Journal of Information Warfare

Volume 18, Issue 1
Winter 2019

Contents

Journal of Information Warfare

Published by
Peregrine Technical Solutions, LLC
Yorktown, Virginia, USA

Print Version
ISSN 1445-3312

Online Version
ISSN 1445-3347

Understanding and Assessing Information Influence and Foreign Interference

M Hammond-Errey

School of Humanities and Social Sciences
Faculty of Arts and Education
Deakin University
Geelong, Australia

Email: m.hammonderrey@deakin.edu.au

Abstract: *The information influence framework was developed to identify and to assess hostile, strategy-driven, state-sponsored information activities. This research proposes and tests an analytical approach and assessment tool called information influence and interference to measure changes in the level of strategy-driven, state-sponsored information activities by the timeliness, specificity, and targeted nature of communications as well as the dissemination tactics of publicly available information. The framework also offers the opportunity to identify possible or unlikely strategic intents and to assess the level of information influence and interference achieved by adversaries.*

Keywords: *Information Influence, Interference, National Security, Information Warfare, Disinformation, Intelligence Assessment, Information Activities, Influence, Information Effects*

Introduction

There are many existing theories, grand strategies, and conceptual frameworks for waging war and conceptualising the role of information in warfare from Sun Tzu to Clausewitz. Whilst there are many military theories on information and warfare (Tulak 2015; Libicki 1995; Shapiro 1991; Thomas 1997), there is no comprehensive approach that situates, contextualises, and assesses information influence and interference—or the information advantage gained as a result of state-sponsored, strategy-driven information campaigns. Absent from the academic scholarship to date has been rigorous testing and validation of analytical frameworks to understand and to explore the strategies and tactics of information influence and interference and dominance driven by state-based, power-projection goals. Without a comprehensive theory of how information—particularly in the public domain—is used to influence and to affect grand strategy and to obtain strategic advantage, it is difficult to discern and to establish the practices of adversaries. The information warfare threat itself has moved from being primarily a military to also a societal concern. This means that a foundational theory of information influence and interference is necessary to gather baseline information, to discern information influence and interference activity, to identify changes, to assess threats, and to respond effectively.

This paper presents a theoretical framework of information influence and interference that has been developed to identify and to understand strategy-driven, state-sponsored information activ-

ities, and an assessment tool to help assess them. The central tenet of information influence and interference is to understand and assess the activities and techniques used to gain an information advantage to exploit the weaknesses of an adversary. This paper focuses on the influence of information predominantly, but not exclusively, occurring in the public domain, embeds these ideas and practices within military theory, and proposes an assessment tool. Further, it tests the theory's ability to establish and to explain the phenomena of information influence and interference by application to Russian information activities in Crimea, Eastern Ukraine (including relating them to the downing of MH17). While the concept is designed to assess information influence and interference from an adversarial strategic threat and advantage perspective, it is possible that the concept could also be applied in reverse, as a basic tool to better understand delivering information effects.

Need for a Theory on Information Warfare

The value of information to military operations has long been acknowledged as crucial to success (Shapiro 1991; Libicki 1995). Historically, there are a wide range of approaches to information warfare, deeply rooted in specific time periods (WW1, WW2, the Cold War and its related conflicts) as well as in historical approaches (such as Russia, US, UK, and China). These concepts are predominantly contained within different and often niche military doctrine. Further, none of the existing approaches fully explains information influence and interference as it can be applied and discerned in contemporary international relations and military strategy (Hammond-Errey 2016). The use of information in warfare is known by a range of terms relating to a myriad of concepts, approaches, and actions used in the East and West. These terms largely describe the tactics, strategies, and roles associated with the use of information. They include Western notions of the 'Information Environment' (Tulak 2015), 'Information Operations' (NATO Military Committee 2014; Dick & Muñoz 2015; Kuehl 2004; Patrick 2006; Tatham 2013),'Information Warfare' (Bishop & Goldman 2003; Nimmo and Lucas 2015; Shapiro 1991; Thomas 2000; Thomas 2004a; Williams 2010; Libicki 1995), 'Information Activities' (Chief of Joint Operations 2013), 'Hybrid War' (Bjerregaard 2012; Hoffman 2009; Tulak 2015), 'Gray Zone Warfare' (Chambers 2016; Echevarria 2016; Hoffman 2016; Mazarr 2015), and 'strategic communications' (Lange-Ionatamishvili & Svetoka 2015; NATO 2015; Schoen 2012; Tatham 2015). Russian information warfare theory has a long history and is derived from special propaganda (spetspropaganda) theory, disinformation (dezinformatsia), and reflexive control. Spetspropaganda is psychological and propaganda warfare that was used under Stalin but disappeared briefly in the 1990s when it was removed from the Russian military curriculum to be reintroduced in 2000 (Darczewska 2014). Disinformation, according to Russian geopolitical expert Igor Panarin, is the; '"spreading [of] manipulated or fabricated information (or a combination thereof)'" (Darczewska 2014). The Russian word dezinformatsiya is somewhat more inclusive: 'it includes all deception except camouflage' (maskirovka) (Greenberg 1982). Holland (2006) described disinformation as operations aiming at pollution of the opinion-making process in the West. However, there are also other conceptualisations, such as China's 'Three Warfares' (Thomas 2001; Thomas 2015a; Pomerantsev 2015) as well as non-national approaches, particularly by terrorist groups (Nissen 2015b; Ingram 2015).

Despite the many existing theories, understanding information warfare remains an analytical minefield (Hammond-Errey 2016). The variety in these terms in many ways reflects the complexity of a field that encompasses projections of national power as well as covert and overt activities, and defines nation-state responses to state, intrastate, and non-state violence. It is an example of how

nations comprehend and express their national security, as well as the utility and application of armed force in international affairs, not to mention the broader achievement of foreign policy outcomes. None of the existing approaches fully considers both the cognitive impact and relationship to kinetic effects of state-sponsored, strategy-driven information campaigns, nor do they provide a mechanism by which to consider information influence and interference as a whole. In short, these approaches do not encompass the full scope, depth, and breadth of information activities on the contemporary geopolitical stage.

Thus, there is a need for theory on information warfare activities that occurs solely outside of the military realm and encompasses two environmental shifts: the trend towards the blurring of the line between war and peace (Hoffman 2009; Hoffman 2016; Mazarr 2015; Giles 2016e) and the shift of conflict into the public domain (Hammond-Errey 2016). The expeditious development of technology has dramatically changed the information environment and the role of information in society (Reynolds 2016). Rapid digitisation, increased connectivity, and reliance on the Internet as well as shifts in the way people communicate, build relationships, and trust (Boyd and Crawford 2012; Kitchin 2014b; Kitchin 2014a; Metzger and Flanagin 2013; Rubin et al. 2014) have increased the impact and effectiveness of hybrid and information warfare techniques and thus their relative value to academic study. It is highly likely that many of these factors are encouraging the shift towards 'grey zone' and hybrid warfare. This shift drives a key component in the concept of information influence and interference: information activities are strategically aligned with military activity occurring covertly at any point on the spectrum of conflict.

