SOCMINT: A Shifting Balance of Opportunity

Abstract:

The current ubiquity of social media platforms has led to optimism around the insight governments will gain for horizon scanning, warning notice, investigations and situational awareness in crises. This paper concludes that SOCMINT offers utility to governments in horizon scanning, offers little for imminent warning notice, and limited traction for situational awareness. The paper further concludes that for Five Eyes nations the threats posed by adversary utilisation of social media platforms and their analysis and utilisation of social media is considerable and outweigh the advantages to western powers. The west is currently losing the information component of hybrid conflict. Consequently, capable and hostile cyber powers understand the western centre of gravity and have been able to undermine confidence in the public's certainty in facts and democratic institutions.

The advent of mass participation social media since 2006[1] has had a transformative impact on social and economic relations across Europe and North America. The growth of these platforms has also led to a parallel growth in private and public sector industries geared to exploiting social media feeds for security and law enforcement purposes. Intelligence Officers have been quick to explore and internally advocate for the insights they believe they will be able to draw for horizon scanning and warning notice, investigations and for situational awareness in crisis incidents.[2] This paper evaluates the intelligence opportunity and scans the horizon for the direct and indirect challenges presented by SOCMINT. In noting the prevalence and use of social media, this paper evaluates the disruption to the character of modern social and economic relations, the changing nature of international conflict, and what role there is a role for

[1] Facebook was founded in 2004, but became open access in 2006. Twitter was also publicly available from 2006. Whilst the less regulated spaces of 4Chan (which is more a posting forum) and Reddit, were founded in 2003 and 2004 respectively, with 8Chan, originally called InfinityChan, which is an even less regulated posting forum established in 2013.

[2] Bradshaw and Howard, Troops, Trolls and Troublemakers

intelligence agencies to utilise defensive and offensive SOCMINT capabilities, activities that are increasingly placed within the wrapper of hybrid warfare.[3]

The weaponization of social media – the transformation of it into a source of intelligence and societal insight, but also to an active security threat has been made across a range of examples that can be organised into three clusters : 1) the localisation of violence, 2) collective action, and 3) information conflict, and this is a threat matrix that continues to co-exist, overlap and evolve.

In the UK, the first significant case of social media as a threat that challenged the capabilities of law enforcement and intelligence agencies was the widespread violence in London (and then Birmingham and other significant cities) in August 2011. The so-called 'Tottenham Riots' – contained a hybridised organised reporting loop of publicly available social media, encrypted personal messaging – via the Blackberry Messenger service (BBM) – and traditional media sources.[4] Her Majesty's Inspector of Constabulary concluded in 2011 that "With some notable individual exceptions, the power of this kind of media (both for sending out and receiving information) is not well understood and less well managed".[5] He further concluded that "[t]he police have much to learn about social media, and the quickly shifting modern communications of today", and the gap between the rapidly developing technical and doctrinal capabilities of adversary actors and government authorities means that this observation remains true today. The violence of August 2011 saw social media being used to coordinate, publicise and make sense of localised violence, and the response to it.[6]. In similar ways, we can see the use of messages on 8Chan to effectively pre-warn and position violence against identifiable

[3] Aldrich and Moran, Evidence submitted from Warwick University.
[4] Piero, Emergent Policing Practices; Cammaerts, Technologies of Self-Mediation.
[5] HMIC, The Rules of Engagement.
[6] Tonkin, Pfeiffer, and Tourte, Twitter, information sharing and the London riots?

communities, such as those of the New Zealand massacre in March 2019, and in El Paso, Texas on August 4, 2019.[7]

Internationally, there have been examples of social media as a collective action threat, utilising a hybrid effect with the combination of information channels used in the popularly named 'Arab Spring' movement (although in reality a set of disparate revolutionary movements) in 2011 and after in Tunisia, Egypt, Bahrain, Libya, and Syria. [8]These uprisings (which had different levels of success) were also in part organised and relayed via social media platforms, occasionally via encrypted personal messaging and by traditional media outlets, including short wave radio. These subversive groups were rapidly adapting asymmetric actors, posing a different nature of challenge, but similar sophistication of challenge as the asymmetric military actors of post-invasion Iraq and Afghanistan. After the partially successful action in Libya (it succeeded in removing Gaddafi but not in installing stable, democratic governance) evidence was found that British companies had sold technology to the Gaddafi regime that could be used to intercept mobile phone traffic and place surveillance over activists, whilst in the 2019 protests in Hong Kong the technologies have been developed by Chinese companies and utilised by Chinese security officials, demonstrating the sort of conflict that takes place in the information and social media space.[9]

Social media data has been viewed by public policy officials (in the recent past, and currently) as being capable of delivering data-driven insights that were hitherto impossible to reach, including notably in epidemiology.[10] As Edward Snowden has asserted, the US National Security Agency overcame the challenge of targeted interception with what he describes as the

[7] McMillan, After New Zealand Shooting, Founder of 8chan Expresses Regrets; Arango, Bogel-Burroughs, and Benner, Minutes Before El Paso Killing.
[8] Wolfsfeld, Segev, and Sheafer, Social Media and the Arab Spring; Khondker, Role of the New Media in the Arab Spring.
[9] Cobain, How Britain Did Gadaffi's Dirty Work; Mozur and Qiqing, Hong Kong Takes Symbolic Stand Against China's High-Tech Controls.
[10] Lampos, De Bie, & Cristianini, Flu Detector.

STELLARWIND programme of bulk collection that began in 2001, and which serves to create a comprehensive archive that is accessible to officers.[11] The challenge of STELLARWIND and similar systems are the techniques required to find relevant information, rather than the challenge of collecting it.[12] Part of the premise of these insights is that the platforms are non-discriminatory. The usage of the platforms is fee free where the users themselves are the product, as their data can be repackaged and sold by the platform, and wider insights about the collective community of users can similarly be commercially exploited. The logic runs that if platforms charged fees it would further skew any demographic insights researchers and marketeers might be able to glean from them, but there is self-selection within the user base and some economic access bias present, as equipment and access costs money. The same logic has applied to security use cases around social media data: the broader the user base is on platforms, so it goes, the more accurate the insights are that can be drawn from them. As will be noted later in this piece, there are already structural skews in this data, and the increased use of encrypted and direct messaging further degrades its utility.

The third sweep of weaponization of social media has come in the information conflicts that have been observed – which have included hostile government participation – that surrounded the 2016 US Presidential campaign, the course of politics in the Baltic region, the UK's 2016 EU Referendum and post-referendum political Brexit debate, the 2017 French Presidential election and the aftermath of the March 2018 poisoning of former Russian military intelligence officer Sergei Skripal in Salisbury, England.[13] These case studies – which have an individual resonance for the countries involved - have been subject to a variety of official, judicial and academic inquiries. Pieced together, these case studies create an observable and general trend of a pattern of mis and disinformation – the information component of hybrid warfare - as a

[11] Snowden, Permanent Record, pp177-80
[12] Barquin, To data mine or not to data mine in the fight against terrorism.
[13] Urban, The Skripal Files

matter of course by adversary states and their supporters to create strategic effect, to unseat the public's certainty in knowledge or confidence in authority, or to advance other interests.[14].

