlight the importance of cyberpsychological skills to defend against influence threats. The objective is to determine why language usage and communication methods are relevant from a security perspective. Computational propaganda and cyberpsychological threats are fundamentally transdisciplinary, which can lead to translation issues for researchers crossing social and computer sciences. The challenge is how can cyberpsychological attacks be categorised for analytical research; how can digital communications compound the effect of cyberpsychological threats and how can the construct language of digital communications contribute to cyberpsychological threats?

2. Literature Review

2.1 The new social contract

Social contracts are a fundamental part of functioning society as historically debated by philosophers such as Thomas Hobbes and John Locke whereby freedoms are surrendered to authority for protection. Arguably, modern society has entered into a contract with online platform providers surrendering personal data for convenience and communication services. Attention economics is of increasing interest to providers whereby attention is a commodity in short supply therefore platform providers are refining techniques and information to retain attention longer to acquire more data, thus continuing the cycle. Similarly Bernays (1928) surmises that as the public become more aware of influential tactics, leaders present their objectives more intelligently. Subsequently vast digital footprints are accumulated with highly personal traits that support the propensity of targeted influence attacks. Significantly, attacks of this nature may have debatable legal implications, supported by relative anonymity rendering them highly desirable to a malicious actor adapting historically proven methods to contemporary mediums. Computational propaganda is now a global area of research with increasing interest in light of controversies ranging from vaccine debates to election tampering.

2.2 Computational propaganda

Howard and Wooley (2016) describe computational propaganda as "the use of algorithms, automation, and human curation to purposefully manage and distribute misleading information over social media networks". Their extensive multi-year study considers research from all over the world to assert how computational propaganda is promoted and enacted by different political regimes and actors and the consequences for democracy. Nimmo (2019) proposes a computational method to identify the extent of traffic manipulation which benefits the cybersecurity communities in attack analysis. Techniques employed to render manipulation campaigns effective have been identified by Bradshaw and Howard (2017) that formalise propaganda techniques as applied online. These approaches consider the impact of computational propaganda in the context of democracy and how it is effected online, building on existing research to understand why the online environment increases potential future risk. Accordingly cyberpsychologists endeavour to determine how engagement with technology impacts behaviours and psychological states. Barton (2016) describes models of persuasion and their importance within an online environment detailing how psychological approaches such as compliance, obedience, conformity and persuasion are applied alongside methods such as captology to great effect. This study examines concepts surrounding the 'illusory truth' effect to determine why computational propaganda and cyberpsychological threats are of particular importance to the cybersecurity community on the basis that "If people are told something often enough, they'll believe it" (Hasher, Goldstein and Toppino, 1977).

2.3 The Illusory Truth Effect

Hasher, Goldstein and Toppino (1977) conducted a study to assess whether participants believe a statement to be true if repeatedly exposed to it over a period of time. Using statements from a broad range of knowledge areas that were either true or false, they concluded that people were inclined to believe a repeated plausible statement, commonly referred to as the 'illusory truth effect'. Similarly, Bacon (1979) posited that 'recognition' of statements aligned to pre-existing views are considered more valid then opposing statements. Moreover people believe what they know to be true therefore, if new information confirms this knowledge it is more readily accepted. Arkes, Hackett and Boehm (1989) expanded on these theories by testing statements of 'opinions' instead of 'facts', concluding that the validity of the repetition effect is diminished when the audience is not well versed in the subject matter. Similarly Ozubko and Fugelsang (2010) posited that memory retrieval, or increased familiarity with a statement enhances the persuasive effect. The online environment is primed to build familiarity with statements and concepts as online concepts often translate to more traditional mediums such as national press, television and radio.

Becoming familiar and 'knowledgeable' of facts and statements by persistent exposure however, re-enforced by repetition and recognition of opinions and statements online compounds the perception of truth. Accepting these theories, consider the vast digital footprint of people, available to platform providers that is accurately customised for newsfeeds, information and advertisements based on distinctive personality traits and behaviours. Is it not conceivable that a malicious actor may employ targeted, often legal strategies, to influence the beliefs and opinions of a particular demographic?