Introducing *Information Influence and Interference*

The *information influence and interference* concept was ultimately developed because the existing theories on information warfare were unable to adequately explain Russian information warfare operations, especially large-scale disinformation campaigns. The public nature of this activity requires acknowledgement and consideration outside of a military context alone. *Information influence and interference* is a theoretical framework that identifies, conceptualises, and assesses the impact of state-sponsored, strategy-driven information activities and campaigns designed to influence or interfere in another nation state. This foundational theory is necessary to baseline information, discern *information influence and interference* activity, identify changes, assess threats, and respond effectively in the contemporary information environment. Additionally, there is a need for more specific theory on the role of information warfare activities that occur in the public domain, outside of the solely military realm.

The central objective of *information influence and interference* is to gain an information advantage to exploit the weaknesses of an adversary. *Information influence and interference* is informed by intelligence collection and analysis—as well as by planning, command, and policy considerations—and can occur anywhere on the spectrum of war and peace. It acts as a projection of power (along with military, diplomatic, and economic pressure) and is integrated, coordinated, and intended to operate as an arm of coercion-deterrence. Schelling (2008) offers a formative and significant overview of compellance (forcing someone to do something) and deterrence (keeping them from doing something). Coercion-deterrence within the cyber context can be seen in Hawkins and Nevill (2016) and Lupovici (2011). Focusing on Russia, Thomas (1997) defines deterrence against information assault, while Echevarria (2016) considers coercion-deterrence within the grey zone context. *Information influence and interference* is not confined to an instance or to an individual

activity of information operations but is a part of a multi-faceted strategy to overcome an adversary's superiority in another (military) domain and/or is a part of a coordinated approach to achieve a certain nation state's power-projection goal. Contemporary warfare is generally considered to occur within five domains: outer space, cyber-space, land, sea, and air with information vital to each (Dupont 2015). Increasingly, however, the 'human domain' is being included (Selhorst 2014; Tatham 2015). Because *information influence and interference* is about gaining an advantage to exploit adversary weakness, the concept incorporates cyber warfare (attacks, theft, and intrusions) as a technical representation of *information influence and interference*, while noting that it is the information itself which is important. This activity sits on a spectrum of *information influence and interference*, towards the end of foreign interference. The advantage from cyber operations in this context comes from the release of such information to support the strategy. An example of this can be found in the release of U.S. diplomatic phone conversations regarding Ukraine (Gearan 2014). This distinction is crucial, as the future of exploiting *information influence and interference* over an adversary is not likely to rest solely in public information campaigns that affect cognition or kinetic operations, but rather will be illuminated through the intersections between intelligence and public information.

Information Influence and Interference Assessment Tool

The *information influence and interference* assessment tool draws on the concept outlined above to conceptualise and to assess the impact of state-sponsored, strategy-driven information campaigns. These can be private and public campaigns, and include activity directed at decision makers (for instance, reflexive control) or, much more broadly, at whole populations. *Information influence and interference* campaigns do not necessarily have to be state-sponsored; however, that is the focus of this assessment tool. The assessment tool helps analysts measure changes in activities by the timeliness, specificity, and targeted nature of communication as well as by the dissemination tactics used for manipulating masses of people through publicly available information. It provides an objective means to discern, understand and explain the advantage gained through tactics of mass communication and the strategic use of information in the public domain in pursuit of foreign policy goals. *Information influence and interference* encapsulates communications driven by government (primarily military) strategy including information effects and public communication, disinformation, and (strategic) silence. These communication activities target a specific audience, with a specific message at a particular time to achieve a specific goal (or series of goals)—influencing that audience's behaviour—and, as a result, achieve a level of *information influence and interference* or, when combined with covert methods, achieve a level of foreign interference. This can be seen in **Figure 1**, below. The intent is to achieve a strategic advantage over an adversary, although success is dependent on the ability of the entity being attacked to mitigate the threat of *information influence and interference*.

The *information influence and interference* assessment tool discerns the level of influence on a spectrum, from low influence to extreme influence—or foreign interference. It provides robust measures of timeliness, specificity, and targeting, combined with the level of integration with strategy along with dissemination tactics applied to publicly available information. This establishes a baseline and can then be used to identify changes in the level or intensity of strategy-driven, state-sponsored information activities. The first stage in assessing *information influence and interference* is to identify the information tactics—that is, how the information is disseminated to

audiences. The second stage is to assess the changes in the timeliness, specificity, and targeted nature of communications. The third stage—covered only briefly in this paper—is to identify possible strategic intents and to dispel them. These factors combine to assess an overall *information influence and interference* level. Timeliness includes the time and date of a communication and is often strategically relative to other events. The specificity of the message includes the type and method of communication and how it is transmitted (the mode of communication). Specificity also includes the level of detail in the message, including source, language, and content, as well as message substance. The target component refers to the likely audiences for which it is intended and includes their possible span of control–or potential audience behaviour, actions, and decisions. Span of control is a term developed by this author to refer to potential actions of the intended audience. Included here is the span of control—or potential behaviour, actions, and decisions or ability to influence these of the target audience. Span of control is a term that is useful to understand in terms of reflexive control; strategic intent; and the relationship between information, influence, and action. This includes how the message is targeted as well as how targeted the message is. A practical guide to assessing *information influence and interference* is discussed in this paper.

