State, media and civil society in the information warfare over Ukraine

Golovchenko, Yevgeniy; Hartmann, Mareike; Adler-Nissen, Rebecca

Published in:
International Affairs

DOI:
10.1093/ia/iiy148

Publication date:
2018

State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation

YEVGENIY GOLOVCHENKO, MAREIKE HARTMANN AND REBECCA ADLER-NISSEN*

Digital disinformation has become an increasingly prominent topic in both public and academic debates. In 2016, the World Economic Forum identified online warfare and disinformation as one of the top ten global risks.[1] The use of disinformation—which is distinct from misinformation in being not only false but false as part of a 'purposeful effort to mislead, deceive, or confuse'[2]—preoccupies western audiences.[3] Particularly in the wake of the crisis in Ukraine that erupted in 2013–2014, the Kremlin has been accused of orchestrating disinformation campaigns against the Ukrainian government and western countries by using online trolls and state-controlled online outlets such as RT (formerly known as Russia Today), Sputnik and Life News.[4] This has led to a wave of counter-disinformation measures in the West to combat what is seen as a threat

* We wish to thank Sune Lehmann, Frederik Georg Hjorth, Anders Søgaard, Jason Reifler, Joshua A. Tucker, Richard Bonneau, Fanny Marie Brændholt Sørensen, JungHwan Yang, Bertel Teilfeldt Hansen, Amelia H. Arsenault, Federico Botta, Emily Blout, Steven Livingston, Gregory Asmolov, Jon Kyst, Jonas Gejl Pedersen, Brian Keegan, Pål Røren, Sergey Sanovich and Anders Wivel for their helpful comments. We would also like to thank participants at presentations at the Social Media and Political Participation (SMaPP) lab, the Sunbelt Conference (2017), the Annual Meeting of the Danish Political Science Association (2017) and the lnternational Studies Association's Annual Convention (2018) for their helpful comments. Our research was conducted as part of the 'Digital Disinformation' project (project no. CF16-0012), funded by the Carlsberg Foundation and DIPLOFACE, funded by the ERC (project no. 680102), both directed by Rebecca Adler-Nissen.

1 World Economic Forum, *Global Risk Report* (Geneva: World Economic Forum, 2016).

2 Jim Fetzer, 'Disinformation: the use of false information', *Minds and Machines* 14: 2, 2004, pp. 231–40 at p. 231.

3 Hunt Allcott and Matthew Gentzkow, 'Social media and fake news in the 2016 election', *Journal of Economic Perspectives* 31: 2, Spring 2017, pp. 211–36; David Lazer, Matthew Baum, Nir Grinberg, Lisa Friedland, Kenneth Joseph, Will Hobbs and Carolina Mattsson, *Combating fake news: an agenda for research and action*, report of a conference held 17–18 Feb. 2017 (Cambridge, MA, and Boston: Harvard University and Northeastern University, 2017), https://shorensteincenter.org/wp-content/uploads/2017/05/Combating-Fake-News-Agenda-for-Research-1.pdf; Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini and Filippo Menczer, 'The spread of low-credibility content by social bots', Sept. 2017, https://arxiv.org/abs/1707.07592; Fabio Giglietto, Laura Iannelli, Luca Rossi and Augusto Valeriani, 'Fakes, news and the election: a new taxonomy for the study of misleading information within the hybrid media system', *Convegno AssoComPol 2016*, Dec. 2016, pp. 1–40, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2878774. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 31 July 2018.)

4 Corneliu Bjola and James Pamment, 'Digital containment: revisiting containment strategy in the digital age', *Global Affairs* 2: 2, May 2016, pp. 131–42; Peter Pomerantsev, 'The Kremlin's information war', *Journal of Democracy* 26: 4, Oct. 2015, pp. 40–50; Rod Thornton, 'The changing nature of modern warfare: responding to Russian information warfare', *RUSI Journal* 160: 4, Sept. 2015, pp. 40–48; Andrei Aliaksandrau, 'Brave new war: the information war between Russia and Ukraine', *Index on Censorship* 43: 4, Dec. 2014, pp. 54–60.