SOCMINT and Security

In an early piece on SOCMINT in 2012, Sir David Omand and his co-authors suggested, somewhat optimistically, that social media intelligence (SOCMINT) should be capable of providing near real time intelligence feed and situational awareness for officers. This is a premise that is shared by many practitioners who still view SOCMINT as a form of security panacea, allowing them to create value from freely given open source information.[15] In unguarded remarks, a senior officer of the UK's Metropolitan Police said: "[Social media] almost acts like CCTV on the ground for us. Just like the private sector use it for marketing and branding, we've developed something to listen in and see what the public are thinking."**.**[16] These comments were overdrawn, however, there is not the evidence to suggest that SOCMINT has anything like the level of pervasive traction suggested by this quote despite the efforts of the UK Ministry of Defence, with academic and commercial partners working extensively on social media sentiment analysis. The development of government sentiment analysis algorithms has been to 'take the temperature' of societal cleavages and to predict violence and societal tension. The ongoing challenges to this technology has been in programming an understanding of the emotional context of messaging, and in understanding causal links and trigger points in transforming messaging into violence.[17] There have been individual moments that reveal the power of social media investigations, for example the Project Polar investigation that identified secure sites and the geo-positioning trails of intelligence officers from shared fitness tracker data and the Bellingcat investigations into the Skripal assassination attempt and

[14] Flournoy,and Sulmeyer, Battlefield Internet: A Plan for Securing Cyberspace
[15] Omand, Bartlett, & Miller, Introducing Social Media Intelligence.
[16] Wright, Meet Prism's Little Brother
[17] Hills, Jackson, and Sykora,. Persuasion and the Microblog.

the shooting down of Flight MH17 over Ukraine, where the names of alleged perpetrators and timelines were carefully uncovered, something that is akin to Bigo's notion of shared secrecy that appeared in this journal in 2019.[18]

The key opportunities from SOCMINT lie in individualised targeting (but one would assume that sophisticated adversaries would have adequate countermeasures for this), the mapping of network nodes, situational awareness and near real-time information provision and rebuttals, the management of public messaging, computational propaganda, sentiment analysis and refinement of models around what sits outside of 'normal'. Attendance at any professional or trade conference will provide evidence for the thriving industry in developing technologies to exploit these platforms, the supply of which has partly driven demand and reinforced the anticipated positives.

The potential threats from social media and SOCMINT is the potential for its use as a 'denial and deception' tool, as a means by which to undertake subversion campaigns, and in adversary's using the available data to assess exploitable weaknesses in the west. It is in this attack vector that our adversaries have rapidly developed and honed techniques to optimise their use of social media platforms against North American and European powers. As such it is the attack vectors presented by the offensive use of social media – particularly in disrupting situational awareness, rupturing settled narratives within the sense-making phase of a crisis, and undermining governmental and legacy media narratives, through systematic use of 'fake news' approaches to even the most minor issues - that threatens to become its defining characteristic. Furthermore, it has eroded the technical superiority that western powers believed they had in communications technology.

[18] Tokmetzis, Martjin, Bol, and Postma, Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app; Bellingcat, MH17; Bigo, Shared Secrecy.

The enthusiasm in the academic and grey literature was a mirror of the enthusiasm shown by the public for enhanced connectivity.[19] Other authors, such as Andrus argued that internet technologies would upend the organisation of intelligence agencies, Jaegar and Cavelty interrogate the use of crowd-based intelligence sourcing (but focus upon the indexed web), whilst Shipley and Bowker took a more technical approach to this subject, outlining the processes investigators would need to go through to draw inferences about who targets associate with, where they are located, the use of metadata behind social media posts and the need for an equivalent of a national database of SOCMINT that could be searchable by all police officers.[20] Interviewees diverged on the quality of location (and therefore targeting) data available from social media: two Home Officials told me that the location data was often not accurate to 10kilometres, whilst international law enforcement practitioners contested that it could be accurate to 100metres. [21] I assessed the difference between these two positions as more presentational than literal.

The widespread use of virtual private networks (VPN) and The Onion Ring browser (TOR) complicates this situation further, making straightforward or time-pressed interception more challenging. The hindrance here comes from the levels of technical difficulty, but not impossibility, in unpicking the layers of anonymity to accurately track users.[22] Many internet users incorrectly believe that VPN and TOR provides cast-iron anonymity when using the internet, as analysts like Bellaby and Ronn and Soe assert and further argue are ethically necessary, but this anonymity is far from guaranteed.[23] The technical ability to deanonymize

[19] Bradbury, In plain view: open source intelligence; Gupta,and Brooks, Using Social Media for Global Security
[20] Andrus, Toward a Complex Adaptive Intelligence Community; Shipley and Bowker, Investigating Social Networking Sites; Jaegar & Cavelty, From madness to wisdom.
[21] Private interview data, Home Office interviews June 2017 and international law enforcement officers, July 2017.
[22] Interview with Home Office official, October 2017; Nasr, Bahramali, and Houmansadr, DeepCorr: Strong Flow Correlation Attacks on Tor.
[23] Bellaby, Going dark: anonymising technology in cyberspace; Ronn and Soe, Is social media intelligence private?

VPN and TOR users renders there few 'safe' spaces on the indexed and unindexed internet, something that assists counterterrorism and counterintelligence efforts, but which also makes securing information from friendly sources in target nations more problematic. Practitioners working in information security and electronic intelligence have described this de-anonymisation as being 'when the dish is pointed at a target', a euphemism for when targeting and computing power can undo the technical measures put in place to remain anonymous.[24]

The unindexed internet provides the most fertile battleground for the information war underway, where it is more complicated to discern and understand who are the participants and what their motivations are.[25] Concerted online efforts by a state actor do not clearly track back to a single account or institution, and organised or state sponsored disinformation campaigns often originate in 'chat forums' on the unindexed web.[26] As noted below, this modus operandi was certainly the case in the Integrity Initiative saga in November and December 2018[27]. Posts on the unindexed web might serve the purpose of offering distraction or equally they might be credible and serve as a warning notice. Where the messages are credible they make their way to the indexed web via a concerted effort from the coordinating group, whereupon they are picked up by fellow-travellers who are with or without malicious intent, 'bot' accounts and so on until they reach a tipping point to be reported upon by friendly digital media, which attracts more commentary from those outside of the ambit of state control. Finally, the messages that originated in the unindexed or dark web reach legacy media sources, where they are reported upon often without acknowledging their origins. This interconnected, and therefore only loosely directly controlled, route to public exposure renders it very difficult to counter or

[24] Interview with UK Ministry of Defence official, December 2018.
[25] Dover, UK Response to Hybrid Threat Inquiry.
[26] Ibid.
[27] https://www.statecraft.org.uk/, last accessed 24 October 2019.

control. There are also good philosophical and ideological reasons to resist the urge to try and control the flow of information, even if it is disinformation.

The efforts to combat the impact of disinformation have, in the UK, located themselves officially in the realm of the British Army's information war unit, 77 Brigade, which is focussed on supporting military operations.[28] Away from the exclusively military realm, the Foreign and Commonwealth Office funded the Integrity Initiative, whose stated aim is to highlight and educate the public about the propagation of Russian mis and disinformation. The latter came under tension in November 2018 via what the UK government described as a concerted Russian state effort to undermine the Institute of Statecraft, who run the Integrity Initiative, with a wholesale hack of the Institute's servers and the subsequent unredacted publication of their computer systems in November 2018 later.[29] The hack of the Institute's servers has been attributed to one of the 'Anonymous' online hacking collectives, whilst the UK government has attributed it to Russian state actors. Irrespective of who is culpable for this series of cyber-attacks, it generated considerable interest on social media, on Russian affiliated media (primarily RT and Sputnik) and made it into the mainstream UK media and Parliament too.[30] To track the development of the narrative around the Integrity Initiative , I used the TAGS system of Tweet collection between the 27 November 2018 and 28 February 2019 to collect – or in technical parlance to scrape - Tweets referencing the Integrity Initiative in free text or via the #integrityinitiative hashtag, of which there were 104,000 in that timeframe.[31] The dataset speaks to a modus operandi where core messaging is amplified, where highly selective quotations or partial data is re-spun and pushed, and where a corps of fewer than 50

[28] British Army, Who we are: Bridge 77, Influence and Outreach
[29] Duncan, Institute for Statecraft: Integrity Initative.
[30] Lucas, Don't swallow Labour's claims of 'black ops'.
[31] The TAGS system can be found at: https://tags.hawksey.info/, whilst the Tweet archive can be found at the following archive:

twitter accounts was used to clean and legitimise narratives that were by coincidence or design aligned to Russian state narratives.