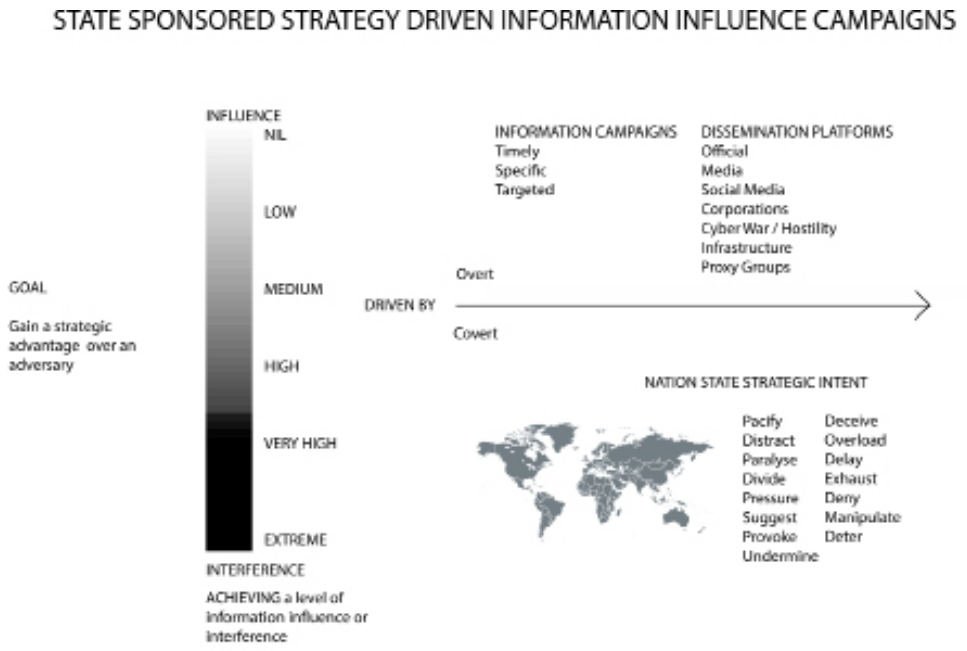

Figure 1: Information influence and interference

The *information influence and interference* assessment tool is intended to drive analysts towards improved (and earlier) identification of adversary information warfare, cyber-attack, and covert influence activities across a range of platforms. The aims of this are to increase the speed and richness of threat and intelligence assessments, to drive policy and operational decision-making, and ultimately to reduce the strategic advantage it affords an adversary. The *information influence and interference* assessment tool is not intended to assess the truthfulness of communication or to prove truthfulness of information—or disinformation. Considerable efforts continue to be devoted to identifying, assessing, and disproving disinformation, which will provide sufficient resources

for academics and analysts (see Pomerantsev 2016; Shawcross 2016; and the Legatum Institute's *Beyond Propaganda* series). Further, the truth is not necessarily a crucial component of *information influence and interference* because the goal is not to inform, but to influence and change behaviour. Unlike other analytical approaches, the *information influence and interference* concept is used to assess the total information advantage obtained through all aspects of state-sponsored, strategy-driven, public communications. It is intended to improve understanding and assessment of adversary strategic intent—or objectives—and level of integration and coordination to provide an overall level of *information influence and interference*. The level of strategic advantage gained is not easily assessable without understanding the threat posed and the ability of the nation state attacked to mitigate that threat.

Information influence and Interference Assessment Tool and Strategic Intent

To date, one of the major challenges for scholars and practitioners has been the ability to link strategic intent to information effect. Strategic intent refers to the objectives (or series of multiple objectives) to which the techniques and tactics are deployed to achieve an impact or effect. **Table 1**, below, is a preliminary attempt to describe some of the possible strategic intents.

Strategic Intent	Impact/Effect/Span of control
Deceive	Force reallocation of resources through deliberate misleading
Overload	Send large volumes of information, often conflicting
Delay	Prevent timely delivery of messages or capabilities to delay opponents' decision-making
Exhaust	Compel an adversary to expend unnecessary energy prior to engagement
Deny	Restrict information access to opponent in order to frame perspective
Manipulate	Engineer markets, systems, and popular opinion or otherwise compromise their integrity
Deter	Create the perception of an insurmountable threat or obstacle
Pacify	Reduce vigilance by quelling anticipation of threats and offensive activity—for example, leading an adversary to believe that pre-planned operational training is occurring (rather than offensive preparation)
Distract	Create a real or imaginary threat, issue, or challenge to prevent an adversary from concentrating on the target's actions or threat
Paralyse	Partly or wholly incapacitate adversary movement by creating perception of a specific threat to a vital interest or by exploiting vulnerabilities
Divide	Convince a nation state to operate in opposition to alliance interests
Pressure	Persuade or intimidate an adversary into action contrary to their national interests
Suggest	Proffer information or engage in intrusion activity that affects an adversary legally, morally, ideologically
Provoke	Force adversary into offensive action advantageous to the target
Undermine	Discredit adversary government to own population in order to erode confidence

Table 1: Strategic intent (mechanisms of reflexive control using information)

Consistent with a broader military strategy, there are likely to be smaller components—or multiple

strategic intents—to an end-state and its supporting objectives. Sometimes these are called lines of effort. Some aspects of strategic intent will be highly planned, and others will be opportunistic and reliant upon the operators in the field. Some will work quickly and others slowly—and some not at all. Strategic intent is a term the author developed to encapsulate military and communication objectives that are strategy-driven and incorporate aspects of reflexive control and perception management. It is drawn from military strategy as well as business management and communications theory. Reflexive control as defined by Thomas (2004a; 2015a) is a means of conveying information to an opponent that is specially prepared to incline them to voluntarily make a predetermined decision desired by the initiator. It is raised here as a key component of strategy and integration. Reflexive control is a crucial component of the Russian approach to disinformation and broader information operations; hence, it is so important to understand this in relation to tactics as well as timeliness, specificity, and targeting. The author has adapted existing work on reflexive control, hybrid warfare, and cyber warfare into **Table 1**, above, to help readers understand and conceptualise strategic intent by categorising overall strategic intent and the potential impact or effect. It is heavily reliant on the notion of reflexive control (from Selhorst 2016, p. 152; Thomas 2011, pp. 129-130) and perception management, but it also draws on cyber warfare and information warfare material (Bishop and Goldman 2003, p. 124) to identify key strategic goals that public information campaigns (and disinformation) are intended to support and that ultimately assist in the identification of a broad strategy or goal (Paul 2011). Assessment of these goals occurs at the final stage of the *information influence and interference* assessment tool process; however, it is very valuable to understand them throughout the process.

Application of the *Information Influence and Interference* Assessment Tool

The *information influence and interference* assessment tool measures changes in the level of strategy-driven, state-sponsored information activities by the timeliness, specificity, and targeted nature of communication as well as by the dissemination tactics of publicly available information. The first stage in assessing *information influence and interference* is to identify the information tactics—that is, how the information is disseminated to its audience. For the purposes of this assessment, it is not necessary to distinguish truth within the information streams—although identifying clear disinformation and falsehoods is advantageous. The second stage is to assess the changes in the timeliness, specificity, and targeted nature of communications. The third stage is to identify possible and to dispel unlikely strategic intents. The final stage is to assess the level of *information influence and interference*.

The assessment tool

- Provides a baseline for public information campaigns,
- Highlights key military and social effects,
- Aggregates effects and overall effectiveness in achieving stated objectives,
- Helps collate quantitative and qualitative data,
- Shows shifts in public information campaigns,
- Highlights where to focus advanced analytics and analyst resources, and

- Provides a cost-benefit analysis of the potential advantages gained through the strategy and tactics of mass communication in pursuit of foreign policy goals.

Again, timeliness includes the time and date of a communication and is often strategically relative to other events. The specificity of the message includes the type and method of communication and transmission (that is, its mode of communication). Specificity also includes the level of detail in the message, including source, language, and content, as well as message substance. The target component refers to the likely audiences for which the message is intended and includes their possible span of control—or potential audience behaviour, actions and decisions. This includes how the message is targeted as well as how targeted the message is.

