How Do You Define a Problem Like Influence?

A Wanless[1], J Pamment[2]

[1]Department of War Studies
King's College, London
London, United Kingdom

E-mail: Alicia.wanless@kcl.ac.uk

[2]Department of Strategic Communication
Lund University
Helsingborg, Sweden

E-Helsingborg: james.pamment@isk.lu.se

***Abstract**: While increasing media coverage is dedicated to how information is used to influence target audiences, a common terminology for describing these activities is lacking. This paper offers a literature review of terms currently used by industry, government, and media related to in-fluence operations; analyses the challenges posed by many of these definitions for use in practical policy development; and ultimately argues for a broader definition of such.*

Keywords: *Influence Operations, Information Operations, Propaganda*

Introduction

Myriad actors attempt to shape the information environment for specific aims. The capabilities enabled through information communication technologies to those aiming to shape the information environment have far outstripped the general understanding of what can and is done through such pursuits. The gap between what is possible and what is generally understood about such techniques is exacerbated by a lack of terminology flexible enough to accurately describe how the information environment is shaped – a challenge particularly experienced by policymakers attempting to address threats associated with the shaping of the information environment.

Many terms are used to attempt to explain how the information environment is being shaped for specific outcomes. Terms like information operations, reflexive control, propaganda, mis- and dis-information, and fake news abound, but there is little consistency in usage, particularly in media coverage of the topic, and many of these words are also poorly defined or understood. Far from helping to foster a deeper understanding of how the information environment is shaped, such inconsistent usage leads to more confusion. At the same time, as more details come to light on how actors attempt to deliberately shape the information environment, pressure on governments and industry to do something about undesirable practices grows. Existing terms often lack the flexibility to create policy capable of tackling such threats, particularly at scale.

A changing ability to influence target audiences in a Digital Age is a growing concern for many. Indeed, in its coverage of "Russian Hacking and Influence in the U.S. Election", the *New York Times* has published more than 1800 articles since 14 June 2016 (2019), indicating a preoccupation with the topic. There is a landing page that aggregates all the articles tagged as related to the topic of 'Russian Hacking and Influence in the U.S. election'. The search function on this page lets readers filter the articles by additional keywords in the text and various terms used to describe the use of information to influence target audiences. The authors' search of the keywords in **Figure 1**, below, indicates the variety of possible keywords and suggests there is confusion regarding how to describe such influence activities, with fake news, misinformation, propaganda, disinformation, and others featured.

Keywords	Number of Returned Articles
Fake News	138
Misinformation	119
Propaganda	115
Disinformation	115
Influence Campaign	83
Influence Operations	45
Information Operations	15
Information War	10

Figure 1: Number of returned articles mentioning keywords as searched on 15 July 2019 via the *New York Times* landing page featuring articles on "Russian Hacking and Influence in the U.S. Election"

While increasing media coverage is dedicated to how information is used to influence target audiences, common terminology for describing these activities is lacking. Drawing from the *New York Times* coverage, this paper offers a literature review of terms currently used by industry, government, and media related to influence operations, analyses the challenges posed by many of these definitions for use in practical policy development, and ultimately argues for a broader definition of such activities.

A Confusion of Terms

Much of the challenge lies in finding the appropriate terms. While many terms are currently being used to describe individual problems associated with the shaping of the information environment, many lack clarity in definition. Other challenges are also present, such as philosophical dichotomies, inherent immeasurable intent, foreign-actor focus, and pre-existing connotations, making them impractical for developing policies to address threats.