International Affairs **94**: 5 (2018) 975–994; DOI: 10.1093/ia/iiy148

to democracy, international security and stability. Yet while we know a certain amount about top-down regime tactics and strategies, we know much less about who actually spreads digital disinformation and who counters it.

Within the field of political science as well as within propaganda and security studies, disinformation campaigns are often described as 'information warfare', sponsored more or less directly by governments.[5] The term refers to the strategic use of information and disinformation to achieve political and military goals.[6] While this concept highlights the importance of ordinary citizens, it implies that information is used as a weapon and the minds of citizens are the 'battlefield'.[7]

One significant example of information warfare in the western debate is the Russian mainstream media's dissemination of the Kremlin's disputed statements about Russia's annexation of Crimea in 2014. At first, the Kremlin claimed that the Russian armed forces were not conducting an operation to capture Ukrainian territory, framing the presence of armed men as an uprising led exclusively by local citizens in Crimea against the new government in Ukraine. The Russian government later withdrew this statement, acknowledging its military involvement in Crimea in support of the local rebels.[8] At the height of the crisis, false information about what was alleged to be a purely local conflict may have helped the Kremlin create confusion as to whether Ukraine was actually at war and, if so, with whom. At the same time, it also made political or military confrontations with Russia more difficult to legitimize.[9] General Philip Breedlove, Supreme Allied Commander for NATO in Europe at that time, went as far as calling the Russian operation 'the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare'.[10]

While many western scholars use the term 'information warfare' to describe the spread of pro-Kremlin information to western audiences, Russian public officials and academics argue that western countries are also waging information warfare against Russia.[11] According to these Russian observers, the West seeks to destabilize Russia's current political regime, weaken the country's position in the international arena and spread 'Russophobia'.[12]

[5] Thornton, 'The changing nature'; Brett van Niekerk, 'Information warfare in the 2013–2014 Ukraine crisis', in Jean-Loup Richet, ed., *Cybersecurity policies and strategies for cyberwarfare prevention* (Hershey, PA: IGI Global, 2015); Edward Spiers, 'NATO and information warfare', in David Welch, ed., *Propaganda, power and persuasion: from World War I to WikiLeaks* (London: I. B. Tauris, 2013); Philip M. Taylor, *Munitions of the mind: a history of propaganda* (Oxford: Oxford University Press, 2013).

[6] Thornton, 'The changing nature', p. 43.

[7] Myriam Dunn Cavelty and Victor Mauer, 'The role of the state in securing the information age: challenges and prospects', in Myriam Dunn Cavelty and Victor Mauer, eds, *Power and security in the information age: investigating the role of the state in cyberspace* (London: Routledge, 2008); see also Thornton, 'The changing nature'.

[8] 'Putin acknowledges Russian military serviceman were in Crimea', *RT International*, 17 April 2017, https://www.rt.com/news/crimea-defense-russian-soldiers-108/.

[9] Roy Allison, 'Russian "deniable" intervention in Ukraine: how and why Russia broke the rules', *International Affairs* 90: 6, Nov. 2014, pp. 1255–97.

[10] Quoted in Peter Pomerantsev, 'Russia and the menace of unreality', *The Atlantic*, 9 Sept. 2014, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

[11] Igor Panarin, 'SMI, Propaganda I informatsionnije vojni', *Litres*, 2017; Jolanta Darczewska, 'The anatomy of Russian information warfare: the Crimean operation. A case study', *Point of View* 42: 5, May 2014, pp. 5–37; Igor Panarin, 'Vtoraja mirovaja informatsionaja vojna—vojna protil Rosii', Km.ru, 10 Jan. 2012, http://www.km.ru/node/631035/c.