Assessment Tool—Information Tactics

To achieve a desired impact and overall *information influence and interference*, it is necessary to engage in public information campaigns using specific tactics to disseminate information and disinformation. This section identifies the techniques and categorises them into key *information influence and interference* tactics used to achieve strategic goals, which operate like a toolbox of available collection, analysis, decision-making, and communication tools needed to achieve dissemination of public information in line with strategic intent. This can be seen in **Table 2**, below. The tactics represent the key methods of dissemination of public information and disinformation intended to inform and to influence. To identify whether the release of disinformation is strategy driven, it is necessary to analyse the tactics of dissemination using specifically selected information sources, methods of communications, release on multiple platforms, and integration with kinetic operations. The most distinctive features of contemporary disinformation are high-volume and multichannel as well, as rapid, continuous, and repetitive.

The unassailable core of strategic communications is to inform, influence, and persuade domestic, foreign, and adversary audiences in pursuit of policy objectives. In the case of disinformation, there is an additional requirement—an intent to deceive or dis-inform—which distinguishes it from misinformation (or even accidental communication of false information). The selection of tactics is driven by the strategic intent and desired goals and often includes consideration of the information source (both how the information was obtained and the public attribution of information source), the method of communication, the platforms through which information is disseminated, and the overall interface between information warfare and cyber warfare.

In a nutshell, this paper argues that changes in the level of strategy-driven, state-sponsored information activities can be measured by the timeliness, specificity, and targeted nature of communication as well as by dissemination tactics. The *information influence and interference* concept includes measures of timeliness, specificity, targeting, as well as the level of integration and strategy which can be understood by analysing tactics of disinformation.

Targeting

Targeting refers to the likely audiences for whom information is intended and includes an understanding of their potential audience behaviour, actions, and decisions—span of control. Span of control is useful to understand in terms of reflexive control, strategic intent, and understanding the relationship between information, influence, and action. The targeting of a communication can be

Platform of Dissemination	Tactic of Release	Narrative and Results of Analysis of Targeting, Timeliness and Specificity
Official Release (and Silence)	Press Conference/Release	
	Official Statements	
Media	Television & Video	
	Radio & Audio	
	Print	
	Online Media & Multimedia	
	Information Sources and Framing Traditional Media Discussions	
Corporations	Information Release	
Social Media	Official Accounts	
	Trolling and Botnets (Paid Comments, Social Media Rumours, and Fake Accounts)	
Cyber Attack	Intrusion/Attack/Theft of Information	
Infrastructure	Telecommunications Energy Elections	
'Grassroots' Groups or Organisations	Funding, Agitating, or Supporting Groups of Cultural, Political, and Social Natures	

Table 2: Information influence and interference tactics

connected to the timeliness as it can highlight whom is being targeted and what the intended or desired outcome is—especially on more specific communications that influence actors (the audience) to think, act, or decide something in a certain way.

The targeting metric includes the analytics of message targeting as well as how targeted the actual communication is. There is currently a gap in the scholarship with respect to how nation states target disinformation audiences; and while this research contributes to the scholarship, it is a subject worthy of further study. Factors that further research should address include

- [LANGUAGE] Which language(s) is this communication (or group of communications) in?
- [AUDIENCE] Who is the intended audience(s) for this communication (or group of communications)?
- [AUDIENCE SPAN OF CONTROL] What is the span of audience control/behaviour of the intended audience(s) for this communication (or group of communications)?
- [TARGETING] How focused or well targeted is this communication (or group of communications)?

- [TARGET ANALYSIS] How is the communication (or group of communications) targeted to the audience (the analytics of targeting)?

Specificity

Specificity is a crucial metric of *information influence and interference* measurement because it includes the tactics of communication and how they are transmitted. Specificity also includes the level of detail in the message, including content and message substance as well as alignment with known disinformation narratives. This detail can range on a spectrum from broad 'distrustful Internet' to narrow—such as very specific counter claims and fake reports and/or sources. 'Distrustful Internet' refers to oft-stated, Russian strategic intents to create an Internet that global citizens do not trust (Pomerantsev and Weiss 2014) and to sow discord. Specificity is an important diagnostic measure in *information influence and interference* due in part to recent improvements as well as increased access to technology. These improvements in the specificity of messaging include efforts across single communications and across entire campaigns. Further, they include enhancements in the nuancing of key messages, increased use of narratives, and increased number of multi-channel dissemination platforms. Additionally, specificity is deeply connected to other metrics, including tactics used, timeliness, an understanding of the audience (targeting), as well as strategy and integration. The factors needed to assess specificity include

- [DISSEMINATION MEANS AND TACTICS] How is this communication (or group of communications) transmitted (means) and why (tactics)?
- [SUBSTANCE] Where does this communication (or group of communications) sit on the spectrum of message content and substance (broad—'distrustful Internet'—to narrow)?
- [LEVERAGE] Does this communication (or group of communications) engage with or leverage off other events?
- [DETAIL] What level of detail is included in this communication (or group of communications)?
- [SOURCES] What information sources are included in this communication (or group of communications)?
- [NARRATIVE] Does the narrative of this message align with known disinformation narratives?

Timeliness

The timeliness of a message includes when a communication is disseminated and can be relative to other events. Timeliness is crucial in communications' being understood by the receiver especially when the intention of a communication is to influence actors (referred to here as the audience) to think, act, or decide in a certain way. Timeliness, when considered in conjunction with the specificity and targeted nature of the communication, can be a diagnostic indicator of the level (and type) of intelligence collection as well as the overall strategy. While its value should not be overstated in isolation, timeliness (along with specificity and targeting) can offer insight into and can potentially narrow the scope of possible adversary strategic intent by excluding possibilities based on the timing of communications. Timeliness also provides insight into the extent of intelligence collection (covert, overt, cyber activity) as well as the resourcing occurring to inform strategic decision-making. Factors to assess timeliness include

- [INFLUENCE] Does the time and date of a piece or group of communications enable influencing actors (the audience) to think, act, or decide something in a certain way?
- [RESPONSIVENESS] Are the time and date of this communication relative to or responsive to events?
- [TIMING] Does the timeliness of this communication indicate intelligence collection or kinetic activity?
- [SCOPE OF INTENT] Does the timeliness of this communication broaden or narrow the scope of the strategic intent?

Timeliness is not an isolated measure; in fact, much can be gained from the consideration of 'groups' of messages—that is, those that share a common narrative or those which are intended to engage the audience or specific actors and inform their behaviour. Timeliness of disinformation can provide insight into the extent and type of intelligence collection undertaken and can act as an enabler of action, supporting military objectives and kinetic operations.