If people had to weigh up the risks and consequences, or read the terms and conditions surrounding their online activity, their time online would increase exponentially in parallel with a dramatic decrease in productivity. Thus

when faced with thousands of decisions a day, people trust their instincts and those around them to make assumptions that the tools and platforms they use are safe. It is perceived that influence tactics are recognisable and defensible when educated accordingly however, cognitive ability does not defend against the illusory truth effect as demonstrated by De keersmaecker et al. (2019). In their study, aspects pertinent to influence were assessed: cognitive ability, the need for cognitive closure, and cognitive style. Their conclusions demonstrated that people are predisposed to believe repeated statements regardless of their cognitive ability. Therefore highly personal traits are available for sustained targeted influence campaigns to those who wish to express a perspective to an audience known to be 'susceptible' to the view. For the campaign to be successful, the statement or opinion needs to be framed in a manner that the targeted audience is likely to accept. Danesi (2015) describes the craft of advertising as "*a way of presenting something in a socially appropriate way…in the same way that effective orators attempt to convince audiences to accept their messages and act upon them*". Moreover, the characteristics of discourse are synonymous with keywords and cognitive styles that are familiar to people based on a 'shared knowledge system' or 'common ground'. Further, effective advertising builds an association of 'personal amelioration'. Importantly, Danesi asserts that although the delivery of advertising has changed with technological advances, the fundamental persuasive tactics have not.

Contagious ideas generally originate by the few. Consider fashion, whereby exceptional people lead to disproportionate influence and propagation of a trend. Propagation is dependent on certain conditions described by Gladwell (2006) as connectors, mavens and salesmen. Connectors have the network of relevant people, mavens are experts on the cutting edge espousing new information, and salesmen have the power to persuade people to make decisions they may not necessarily have taken. The combination or connection between these three elements results in powerful carriers of concepts, ideas and changes, often based on simple changes. There is limited research considering these perspectives through a cybersecurity lens.

In summary, a threat actor need only target those that are 'undecided' to affect the success or failure of any topic, product or service. What facilitates an ad, or topic's importance aligns with what is important to 'me' and is incorporated then into general conversation. Computational propaganda informs the beliefs that 'I' am susceptible to, therefore we suggest that a critical discourse study may highlight why the construct and delivery of a message impacts the perceptions of a susceptible audience. The cybersecurity community must understand 'how' a message can impact the perception of an undecided audience. There is intelligence is to be gathered by understanding why a particular audience is targeted and who would gain by influencing them. Incorporating this into the lifecycle of an attack would help support interventive deflection measures.

3. Methodology

The underlying problem is that computational propaganda and cyberpsychological threats are not well understood or addressed within the cybersecurity community. To address the interdisciplinary nature of this problem, we employ van Dijk's sociocognitive approach (2016). Because "*...social interaction, social situations and social structures can only influence text and talk through people's interpretations of such social environments ..[and] discourse can only influence social interaction models, knowledge, attitudes and ideologies*" (van Dijk 2016) we focus on critically analysing the online discourse surrounding computational propaganda. According to Wodack (2012) "*Critical discourse studies (CDS) are therefore not interested in investigating a linguistic unit per se but in analysing, understanding and explaining social phenomena that are necessarily complex and thus require a multidisciplinary and multi-methodical approach*"

3.1 Explanatory Sequential Design

The premise of this study is based on the hypothesis that: how information is presented online may solidify views in an 'undecided' group with 'some' knowledge of an argument. To carry out our investigation we employ an explanatory sequential design. We first analyse our dataset from a quantitative perspective, followed by a qualitative study to explain the results in greater depth (Creswell, 2015). The objective is to ascertain whether there are identifiable patterns in the way language is used in computational propaganda discourse that may be built upon for future defences against cyberpsychological threats. The focus is not on the ideation of the content but the 'construct' and delivery of the message

3.2 Quantitative Data Collection and Analysis

Using political adverts relating to Brexit, we analyse content from the BeLeave campaign to determine patterns surrounding the delivery and construct of online targeted ads. We use the corpus linguistics approach of analysing textual content to obtain statistical evidence of word frequencies, context and collocations. For

example, at first glance, much of the language used appears relatively neutral, however when evaluated based on concordance and collocation evidence for example, other patterns may become apparent.