[12] Tatiana Sergeevna Kovaleva, quoted in Rolf Fredheim, 'Filtering foreign media content: how Russian news

Both the western and the Russia-favoured conceptions of information warfare share the assumption that waves of 'weaponized' information are generated by the state or state-sponsored agents.[13] From this perspective, civilian support for or mistrust towards governments is acknowledged, but citizens are mainly seen as targets for manipulation in large-scale online information operations. Few scholars and security practitioners have systematically explored the active role citizens actually play, as social media 'users who are not professionally active in politics but express political opinions or comment on events'.[14]

This article presents a different understanding of digital (dis)information by examining the role and scale of citizen engagement in relation to state and commercial media during an international conflict.[15] We have selected one of the most controversial examples of information warfare in the Ukrainian crisis: the downing of the Malaysian Airlines Flight 17 (MH17) in the Ukrainian war zone in 2014. This case is relevant for the exploration of digital disinformation during international conflicts since information about the event has generally been seen to come from sources within, or close to, governments. We focus specifically on the social media network Twitter, which differs from Facebook and the Russian social media site VKontakte (similar to Facebook) in that it centres on news sharing and has the ability to facilitate global engagement among audiences in Russia, Ukraine and the West.

To this day, different media outlets, public officials and activists are supplying the global online public with different, often contradictory, answers to the key question: who shot down flight MH17 on 18 July 2014, killing the 298 civilians on board? One of the dominant narratives, largely supported by Russian mainstream media, suggests that Ukrainian forces were responsible for shooting down the plane.[16] The opposing narrative, largely supported by the Ukrainian government, citizen activists, and citizen journalist collectives such as Bellingcat, holds Russian separatists or the Russian government responsible.[17] Depending on the answer to this question, the parties involved will be found either responsible or not responsible for the MH17 plane crash—and, subsequently, guilty or not guilty of promoting false information about one of the most important events in the Ukrainian crisis.

The article proceeds as follows. First, we provide brief background to the MH17 incident and the way in which the notion of information warfare has hitherto been understood. We point to the methodological limitations and empirical blind spots of this state-centric concept and propose instead to conceptualize citizens as *curators* of (dis)information. Then we move on to present our research design,

agencies repurpose western news reporting', *Journal of Soviet and Post-Soviet Politics and Society* 1: 1, 2015, pp. 37–39.

[13] Thornton, 'The changing nature'; Spiers, 'NATO and information warfare', Panarin, 'Vtoraja mirovaja'; Taylor, *Munitions of the mind*.

[14] Julian Ausserhofer and Axel Maireder, 'National politics on Twitter', *Information, Communication and Society* 16: 3, 2013, p. 298.

[15] For distinctions among state, market and civil society, see Jean L. Cohen and Andrew Arato, *Civil society and political theory* (Cambridge, MA: MIT Press, 1994), p. ix.

[16] Sarah Oates, 'Russian media in the digital age: propaganda rewired', *Russian Politics* 1: 4, 2016, pp. 398–417; Irina Khaldarova and Mervi Pantti, 'Fake news: the narrative battle over the Ukrainian conflict', *Journalism Practice* 10: 7, April 2016, pp. 891–901.

[17] Matt Sienkiewicz, 'Open BUK: digital labor, media investigation and the downing of MH17', *Critical Studies in Media Communication* 32: 3, July 2015, pp. 208–23.

which draws on a dataset of approximately 950,000 tweets related to the MH17 event. In the third section we present our findings, using social network analysis to decipher the network of retweets and identify its core of 2,434 most engaged users. In the fourth and final section, we discuss the results of our enquiry. Our findings clearly show that citizens are not just the purveyors of government messages; they actually generate the most popular content about the MH17 event among the most engaged Twitter users. Citizens are curators of both disinformation and counter-disinformation, even in the context of state-sponsored information and state-controlled media.