Using the matrix set out in **Table 2**, above, the first stage in assessing *information influence and interference* is to identify the information tactics—or how the information is disseminated to its audience. The second stage is to assess the changes in the timeliness, specificity, and targeted nature of communications using the factors proposed above. The third stage is to identify possible and dispel unlikely strategic intents and form the list. The final stage in the current assessment tool process is to assess the level of *information influence and interference* as low, medium, high, very high, and extreme.

Applying *Information Influence and Interference* to Contemporary Russian Operations

Russia is a particularly interesting and informative case study to understand the application of *information influence and interference* because it has a long and public history in the use of denial, deception, and information operations. The *information influence and interference* concept was developed because existing analytical approaches were not comprehensive enough to explain Russian operations in 2014 and 2015. This researcher initially proposed and tested the *information influence and interference* assessment tool on Russian operations in Crimea, Eastern Ukraine, and the downing of MH17. The results demonstrated that the approach is a robust and sound method of assessing public information campaigns. Additionally, the test illuminated the increasing intersections between intelligence activities and publicly available information, or what can be referred to as an evolving nexus between covert and overt.

Information—and disinformation—activities form a central pillar of Moscow's approach to statecraft, influence, and conflict (Blank 2011; Giles 2016d; Giles 2009; Thomas 2001; Kofman 2015) and have been considered a staple of Russian operations since at least the Cold War (Darczewska 2015; Giles & Monaghan 2014; Krēķis 2015; Mazarr 2015; Thomas 2014; Franke 2015). Russia has been at the forefront of the field since then (Giles et al. 2015; Giles 2015b; Renz & Smith 2016; Thomas 2004b; Thomas 2015b; Thomas 2011; Thomas 2000; Thomas 2004a) and is arguably the most advanced nation in relation to information warfare, particularly in its use of disinformation (Bartles 2016; Galeotti 2016; Giles 2016b; Giles 2016a; Thomas 2015c). Drawing on its long historical practice, Russia has adapted to using new technologies, both conceptually and tactically

(Bartles 2016; Darczewska 2015; Galeotti 2016; Nissen 2015b; Mazarr 2015; Selhorst 2016).

Blank (2011), Nissen (2015b), and Thomas (2000, 2011) concur that Russian military experts have conceived of a single global information space emerging since the late 90s and that dominance of that space would allow a country to exploit this space to alter the global balance of power. Consistent with these assessments, Russian Chief of General Staff, Valeriy Gerasimov, noted the increasingly significant role of 'non-military measures' in warfare generally. He indicated that they occur in Russian Federation operations at a rate of 4:1 over military measures (Thomas 2015c). Since 2014, Russian *information influence and interference* capability has progressed in sophistication (Giles 2016d; Giles 2016e; Giles 2016a; Nimmo and Lucas 2015; Fedchenko 2016) and has escalated in deployment so rapidly that the Russian Federation is now engaging in information provocation towards opponents, predominantly NATO members and especially the U.S. (Calha 2015; Meister 2016; Ştefănescu 2015; Giles 2016e).

Russian disinformation campaigns employed in Crimea, Eastern Ukraine, and in the downing of MH17—as set out in **Figure 2**, below—reveal an increase in the volume and sophistication of information operations in the public domain. This research assessed a variety of dissemination strategies used by Russia to achieve an information advantage, highlighting in all three case studies that communications on social media, official statements, and cyber-warfare were key, as was the coordination of narratives. Ultimately, this research highlights changes in the level of strategy-driven, state-sponsored *information influence and interference* which can be measured by the timeliness, specificity and targeted nature of communications as well as dissemination tactics. The full analysis cannot be covered in this paper, so a short synopsis is outlined below. The same analysis has subsequently been applied to other incidents, such as U.S. presidential elections and the poisoning of Sergei and Yulia Skripal in the UK.

Crimea

In February and March 2014, following the removal of Ukraine's pro-Moscow President Viktor Yanukovych, the Russian Federation militarily supported and encouraged Crimea's largely ethnic Russian population to 'declare independence' from Ukraine. Russia's occupation of Crimea began with a mix of hybrid warfare tactics: use of covert forces, an extensive disinformation campaign, as well as electronic warfare. Russia's airborne, naval, infantry, and motor rifle brigades were also employed (Kofman & Rojansky 2015). The annexation of Crimea could be seen as a turning point in modern successful Russian military operations which exploited *information influence and interference*, considered the first contemporary Russian use of cyber warfare and information operations alongside conventional military activity (Snegovaya 2015; Giles 2014; Giles 2016b). The annexation of Crimea also indicated that Russian military developed a 'feedback' loop to improve tactics and coordination efforts from operations in South Ossetia (NATO 2015; Giles & Monaghan 2014; Thornton and Karagiannis 2016). Timeliness in this instance acted as an enabler of action—supporting military objectives and kinetic operations to enable 'elections' to take place. The specificity of the narratives varied, and Russia actively engaged with key audiences on different mediums, often concurrently, with messages designed to influence behaviour. Western audiences were targeted with English messages at a very high level (including directly from the President) (Darczewska 2014; Giles 2016c) incrementally acknowledging involvement of 'Little Green Men'—later admitted to be Russian State forces occupying airports and military bases in

Crimea. In contrast, Russian forces effectively controlled the targeting of local messages through control of telecommunications capabilities (Giles 2016e; Nissen 2015b) as well as media, TV, and radio in particular (Nissen 2015b; Nissen 2015a; Giles 2016d; Giles 2016c; Snegovaya 2015). Additionally, they used local social media campaigns referring to the soldiers as polite people and encouraging support for their presence (Nimmo and Lucas 2015; Darczewska 2014; Snegovaya 2015; Szwed 2016).

Platform of Dissemination	Tactic of Release	Narrative and Results of Analysis of Targeting, Timeliness and Specificity
Official Release (and Silence)	Press Conference/Release	
	Official Statements	
Media	Television & Video	
	Radio & Audio	
	Print	
	Online Media & Multimedia	
	Information Sources and Framing Traditional Media Discussions	
Corporations	Information Release	
Social Media	Official Accounts	
	Trolling and Botnets (Paid Comments, Social Media Rumours, and Fake Accounts)	
Cyber Attack	Intrusion/Attack/Theft of Information	
Infrastructure	Telecommunications Energy Elections	
'Grassroots' Groups or Organisations	Funding, Agitating, or Supporting Groups of Cultural, Political, and Social Natures	

Figure 2: Overview of information influence and interference assessment (conducted in 2016)
This chart was derived using a large body of primary sources of proven disinformation. Each source was analysed from the perspective of tactics of dissemination, and a part of the whole campaign with respect to timeliness, specificity, and targeting. That each tactic was evidenced is represented here with black shaded boxes however, the full data is available.