3.2.1 Dataset

Verified targeted ads were used as the basis to build a control dataset for future studies. 120 ads were selected from the BeLeave campaign ran in June 2016 (House of Commons, 2019). These ads achieved an impression[1] rate between 46,650,000 and 104,836,880 by the British electorate in the days prior to the Brexit referendum. 18% of these ads were slight variations of the same text. Duplicate ads was removed resulting in 43 ad instances. Analysis is based on text only. The AntConc tool is used for initial analysis to determine high level patterns.

3.2.2 Results and Discussion

Table 1: Most frequently used words

Rank	Freq	Word
1	90	we
2	87	the
3	87	to
4	78	a
5	78	beleave
6	78	eu
7	77	our
8	67	and
9	59	future
10	50	in

Table 1 shows the ten most frequently used words, ranked from 1 to 10. Grammatically, the majority of these words are function words, such as pronouns (we, our), articles (the, a) or prepositions (in), words typically discarded from analysis, being considered stop words that carry out little or no semantic value. However, we believe that they are essential in understanding the discourse of computational propaganda. For instance, there are 90 instances of the personal pronoun 'we' which may be explained by the fact that 'we' aligns the group ideology with the target's identity, adding to the sense of familiarity between the sender and the recipient. In addition, when one considers the context in which 'we' occurs (Table 2), it can be observed that the concordance of 'we' covers both positive and negative connotations. When 'EU' is presented prior to 'we' there is observable negative semantic prosody (Louw, 1993), resulting in an ideological polarisation effect with the ingroup 'Britain' which is positively represented, representations that can be further explained by van Dijk's (2016) 'idealogical square' which represents the 'self' as positive and the 'other' as negative. The polarisation of the contextual information associated with the pronoun 'we' is consistent throughout the dataset as evidenced by the fact that 'we' negatively relates to emotional terms such as 'powerless' and 'out of control' when co-occurs in the same context as 'EU', whereas 'we' positively relates to positive actions such as 'we can' when used to refer to the to the ingroup 'Britain' since they reflect empowerment. The prevalence and emphasis of the positive self-description 'we' exacerbates the division between the in-group British, and the negative other-description referring to the EU. Similarly, frequent use of the pronouns 'ours', 'they' and 'theirs' are synonymous with political groups and can achieve a polarising effect for example "Are *they* focused on *their* priorities or *ours".* Repeated instances of the activities that 'we' have to do, is consistent with the identification and alignment of ideological groups. Further the objective ideological 'norms and values' are expressed explicitly and implicitly with verbs such as *can* have, *can take back*.

[1] "Impressions is a common metric used by the online marketing industry. Impressions measure how often your ads were on screen for your target audience." (Facebook, 2019)

Table 2: Negative and Positive use of 'we'

Negative – 'we'		Positive – 'we'	
Inside the EU,	we are powerless	So	we can bring
Under EU laws	we are unable	Under our control	we can bring
Under EU regulations	we are unable	On 23 June so	we can chart
Shouldn't	we be in control	On 23 June so	we can have
Isn't it time	we became an independent	Today, 23 June, so	we can have
It is time	we break free	On 23 June so	we can make
		Today, 23 June, so	we can make
		23 June so that	we can take back
		23 June so that	we can take back
		Isn't it time	we chart our own
		Opportunities	we could have outside
		Is so important.	We have an opportunity
		The opportunities	we know will make
		Why do	we let them do
		It is time	we take a stand
		It is time	we unite to give
		Of the EU	we will become

The definite article 'the' appears 87 times, and a collocational analysis links the use of 'the' to 'eu' on 62 occasions. This further enhances the polarisation effect, indicating that 'the' is used to underline the definite and real threat of an entity that opposes the referred to by the pronoun 'we'. Similar to the word 'the', there are 87 instances of the word 'to'. When clustered with three subsequent words, 'to' seems to almost exclusively serve as verb particle indicating that the target audience should take action '*to* leave the eu' or '*to* build a bright future'. By analysing these clusters further, we can also determine a link between the eu, British nationals, and an action to 'leave the eu' to assume the underlying message. Observe the use of positive self-descriptions such as 'our nation', and prepositions '*to* build', '*to* be a prosperous', which align the audience with the sender.