Information warfare and the case of MH17

On 17 July 2014, four months into the war between Russian-backed separatists and the Ukrainian military, a Malaysian Airlines passenger flight (MH17) was shot down over Ukraine, killing all 298 passengers and crew members on board, including 193 Dutch, 43 Malaysian, 27 Australian, 12 Indonesian, 10 British and 13 citizens with other nationalities.[18] There was a clear global consensus that the crash was a tragedy; but in the hours following the event rival explanations of its cause began to circulate on social media. Western media outlets claimed that the plane was brought down by pro-Russian separatists. The Russian government, on the other hand, claimed that the Ukrainian military had shot down the plane. The downing of MH17 helped turn the Ukrainian crisis into an international conflict, prompting the EU and NATO to introduce tougher sanctions against Russia. Meanwhile, the Russian government maintained (and continues to maintain) that no missile had crossed from Russia into Ukraine.

In 2015, following several months of investigation, the Dutch Safety Board brought out its final report on the cause of the MH17 crash. It concluded that the plane had been shot down by a missile launched by a BUK surface-to-air system.[19] In September 2016, a Dutch-led joint investigating team (JIT)—which included police and judicial authorities from Australia, Belgium, Malaysia, the Netherlands and Ukraine—presented the results of its investigation into the crash. These results were based on extensive forensic analysis, audio intersections, and more than 100 interviews with eyewitnesses and other informants. The JIT found that flight MH17 was shot down by a missile from an area controlled by pro-Russian separatist rebels. The investigation discovered that the BUK had been transported from the Russian Federation to a separatist-controlled area, and, after the downing of MH17, had been returned to Russia.[20] The JIT linked the missile system to Russia's 53rd anti-aircraft missile brigade based in Kursk in the Russian Federation.[21] Subsequently,

[18] Dutch Safety Board, *Crash of Malaysian Airlines flight MH17* (The Hague, 2015), https://www.onderzoeksraad.nl/uploads/phase-docs/1006/debcd724fe7breport-mh17-crash.pdf?s=678D995FE7E3080B6256880A456CED959FE4ECBC, p. 27

[19] Dutch Safety Board, *Crash of Malaysian Airlines*.

[20] Joint Investigation Team (JIT), *Presentation preliminary results criminal investigation MH17*, 28 Sept. 2016, https://www.om.nl/@96066/presentation/.

[21] Joint Investigation Team (JIT), *Update in criminal investigation MH17 disaster*, 24 May 2018, https://www.om.nl/vaste-onderdelen/zoeken/@103183/update-criminal/.

Australia and the Netherlands stated that they held Russia responsible under international law.[22] In 2018, referring to the JIT's findings, the G7 called for Russia to 'account for its role' in the MH17 affair.[23]

This article accepts the JIT's findings as reliable and accurate. Accordingly, as will be further explained in the section on methods below, social media posts that question the JIT findings (that the plane was shot down from territory controlled by Russian separatists using Russian weapons) are seen as examples of pro-Russian disinformation. An example is the Twitter post: '#Ukraine MH17 may be CIA false flag and it ain't flying Alex Jones' Infowars: There's a war on for your mind!' Here, the user refers to the conspirationalist American site InfoWars, which claims that the CIA shot down the plane in order to discredit Russia, without counterbalancing the claim. For that reason, this tweet is seen to represent disinformation.

Understanding information warfare in the Ukraine crisis

The burgeoning literature on digital information warfare sees civil society as the main target of disinformation. However, in our view the role of citizens has not yet been fully explored. Most research on the online spread of pro-Kremlin information tends to focus on state agents or state-controlled agents.[24] This tendency is particularly prevalent in work carried out in political science and security studies that explores the roles played by the military, established political decision-makers or government-controlled news media in Russia.[25] While they may differ in approach, these studies of pro-Kremlin disinformation share the underlying assumption that the Russian government pursues its political and military goals by mobilizing support among the civilian population; and that this is achieved through disinformation and manipulation in conventional and digital media. However, few empirical studies actually examine *how* citizens are mobilized and *what role* they play.