Philosophical dichotomies

Some terms used to describe how the information environment is shaped suffer from philosophical dichotomies, often drawing hard lines between black and white that are difficult to classify objectively and at scale. Concepts such as misinformation and distortion fall into this category. Misinformation or "false or misleading information" (Lazer *et al.* 2018) implies a sense of veracity to which the content can be compared and contrasted. Likewise, to distort or "change something so that it is false or wrong, or no longer means what it was intended to mean" (*Cambridge Dictionary* 2008) suggests some original pristine state that is true and has been altered. Setting aside an ongoing philosophical debate on the nature of information, with some viewing information as inherently truthful (Dretske 1981; Grice 1989; Frické 1997; Floridi 2009) and others seeing any sort of data as information, regardless of its accuracy, (Fox 1983; Fetzer 2004b; Fallis 2011; Scarantino & Piccinini 2010), deciding what is or is not true can be extremely subjective (Karlova & Lee 2011) and resource intensive, complicated further by those who were exposed to misinformation not seeing corrective information (Silverman 2015) or becoming more polarized by the correction (Bail *et al.* 2018).

Does truth matter in the context of information as it is used to influence a target audience? It does, insomuch as truth is often used as a defining line between what is acceptable in terms of using information to influence those audiences. Frické made this distinction between information and propaganda, for example, in that the former must be true, while the latter is not (1997). Truth is often used to distinguish between activities Western countries undertake to influence audiences within a democratic framework, such as 'public information policy' (Taylor 1990, 2003), 'press/media relations' (Taylor 1990, 2003), public affairs, (Moloney 2006), and public diplomacy (Garrison 1999), which are claimed to be truth-based, versus the products of authoritarian regimes such as Russia, for example, which are not (E.U. Committee on Foreign Affairs 2016). Truth is also used in community standards on social networks and an increasing body of legislation (Funke 2019) to address the use of information to influence target audiences. Facebook, for example, regulates activity on its platform along the concept of truth, prohibiting fake accounts, the misrepresentation of oneself, as well as "fake news" (2019). Of course, these attempts to euphemize communications and police content along lines of truth from falsehood do not work so well in practice, for one person's truth might not be another's.

As already noted, the very act of determining what is true can be subjective. Habermas explored the challenges around truth within the context of communication theory and the human ability to reach mutual understanding. As Habermas explains, "the evidence theory of truth fails to take into account the fact that the concept of truth is interwoven with that of fallible knowledge" whereas in a "consensus theory of truth" (2018, p. 96), what is true is based not on "any knock-down arguments, only more or less 'good' arguments, in substantive controversies"; and in a "deontic meaning of validity" (p. 102), truth is based on norms, however that is decided. Habermas concluded that none of these ideas of truth are without subjectivity.

The subjectivity of determining what is truthful is further complicated by human perception, with people processing information in terms of how they already understand the world, not necessarily corresponding to a shared reality with others (Bering 2012).

Inherent immeasurable intent

Other terms such as 'disinformation' and 'deception' carry an inherent sense of intent in their meaning. For many researchers, disinformation is the spreading of false information to deliberately deceive (Lazer *et al.* 2018; Floridi 2011; European Commission 2018), (although not all accept that the information must be false [Fallis 2011] or that there is a distinction between misinformation and disinformation [Zhou & Zhang 2007]). Similarly, to deceive, as Mahon explains,

> must be intentional; deceiving requires that another acquires or retains a false belief, and not merely loses or fails to gain a true belief; deceiving must involve the agency of the deceived; and the deceiver must know or truly believe that what the deceived believes to be true is false. (2007, p. 192)

In their experiment, Rutschmann and Wiegmann found that a person's intent to deceive had little impact on whether what they said or not was believed to be a lie, questioning how necessary intent was for the definition of deception (2017). This notion of intent is also problematic for Karlova and Lee as "the dichotomy of benevolent and malevolent intent when disinforming is unsatisfying, since social situations sometimes require or encourage people to disinform" without meaning harm (2011, p. 8). Little white lies, in other words, are not satisfactorily accounted for by this terminology.

Discerning and measuring intent is extremely difficult, especially from a proactive stance of addressing the spread of false information at scale. Motives might never be proven and make for poor lines to draw in the sand of what is acceptable engagement in the information environment. This is to say nothing of complications in distinguishing misinformation from disinformation along lines of intent – does disinformation that is unwittingly spread by a target audience become misinformation the moment somebody believes and unwittingly spreads it, for example? Given that terms such as 'misinformation', 'disinformation', and 'deception' are still mired by academic debate as to what their exact meanings are, they are rendered poor choices for adopting into policy.