Table 3: Clusters of 'to'

Total No. of Cluster Types	17	**Total No. of Cluster Tokens**	87
Rank	Freq	Range	Cluster
1	41	1	to leave the eu
2	6	1	to control our nation
3	5	1	to build a bright
4	4	1	to be a prosperous
5	4	1	to give our country
6	4	1	to lead on a
7	4	1	to vote on 23 june
8	3	1	to brexit and chill
9	3	1	to pave a prosperous
10	3	1	to tax and force
11	2	1	to create a fair
12	2	1	to grow and reach
13	2	1	to us! shouldn't
14	1	1	to bring in a
15	1	1	to take back control
16	1	1	to think of our
17	1	1	to us! let's

There are 77 instances of the pronoun 'our' and 78 instances of the noun 'eu'. By assessing the collocates of these two words (Table 4) provides an insight into the tone of the text body. 'Our' relates to the Britain ingroup 'nation', 'country', 'national' with positive connotations such as 'great' and 'control', whereas 'EU' relates to the EU outgroup with negative connotations such as 'regulators' and 'protectionism'.

Table 4: Collocates of 'our and 'eu'

Total No. of Collocate Types: 16					Total No. of Collocate To
Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	24	0	24	4.78238	own
2	9	0	9	3.42874	nation
3	6	0	6	4.55999	country
4	5	0	5	4.51935	generation
5	5	0	5	1.22167	future
6	4	0	4	3.97503	regulations
7	4	0	4	4.19742	great
8	3	0	3	4.78238	streaming
9	3	0	3	4.36734	priorities
10	3	0	3	4.78238	national
11	3	0	3	4.78238	money
12	2	0	2	4.78238	full
13	2	0	2	2.08194	control
14	2	0	2	4.78238	ability
15	1	0	1	3.19742	laws
16	1	0	1	4.78238	chance

Total No. of Collocate Types: 15					Total No. of Collocate To
Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	34	0	34	4.23652	on
2	10	0	10	1.59384	we
3	7	0	7	4.40120	today
4	4	0	4	4.76377	regulators
5	4	0	4	4.76377	protectionism
6	3	0	3	4.76377	should
7	3	0	3	3.54137	regulations
8	3	0	3	0.08194	our
9	2	0	2	4.76377	rule
10	2	0	2	4.17880	laws
11	2	0	2	4.76377	controls
12	1	0	1	1.59384	under
13	1	0	1	2.17880	over
14	1	0	1	2.17880	officials
15	1	0	1	-1.30232	and

There is a significant use of imperatives which are frequently applied in advertising to essentially tell someone to do something by making commands or recommendations for example 'Let's stop', Let's spend' and 'Let's vote' with the latter represented in 43 instances. Presupposition (or implied) meaning is present by 'Let's stop EU regulators from controlling…" whereby a reader infers that EU regulators already 'are' controlling. Similarly the definite 'the' is used in the context 'the freedom to be' and 'chase the opportunities' presuppose that 'a' freedom has been taken and 'an' opportunity has been taken. Advertising techniques such as slogans and taglines are present with 78 instances of 'BeLeave'. Similarly rhetorical questions introduce familiarity by engaging the audience to participate in conversation. For example: 'Are they focused on their priorities or ours?', 'Did you know that the EU controls over 60% of our regulations? Why do we let them do this?', 'Shouldn't we be in control of our future?', 'Isn't it time we chart our own destiny and chase the opportunities we know will make Britain successful?', ' Let's vote to leave the EU on 23 June so we can have a clear and prosperous future?'

Another discourse factor that impacts the effectiveness of computational propaganda in the present dataset is modality which is represented by 44 concordances relating to 'can'. 'Can' reflects the audiences ability to effect change . Modal claims combined with verbs invoke a sense of possibility for a positive outcome: 'Can bring in talent', 'Can chart our own destiny', 'Can have a clear and prosperous future', 'Can make our own decisions' and 'Can take back control'. Predicational strategies (Reisigil and Wodak, 2001) describe the linguistic assignment of qualities to induce judgement by the audience as demonstrated by the use of the word 'unelected': 'unelected EU officials', 'unelected foreign officials', 'unelected officials that have no idea'.