Eastern Ukraine

The conflict in Eastern Ukraine relates to the evolution in Ukraine-Russia-EU relations and is

connected to historical separatism in Post-Soviet Ukraine. In 2014, events escalated with demonstrations and protests occurring in the Donbas region, including the Donetsk and Luhansk Oblasts of Ukraine, along the border of Ukraine and Russia. These events involved pro-Russian separatists, Russian military, and anti-government activists and led to armed conflict with the Ukrainian military. Russia's ongoing agitation along the border and sustained campaign in Eastern Ukraine were revealed to the West. The resultant sanctions, as well as global focus and attention, led to an increase in Russian disinformation in English (Giles 2016d; Giles 2016e; Giles 2016b; Paul 2011; Popescu 2014) but also in other languages, including French, Arabic, German, and Spanish (Wilson 2015; Jonsson and Seely 2015; Giles 2015b), all occurring concurrently with Russian disinformation targeting Ukrainian and Russian audiences. Assessing the information activities in relation to Eastern Ukraine using the tactics, timeliness, specificity, and targeting outlined in the *information influence and interference* approach highlights multiple Russian strategies. Timeliness in this instance enabled military objectives and kinetic activity. The specificity and targeted nature attempted to deny Western access to information (including through cyber-intrusion, telecommunications control, and framing sources as well as through the kidnapping of journalists). In contrast, Russia exploited a distinct telecommunications, language, and cultural advantage (Geers 2016, Giles 2015a) to pursue targeted social media and localised campaigns to escalate violence and to create a "wartime siege mentality" (Hyde 2014) amongst the local population.

Downing of MH17

Malaysia Airlines flight MH17 disappeared from radar on 17 July 2014, and debris was subsequently found over multiple sites in the Donetsk Oblast region of Ukraine. Subsequently, widespread and global speculation about how and why it was downed emerged with criminal (Jozwiak 2016; Joint Investigation Team 2016), civil (Board 2015), and citizen (Luhn 2014; Bellingcat 2016) investigations indicating it was shot down by a Russian surface-to-air missile system. The downing of MH17 is, in many ways, responsible for fully exposing the extent of Russia's information operations and hybrid warfare capabilities to the West. Timeliness in this instance is an indicator of the extent of (usually covert) intelligence collection and resourcing which can be seen by Russian government disinformation releases relating to the downing of MH17. As more information about the downing of MH17 emerged, Russia has actively engaged with multiple audience types in different languages, on different mediums, and with different messages (McIntosh 2015; Pomerantsev 2014; Pyung-Kyun 2015; Szostek 2014). They have been timely and targeted towards certain audiences and actors in the investigation with messages specific to each audience (Giles 2015a; Giles 2016a; Pomerantsev 2014). The messages occurred in conjunction with cyber-intrusion and physical intimidation as well as bots and trolls (Reynolds 2016). Specificity, in this case, indicates very broad tactics of dissemination—including fake sources and corporate information release—as well as a range of details and narratives. Public information emanating from Russia can be attributed to a wide range of sources, including directly from the Russian government and from agencies likely under state control, as well as originally unknown or un-attributable sympathisers that are slowly and retrospectively being connected to Russian government (Snegovaya 2015; Giles 2016d; Paul and Matthews 2016). Assessing the Russian disinformation in relation to the downing of MH17 using the tactics, timeliness, specificity, and targeting outlined in the *information influence and interference* approach makes it difficult to come to any other conclusion than that the disinformation campaign was deployed to obfuscate conclusive evidence of Russian government, systems, or person involvement in the downing of MH17. It appears as

though this approach was intended to distract from the findings of the official investigation (continuous disinformation campaign, official and company statements) and prevent assigning legitimacy to investigation processes (vetoing UN SC vote and attacks on process itself, potential evidence, and information content) as well as reducing culpability within the domestic Russian audience. The information—and disinformation—campaigns surrounding the downing of MH17 highlight the significance of understanding audiences. In particular, the communications to domestic audiences are centralised on ensuring support for ongoing military activity, and the current regime is crucial (Giles 2016a; Giles 2016e). A Levada Centre poll indicated that 97% of Russians do not believe the separatists were responsible for shooting down MH17 (Luhn 2014). Given the control of domestic broadcasting, Russian access to contradictory views and information is limited.

Conclusion

This theory of *information influence and interference* is only the first step in conceptualising adversary information activities. Testing this research through application of the *information influence and interference* assessment tool on contemporary Russian operations revealed that it is possible to derive some information about the extent to which activities are informed by and integrated into military and strategic planning, and reveal insight into broader national security and geopolitical strategies. However, further applying this concept to more instances and to other regions is necessary. This is important because the enabling infrastructure and dissemination methods of information activities and especially disinformation are evolving rapidly in volume, velocity, variety, and breadth amid heightened conflict and global insecurity. For a more comprehensive and sophisticated view of *information influence and interference*, the next steps may be to build a formal framework and test it across a broader number of case studies—historical and current—to develop an improved understanding of the links between information effect and strategic intent and to begin to explore automated advanced analytics to reduce the manual load on analysts.

References

Bartles, CK 2016, 'Getting Gerasimov right', *Military Review*, January-February, pp30-38.

Bellingcat 2016 'MH17 The open source investigation, two years later', viewed 15 July 2016, <https://www.bellingcat.com/news/uk-and-europe/2016/07/15/mh17-the-open-source-investigation-two-years-later/>.

Bishop, M & Goldman, E 2003, 'The strategy and tactics of information warfare', *Contemporary Security Policy*, vol. 24, no. 1, pp. 113-39.

Bjerregaard, LCT 2012, 'Hybrid warfare: A military revolution or revolution in military affairs?', Master of Military Art and Science thesis, US Army Command and General Staff College. Fort Leavenworth, Kansas, US.

Blank, S 2011, *Russian military politics and Russia's 2010 defense doctrine*, Strategic Studies Institute and U.S. Army War College Press, Carlisle, PA, US.

Boyd, D & Crawford, K 2012, 'Critical questions for big data', *Information, Communication & Society*, vol. 15, no. 5, pp. 662-79.

Calha, J 2015, *Hybrid warfare: NATO's new strategic challenge?*. General Rapporteur of NATO Parliamentary Assembly, 7 April.

Chambers, J 2016, *Countering gray-zone hybrid threats: An analysis of Russia's 'New Generation Warfare' and implications for the US Army*. US Military Academy at West Point, West Point, NY, US.

Chief of Joint Operations 2013, *Information Activities Edition 3: Australian Defence Doctrine Publication 3.13*, Operation Series, Defence Publishing Service Canberra, AU.

Darczewska, J 2014, *The anatomy of Russian Information Warfare: The Crimean operation, A case study*, OSW Centre for Eastern Studies, Warsaw, PL.