Focusing on foreign actors

Following disclosures from senior U.S. intelligence officials regarding Russian efforts to interfere in American elections (Johnson 2018), considerable focus by many Western countries has been placed on preventing foreign interference in elections, including by the G7 where a key theme for the 2018 summit was protecting democracy from "foreign threats" (Group of Seven 2018). Indeed, Facebook's initial attempt to articulate how the information environment was being manipulated used the term 'information operations', defining it as "as actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome" (Weedon, Nuland & Stamos 2017, p. 4). However, 'foreign' is mostly a legal term that in an interconnected age is increasingly tricky to define. Most definitions use 'foreign' as a qualifying word, such as 'foreign policy' or 'foreign national'. For example, Cornell Law School's Legal Information Institute defines a foreign national as "a person who is not a citizen of the United States and who is a citizen of a foreign country." These definitions position 'foreign' in terms of citizenship and statehood, but a definition in the context of the information environment might be less simple to delineate.

A key challenge with using foreign actors as a line in the sand in determining what is acceptable or not in terms of shaping the information environment is the ability to identify them as such. A pro-

liferation of actors (Betz 2015, p. 180) beyond states, capable of shaping the information environment renders the situation more ambiguous (Van der Putten, Meijinderes & Rood 2015; Kallberg & Rowlen 2014; Thornton 2015). This ambiguity, where "proxy forces, covert action, cyber operations, and political manipulation can achieve strategic goals," (Lewis 2016, p. 5) makes it difficult to identify if an attack occurred, who might be behind it (Thomas 2016), and what their intent is. This emphasis on foreignness also raises key philosophical questions such as the following: How relevant is a country's legal definition of foreign to determining how acceptable a participant is in public debate? Are diasporas in their new home legitimate actors in public debate in their country of origin? Are illegal immigrants legitimately able to influence the politics in the countries in which they hope to stay? How does one account for proxy or sympathetic actors ('useful idiots') who may be persuaded or coerced into supporting the goals of a foreign state? What about public diplomacy or grant programs that help activists in other countries—or even one community in the same country who disagrees with the decisions of another?

Pre-existing connotations

Many terms used to describe the shaping of the information environment, such as 'propaganda' and 'information warfare', have pre-existing connotations that render them confusing for use in policy. These concepts also tend to be extremely broad, making it difficult to discern lines between what makes one type of communication acceptable and another not.

Propaganda

Propaganda is a prime example of this. "Propaganda, in the most neutral sense, means to disseminate or promote particular ideas" (Jowett & O'Donnell 2015, p. 7) with the aim of manipulating a target audience into a behaviour as desired by the propagandist (Taylor 1990, 2003). Propaganda is an agnostic tactic (Jowett & O'Donnell 2015). As such, propaganda is an exceptionally broad concept, difficult to distinguish (if at all) from advertising, marketing, and public relations. As such it is impossible to identify and enforce against at scale.

While some governments distinguish between informative and influence activities (Darley 2005), in practice this amounts to an exercise in semantics to convince target audiences that public relations and public diplomacy are not persuasive in intent. One person's public broadcast is another's propaganda. Propaganda has a troubled relationship with liberal democracy, where the supposed freedom of choice by citizens is expected to influence politics and power structures (Irwin 1919); and, thus, the term tends be viewed negatively and more as something that an adversary does. This misuse of the term, coupled with a lack of general understanding for its meaning, make it unrealistic to use in policy circles for the problem-set at hand, despite its flexibility and better overall applicability.

While some definitions of propaganda are being updated to reflect changes in information communications technologies, they fail to address either the underlying broadness of propaganda or the pre-existing connotations. For example, Benkler, Faris and Roberts coined the concept of "network propaganda" as "the ways in which the architecture of a media ecosystem makes it more or less susceptible to disseminating persuasive messaging" (2018, p. 24). Wooley and Howard's "computational propaganda" considers "the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion." (2016, p. 4886). And, Wan-

less and Berk proposed "participatory propaganda" as a model that reflects the propagandist's ability to not just persuade a target audience to the propagandist's benefit, but also to co-opt them into engaging, adapting, and spreading propaganda themselves through tools such as social media (2019, in Press), which is their take on Jowett and O'Donnell's earlier definition. What most of these concepts of propaganda describe, however, is how propaganda works, not so much how it can be distinguished easily and at scale from other types of communication, particularly from that which is acceptable and that which is not.