'The Choice' presented to the audience is synonymous with pro-war propaganda and is designed to end debate on the topic (Richardson, 2007) whereby the audience perceives only two options. In the context of this study the audience perceives that a) a 'remain' vote equates to 'doing nothing' and 'doing nothing' equates to 'losing control / jobs', or b) a 'leave' vote equates to 'doing something' and 'doing something' equates to a 'brighter future' with 'prosperity'.

From the initial analysis we have determined that the principles surrounding the illusory truth effect are relevant to computational propaganda insofar as how the message is framed, interpreted and repeated may provide insight to the cybersecurity community. Consequently we can conduct a brief qualitative analysis to extrapolate what audience may be influenced by this message and why. This brief secondary study is applied to give context to the overall nature of the study.

3.3 Qualitative Data Collection and Analysis

In addition to the conclusions drawn , an individual ad from BeLeave's Facebook page is briefly assessed using elements of van Dijk's discourse-cognition-society triangle to link these complex theories. This assessment is not exhaustive as a detailed analysis is outside the scope of this paper, moreover it is applied to add context to the initial study. van Dijk asserts that although critical discourse studies surround society and discourse, *"a sociocognitive approach claims that such relations are cognitively mediated. Discourse structures and social*

structures are of a different nature, and can only be related through the mental representations of language users as individuals and social members" (van Dijk, 2016).

Figure 1: BeLeave Facebook ad (BeLeave, 2019)

Firstly we consider a discursive and semiotic analysis to study the implied and inferred meaning of the ad in figure 1. It is assumed that there is a shared sociocultural awareness of the topic which is facilitated by online advertising. Numerous cognitive structures are required to interpret the message. By using the semiotic hashtag #SaveOurNHS, the reader is commanded to commit to the concept supported by this campaign. The possessive pronoun 'our' contextually refers to Britain with the presupposition being that the EU is responsible for the problems within the NHS. Social identity of an authoritative figure is semiotically denoted by the title 'Professor' and represented by formal appearance suggests authority and leads to greater likelihood that a reader will submit to the theory presented by a knowledgeable authoritative figure. People may not be familiar with the intricacies of the argument but assume an authoritative figure can be trusted. Observe also the use of the hashtag also supports analysis and measurement of sentiment surrounding the topic for success or failure of the approach. The inferred message is that the health of the British public is in imminent danger. There is a sense of urgency implied by the use of red highlighting 'intolerable strain' and 'collapse completely' against the backdrop of the NHS logo. The urgency implied prompts the reader to an emotional, urgent response. Essentially EU equates to 'intolerable' and 'collapse' of a fundamentally British institution resulting in a polarising effect between Britain and the EU.

In consideration of the cognitive structures we observe that sociocultural knowledge is assumed surrounding the struggling health service that people depend on and are likely familiar with either directly or indirectly which gives a personal context for doubt in the EU, that may result in an emotional response. There are implications for online focus as it facilitates targeted areas and demographics who are more readily impacted by these events to increase the polarising effect in the context of the ideological square. There is a suggestion that the readers way of life is at risk by presupposing that the EU has taken control implying that control has already being lost, which places the reader on the defensive. BeLeave, the advertiser, is communicating interactively with 'you' the British public.

4. Inferences Drawn

This foundational study supports the theory that adopting a sociocognitive perspective to discourse can contribute to the 'intelligence' derived from computational propaganda strategies. Through content analysis, cybersecurity professionals may extrapolate who is being targeted with a particular message allowing them to extrapolate which threat actors have the motivation, opportunity and capability to conduct such campaigns. The inferences drawn are based on the principle that content analysis is in place within an organisation, and there is an established baseline. Traffic patterns can then be analysed using the quantitative and qualitative methods discussed to identify who is being targeted with what message, followed by analysis for more detailed intelligence. When collocational profiles become synonymous with social issues there can be a psychological association for individuals as determined by Richardson's 'choice'.

A target audience is selected based on sociocultural knowledge that is available from social analytics. In consideration of recognised psychological assumptions, a simple easily recognisable message is constructed and repetitively presented and delivered under different guises until target takes a perspective and aligns with one view or another. The cycle is then repeated to reinforce the perspective in the targets view until target adopts perspective as their own opinion. Analytics furnish an attacker with feedback on the success or failure of a campaign allowing the approach to be refined.