Studies of pro-Kremlin disinformation—in the context of the increasing hostility between the West and Russia—can be grouped into three categories. One category of scholarship concentrates on strategic narratives and disinformation discourses developed by the Kremlin or state-controlled Russian media. For example, in her analysis of Russian media and the MH17 crash, Sarah Oates finds

[22] Shaun Walker, 'MH17: Australia and Netherlands accuse Russia of complicity', *Guardian*, 25 May 2018, https://www.theguardian.com/world/2018/may/25/mh17-australia-and-netherlands-accuse-russia-of-complicity.

[23] Agence France-Presse, 'Russia must "account for role" in shooting down MH17, says G7', *Guardian*, 16 July 2018, https://www.theguardian.com/world/2018/jul/16/russia-must-account-for-role-in-shooting-down-mh17-says-g7.

[24] Thornton, 'The changing nature'; Alexander Lanoszka, 'Russian hybrid warfare and extended deterrence in eastern Europe', *International Affairs* 92: 1, Jan. 2016, pp. 175–95; Niekerk, 'Information warfare'; Ralph D. Thiele, *Crisis in Ukraine: the emergence of hybrid warfare*, ISPSW Strategy Series (May 2015), https://www.files.ethz.ch/isn/190792/347_Thiele_RINSA.pdf.

[25] Christina Cottiero, Katherine Kucharski, Evgenia Olimpieva and Robert W. Orttung, 'War of words: the impact of Russian state television on the Russian internet', *Nationalities Papers* 43: 4, March 2015, pp. 533–55; Thornton, 'The changing nature'; Pomerantsev, 'The Kremlin's information war'; Fredheim, 'Filtering foreign media content'; Elizaveta Gaufman, 'Memory, media, securitization: Russian media framing of the Ukrainian crisis', *Journal of Soviet and Post-Soviet Politics and Society* 1: 1, 2015, pp. 141–74; Stephen J. Cimbala, 'Sun Tzu and salami tactics? Vladimir Putin and military persuasion in Ukraine', *Journal of Slavic Military Studies* 27: 3, July 2014, pp. 359–79.

that Russian state elites have consolidated 'information dominance' over citizens.[26] Studying primarily state television and its response to online information on the MH17 event, Oates concludes that the Russian state has effectively 'rewired' its propaganda to take account of the global information flows and domestic online content. While Oates's tracing of the strategic narrative is very compelling, she examines only the way in which particular ideas are projected, primarily on state television; she does not look into who actually spreads them online.

The second category of scholarship analyses the specific techniques used by the Russian regime to spread disinformation online—including trolls, bots, influence campaigns, hacking and smear campaigns, and fake news.[27] Here, scholars have emphasized the continuation of Cold War propaganda strategies.[28] As Sanovich puts it, 'the ability of Russian propaganda to infiltrate dark corners of social media platforms—from the alt-right subreddits to the far-left Twitter threads—with self-serving narratives should not be surprising: this is Russian modus operandi in more traditional media too'.[29] While these studies recognize the important role of civilian support, they tend to conceptualize civil society in passive terms, and see social media as a fertile ground for state-controlled flows of information.

The third category of scholarship focuses specifically on the use of disinformation in the conflict over Ukraine and the Russian annexation of Crimea. These studies interpret the online battle in military and strategic terms, as a conflict driven by state agents in 'hybrid warfare'—that is, the combination of conventional deterrence using guerrilla tactics and information warfare.[30] In such conceptualizations, the civilian population is crucial, but it is still understood as something that can be easily manipulated. For example, in Alexander Lanoszka's convincing analysis of hybrid warfare, Ukraine is described as having a 'weak civil society' with many cleavages where distrust can be exploited by the belligerents.[31]

Other scholars have argued that studies of the online struggle over Ukraine should give more prominence to the online activity of ordinary citizens.[32] As Mejias and Vokuev explain, citizens use social media to generate, consume or distribute false information, contributing to a new order 'where disinformation acquires a certain authority'.[33] Yet Mejias and Vokuev offer limited evidence on *who* these citizens are, and *how* they relate to state elites or media. In another inter-

[26] Oates, 'Russian media', p. 399.