Information Warfare

At its simplest definition, 'information warfare' is "a conflict or struggle between two or more groups in the information environment" (Porche *et al.* 2013, p. xv). Szafransky defines 'information warfare' as "hostile activity directed against any part of the knowledge and belief systems of an adversary" (1995). Finding an internationally accepted definition of information warfare has been a challenge (Munro 2004; Johnson 2007). Some countries, such as Russia, have openly defined it (Russian Ministry of Defence 2018), whereas the U.S. (U.S. Department of Defence, 2018) and NATO (2018a) have not. Existing Western definitions are varied, narrowly focusing on technology (Schwartau 1994; Ventre 2016) and cyber operations (Rattray 2001) with others emerging that speak more to influence operations (Libicki 1995; Darley 2006). Regardless, use of the term warfare lends an inherently militaristic and negative connotation to the term, suggesting it only occurs within the context of conflict, despite the fact that some countries, such as Russia, have stated that the shaping of the information environment can occur in peacetime as well (Russian Ministry of Defence 2011). Others still have questioned whether the use of information alone even constitutes as warfare, suggesting a misuse of the term in this context (Strachan 2006). Given the lack of universality in the term 'information warfare', the militaristic undertones, and a misleading notion that its practice is limited to open hostilities, the term 'information warfare' does not lend itself particularly well for use outside of specific areas of security policy.

Information Operations

As already noted, Facebook has been using the term 'information operations' to describe the phenomena of shaping the information environment. 'Information operations' is also a term used in military circles to describe

> the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (Joint Staff U.S. Army 2012, 2014, p. ix)

NATO in turn defines information operations as "a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives," whereas, "information activities are actions designed to affect information and or information systems. They can be performed by any actor and include protective measures" (2009).

The term 'information operations', like 'information warfare', is predominately used in a military context and thus has a militaristic connotation. The term 'information operations' is very little understood outside such circles (and arguably not well understood in some military ones). While there are opportunities in using a term not well known, it too could easily be associated only within the context of conflict and not be well-suited to communicating to a more general audience. Moreover, the very role of militaries in most liberal democracies is quite restrictive in nature, with missions clearly delineated by time, audiences, and geographies—all limitations which the global hyper-connectivity has shattered, which begs the question as to whether military terms are the best suited for understanding a more dynamic operating environment?

Influence Operations

A thread connecting many of these definitions together is an aim to influence by whoever is behind such activities. This has led some researchers to define such efforts as "information influence activities" or "the targeting of opinion-formation in illegitimate, though not necessarily illegal ways, by foreign actors or their proxies" (Pamment *et al.* 2018, p. 8), the very definition aiming to draw a distinction between that which is acceptable and that which is not. Legitimacy becomes a yardstick for distinguishing between the acceptable parts of the influence industry and those that make use of manipulation or intend to deceive. Drawing upon definitions developed by the Swedish government, influence operations are part of a hierarchy of activities conducted by foreign adversaries: influence activities (single use of illegitimate techniques); influence operations (multiple coordinated activities); and influence campaigns (multiple coordinated operations across the hybrid spectrum).

Authors at RAND took a broader view, defining influence operations as "efforts to influence a target audience, whether an individual leader, members of a decision-making group, military organizations and personnel, specific population subgroups, or mass publics". This concept was conceived as part of a toolbox for furthering "U.S. interests and objectives" and as such is "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and postconflict to foster attitudes, behaviors, or decisions by foreign target audiences" (Larson *et al.* 2009, p. 2).