Table 5: Adapted Context Model

Context parameters	Discourse Structures	Intelligence
Spatiotemporal dimension of online communication	Date: Leadup to Brexit referendum. Location: UK. Present tense as of February 2016	Opportunity: Event and duration of campaign
Advertiser: British citizen in the role of concerned citizen or campaigner	Ads: deictic expression: 'our'	Capability: Extent, expense and sophistication of campaign, and ancillary campaigns.
Engaged in asserting perceptions of societal injustices in the form of advertising which is an element of social media targeted advertising	Opinion expressed: health of the British public is at risk 'intolerable strain', 'on its knees', collapse completely'.	Motivation: To achieve polarizing effect between the EU and British electorate in support of votes. Who gains if objective is achieved?
Objective is to influence opinion of undecided voter	'voteleavetakecontrol.org'	Target: undecided groups. Induce heightened sense of uncertainty. Emotional response

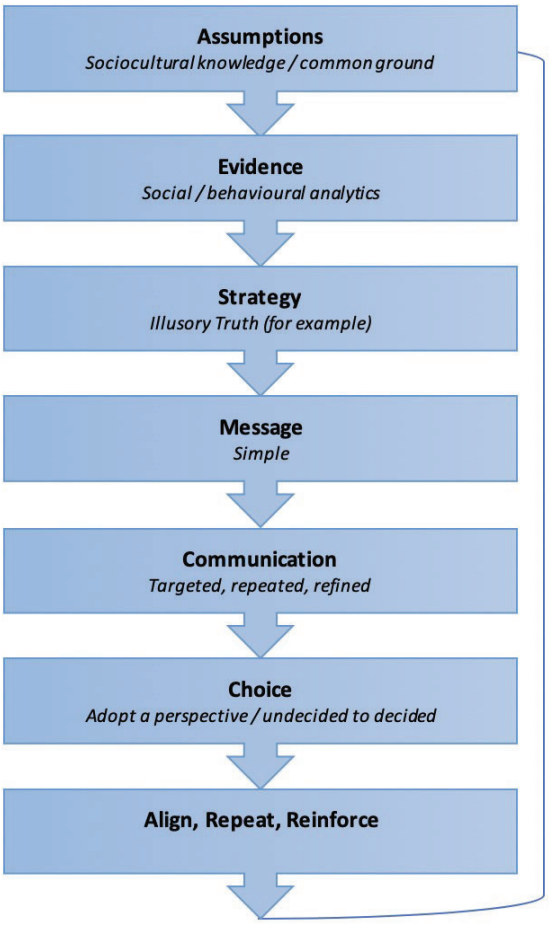

Figure 2: Attack Lifecycle

Results align with principles of illusory truth effect and support the value of computational propaganda to an attacker. Social media supports the use of personalised targeting resulting in the ability to communicate a medium to an audience susceptible to the view. When messages become familiar to an audience they are more readily willing to accept the statements. How the message is interpreted is based on many factors as evidenced by van Dijk's sociocognitive approach. For example van Dijk's ideational square determines the ingroup and outgroup, Richardson's 'choice' solidifies a view and social media platform providers provide the means and

basis to analyse response for improved results. To conclude, cyberpsychology is a key requirement within the cybersecurity community to respond to non-traditional cyber threats.

5. Criticisms of Approach

There are many criticisms of critical discourse studies that pertain to the broad and imprecise nature of the approach which is in contrast to the analytical approach generally adopted to technical threats, however as identified in this study, the prevalence of analytical tools for online communications supports the use of sociocognitive discourse studies to identify at a high level that a cyberpscychological attack may be present or emerging. Considering threats of this nature, allows the cybersecurity community to prepare and build appropriate responses for future threats.

6. Future

The objective of this study was to highlight why psychological attack methods are critical to the cybersecurity community. Future studies may broaden the psychological theories and analytical methods employed and overlay the results with other technical methods for greater results.