——2015, *The devil is in the details: Information warfare in the light of Russia's military doctrine*, ośrodek Studiów Wschodnich im. Marka Karpia, Centre for Eastern Studies, Warsaw, PL.

Dick, E & Muñoz, A 2015, *Information Operations: The imperative of doctrine harmonization and measures of effectiveness*, RAND Corporation, Washington, DC, US.

Dupont, A 2015, *Full spectrum defence: Re-thinking the fundamentals of Australian defence strategy*, Lowy Institute for International Policy, Sydney, AU.

Dutch Safety Board 2015, *Crash of Malaysia Airlines Flight MH17*, 13 October 2015, The Hague, NL.

Echevarria, AJI 2016, O*perating in the gray zone: An alternative paradigm for U.S. military strategy*, United States Army War College Press. Carlisle, PA, US.

Fedchenko, Y 2016, *Kremlin propaganda: Soviet active measures by other means*, viewed on 5 September 2016, <http://www.stopfake.org/en/kremlin-propaganda-soviet-active-measures-by-other-means/#_ftn41>.

Franke, U 2015, *War by non-military means: Understanding Russian information warfare*, Swedish Defence Research Agency (FOI), Stockholm, SE.

Galeotti, M 2016, ''Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"?', *Small Wars & Insurgencies*, vol. 27, no. 2, pp. 282-301.

Gearan, A 2014, 'In recording of U.S. diplomat, blunt talk on Ukraine', *The Washington Post*, 6 February 2014.

Geers, K 2016, 'Cyber War in perspective: Analysis from the crisis in Ukraine', *BlackHat USA 2016*, 3 August 2016, Las Vegas, NV, US.
Giles, K 2009, *Russia's national security strategy to 2020*, NATO Defense College, Rome, IT.

——2015a, 'Panel discussion: Cyber war in perspective: Analysis from the crisis in Ukraine on 5 December 2015', Moderated by Dr Kenneth Geers, NATO CCD COE Ambassador, Taras Shevchenko National University of Kyiv (ed.), Tallinn, EE.

——2015b, 'Russia and its neighbours: Old attitudes, new capabilities', K Geers (ed.), *Cyber war in perspective: Russian aggression against Ukraine*, NATO CCD COE, Tallinn, EE.

——2016a, *Handbook of Russia information warfare*, Research Division, NATO Defense College, Rome, Italy.

——2016b, 'Interview with O Oliker: Continuity and innovation in Russia's way of war', 11 May 2016 ', Washington DC, US.

——2016c, *NATO must work harder to debunk Russia's claims of provocation*, Chatham House, London, UK.

——2016d, *Russia's 'new' tools for confronting the West: Continuity and innovation in Moscow's exercise of power*, Chatham House, London, UK.

——2016e, *The next phase of Russian information warfare*, NATO Strategic Communications Centre of Excellence, Riga, LV

Giles, K & Monaghan, A 2014, *Russian military transformation— Goal in sight?*, Strategic Studies Institute and U.S. Army War College Press. Carlisle, PA, US.

Giles, K, Lyne, P, Nixey, J, Sherr, J; Wood, A & Lyne, R 2015, *The Russian challenge*, Chatham House, London, UK.

Greenberg, I 1982, 'The Role of deception in decision theory', *The Journal of Conflict Resolution*, vol. 26, no. 1.

Hammond-Errey, M 2016, 'Information influence and interference in an era of global insecurity and digital connectivity, Russian disinformation strategies and hybrid war: Implications for government and national security operations', Master's (advanced) thesis, Australian National University, Canberra, AU.

Hawkins, Z & Nevill, L 2016, *Deterrence in cyberspace: Different domain, different rules*, Australian Strategic Policy Institute (ASPI), Canberra, AU.

Hoffman, FG 2009, 'Hybrid warfare and challenges', *Joint Force Quarterly*, vol. 1, no. 52, pp. 34-9.

——2016, *The contemporary spectrum of conflict: Protracted, gray zone, ambiguous, and hybrid modes of war*, The Heritage Foundation. Washington DC, US.
Holland, M 2006, 'The propagation and power of communist security services', Dezinformatsiya', *International Journal of Intelligence and Counter Intelligence*, vol. 19, no. 1, pp. 1-31.

Ingram, HJ 2015, 'The strategic logic of Islamic State information operations', *Australian Journal of International Affairs*, vol. 69, no. 6, pp. 729-52.

Jonsson, O & Seely, R 2015, 'Russian full-spectrum conflict: An appraisal after Ukraine', *The Journal of Slavic Military Studies*, vol. 28, no. 1, pp. 1-22.

Jozwiak, R 2016, 'International criminal probe blames missile from Russia for MH17 tragedy', *Radio Free Europe/Radio Liberty (RFE/RL)*, 28 September.

Kitchin, R 2014a, 'Big data, new epistemologies and paradigm shifts', *Big Data & Society*, vol. 1, no. 1 pp. 1-12.

——2014b, *The data revolution: Big data, open data, data infrastructures & their consequences*, Sage Publications, London, UK.

Kofman, M & Rojansky M 2015, *A closer look at Russia's hybrid war*, Kennan Institute. Washington DC, US.

Krēķis, JN 2015, 'Collective memory as a resource in Russian information warfare against Latvia', *Science Journal (Communication and Information)*, vol. 8, no. 1 pp 98-115.

Kuehl, DD (ed.) 2004, *Information operations: The hard reality of soft power*, Joint Forces Staff College, Washington, DC, US.

Lange-Ionatamishvili, E & Svetoka, S 2015, S*trategic communications and social media in the Russia Ukraine conflict*, 12, NATO CCD COE, Tallinn, EE.

Libicki, MC 1995, *What is information warfare?*, National Defense University, Institute for National Strategic Studies, Washington DC, US.

Liñán, MV 2010, 'History as a propaganda tool in Putin's Russia', *Communist and Post-Communist Studies*, vol. 43, no. 2, pp. 167-78.

Luhn, A 2014, 'MH17: Vast majority of Russians believe Ukraine downed plane, poll finds', *The Guardian*, viewed 08 January 2016, <http://www.theguardian.com/world/2014/jul/30/mh17-vast-majority-russians-believe-ukraine-downed-plane-poll>.

Lupovici, A 2011, 'Cyber warfare and deterrence: Trends and challenges in research', *Military and Strategic Affairs*, vol. 3, no. 3, pp. 49-62.

Mazarr, MJ 2015, *Mastering the gray zone: Understanding a changing era of conflict*, Strategic Studies Institute and U.S. Army War College Press, Carlisle, PA, US.
McIntosh, SE 2015, 'Kyiv, international institutions, and the Russian people: Three aspects of Russia's current information campaign in Ukraine', *The Journal of Slavic Military Studies*, vol. 28, no. 2, pp. 299-306.
Meister, S 2016, *Isolation and propaganda: The roots and instruments of Russia's disinformation campaign*, Transatlantic Academy, Washington, DC, US.