The hacked Institute documents, which at the time of writing are still available online, also provide a fascinating insight into how counter-information and counter-influence campaigns can be run with a carefully constructed network of well-placed individuals. The document cache suggests that there was a curated network of contacts across continental and Eastern Europe in diplomatic, education and journalistic circles. But it is important to note that the validity of these documents is open to question. This author and The Times journalists, Edward Lucas and David Aaronivitz all appeared on a document labelled 'UK Hub', but all three have confirmed that they did not belong to, nor had heard of this initiative or hub. Further commentary is also problematic due to the cache appearing via a cyber-theft, and without the consent of the Institute..

One of the clear lessons from the online response to the 77 Brigade activities and the energetic online response to the hacking of the Institute for Statecraft is that engaging in the information component of (another state's) hybrid war is fraught with reputational dangers, particularly if veneers of plausible deniability are eroded. The reputational risk is but one dimension, with there being more fully formed dangers to human and other types of assets justifiably or erroneously revealed and rendered vulnerable during these exchanges.

Guidelines for Usage

There is a lack of consensus in the literature about what academics can do with social media data, ranging over some 17,000 articles on SCOPUS where Twitter features in the title.[32] For

[32] Pfaffenberger, Beyond #covfefe - a critical look at Twitter as a scientific base.

some it is publicly available and 'pushed' by the users and therefore can be used for analytical purposes. For others, the repurposing of this data means it is ethically problematic. For practitioners, however, the situation is legally, if not ethically clearer. In the UK and for investigative purposes, practitioners use the Regulation of Investigatory Powers Act (RIPA), and Investigatory Powers Act to access this material. When Omand and his collaborators coined the term SOCMINT in 2012 they sought to place a quasi-ethical wrapper around the activity, with five tests for intelligence officers seeking to collect in this way: 1) Sufficient, sustainable cause; 2) There must be integrity of motive (access is justified); 3) The methods used must be proportionate and necessary; 4) There must be the correct authorities in place; and 5) Recourse to secret intelligence must be a last resort if more open sources can be used (a moral hazard point).[33] But as is discussed at several points in this article, critical incidents are becoming highly vulnerable to mis- or dis-information campaigns by belligerent actors and so justification can be made for more intrusive techniques to verify the identity of a poster and to prevent them from publishing particular sources of information. In the aftermath and sense-making phase the five tests no longer apply so obviously, particularly when the necessities of information conflicts push participants into more pro-active and aggressive actions.

The management of critical incident messaging has been seen in public relations terms, and much of the crisis communications literature echoes this point.[34] But it is precisely this set of activities that has been weaponised by adversary actors into denial and deception operations, a form of what David Gioe describes as hybrid intelligence, and which should now be brought into the orbit of SOCMINT and countersubversion.[35] As a consequence, what is missing from our understanding of SOCMINT is where it fits into an emerging political-military information

[33] The original DEMOS paper on SOCMINT by Omand et al had a sixth principle, which was 'the reasonable prospect of success', and interviewee evidence suggests that this paper was widely circulated by practitioners who were trying to make sense of how SOCMINT fitted within the new Regulation of Investigatory Powers Act 2000.
[34] Ruggiero and Vos, Social Media Monitoring for Crisis Communication.
[35] Gioe, Cyber operations and useful fools: the approach of Russian hybrid intelligence.

battlespace, the necessity for doctrinal (and methodological) developments around the rapid verification of social media information, a development of doctrine for projecting information and rebutting misinformation, and for more active measures to manage cyber space in the event of crisis incidents.

Hybrid War / Hybrid Intelligence – The Role of Social Media in Modern Warfare

Carl von Clausewitz described warfare as: "an act of force to compel our enemy to do our will". Writing towards the end of the 19th century, Clausewitz was thinking mostly about acts of force being between armed combatants. Consequently, one his most persuasive concepts – 'the centre of gravity' – was geared around military vulnerabilities but ultimately manifests itself as the pivotal weakness of the adversary, against which overwhelming effort should be directed.[36]This concept is still useful in analysing SOCMINT because it is now widely viewed across scholarly, journalistic and official texts that the mis- and disinformation campaigns that have been effective against governments and societies in Europe and North America are component parts of a strategic effort by our adversaries seeking to undermine certainty of knowledge and political and social cohesion in the west.

The attempts to unseat 'certainty' fit into the Clausewitzian concept of 'the centre of gravity'. This is the point at which an adversary is most vulnerable, and to which a focussed effort from the attacking side will result in significant strategic effect.[37] Echevarria describes the centre of gravity – more usefully – as the capability or asset which can be said to 'hold everything together'.[38] Clausewitz's 'Centre of Gravity' analyses have become contested in the strategic studies field between those who believe he was only concerned with assessments of military

[36] Clausewitz, On War.
[37] Iron, What Clausewitz Really Meant by Centre of Gravity.
[38] Echevarria, Clausewitz's center of gravity: it's not what we thought

strength,[39] and those who have sought to update the concept to include things such as public opinion, and identity politics.[40] The advent of hybrid or combined warfare leads us to have to use this latter interpretation and evolution of Clausewitz, in the same way that organisations like NATO have, to describe patterns of offensive activities that are 'characterised by multi-layered efforts to undermine the functioning of the State or polarise society'. We might also reasonably follow Robert Johnson's interpretation that this is simply the way that war works today, and that the label 'hybrid war' is obscuring our understanding of the processes that underpin it.[41]

Uncertainty or insecurity in knowledge is often posited as a modern phenomenon, connected to the prevalence of network enabled devices and the ubiquity of the internet and social media. More recently, the 'shocks' (and it is possible to read these events as shocks against received opinion as opposed to shocks in the truest sense of intelligence studies) of the Arab Spring (2011)[42] , of globalised and network affiliated asymmetric military actors (most notably Al-Qaeda, Da'esh)[43] , of electoral shocks in Greece (2015)[44] , of shocks in party leaderships and election results in the UK (2015/17)[45], of Brexit (2016)[46], and in the election of US President Trump have a common theme of attribution of challenging 'mainstream' truths and narratives, via guerrilla-style, network enabled and social media activism.[47] But it not yet possible to say

[39] Eikmeier, Center of Gravity Analysis; Neumann, Evans, and Pantucci, Locating Al Qaeda's Center of Gravity;
[40] Given that Clausewitz is a long time dead, we might reasonably say that he was only ever capable of expressing the view about military capabilities. Harley, Information, technology, and the center of gravity; Strange, Centers of Gravity and Critical Vulnerabilties; Niglia, Critical Infrastructure Protection.
[41] Johnson, Hybrid war and its countermeasures.
[42] Khondker, Role of the New Media in the Arab Spring; Eltantawy & Wiest, Social Media in the Egyptian Revolution.
[43] Farwell, The Media Strategy of ISIS; Amble, Combatting Terrorism.
[44] Engesser, Ernst, Esser, and Buchel, Populism and social media; Georgakopoulou, Small stories transposition and social media.
[45] Margetts, Why Social Media May Have Won the 2017 General Election.
[46] Seaton, Brexit and the Media.
[47] Sunstein, #Republic: Divided Democracy in the Age of Social Media*;* Allcott,and Gentzkow, Social Media and Fake News in the 2016 Election.

whether the social media interventions or dynamics in those cases was persuasive or compelling, because the literature does not yet have a sufficient grasp of how these messages translate into real-world action.