As with propaganda and information warfare or operations, influence activities have been tied to the efforts of governments or militaries, suggesting if it is widely understood it, too, will come with connotations. For example, the Canadian Army promotes a unit under its 5th Canadian Division called "Information Activities" defined as "activities that are planned and conducted to have behavioural and psychological effects in support of the Commander's intent or mission," under which "key enablers" include Psychological Operations (2019), which itself is yet another term that has been used to describe the role of information in influencing target audiences (NATO 2018b). The definition of 'information activities' here is strikingly similar to others for propaganda, such as "the deliberate attempt to persuade people to think and behave in a desired way" (Taylor 1990, 2003, p. 6). This begs the question of why use a different term at all, except as already noted to euphemize what is deemed acceptable behaviour as it is done by one actor (us) and not another (them). Complicating matters further, NATO has moved towards an umbrella concept of

Strategic Communications, or "the coordinated and appropriate use of NATO communications activities and capabilities - Public Diplomacy, Public Affairs (PA), Military Public Affairs, Information Operations (Info Ops) and Psychological Operations (PsyOps), as appropriate – in support of alliance policies, operations and activities, and in order to advance NATO's aims" (2010, p. 1).

While those working in these various areas within 'strategic communications' might see distinctions, it can hardly be surprising that lay people and journalists struggle to see a difference and that there is such a proliferation and confusion of terms related to the use of information to influence.

Utility to policymakers

So far, we have considered the problem in terms of the *intent* behind communication; the *truth* of the communication; the *origin* of the communicating actor; and the *legitimacy* of the communication techniques used. Each part of the debate reveals conceptual problems. Existing terminology grasps many of these factors but is hampered by negative connotations. Laws in different countries mean that government institutions only have mandates on certain factors. Furthermore, analysing and attributing factors such as intent, truth, origin and legitimacy are prescriptive: one must suspect a problem in order to investigate further, which means that value judgments are made before evidence is collected. This does not render these factors useless to policymakers, but it does demonstrate significant challenges in producing a common terminology.

Nonetheless, it is possible to begin breaking down the terminology and assess which factors are treated. This can support a more considered assessment of the utility of the terms to policymakers, and at the very least enables terms to be ruled out. **Figure 2**, below, offers a breakdown of the terms and some of the main considerations. Clearly, some of these terms can be ruled out on the grounds that they are vague, pejorative, or are too one-dimensional: fake news, propaganda, information warfare, and information operations all lack core elements useful to forming policy. Mis- and dis-information clearly have some utility but lead analysis down the rabbit hole of whether an actor intends to lie or not. Influence operations seems to have the most potential; its most obvious point of departure from the others being its lack of focus on truth to instead focus on communication techniques. Problems remain, but these terms seem less problematic than comparable terms.

Conclusion

It is evident that more effort must be put into understanding the information environment and how information is used to influence target audiences. The growing number of overlapping terms is symptomatic of a weak understanding. Information is fundamental to democracy, which is a system that derives its legitimacy from the notion that voters are making informed decisions of their own free will. Human cognition, in terms of the ability of citizens to make informed choices, is thus a form of critical infrastructure in a democratic system. The use of information to influence people ultimately calls into question a target audience's ability to be reasonably and fairly informed – for instance, where is the line between unacceptable manipulation in communications and acceptable political discourse?

Term	Operative factors	Main considerations
Fake news Junk news	*Truth*: defines poor-quality, often untrue information	Emphasises democratic concerns Poorly defined Value-judgements on quality & legitimacy of content
Misinformation Disinformation	*Truth & intent*: defines circulation of untrue information by intent	Distinguishes between malign & innocent motivations Intent difficult to distinguish Many other factors ignored
Propaganda	*Intent*: defines circulation of information by objectives of propagandist	Widely used and recognised Pejorative Struggles to account for intent of public participants
Information warfare	*Intent & origin*: defines struggle over information and knowledge by adversaries	Captures a military angle Uses warfare as a metaphor
Information operations	*Intent*: defines planned, coordinated use of information	Describes techniques for influencing communication environment Militaristic connotations
Influence operations	*Intent, origin & legitimacy*: defines targeting of public opinion by foreign actors	Questions the legitimacy of techniques used Places information in broader hybrid context Difficult to assess & define