[27] See e.g. Peter N. Tanchak, 'The invisible front: Russia, trolls, and the information war against Ukraine', in Olga Bertelson, ed., *Revolution and war in contemporary Ukraine* (Stuttgart: Ibidem Verlag, 2017). For a different reading of trolling, emphasizing differences with past strategies, see Xymena Kurowska and Anatoly Reshetnikov, 'Neutrollization: industrialized trolling as a pro-Kremlin strategy of desecuritization', *Security Dialogue*, forthcoming.

[28] Andrew Hoskins and Ben O'Loughlin, 'Arrested war: the third phase of mediatization', *Information, Communication and Society* 18:11, Aug. 2015, pp. 1320–38.

[29] Sergey Sanovich, *Computational propaganda in Russia: the origins of digital misinformation*, Oxford Computational Research Project, working paper no. 2017.3, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf, p. 5.

[30] Lanoszka, 'Russian hybrid warfare', see also Sten Rynning, 'The false promise of continental concert: Russia, the West and the necessary balance of power', *International Affairs* 91: 3, May 2015, pp. 539–52.

[31] Lanoszka, 'Russian hybrid warfare', pp. 178–9.

[32] See e.g. Khaldarova and Pantti, 'Fake news'.

[33] Ulises A. Mejias and Nikolai E. Vokuev, 'Disinformation and the media: the case of Russia and Ukraine', *Media, Culture and Society* 39: 7, Oct. 2017, pp. 1027–42 at p. 1029.

esting study, Toal and O'Loughlin examine the effects on citizens of exposure to television, specifically how it influences their opinion of who is responsible for the crash of flight MH17. But they do not analyse online debates.[34]

Citizen engagement with pro-Kremlin online disinformation, then, remains relatively uncharted territory. This leaves a number of questions open, including which profiles are most active in propagating disinformation online.

Conceptualizing citizen curators

Social media challenges the control that traditional media previously had over the production and dissemination of news. The digital age facilitates user-generated content and visibility as citizens actively search for, and produce, new information in an environment characterized by growing distrust of professional journalism and established authorities. This development has challenged the information gatekeeping role of professional media, and has enabled citizens, social movements, voluntary groups and citizen journalist collectives to move from being passive audiences to active *curators* of information.

'Curation' is the term that has come to be used to describe the way organizations and individuals behave online on a range of digital platforms from Wikipedia to Instagram. Curation was traditionally linked to the care and preservation of artefacts in museums or galleries. But a curator is now seen as someone who 'adds cultural value to artefacts when drawing individual items together into a collection, interpreting their relevance to a theme [and] then re-representing them through a story or visuals'.[35] On social media, curation involves producing, selecting and spreading information online.[36] So on Twitter, a tweet or a retweet can be seen an act of information curation. In the case of MH17, curation is about actively shaping competing narratives about why the plane crashed.

However, just as the museum and art worlds are stratified into hierarchies,[37] so online curators differ in their influence. Social media sites are not egalitarian platforms where attention is distributed equally among users; these sites are embedded in pre-existing inequality structures, which explains why the most popular users in the entire Twitter sphere are primarily celebrities from the entertainment industry, established political figures or large news corporations.[38] States and corporations have the economic resources to promote content as well as engage professional staff to manage their accounts. Such resources are less accessible to ordinary citizens. Consequently, the struggle for visibility takes place in a network where some curators are more capable of shaping the public debate than others.

[34] Gerard Toal and John O'Loughlin, '"Why did MH17 crash?": blame attribution, television news and public opinion in southeastern Ukraine, Crimea and the de facto states of Abkhazia, South Ossetia and Transnistria', *Geopolitics*, published online 22 Sept. 2017, https://www.tandfonline.com/doi/full/10.1080/14650045.2017.1364238.