At least two of these strategic shocks have the other common attribute of aggressive Russian information operations as their alleged context, and currently the Russian information operations are the most visible and most effective that we can observe, even though the Russian government is by no means the only nation engaged in such activities. For reasons of balance we should note that Jihadists, Chinese and North Korean military officers and the far right, including those who have attracted the label of populists, are all actively engaged in these activities. Indeed, as noted earlier, the British government has also been accused of engaging in similar activities via the Army's 77 Brigade and in its funding of projects. But Russian misinformation campaigns – for historical reasons - have most publicly vexed British authorities. The operational concept of "dezinformatsiya" (disinformation) has a long contemporary lineage in Russia, and was notably practiced by the *Dezinformatsiya Directorate* of the KGB during the Soviet era, as it has been by all competent intelligence agencies during and since.[48] The aim of this operational concept for the Russian state was and is to unseat certainty of knowledge in the minds of the citizens of target countries. Under the Soviet era doctrine of 'active measures' (*kompleksnoye akitivnoye meropriyatiye*), which we now cast forward to today, the social media programme (coupled with targeted hacking and leaking) comes under the demoralise and disorient strands that precede more kinetic activity.[49] The British Parliamentarian Bob Seely has framed a new Russian way of war where these active measures sit in the first block of four as 'hidden genesis and escalation', so action short of or

[48] Cunningham, The Idea of Propaganda: A Reconstruction; Holland, Holland, Dezinformatsiya.
[49] Mitrokhin, The Soviet Intelligence Officers Handbook

prior to kinetic activities.[50] Seely's analysis is energetically refuted by Russian area specialists who say that it provides far too clear a strategic purpose and cohesion to a level of fragmentation in the Russian governmental system that we (in the west) underplay and ignore, and which is a form of defensive doctrine, built from a mindset of encirclement.[51]

For Seely and those who give credence to the Henry Jackson Society analysis, the Russian disinformation campaign is prosecuted partly for the purposes of creating external disunity, to establish a platform where a citizen will also question what they are being told about Russia, Russian capabilities and intentions. For this school of thought, the internet age has not changed Russian (or Chinese, Iranian and North Korean) sensibilities on this matter, it has merely provided new and different tools, a magnitude of scale and speed by which to pursue this agenda. Recent research by official inquiry in the United States[52], by Parliamentary inquiries in the UK[53] and by university researchers in the UK has found good evidence of Russian controlled activity in the US Presidential Election (individual advert targeting, disinformation campaigns and hacking)[54], in the 2016 UK Brexit Referendum (individual advert targeting, political funding that is under investigation, disinformation campaigns)[55], and in the 2017 French Presidential Campaign (hacking, disinformation and funding).[56]

NATO have analysed the nature and magnitude of this threat - which has the Clausewitzian quality of degrading the ability to mount a military defence of territory – which has been observed in the Russian campaigns against Georgia (2008), Ukraine (2014), and Syria (2015-

[50] Seely, A Definition of Contemporary Russian Conflict
[51] Monaghan, Dealing with the Russians.
[52] House Intelligence Committee, *The Russia Investigation Taskforce;*
[53] Digital Culture Media and Sport Select Committee. 'Fake News' Inquiry; Defence Select Committee, UK Response to Hybrid Threats
[54] In which Democrat members of the House compiled lists of alleged Russian controlled accounts: https://democrats-intelligence.house.gov/uploadedfiles/exhibit_b.pdf
[55] University of Swansea, Bots Generated Social Media Stories.
[56] Rogers, Commander US Cyber Command.

17). The NATO analysis of these operations led them to attach them to a term coined in 2006 by Frank Hoffman, of 'hybrid warfare', which has become common currency in security circles since, but was not Hoffman's original intent.[57] The NATO definition is that hybrid warfare is a military strategy that blends conventional warfare, irregular warfare and cyber-warfare. By combining kinetic operations (traditional military force) with subversion, the aggressor intends to avoid attribution or retribution, something that is ideal using networked technologies. We can see this through the work of those who seek to reinterpret Clausewitz in modern contexts who have written about the non-kinetic means by which states can seek to impact target states, to persuade or coerce those states to act against their own interests or to leave the enemy intact but transformed in some way: in other words to create change without using hard military capabilities.[58]

The Russian military deny any such campaign exists but have had this way of war attributed as the *Gerasimov Doctrine*, after the memorandum written by the Chief of the Defence Staff which examined what he saw as the western approach to combining military, technological, information, diplomatic, economic, cultural and other tactics (commonly called 'jointery') that might be deployed against Russia in a unified set of strategic objectives. Gerasimov's analysis has ironically been morphed into an articulation of Russian offensive operations.[59] The UK military has noted its assessment that offensive cyber capabilities might be capable of 'over-matching' conventional forces (defeating them, in plain English) therefore requiring an escalated kinetic military response, and that these cyber activities represented a permanently operating front in the UK and elsewhere.[60]

[57] NATO, Hybrid Warfare.
[58] Nye, Soft Power; Mearsheimar and Walt, US Foreign Policy; Brister, Revisiting the Gordian Knot.
[59] Monaghan, Dealing with the Russians; Deep, Hybrid War: Old Concept, New Techniques; Bartles, Russia's Indirect and Asymmetric Methods.
[60] UK Ministry of Defence, Joint Doctrine 1/18.

Reduced to its fundamental core, what is described as hybrid warfare is the combination of two or more facets of war to a focused endpoint: the combination of which facets and how is the element that remains obscured to the enemy. Quite starkly, the Director General of the Security Service (MI5) described this approach as: "The Russian state's now well-practised doctrine of blending media manipulation, social media disinformation and distortion along with new and old forms of espionage, and high-levels of cyber-attacks, military force and criminal thuggery is what is meant these days by the term hybrid threats.".[61] There are some for whom the concept has become so wide that it no longer serves a useful definitional purpose. For these scholars the term hybrid war is a new title for for age-old security tactics, or that it is a deliberate misreading of Russian military concepts.[62] For Robert Johnson, the term amounts to a 'manifestation of current anxieties in armed conflict', but that there is a spread of operations fitting the broad definition of hybrid warfare is well evidenced, and the benefits of this type of warfare include economic efficiency and it should be noted that for the estimated expenditure, this doctrinal approach has generated very notable effects: it has been relatively inexpensive and highly effective.[63] David Gioe argues for the range of operations covered here ('HUMINT, tradecraft with cyber operations and information warfare') to be called hybrid intelligence, which also covers the utilization of *useful fools* (his term) as can arguably be seen in the Salisbury case, although the term is controversial and may obscure more than it usefully reveals .[64] We might reasonably conclude that the terms hybrid warfare and hybrid intelligence merely accounts for the way that states currently prosecute aggressive action, and that its utility in this realm is to alert those in civilian responder roles that they are vulnerable to modern ways of war fighting. The term hybrid warfare is so wide, however, that we might usefully break it up

[61] Parker, statement.
[62] Monaghan, Putin's way of war; Monaghan, Power in Modern Russia; Renz, Russia and 'hybrid warfare'.
[63] Johnson, Hybrid war and its countermeasures.
[64] Gioe, Cyber operations and useful fools; Omand, From nudge to Novichok.

into its component parts, be it to describe information operations, or the use of proxy fighters, to name but two.

To read Bob Seely's report, or the premise of recent UK Parliamentary inquiries, one could be convinced by a sense that all significant incidents of mis- or disinformation in the social media or direct communications realm in crises are the result of the hostile activities of belligerent states. There will inevitably be a proportion of mis or disinformation that is created by people wishing to speculate with or without earned confidence, a further proportion who keenly feel that official narratives are erroneous and who feel more aligned with narratives that are commonly considered to be 'conspiracies', or those who are honestly imparting information they have acquired by various means, as was visibly seen throughout the Salisbury example. There is often little regard – amongst practitioners and in the literature for the potential for orchestrated and deliberate misinformation campaigns and it is here that social media threat outweighs the opportunity. Where misinformation is discussed, there is usually presumed to be a remedy that an organisation can take to mitigate against the issue, but in the rapidly emerging circumstances of a crisis incident – be it an act of terrorism or some other kind of fluid and anxiety inducing situation - that is unlikely to be true, certainly within an appropriate timeframe. Thus, crisis communications will be peculiarly vulnerable to outside interference in a way that could have a serious impact upon the incident area, and the health, psychological outcomes and long-term impact of the incident. The consequential effect will be upon societal understandings of the incident and in turn may serve to influence government responses and any groups or nation states implicated in the incident, should it be a deliberately targeted attack: the slow pace at which the British government responded to the Skripal poisoning is a reflection of this desire to avoid rushing a response, making a voluntary mistake and then being left with expensive and complicated consequences.