Figure 2: Overview of terminology and its main operative factors and considerations

There are clear challenges in adopting definitions for use in policy to address the shaping of the information environment. Terms that are not well-defined fail to provide clear guidance for those enforcing policies as well as the wider public in terms of being able to understand what is meant by these terms. Terms that aim to draw clear black and white lines between concepts of what is true and false run the risk of creating policies that are mired in subjectivity and are labour intensive to implement. Moreover, such policies are easily critiqued by those who find themselves on the condemned end of enforcement, using relativity as an argument. Rather than protecting democracy, there is the profound risk that large organised social groups find themselves disenfranchised based on poorly defined terminology.

Using intent to define who a legitimate actor is in shaping the information environment raises questions about how such motives are measured and how they may be achieved at scale. Nonetheless, there may be value in a broader public debate about what kinds of communication are acceptable and unacceptable from companies, politicians, citizens, and foreigners in different contexts. Equally problematic is the excessive focus on actors, when attribution is often the last piece of the puzzle in analysing how the information environment is shaped. This hinders the development of proactive measures. And finally, concepts that inherently attempt to delineate between bad and good run the risk of introducing value judgments on activities from the outset, before analysis has taken place. Such an approach introduces further risk of subjective assessment that might cause unintended consequences in international relations.

References

Bail, C, Argyle, L, Brown, T, Bumpus, J, Chen, H, Fallin Hunzaker, M, Lee, J, Mann, M, Merhout, F, and Volfovsky, A 2018, 'Exposure to opposing views on social media can increase political polarization', *Proceedings of the National Academy of Sciences* Aug 2018, 201804840; DOI: 10.1073/pnas.1804840115.

Benkler, Y, Faris, R, & Roberts, H, 2018, *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford: Oxford University Press.

Bering, J, 2012, *The Belief Instinct*, New York: W.W. Norton & Company, Kindle Edition.

Betz, D, 2015, *Carnage and connectivity: Landmarks in the decline of conventional military power*, C. Hurst & Co., London, UK.

Cambridge Dictionary 2008, Cambridge Advanced Learner's Dictionary: PONS-Worterbucher, Klett Ernst Verlag GmbH, DE.

Canadian Army 2019, 'Influence Activities,' viewed 15 July 2019 < http://www.army-armee.forces.gc.ca/en/5-cdn-div-ia/index.page>.

Darley, W 2005, 'Why Public Affairs is not Information Operations', *Army Magazine*, vol. 55, no. 1.

——2006, 'Clausewitz's Theory of War and Information Operations', *Joint Force Quarterly*. Issue 40, 1st Quarter 2006, pp. 73-9.

Dretske, F 1981, *Knowledge and the flow of information*, MIT, Cambridge, MA, US.

European Commission 2018, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions tackling online disinformation: a European approach COM/2018/236 final', viewed 15 July 2019, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018DC0236>.

E.U Committee on Foreign Affairs 2016, 'Report on EU strategic communication to counteract propaganda against it by third parties', European Parliament, Brussels, BE, viewed 21 April 2019, <http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html>.

Fallis, D 2011, 'Floridi on disinformation', Etica & Politica, vol. 13, no. 2, pp. 201-14. Facebook 2019, 'Community standards on integrity and authenticity', viewed 21 April 2019, <https://www.facebook.com/communitystandards/integrity_authenticity>.

Fetzer, J 2004, 'Disinformation: The use of false information', Minds and Machines, vol. 14, pp. 231-40.

Floridi, L 2009, 'Philosophical conceptions of information', Formal theories of information: From Shannon to semantic information theory and general concepts of information, ed. G Sommaruga, Springer-Verlag, Heidelberg, DE, pp. 13-53.

——2011, The philosophy of information, Oxford University Press, Oxford, UK.
Fox, C, 1983, *Information and misinformation*, Greenwood Press, Westport, CT, US.