7. Conclusion

It is readily accepted that people are susceptible to influence campaigns of all descriptions however it is assumed that we are protected by educational strategies, or cognitive defences. This paper considered why psychological strategies when applied effectively are powerful when combined with the global nature of social media. On the premise that computational propaganda and cyberpsychological threats are fundamentally transdisciplinary, we considered how cyberpsychological attacks can be categorised for analytical research by proposing an attack lifecycle to be expanded on in future studies. We conclude that analytical tools available by social media providers ensure that targeted campaigns can be refined for greater effect. Impression rates, combined with content and sentiment analysis determine, and compound the effect of cyberpsychological threats. We determined that the construct language and delivery of digital communications can contribute to cyberpsychological threats when communicated and delivered to an audience susceptible to a view. To conclude, the symbiotic relationship between technology and people demands symbiotic consideration from the cybersecurity community to defend against emerging threats.

References

Arkes, H.R., Hackett, C. and Boehm, L. (1989). The generality of the relation between familiarity and judged validity. *Journal of behavioural decision making.* 2. 81-94.

Bacon, F.T. (1979). Credibility of repeated statements: Memory for trivia. *Journal of experimental psychology. 5(3). 241-252.*

Barton, H. (2016). *Persuasion and compliance in cyberspace*. In Connolly, I. et al (eds) An introduction to cyberpsychology. Oxen/New York: Routledge

BeLeave (2019) 20 May. BeLeave. Available at: https://www.facebook.com/voteleave/posts/each-week-we-send-350-million-to-the-eu-enough-to-build-a-new-fully-staffed-nhs-/552289318281330/ [Accessed 20 May 2019]

Bernays, E. (1928). *Propaganda.* New York. H. Liveright.

Bradshaw, S. and Howard (2017) 'Troops, trolls and troublemakers: A global inventory of organized social media manipulation'. The Computational Propaganda Project. University of Oxford.

Creswell, J.W. (2015). *A concise introduction to mixed methods research*. US. Sage.

Danesi, M. (2015) *Advertising discourse.* In Tracy, K., Ilie, C. and Sandel, T. (eds) The international encyclopedia of language and social interaction. John Wiley & Sons.

De keersmacker, J., Dunning, D.A., Pennycook, G., Rand, D.G., Sanchez, C., and Roets, A. (2019). Investigating the robustness of the illusory truth effect across individual differences in cognitive ability, need for cognitive closure, and cognitive style [online]. Available at: https://psyarxiv.com/n7bze/ [Accessed 23 July 2019]

Facebook. (2019). Impressions. Available at: https://www.facebook.com/business/help/675615482516035 [Accessed 8 October 2019]

Gladwell, M. (2006) *The tipping point: how little things can make a big difference*. Available at: http://www.innovationlabs.com/tipping_point.pdf (Accessed 1 May 2018).

Hasher, L. and Goldstein, D. (1977). Frequency and the conference of referential validity. *Journal of verbal learning.* 16. 107-112.

House of Commons (2019) Fake news evidence. Available at: http://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Fake_news_evidence/Letter-from-Rebecca-Stimson-Facebook-to-Chair-re-question-29-19-July-2018.pdf [Accessed: 10 May 2019]

Louw, Bill (1993) *Irony in the Text or Insincerity in the Writer? The Diagnostic Potential of Semantic Prosodies*. In Baker, M., Francis, G. & Tognini-Bonelli, E. (eds) Text and Technology: In Honour of John Sinclair. Philadelphia/Amsterdam: John Benjamins

Nimmo, B. (2019). *Measuring Traffic Manipulation on Twitter.* Working Paper 2019.1. Oxford: Project on Computational Propaganda. Available at: https://comprop.oii.ox.ac.uk/research/working-papers/twitter-traffic-manipulation/

Ozubko, J.D. (2010). Remembering makes evidence compelling: Retrieval from memory can give rise to the illusion of truth. *Journal of experimental psychology: Learning, memory, and cognition.* 1. 1-7

Reisigl, M. and Wodak, R. (2001) *Discourse and Discrimination. Rhetorics of racism and antisemitism*. London: Routledge

Richardson, J. (2007) *Analysing Newspapers: An approach from critical discourse* analysis. Hampshire / New York: Palgrave

van Dijk, T. (2013) *CDA is not a method of critical discourse analysis*. In: EDISO Debate – Asociacion de Estudios Sobre Discurso y Sociedad. www.edisoportal.org/debate/115-cda-not-method-critical-discourse-analysis, accessed [12 July 2019]

van Dijk, T. (2016*) Critical discourse studies: A sociocognitive approach*. In Wodak, R. and Meyer, M. Methods of Critical Discourse Studies, 3rd Edition London: Sage

Wodak, R. (2012) *Editor's Introduction: Critical discourse analysis – challenges and perspectives*. In: R. Wodak (ed.) Critical Discourse Analysis. London: Sage.