There is a high potential for rumours and misinformation on social networking sites during crises, particularly those conditioned by radical uncertainty. There is also some evidence that online communities tends to be 'self-correcting' and often rapidly so .[65] This entails users responding to other users who may be spreading misinformation, before the misinformation has a chance to take root. This does depend upon users being broadly similarly engaged in monitoring social media feeds, which at a time of high stress there is a greater chance they will be. There is also an issue around the assumed or actual knowledge of those involved in the incident or those consuming content, and in the case of terrorism or other types of life-threatening incidents this cannot be assumed with any degree of safety. The appropriate mitigations that we find in the literature for this type of online activity are: supremacy of situational awareness (be this through surveillance or similar), exposure of enemy or false accounts and narratives,[66] and 'well-rehearsed (and swift) information operations' across multiple axes to counteract emergent false narratives.[67] Added to this mix should be increased public resilience and awareness, because the public are a considerable point of vulnerability in these incidents, particularly if they have a disposition towards not trusting official sources or are persuaded to question or ignore official sources.

Controlling the Message

Information provision is not a core element of the work of intelligence agencies, but agencies have tended to provide brief instruction and commentaries on public attacks or incidents: in the UK this has been via the local constabulary (e.g. @metpoliceuk), via national response handles (e.g. @TerrorismPolice) or national coordinating forums (e.g. @PoliceChiefs). The public's

[65] Veil, Buehner, and Palenchar, A Work-In-Process Literature Review.
[66] Bradshaw and Howard. Troops, Trolls and Troublemakers
[67] Johnson, Hybrid War and Its Countermeasures, 159.

demands for instrumental and sense-making information are enormous in such crises, and they produce a risk of widespread feelings of fear, vulnerability, dread and helplessness.[68] In these scenarios the public actively pulls information in, rather than necessarily needing it be pushed at them and therefore engaging in passive consumption. Central analysis of social media feeds can provide important information on potential logistic lines, secondary targeting information, and community sentiment, which might help to mitigate community violence, depending on the circumstances. Effective communication (in preparation, response and recovery) has therefore become widely recognised as integral to the goal of minimising harm from crisis incidents[69] and to restore calm and confidence in the professional and society response to crises .[70] The balance for intelligence agencies is, therefore, around the information that can be extracted from an incident to help inform assessment, and potentially to help inform countermeasures. Analysis and assessment of social media feeds might also be useful in informing strategic policy makers about how to shape understandings of an incident, but this heavily depends upon the techniques to rapidly verify information (against robot accounts, known as bots) and also in the ability to accurately 'test the temperature' of society's collective anxiety and sentiment towards the incident, victims or early accounts of who perpetrators might be.

One reading of the communications strategy around the March 2018 Salisbury poisoning, was that the British government wanted to control the pacing and flow of information to mitigate the potential push into an active or aggressive foreign policy response. The downside of that approach was the creation of an information vacuum in Salisbury that many social media and broadcast commentators moved into, creating rapid cycles of reinforcement between

[68] Ruggiero & Vos, Social Media Monitoring; Rubin, Amlot and Page, The London Polonium Incident.
[69] Palttala & Vos, Quality Indicators for Crisis Communication.
[70] Reynolds, Response to Best Practices.

narratives. All the social media platforms have been designed and geared to provide for rapid dissemination of views, consequently mis and disinformation is as likely to quickly spread as any other type of information feed, some research suggests it moves more quickly.[71]

The majority of the literature assumes a primacy for the legacy or mass media for critical messages from government communicators .[72] It is more realistic now to note that the hybridity and interconnectedness between the legacy media and social media, where many of the initial reports and rolling updates have come from recognises the contemporary reality and contingencies of the media system responders and the public operate in .[73] This opens up a role for government intelligence agencies to be involved in counter-subversion roles. Most crisis communications plans (including globalised ones such as INTERPOL's Operation Stadia) include provisions to push messages out on mobile phone and social media networks, as was seen in Hawaii and Japan in 2018, during North Korean missile testing.[74] During the past decade there has been an increasing interest in the potentially facilitating or disruptive role that social media, particularly from institutions and individuals using social networking sites, may play in developing operational best practices. What is less well developed, and practitioners seem to confirm this, is what holistic approaches can be put in place that take account of the hybridity of the contemporary media environment, where social media and 'legacy' media are part of interlinked and often mutually dependent systems. Governments will seek to exert strategic control over the dominant narrative, and this is aided by an interconnected communication system, it is just that there are equally persuasive and interconnected countervailing pressures.

[71] Vosoughi, Roy, and Aral, The spread of true and false news online.
[72] Reuter, Kaufhold, Spielhofer, and Hahne, Social media in Emergencies; Vos, Lund, Reich and Harro-Loit, Developing a crisis communication scorecard.
[73] Chadwick, The Hybrid Media System
[74] Burgess, The UK has no public nuclear alert system.

Contemporary politics, certainly since the innovative use of internet and messaging technologies by the 2012 Obama campaign, has become part of an ongoing information war. Information war during election campaigns has the capacity to draw intelligence agencies into counter-subversion work, as adversary actors escalate their mis- and disinformation campaigns against government actors, but equally moves the intelligence community closer to being political participants themselves. Counterintuitively, however, government communicators – who get first mover advantage – will need to be the first to break, as credibly as possible, crisis incident stories, and to establish themselves as the authoritative single voice on the incident .[75] The contestation in cyberspace between government communicators, the ill-informed and speculative, and the adversary communicator attempting to do the modern variant of denial and deception is therefore likely to get worse, not better and it will take intelligence agencies – focussed on bulk interception and analytical techniques – to identify and disrupt those actors. For the longer term there must be a case for questioning the utility of using social media as a means by which to transmit life-critical information, with there being potentially fewer hazards (unless adversaries build capabilities in this sphere) in utilising direct forms of messaging, such the SMS network or WhatsApp / Facebook messenger messaging direct to clusters of phones in proximity to defined mobile telephony masts. In the EU, the December 2018 Directive on European Electronic Communications Code (EECC) makes it obligatory for member states to have a public warning system in place by June 2022, and there is a divide between member states around which will be using SMS and which will be using Cell Broadcast which requires no mobile phone number to operate.[76] Whether these official routes or the political-insurgent parallel routes will be seen to be more effective, is moot. A research focus on how forms of

[75] Coombs, Protecting organization reputations during a crisis.
[76] European Council and The European Parliament, DIRECTIVE (EU) 2018/1972

social media create subversive narratives, that in turn translate into collective action, remains reasonable.

The initial stages of critical incidents (such a terrorist attack) are likely to be beset with uncertainty and misunderstanding. As the Salisbury poisoning of 2018 shows us, this uncertainty can last for days and sometimes a number of weeks. Moreover, some defence officials have commented privately that they think that more significant impact from Salisbury occurred in the anxiety and uncertainty in the city, rather than the direct impact of the poisoning.[77] It is natural to assume that the public is challenged by uncertainty, but inauthentic certainty harms the government's position as the authoritative voice and research shows that it is more effective to engage in as transparent a conversation as is possible with the public,[78] even if that conversation is somewhat repetitive to reinforce the key messages[79] Government control of the information space around a crisis incident is possible – via surveillance, monitoring and messaging – but will require new techniques, some of which may be adapted from traditional SIGINT verification practices.