Frické, M 1997, 'Information using likeness measures.' *Journal of the American Society for Information Science*, vol. 48, pp. 882-92.

Funke, D 2019, 'A guide to anti-misinformation actions around the world', Poynter Institute, viewed 21 April 2019, <https://www.poynter.org/ifcn/anti-misinformation-actions/>.

Garrison, WC 1999, 'Information operations and counter-propaganda: Making a weapon of public affairs', Army War College, Carlisle Barracks, PA, US.

Grice, P 1989, *Studies in the way of words*, Harvard University Press, Cambridge, MA, US.

Group of Seven 2018, 'Defending democracy–Addressing foreign threats', Global Affairs Canada, viewed 15 July 2019, <http://publications.gc.ca/site/eng/9.857739/publication.html>. Habermas, J 2018, *Philosophical introductions*, Kindle edn, Polity.

Irwin, W 1919, 'An age of lies: How the propagandist attacks the foundation of public opinion', *Sunset*, vol. 43, pp. 56-66.

Johnson, S 2007, 'Toward a Functional Model of Information Warfare', Center for Study of Intelligence, 14 April, viewed 12 September 2017, <http://bit.ly/2vSe5EA>.

Johnson, K 2018, "'The United States is under attack": Intelligence chief Dan Coats says Putin targeting 2018 elections', *USA Today*, viewed 15 July 2019, <https://goo.gl/hbUuiE>.

Joint Staff U.S. Army 2012, 2014, *Joint Publication 3-13: Information Operations*, viewed 26 October 2019, <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf>.

Jowett, G, & O'Donnell, V 2015, *Propaganda & persuasion*, Sage, Los Angeles, CA, US.

Kallberg, J and Rowlen, S 2014, 'African nation as proxies in covert cyber operations', African Security Review, vol. 23, no 3., pp. 307-11.

Karlova, N. & Lee, J 2011, 'Notes from the underground city of disinformation: A conceptual investigation', Proceedings of the ASIST 2011, viewed 15 July 2019, <https://goo.gl/dzffTL>.

Larson, E, Darilek, R, Gibran, D, Nichiporuk, B, Richardson, A, Schwartz, L, & Quantic Thurston, C 2009, 'Foundations of effective influence operations: A framework for enhancing army capabilities', RAND Corporation, viewed 15 July 2019, <https://www.rand.org/pubs/monographs/MG654.html>.

Lazer, D, Baum, M., Benkler, Y. Berinsky, A, Greenhill, K, Menczer, F, Metzger, M, Nyhan, B, Pennycook, G, Rothschild, D, Schudson, M, Sloman, SA, Sunstein, C, Thorson, E, Watts, D, Zittrain, J 2018, 'The science of fake news', *Science*, vol. 359, pp. 1094-6.

Legal Information Institute 2018, 'Foreign national'. *Cornell Law School*, viewed 15 July 2019, <https://www.law.cornell.edu/wex/foreign_national>.

Lewis, JA 2016, 'Rethinking deterrence: New paradigms for deterrence strategy', Brzezinski Institute on Geostrategy, Center for Strategic and International Studies.

Libicki, M 1995, 'What is information warfare?', Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, Washington, DC, US.

Mahon, JE 2007, 'A definition of deceiving', *International Journal of Applied Philosophy*, vol. 21, no. 2, pp. 181-94.

Moloney, K 2006, *Rethinking public relations: PR propaganda and democracy*, Routledge, Abingdon, UK.

Munro, I 2004, *Information warfare in business: Strategies of control and resistance in the network society*, Routledge, Milton Park, UK.

NATO 2009, *Allied Joint Doctrine for Information Operations, AJP-3.10*, November.

——2010, *NATO military concept for strategic communications*, viewed 15 July 2019, <https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf>.

——2018a, 'NATOTerm: The official NATO terminology database', viewed 18 November 2018, <https://nso.nato.int/natoterm/Web.mvc>.

——2018b, 'NATO military policy for information operations, Draft MC 0422/6', viewed 15 July 2019, <https://shape.nato.int/resources/3/images/2018/upcoming%20events/MC%20Draft_Info%20Ops.pdf>.