[35] StefanNowatny, quoted in Anita Howarth, 'Exploring a curatorial turn in journalism', *M/C Journal* 18: 4, 2015, http://journal.media-culture.org.au/index.php/mcjournal/article/view/1004>.

[36] Sarah Pedersen and Simon Burnett, '"Citizen curation" in online discussions of Donald Trump's presidency: sharing the news on Mumsnet', *Digital Journalism* 6: 5, 2018, pp. 545–62, https://doi.org/10.1080/21670811.2017.1399806.

[37] Pierre Bourdieu, *Distinction: a social critique of the judgment of taste* (London: Routledge, 1984).

[38] Christian Fuchs, *Social media: a critical introduction* (London: Sage, 2017), p. 232.

By using the concept of curation, we are not suggesting that citizens are isolated from discourses propagated by governments and mainstream media. Moreover, the fact that citizens curate information originally produced by governments or government-sponsored agents—while also generating their own content—is in line with previous studies of information warfare. However, some citizens may have interpreted the MH17 crash in accordance with the Kremlin's narrative (or with the findings of the JIT) without ever being directly exposed to, or manipulated by, news sources loyal to the Kremlin (or to the JIT). Indeed, many of the most prolific disseminators of disinformation use sophisticated arguments that they construct—or partly construct—themselves. Yet so far we have had limited insight into how, and to what extent, citizens actively shape the stream of information through curation.

Methods and data

To understand the interrelations between state, citizens and media in the spread of disinformation, we have drawn on social network analysis. In recent years, social network analysis has become more central to International Relations and security studies. It has been used to analyse terrorist networks and gang-related crime,[39] and it has been applied to social media data on foreign policy issues. To our knowledge, social network analysis has not yet been applied in scholarly analyses of pro-Kremlin digital disinformation. One of the merits of social network analysis is that it is deeply data-driven. There are few theoretical assumptions other than the ideas that people relate to each other, and that the structure and strength of these relations matter. One of the most important ways in which people relate to each other is by sharing information. For this reason, we believe social network analysis is particularly suitable for a study of the curation of digital disinformation.

As noted above, we have chosen to focus on Twitter as it remains one of the most important sites for global debates on 'truths' in international conflicts. Moreover, the debate on Twitter is embedded in narratives propagated by governments and mainstream media. In addition, it is possible to gather a large and representative sample of tweets (unlike Facebook data, which are generally not so readily accessible).

Our data consist of tweets starting from the day of the crash on 17 July 2014 and ending on 9 December 2016. The dataset was collected using 'Gardenhose', a tool for downloading the platform's public data and as such a part of Twitter's own application programming interface (API).[40] This approach generated a random sample of 10 per cent of all the tweets within the specified period that contained one or more keywords related to MH17 (in total 941,028 tweets). Specifically, we searched for at least one keyword or hashtag in the tweet or profile name that

[39] Carlo Morselli and David Décary-Hétu, 'Crime facilitation purposes of social networking sites: a review and analysis of the "cyberbanging" phenomenon', *Small Wars and Insurgencies* 24: 1, Feb. 2013, pp. 152–70; Thomas Zeitzoff, John Kelly and Gillad Lotan, 'Using social media to measure foreign policy dynamics: an empirical analysis of the Iranian–Israeli confrontation (2012–13)', *Journal of Peace Research* 52: 3, 2015, pp. 368–83.

[40] We thank Professor Alan Mislove, Northeastern University, for access to MH17 tweets based on the Twitter Gardenhose feed.

related to MH17: *MH17*, *MH17* (with Cyrillic letters), *Malazijskij* [and] *Boeing* (in Russian), *#MH17*, *#Pray4MH17*, *#PrayforMH17*. The hashtags and keywords were selected to make sure they clearly related to the crash of MH17 (and not the Ukraine crisis as such), and that they were neither pro-Ukrainian nor pro-Russian.