Balancing the Opportunity

As noted above, the social media ecosystem offers intelligence agencies a wide scope to collect, aggregate and discern the preferences, beliefs and activities of target individuals, and consequently to be able to horizon scan for emergent trends and threats, and also through which to improve targeting by constructing more accurate contextual networks. There are, however, considerable counterbalancing threats from the operation of social media platforms and there

[77] Private interview data with a Ministry of Defence and National Ambulance Resilience Unit officials, April 2018.
[78] Woon and Pang, Explicating the information vacuum.
[79] Kreiger, Amlot, and Rogers, Understanding public responses.

is a burgeoning grey literature on the surveillance that has been enacted by private companies, handset manufacturers utilising social media data.[80] Far less has been written about what should shape assertive cyber campaigns carried out by western powers using social media. This article has argued that government agencies should use social media as part of multichannel efforts to shape the communication environment during critical incidents and to shape public understanding of these incidents after they have been resolved, as part of a tactical and operational level amelioration of risk, and strategic level positioning. The public resistance to governments using technology in this way is, in part, understandable. It resonates strongly with historical and cultural impulses of the East German Stasi and Orwell's 1984, but there remains the paradox that the public are content to allow far greater levels of surveillance and manipulation of their views and purchasing habits, for commercial ends, via the large advertising bureaus of Google and Facebook.

SOCMINT offers a very limited imminent predictive capacity around critical incidents. Where this predictive capacity exists, it does so only where pre-targeting of adversaries has occurred. Because of the sheer quantity of social media data that needs to be processed, there are many points of vulnerability and potential failure in a system that necessarily relies upon systems of automated escalation. The development of ontologies to rapidly verify SOCMINT currents lags behind those which have been developed for older, and related INTs, SIGINT and ELINT. Rapid, 'best guess' verification of social media feeds can be achieved by triangulating geographical proximity of the user to the incident, a basic verification check of the history of the account (essentially a 'bot or not' check) and through using software that makes an assessment of natural language usage.

[80] Glueck, How to Stop the Abuse of Location Data; Perlroth, Conger and Mozur, China Sharpens Hacking.

SOCMINT can, however, be used to predict or detect long-term systemic level transformations and trends, and therefore can be utilised in support of horizon scanning activities albeit that these datasets present with gaps, with the caveat of the inherent limitations of self-selected social media communities. Other researchers have found that social media communities provide a skewed representation of the general population, but an accurate representation of those identifiable traits present both in social media and general society.[81] So, social media can be used to detect societal shifts in those cleavages that are present on social media, but it cannot be reliably used to detect wider shifts, nor those that occur within direct or discrete messaging services which is below that which can be reasonably observed by scholars.[82]

Social media feeds have the potential to be useful in the immediate aftermath of a critical incident in forming a contextual and sometimes tactical picture of an unfolding incident. Very little in these feeds would be counted as verified OSINT (V-OSINT) and therefore must be viewed with a high degree of caution. This is particularly so in the context of the evidence that the most recent terrorist and chemical crises which have been characterised by the appearance of disinformation appearing in the information void created in the immediate aftermath of the incident.[83] The opportunity from social media analysis and SOCMINT comes not only from its 'surveillance capacity' to its 'offensive capacity'.

Government security agencies across Europe and North America are still working through doctrinal developments and ontologies to untap SOCMINT's potential. There should be some serious concerns regarding the credibility and level of value being attributed to SOCMINT, particularly when some of this enthusiasm is being driven by a large number of commercial organisations prospecting for government contracts, with vertically integrated business models

[81] Barbero, and Riverio, Understanding the Political Representations of Twitter Users; Mellon, and Prosser, Twitter and Facebook are not representative of the general population.
[82] Kreiss, Lawrence, and McGregor, In Their Own Words.
[83] Dover, Downey, and Smith, Communicating in a Haze.

of providing hardware, systems and then advisory and maintenance work as part of an overarching package. The promises made by these businesses are strong and ambitious, but there is yet to be a sufficient number of systematic reviews of the predictive capacity of these tools, suggesting that current public investment is on a risk basis.

The weight of literature on social media is focused upon systems, rather than humans. There is a absence of material about the political preferences of programmers who create operational algorithms. This is important because machine learning is vested with the unacknowledged preferences of the programmers and stands in contrast to the belief of politicians and the public that these technologies are objective. Similarly, there is an absence of research on those inputting messages into the social media realm, be they ordinary users or practitioner users, with a few exceptions.[84] Most importantly, though, our understanding of how messages are received by users, and by what mechanism users translate a single or many messages they receive into changes of opinion, or into some form of action is underspecified, and this is the chain of causation that gives social media its potency. There are soft explanations offered in marketing and political communications studies around purchasing and voting intentions but done across small groups of self-selected subjects. The field's lack of understanding about why certain groups cluster to certain platforms, or why certain people are more persuaded by x or y type of message, needs to be addressed, or intelligence analysts will remain in danger of overreading partial and skewed datasets, from self-selected communities.

Conclusion

With caveats, SOCMINT is capable of providing horizon scanning services and strategic warning, but it is less useful in providing imminent threat data. In the aftermath of incidents, it

[84] Dencik, Hintz, Carey, Prediction, pre-emption and limits to dissent.

has some utility in providing situational awareness, but the threats from mis and disinformation remove much of that conceptual utility, and the resourcing requirement to run a situational awareness capability properly will be prohibitive for most agencies. The provision of information, be it via social media, or via legacy broadcast mediums are heavily contested non-kinetic battlegrounds, some of which are described as hybrid warfare. The level of contestation in the information space is high even in the absence of an incident, but framed by a crisis the contestation ramps up, and officials seek to push accurate, actionable advice to secure better outcomes for victims, those who might become victims and first responders, and to assert some control over the legacy and sense-making phase of the incident.

Ultimately, whilst the surveillance and analysis of open platform social media sources (which is the typical definition of SOCMINT) will be an important part of the intelligence mix, particularly in horizon scanning and during crises, there will be even greater utility in continuing to develop and refine technological ways and techniques to access 'dark web' forums. Intercepting dark web content will assist horizon scanning, warning notice and targeting, whilst refining the technical and analytical techniques around meta-data will further inform targeting. Lastly, there will be further utility in further refining the means by which to access networked devices or break cryptography, which would fit within the warning notice, targeting, and SIGINT functions. The relatively modest gains possible through SOCMINT, are outweighed by our adversaries utilisation of social media platforms (and the data from these platforms) to undermine the confidence in and operation of our democratic institutions, and from the insights into our collective centre of gravity, that our open societies provide to adversaries via these online platforms. One of the tools of contemporary globalisation is being leveraged against the way of life that generated it.

References:

Aldrich, Richard, and Christopher Moran. 2019. "Evidence submitted from Warwick University." *UK Select Committee on Defence: Hybrid Warfare Inquiry.* July 16. Accessed October 24, 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/uk-response-to-hybrid-threats/written/103533.html.

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 211-236.

Amble, John Curtis. 2012. "Combating Terrorism in the New Media Environment." *Studies in Conflict and Terrorism* 339-353.

Andrus, D.Calvin. 2005. "Toward a Complex Adaptive Intelligence Community: The Wiki and the Blog." *Studies in Intelligence* 1-30.

Arango, Tim, Nicholas Bogel-Burroughs, and Katie Benner. 2019. "Minutes Before El Paso Killing, Hate-Filled Manifesto Appears Online." *New York Times*, August 3.

Barbero, P, and G Riverio. 2014. "Understanding the Political Representations of Twitter Users." *Social Science Computer Review* 712-729.

Barquin, Ramon. 2010. "To data mine or not to data mine in the fight against terrorism ." *BeyeNetwork.* August 24. Accessed October 24, 2019. http://www.b-eye-network.com/view/14227.

Bartles, Charles K. 2016. *Russia's Indirect and Asymmetric Methods as a Response to the New Western Way of War.* Accessed 3 5, 2018. http://tandfonline.com/doi/full/10.1080/23296151.2016.1134964.

Bellaby, Ross. 2018. "Going dark: anonymising technology in cyberspace." *Ethics and Information Technology* 1-17.

Bellaby, Ross. 2018. "Going dark: anonymising technology in cyberspace." *Ethics and Information Technology* 189-204.

Bellingcat. 2019. "MH17." *Bellingcat.* October 23. Accessed October 24, 2019. https://www.bellingcat.com/tag/mh17/.

Bigo, Didier 2019. Shared secrecy in a digital age and a transnational world, *Intelligence and National Security*, 34:3, 379-394

Bradbury, Danny. 2011. "In plain view: open source intelligence." *Computer Fraud and Security* 5-9.