New York Times 2019, 'Russian hacking and influence in the U.S. election', viewed 15 July 2019, < https://www.nytimes.com/news-event/russian-election-hacking>.

Pamment, J, Nothhaft, H, Agardh-Twetman, H &Fjällhed, A 2018, 'Countering information influence activities: The state of the art', Department of Strategic Communication, Lund University, Lund, SE.

Porche, I, Paul, C, York, M, Serena, C, & Sollinger, J 2013, 'Redefining information warfare boundaries for an army in a wireless world', Rand Corporation, viewed 15 July 2019, <https://www.rand.org/pubs/monographs/MG1113.html>.

Rattray, G 2001, *Strategic warfare in cyberspace*, MIT, Cambridge, MA, US.

Russian Ministry of Defence 2011, 'Conceptual views on the activities of the armed forces of the Russian Federation in the information space', viewed 14 October 2017, <http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle>.

——2018, 'Information warfare', *Military encyclopaedic dictionary*, viewed 20 November 2018, <http://encyclopedia.mil.ru/encyclopedia/dictionary/details.ht-m?id=5211@morfDictionary>.

Rutschmann, R, and Wegmann, A 2017, 'No need for an intention to deceive? Challenging the traditional definition of lying', *Philosophical Psychology*, vol. 30, no. 4, pp. 438-57.

Scarantino, A, and Piccinini, G 2010, 'Information without truth', *Metaphilosophy*, vol. 41, pp. 313-30.

Schwartau, W 1994, *Information warfare: Chaos on the electronic superhighway*, Thunder's Mouth Press, New York, NY, US.

Silverman, C 2015, 'Lies, damn lies and viral content', Tow Center for Digital Journalism, viewed 15 July 2019, <https://academiccommons.columbia.edu/doi/10.7916/D8Q81RHH>.

Strachan, H 2006, 'The changing character of war', Europeaum Lecture, 9 November 2006, the Graduate Institute of International Relations, Geneva, CH, viewed 15 July 2019, <https://bit.ly/2qN3Sbi>.

Szafranksy, R 1995, 'A theory of information warfare', *Airpower Journal*, Spring 1995, viewed 13 September 2017, <http://bit.ly/2jlTQxh>.

Taylor, P 1990/2003, *Munitions of the mind: A history of propaganda from the ancient world to the present day*, Manchester University Press, Manchester, UK.

Thomas, T 2016, 'Cyber/Information Deterrence: How does China Understand the Concept?', Digital.Report, viewed 28 September 2017, <http://bit.ly/2xQIKW7>.

Thornton, R 2015, 'The changing nature of modern warfare', RUSI Journal, vol. 160, no. 4, pp. 40-8.

US Department of Defense 2018, 'DOD dictionary of military and associated terms', viewed 18 November 2018, <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pd-f?ver=2018-09-28-100314-687>.

Van der Putten, FP, Meijinders, M & Rood, J 2015, 'Deterrence as a security concept against non-traditional threats', *Clingendael Monitor*, p. 17.

Ventre, D 2016, *Information warfare*, John Wiley & Sons, Hoboken, NJ, US.

Wanless, A and Berk, M 2019, in press, 'The audience is the amplifier: Participatory propaganda', *The SAGE handbook of propaganda*, eds. P Baines, N O'Shaughnessy & N Snow, Sage, London, UK.

Weedon, J, Nuland, W, and Stamos, A 2017, *Information operations and Facebook*, Facebook, viewed 15 July 2019, <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-infor-mation-operations-v1.pdf>.

Wooley, S & Howard, P 2016, "Automation, algorithms, and politics| Political communication, computational propaganda, and autonomous agents—Introduction', *International Journal of Communication*, vol. 10, pp. 4882–90.

Zhou, L & Zhang, D 2007, 'An ontology-supported misinformation model: Toward a digital misinformation library', *IEEE Transactions on Systems, Man, and Cybernetics--Part A: Systems and Humans*, vol. 37, no. 5, 804-13.