Wodak, R. and Meyer, M. (2016) *Methods of Critical Discourse Studies*, 3rd. Edition. London: Sage

Woolley, S. C. and Howard, P.N. (2016). Automation, algorithms and politics: Political communication, computational propaganda, and autonomous agents. *International Journal of Communication.* 10(0) 9.

Harmi Armira is a security analyst from Cyber Security Malaysia. She received her Master in Information Security (MIS) from University Putra Malaysia (UPM) in 2018. She now is an active security assessor and also conducting research on malware forensics, threat modelling, and web security.

Dr Panu Moilanen is a senior lecturer and a head of MDP in security and strategic intelligence at the University of Jyväskylä, Finland. He is interested in the technology use in everyday life and its effects on societies. Currently, he is especially interested in the role of technology in the comprehensive security of modern societies.

Michael B. Motlhabi received his BSc CS Honours (Cum Laude 2011) and his Master of Science degree in 2014 from the University of the Western Cape (UWC). He worked in the Telecommunications industry as a Packet Optical Transport Network engineer for 6 years. He is currently a Senior Cybersecurity Engineer at the Council for Scientific and Industrial Research (CSIR).

Dr. Francois Mouton is an Associate Professor in Cyber Security at Noroff University College based in Oslo, Norway. His fields of expertise are social engineering, penetration testing and digital forensics. His research has had a significant impact within the field of social engineering and he currently has an h-index and an i10-index of 9.

Julie Murphy is a PhD researcher with interests in cybersecurity and cyberpsychology. Julie works in IBM and has over 10 years' experience in the telecommunications industry. She holds an MSc in Cybersecurity, and a BA in MIS. Julie is actively involved in community efforts to promote cybersecurity, advocating education as a primary defense.

Erja Mustonen-Ollila is currently a doctoral student in the University of Jyväskylä, Finland. Her thesis covers the areas of hybrid information environment (HIE), hybrid warfare, information influence, information operations, defence strategies and actors. She has previously published in high quality journals and conferences in the areas of Information Systems Science, Software Engineering and Knowledge Management.

Dr Teija Norri-Sederholm is an adjunct professor at the Finnish National Defence University's Department of Leadership and Military Pedagogy. Her main research areas are situational awareness, inter-organisational communication in command centres and hybrid environments, national security, and the dark side of social media.

Daniel Nussbaum is a faculty member in both the Operations Research Department and the Business School at Naval Postgraduate School (NPS). He chairs the NPS Energy Academic Group and provides leadership to SECNAV Executive Energy Education program.

Christopher O'Flaherty studied a BCOM at Stellenbosch University, South Africa. Following that, completed his postgraduate degree in Information Systems Management at Stellenbosch University. Christopher currently works at BDO in Cape Town as a financial services technology junior analyst and has a passion for cyber security, technology, while also being an avid runner.

Olav Opedal has worked as an information security professional since 2001 after leaving the US Army. Fourteen years with Microsoft, three years at T-Mobile, and three years as a psychotherapist. Olav Opedal graduated as a Ph.D. in psychology in November 2019 and holds an MS in clinical psychology and a BS in computer science.

Toyosi Oyinloye is a 2002 graduate of University of Ilorin, Nigeria, with BSc in Computer Science. She obtained her MSc (with distinction) in Cyber Security from the University of Chester in 2019. She is currently undertaking PHD research in the area of Software Protection Methods and Techniques including Control Flow Integrity.

Stefan Pickl is full Professor and Chair for Operations Research at the University of the Bundeswehr in Munich. Previously, he was scientific assistant and project manager at the Center for Applied Computer Science Cologne (ZAIK).

Dr Heloise Pieterse is currently employed as a senior researcher within the Cyber Warfare research group at the Council of Scientific and Industrial Research. She completed her PhD Computer Science degree in 2019, with a