Bradshaw, S, and P Howard. 2017. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.* Working Paper, Oxford: Oxford Internet Institute.

Brister, Paul. 2011. "Revisiting the Gordian Knot: Strategic Considerations for Hybrid Warfare." In *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* , by Paul Brister, William Natter and Robert R Tomes, 49-59. New York: Council .

Burgess, Matthew. 2018. "The UK has no public nuclear alert system. SMS may be the answer." *Wired*, January 16.

Cammaerts, Bart. 2015. "Technologies of Self-Mediation: Affordances and Constraints of Social Media for Protest Movements." In *Civil Engagement and Social Media* , by Julie Uldam and Anne Vestergaard, 87-110. Berlin: Springer.

Chadwick, Andrew. 2017. *The Hybrid Media System: Politics and Power*, Oxford: Oxford University Press.

Clausewitz, Carl von. 1993. *On War .* London: David Campbell Publishers Ltd.

Cobain, Ian. 2017. "How Britain Did Gadaffi's Dirty Work." *The Guardian*, November 9.

Coombs, W. T. (2007). "Protecting organization reputations during a crisis: The development and application of situational crisis communication theory", *Corporate Reputation Review*, 1-14.

Cunningham, Stanley B. 2002. *The Idea of Propaganda: A Reconstruction.* Greenwood Publishing Group. Accessed 3 5, 2018. https://books.google.com/books?id=2kCFgv6FzuUC&pg=PA184.

Deep, Alex. 2015. "Hybrid War: Old Concept, New Techniques." *Small Wars Journal.* Accessed 3 5, 2018. http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques.

Defence Select Committee. 2019. *UK Response to Hybrid Threats.* https://www.parliament.uk/business/committees/committees-a-z/commons-select/defence-committee/inquiries/parliament-2017/uk-response-hybrid-threats-17-19/.

Dencik, L, A Hintz, and Z Carey. 2018. "Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom." *New Media & Society* 1433-1450.

Digital Culture Media and Sport Select Committee. 2017. *'Fake News' Inquiry.* 11 12. http://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/.

Dover, R. 2019. "UK Response to Hybrid Threat Inquiry." *UK Parliament.* January 8. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/uk-response-to-hybrid-threats/written/94257.pdf.

Dover, Robert, John Downey, and David Smith. 2019. "Communicating in a Haze: the Challenges of Hybrid Media and Hybrid Threats in Crisis Communication." *Media, Communication and Cultural Studies Association.* Stirling. 20.

Duncan, Alan. 2018. "Institute for Statecraft: Integrity Initative." *Hansard.* December 12. Accessed October 23, 2019. https://hansard.parliament.uk/commons/2018-12-12/debates/298F9A3C-307A-40ED-9CB1-3B2A98F14165/InstituteForStatecraftIntegrityInitiative.

Echevarria, Antulio. 2003. "Clausewitz's center of gravity: it's not what we thought." *Naval War College Review* 108-123.

Eikmeier, Dale. 2004. "Center of Gravity Analysis." *Military Review* 2-5.

Eltantawy, Nahed, and Julie Wiest. 2011. "Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory ." *International Journal of Communication* 1207-1224.

Engesser, Sven, Nicole Ernst, Frank Esser, and Florin Buchel. 2017. "Populism and social media: how politicians spread a fragmented ideology." *Information, Communication and Society* 1109-1126.

European Council and The European Parliament. 2018. "DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: establishing the European Electronic Communications Code." Brussels: European Commission, December 11.

Farwell, James. 2014. "The Media Strategy of ISIS." *Survival* 49-55.

Flournoy, M, and M Sulmeyer. 2018. "Battlefield Internet: A Plan for Securing Cyberspace." *Foreign Affairs* 40-46.

Georgakopoulou, Alexandra. 2014. "Small stories transposition and social media: A micro-perspective on the 'Greek crisis'." *Discourse and Society* 519-539.

Gioe, David. 2018. "Cyber operations and useful fools: the approach of Russian hybrid intelligence." *Intelligence and National Security* 1-20.

Glueck, Jeff. 2019. "How to Stop the Abuse of Location Data." *The New York Times*, October 16.

Gupta, R, and H Brooks. 2013. *Using Social Media for Global Security.* London: Wiley and Sons.

Gussow, Leon. 2018. "Toxicology Rounds: The Mysteries of Novichok and Brodifacoum." *Emergency Medicine News* 30.

Harley, Jeffrey. 1997. "Information, technology, and the center of gravity." *Naval War College Review* 66-87.

Her Majesty's Inspector of Constabulary. 2011. *The rules of engagement: A review of the August 2011 disorders.* London: HMSO.

Hills, Stefanie Anja, Thomas Jackson, and Martin Sykora. 2017. "Persuasion and the Microblog: A Model of Persuasive Communications in Terse Text." *ECSM 2017 4th European Conference on Social Media.* Vilnius: ECSM. 364.

Hoenig, Stephen. 2007. *Compendium of Chemical Warfare Agents.* New York: Springer.

Holland, Max. 2006. "The Propagation and Power of Communist Security Services Dezinformatsiya." *International Journal of Intelligence and Counterintelligence* 1-31.

HomeOffice, interview by Dover. 2017. (October 17).

House Intelligence Committee. 2018. *The Russia Investigation Taskforce of the House Intelligence Committee.* https://intelligence.house.gov/.

Iron, Richard. 2001. "What Clausewitz Really Meant by Centre of Gravity." *Defence Studies* 109-112.

Jaeger, Mark & Cavelty, Myriam Dunn (2019) From madness to wisdom: intelligence and the digital crowd, Intelligence and National Security, 34:3, 329-343

Johnson, Robert. 2018. "Hybrid War and Its Countermeasures: A Critique of the Literature." *Small Wars and Insurgencies* 141-163.

Johnson, Robert. 2018. "Hybrid War and Its Countermeasures: A Critique of the Literature." *Small Wars & Insurgencies* 141-163.

Khondker, Habibul. 2011. "Role of the New Media in the Arab Spring." *Globalizations* 675-679.

Kreiger, Kristian; Amlot, Richard and Rogers, Brooke. 2014, “Understanding public responses to chemical, biological, radiological and nuclear incidents — Driving factors, emerging themes and research gaps” *Environment International*, 66-74.

Kreiss, Daniel, Regina G Lawrence, and Shannon McGregor. 2017. "In Their Own Words: Political Practitioner Accounts of Candidates, Audiences, Affordances, Genres, and Timing in Strategic Social Media Use." *Political Communication* 8-31.

Lampos, V, T De Bie, and N. Cristianini. 2010. "Flu Detector - Tracking Epidemics on Twitter." In *Machine Learning and Knowledge Discovery in Databases*, by Balcázar J.L, Bonchi F, Gionis A and Sebag M. Berlin: Springer.

Lucas, Edward. 2018. "Don’t swallow Labour’s claims of ‘black ops’." *The Times*, December 17.

Margetts, Helen. 2017. "Why Social Media May Have Won the 2017 General Election." *The Political Quarterly* 386-390.

McMillan, Brian. 2019. "After New Zealand Shooting, Founder of 8chan Expresses Regrets." *Wall Street Journal*, March 20.

Mearsheimar, John, and Stephen Walt. 2006. "The Israel Lobby and U.S. Foreign Policy." *Middle East Policy* 29-87.

Mellon, Jonathan, and Christopher Prosser. 2017. "Twitter and Facebook are not representative of the general population: Political attitudes and demographics of British social media users." *Research and Politics* 1-9.

Mickiewicz, E. 2017. "Ellen Mickiewicz: “New info re RT”." *Johnson's Russia List.* April 6. Accessed October 5, 2017. http://russialist.org/ellen-mickiewicz-new-info-re-rt/.

Mitrokhin, Vasili. 2002. *The Soviet Intelligence Officers Handbook.* Abingdon: Frank Cass.