Metzger, MJ & Flanagin, AJ 2013, 'Credibility and trust of information in online environments: The use of cognitive heuristics', *Journal of Pragmatics*, vol. 59 no. 1, pp. 210-20.

NATO 2015, *Analysis of Russia's information campaign against Ukraine*, NATO STRATCOM COE, Riga, LV.

NATO Military Committee 2014, NATO Military Policy for Information Operations, North Atlantic Council approved MC 0422/5, North Atlantic Military Committee MC 0422/5 14.

Nimmo, B & Lucas, E 2015, *Information warfare: What is it and how to win it?*, Center for European Policy Analysis, Washington, DC, US.

Nissen, TE 2015a, '#GetUsedToLosingControl: Social media, strategic narratives and STRATCOM', *The Three Swords Magazine*, vol. 28, no. 1, pp. 45-9.

——2015b, *#TheWeaponizationOfSocialMedia- @Characteristics_of_ Contemporary_Conflicts*, Royal Danish Defence College, Copenhagen, DK.

Patrick, A 2006, *Information operations planning*, Artech House Books, Norwood, NJ, US.

Paul, C 2011, *Strategic communication: Origins, concepts, and current debates*, Praeger, Santa Barbara, CA, US.

Paul, C & Matthews, M 2016, *The Russian "Firehose of Falsehood" propaganda model*, RAND, Washington, DC. US.

Pomerantsev, P 2015, *Information at war: From China's three warfares to NATO's narratives*, Legatum Institute. London, UK.
——2016, *How to stop disinformation: Lessons from Ukraine for the wider world*, Legatum Institute, London, UK.

Pomerantsev, P & Weiss, M 2014, *The menace of unreality: How the Kremlin weaponises information, culture and money*, The Institute of Modern Russia, New York, NY, US.

Popescu, A 2014, 'Observations regarding the actuality of the hybrid war, Case study: Ukraine', *Strategic Impact*, vol. 4, pp. 118-33.

Pyung-Kyun, W 2015, 'The Russian hybrid war in the Ukraine crisis: Some characteristics and implications', *The Korean Journal of Defense Analysis*, vol. 27, no. 3, pp. 383-400.

Renz, B & Smith, H 2016, *Russia and hybrid warfare –Going beyond the label, 1457-9251*, Aleksanteri Institute, University of Helsinki, Helsinki, FI.
Reynolds, A (ed.) 2016, *Social media as a tool of hybrid warfare*, Project Director S Svetoka, NATO Strategic Communications Centre of Excellence. Riga, LV.

Rubin, D, Lynch, K, Escaravage, J & Lerner, H 2014, 'Harnessing data for national security', *SAIS Review*, vol. 34, no. 1, pp. 121-8.

Schelling, TC 2008, *Arms and influence*, Yale University Press, New Haven, CT, US.

Schoen, F & Lamb, C 2012, *Deception, disinformation, and strategic communications: How one interagency group made a major difference*, National Defense University Press, Washington, DC, US.

Selhorst, A 2014, 'Operating in the human domain, lessons of a decade of war for the Dutch Army', Master's thesis, US Army Command and General Staff College, Fort Leavenworth, KS, US.

——2016, 'Russia's perception warfare: The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine', *Militaire Spectator*, vol. 185, no. 4, pp. 148-64.

Shapiro, J 1991, 'Information and war: Is it a revolution? *Strategic Appraisal: The Changing Role of Information in Warfare*, ZM Khalilzad and JP White (eds.), RAND, Washington, DC, US.

Shawcross, A 2016, *Facts we can believe in: How to make fact-checking better*, Legatum Institute, London, UK.

Snegovaya, M 2015, *Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare*, Institute for the Study of War, Washington, DC, US.

Ştefănescu, D 2015, 'NATO strategy to defeat enemy forces in the hybrid war', International Conference of Scientific Paper, Brasov, RO.

Szostek, J 2014, 'Russia and the news media in Ukraine: A case of "soft power"?', *East European Politics & Societies*, vol. 28, no. 3, pp. 463-86.

Szwed, R 2016, *Framing of the Ukraine-Russia conflict in online and social media*, NATO StratCom COE, Riga, LV.

Tatham, S 2013, *US governmental information operations and strategic communication: A discredited tool or user failure? Implications for future conflict*, Strategic Studies Institute, US Army War College Press. Carlisle, PA, US.

——(ed.) 2015, *Defence Strategic Communications: The Official Journal of the NATO Strategic Communications Centre of Excellence*, vol. 1, no. 1, Winter 2015.

Thomas, T 1997, 'Deterring information warfare: A new strategic challenge', *Parameters*, vol. 26, no. 4, pp. 81-91.

——2000, *The Russian view of information war*, Foreign Military Studies Office (FMSO) Publications, Fort Leavenworth, KS, US.

——2001, *Information security thinking: A comparison of U.S., Russia and Chinese concepts*, Nuclear strategy and peace technology, International seminar on nuclear war and planetary emergencies, the science and culture series, August 2001, pp. 344-58.

——2004a, 'Russian and Chinese information warfare: Theory and practice,' Foreign Military Studies Office (FMSO) Publications, Fort Leavenworth, KS, US.

——2004b, 'Russia's reflexive control theory and the military', *The Journal of Slavic Military Studies*, vol. 17, no. 2, pp. 237-56.

——2011, *Recasting the Red Star*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, US.

——2014, 'Russia's information warfare strategy: Can the nation cope in future conflicts?', *The Journal of Slavic Military Studies*, vol. 27, no. 1, pp. 101-30.

——2015a, 'China's concept of military strategy', *Parameters*, vol. 44, no. 4, pp. 2014-5.

——2015b, *Russia military strategy*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, US.

——2015c, 'Russia's military strategy and Ukraine: Indirect, asymmetric—and Putin-led', *The Journal of Slavic Military Studies*, vol. 28, no. 3, pp. 445-61.

Thornton, R & Karagiannis, M 2016, 'The Russian threat to the Baltic states: The problems of shaping local defense mechanisms', *The Journal of Slavic Military Studies*, vol. 29, no. 3, pp. 331-51.

Tulak, AN 2015, 'Hybrid warfare and new challenges in the information environment', *Proceedings of the 5th Annual Information Operations Symposium*, 20-22 October 2015, Honolulu, HI, US.

Williams, PAH 2010, 'Information warfare: Time for a redefinition', *11th Australian Information Warfare and Security Conference*, Edith Cowan University, Perth, AU.

Wilson, A 2015, 'Four types of Russian propaganda', *Aspen Review Central Europe*, vol. 4, viewed 16 November 2017 <http://www.aspeninstitute.cz/en/article/4-2015-four-types-of-russian-propaganda/>.