Monaghan, Andrew. 2019. *Dealing with the Russians.* London: Polity Press.

—. 2017. *Power In Modern Russia.* Manchester: Manchester University Press.

Monaghan, Andrew. 2016. "Putin's Way of War: The ‘War’ in Russia’s ‘Hybrid Warfare’." *Parameters* 65-75.

Mozur, Paul, and Lin Qiqing. 2019. "Hong Kong Takes Symbolic Stand Against China’s High-Tech Controls." *The New York Times*, October 3.

Nasr, Milad, Alireza Bahramali, and Amir Houmansadr. 2018. "DeepCorr: Strong Flow Correlation Attacks on Tor." *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* Toronto: Association for Computer Machinery . 1962-1976.

NATO. n.d. *NATO Library Guide – Hybrid Warfare .* http://www.natolibguides.info/hybridwarfare.

NCAInterview, interview by Robert Dover. 2018. *Senior Officer* (March 7).

Neumann, Peter, Ryan Evans, and Raffeollo Pantucci. 2011. "Locating Al Qaeda's Center of Gravity: The Role of Middle Managers." *Studies in Conflict and Terrorism* 825-842.

Niglia, Allessandro. 2016. *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges.* Brussels: NATO .

Nye, Joseph. 2004. *Soft Power. The Means to Success in World Politics.* New York: Public Affairs.

Official, Senior Ambulance, interview by Dover. 2018. (April 18).

Omand, David. 2018. *From Nudge to Novichok: The response to the Skripal nerve agent attack holds lessons for countering hybrid threats.* Working Paper, Helsinki: The European Centre of Excellence for Countering Hybrid Threats.

—. 2009. *Securing the State.* London: Hurst and Company.

Omand, David. 2018. "The threats from modern digital subversion and sedition." *Journal of Cyber Policy* 1-19.

Omand, David, Jamie Bartlett, and Carl Miller. 2012. "Introducing Social Media Intelligence (SOCMINT)." *Journal of Intelligence and National Security* 801-823.

Palttala, P., & Vos, M. (2012). Quality Indicators for Crisis Communication to Support Emergency Management by Public Authorities. Journal of Contingencies and Crisis Management, 20 (1), 39-51

Parker, Andrew. 2018. (May 14).

Perlroth, Nicole, Kate Conger, and Paul Mozur. 2019. "China Sharpens Hacking to Hound Its Minorities, Far and Wide." *New York Times*, October 22.

Pfaffenberger, Fabian. 2018. "Beyond #covfefe - a critical look at Twitter as a scientific base." *68th Annual Meeting of the International Communication Association.* Prague: International Communication Association. 1-21.

Piero, Elisa. 2014. "Emergent Policing Practices: Urban space securitisation in the aftermath of the Manchester 2011 riots." *Surveillance and Society* 38-54.

Public Health England. 2018. *Public Health England statement regarding events in Salisbury.* London, March 23.

Quezada, Mauricio, Barbara Poblete, and Denis Parra. 2017. "Gaining historical and international relations insights from social media: spatio-temporal real-world news analysis using Twitter." *EPJ Data Science* 1-35.

Renz, Bettina. 2016. "Russia and 'hybrid warfare'." *Contemporary Politics* 22 (3): 283-300. Accessed 3 7, 2018. http://tandfonline.com/doi/full/10.1080/13569775.2016.1201316?scroll=top&needaccess=true.

Reuter, Christian; Marc-Andre Kaufhold, Thomas Spielhofer, and Anna Sophie Hahne. 2017. "Social media in Emergencies: A Representative Study on Citizen's Perception in Germany", *PACM on Human-Computer Interaction*, 19 pages

Reynolds, Barbara. 2006. "Response to Best Practices", *Journal of Applied Communication Research*, 249-252

Rogers, Michael. 2017. "Admiral Michael Rogers, Commander US Cyber Command." May 9. https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

Rønn, Kira Vrist & Søe, Sille Obelitz (2019) Is social media intelligence private? Privacy in public and the nature of social media intelligence, Intelligence and National Security, 34:3, 362-378,

Rubin, James: Amlot, Richard, and Lisa Page. 2011. "THE LONDON POLONIUM INCIDENT: LESSONS IN RISK COMMUNICATIONS." *Health Physics* 545-550.

Ruggiero, A., and M. Vos. 2014. "Social Media Monitoring for Crisis Communication : Process, Methods and Trends in the Scientific Literature." *Online Journal of Communication and Media Technologies* 105-113.

Salisbury Journal. 2018. *Man found critically ill at Maltings in Salisbury man is former Russian spy Sergei Skripal.* March 5. Accessed June 6, 2018. http://www.salisburyjournal.co.uk/news/16066343.Critically_ill_man_is_former_Russian_spy/?ref=arc.

Seaton, Jane. 2016. "Brexit and the Media." *The Political Quarterly* 333-337.

Seely, Bob. 2018. *A Definition of Contemporary Russian Conflict: How Does the Kremlin Wage War? .* London: Henry Jackson Society.

Shipley, Todd, and Art Bowker. 2013. "Investigating Social Networking Sites." In *Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, by Todd Shipley and Art Bowker, 315-344. New York: Syngress.

Snowden, Edward. 2019. *Permanent Record.* London: Pan MacMillan.

Strange, Joe. 1996. *Centers of Gravity and Critical Vulnerabilties.* New York: US Marine Corps Press.

Sumiala, J, M Tikka, J Huhtamaki, and K Valaskivi. 2016. "#JeSuisCharlie: Towards a Multi-Method Study of Hybrid Media Events." *Media and Communication* 97-108.

Sunstein, Cass. 2018. *#Republic: Divided Democracy in the Age of Social Media.* New Jersey: Princeton University Press.

The British Army. 2019. *Who we are: Bridge 77, Influence and Outreach.* October 23. Accessed October 23, 2019. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/.

Tokmetzis, Dimitri, Maurits Martjin, Riffy Bol, and Foeke Postma. 2018. "Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app." *De Correspondent.* July 8. Accessed July 20, 2018. https://decorrespondent.nl/8481/heres-how-we-found-the-names-and-addresses-of-soldiers-and-secret-agents-using-a-simple-fitness-app/412999257-6756ba27.

Tonkin, Emma, Heather D Pfeiffer, and Greg Tourte. 2012. "Twitter, information sharing and the London riots?" *Bulletin of the American Society for Information Science and Technology* 49-57.

UK Ministry of Defence. 2018. *Joint Doctrine 1/18 Cyber and Electromagnetic Activities.* Doctrine, London: UK Ministry of Defence.

University of Swansea. 2017. *Research Suggests Bots Generated Social Media Stories During EU Referendum.* http://www.swansea.ac.uk/media-centre/latest-research/researchsuggestsbotsgeneratedsocialmediastoriesduringeureferendum.php.

Urban, Mark. 2018. *The Skripal Files: The Life and Near Death of a Russian Spy.* London: MacMillan.

Veil, Shari; Buehner, Tara and Palenchar, Michael. 2011. "A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication", *Journal of Contingencies and Crisis Management*, 110-122

Vos, Marita; Ragnhild Lund, Zvi Reich and Halliki Harro-Loit. 2011. *Developing a crisis communication scorecard : outcomes of an international research project 2008-2011,* University of Jyväskylä

Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. "The spread of true and false news online." *Science* 1146-1151.

Wolfsfeld, Gadi, Elad Segev, and Tamir Sheafer. 2013. "Social Media and the Arab Spring: Politics Comes First." *The International Journal of Press/Politics* 115-137.

Woon, E. and Pang, A. (2017), "Explicating the information vacuum: stages, intensifications, and implications", *Corporate Communications: An International Journal*, Vol. 22 No. 3, pp. 329-353

Wright, Paul. 2013. *Meet Prism's Little Brother: SOCMINT.* June 26. Accessed March 22, 2018. https://www.wired.co.uk/article/socmint.

Wu, T. 2017. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads.* New York: Atlantic Books