To identify which users had the greatest impact, we analysed a network of retweets, where 'nodes' represent users and 'edges' (i.e. connections) represent retweets. We established the connection between two profiles by linking the Twitter handle name of the retweeted user with the handle name of the one who was being retweeted.[41] By making the network *directional*, we were able to analyse the direction of the retweets, i.e. from whom to whom the particular tweet had travelled.

We relied on the metric of 'in-degree', 'out-degree' and 'betweenness' centrality to analyse this directional network. The user's out-degree centrality score represents the number of profiles that she has retweeted in the network. Users with high out-degree centrality are active in retweeting many different profiles. They play a crucial role in disseminating and amplifying already existing tweets. In-degree centrality refers to the number of accounts that have retweeted the user in question. Users with high in-degree centrality have a high 'impact' at the core of the network. In this case, impact refers to the ability to generate content that is retweeted throughout the network by many users. Accounts that have both high in-degree and low out-degree centrality generate popular content that is retweeted by many users, even though they themselves rarely retweet others. They are the most central curators of information. Normalized betweenness centrality, ranging from 0 to 1, indicates the extent to which the respective users are in 'between' other users in the network. Users with high betweenness centrality play an important bridging role, because they often comprise the shortest path from one user to another in the network of information.[42]

Identifying the most engaged information curators

To identify which Twitter users are most engaged in the debate over the crash of flight MH17, we have used Stephen Seidman's k-core method, which helped us to focus the analysis on the smaller, most engaged subset of the network.[43] The k-core has been found to be the best measure for identifying the top-performing information spreaders on social media.[44] In a network such as Twitter, the centrality of a profile is a quantitative measure of how important the given profile is. A k-core is a maximal subset of the network where all nodes are connected to at least 'k' number of other nodes: so 'k' can be any whole number. In this case, two nodes are defined as 'connected' if one user retweets the other. We limited our analysis

[41] Few users change their handle names, so that they are represented with multiple nodes in the retweet network. This issue occurs rarely. Of the 450,605 profiles in the entire dataset with user IDs known to us, 4,173 have multiple handle names. This is equivalent to only 0.92 per cent. We limit the analysis to links between the users who retweet and the original sources of the tweets, leaving out the intermediary retweeters.

[42] The formal description of the normalized betweenness score used in this study is available in the *igraph* package documentation: http://igraph.org/r/doc/betweenness.html.

[43] Stephen B. Seidman, 'Network structure and minimum degree', *Social Networks* 5: 3, 1983, pp. 269–87.

[44] Sen Pei, Lev Muchnik, José S. Andrade, Jr., Zhiming Zheng and Hernán A. Makse, 'Searching for superspreaders of information in real-world social media', *Scientific Reports* 4: 5547, 2014, pp. 1–12.

to the core of the network by setting k equal to 10. In the following, we will simply refer to it as the k-10 core. In other words, the users in the k-10 core have themselves retweeted—or have been retweeted by—at least 10 other users. The entire network consists of 364,773 users (nodes) with 511,127 retweets (edges), and the k-10 core of the network comprises 2,434 profiles with 47,229 retweets.

Due to the relatively high retweet threshold (k=10), the delimited subset of users differs from the entire Twitter network. The core consists of both high-impact users who generate popular content and those who are highly active in disseminating tweets from other accounts. Each member of the group is therefore both more engaged in the public debate than the average Twitter user and more connected to other highly engaged users. The k-10 core is dominated by the use of English to an even greater extent than the entire retweet network. We define a user as belonging to a specific language group if at least 75 per cent of all original tweets posted by her are in the language. By this standard, 66.9 per cent of all users in the k-10 core are part of the English-speaking group (compared to 50.8 per cent in the entire retweet network). Among the top five languages in the network core, English-speaking users are the most prevalent (66.9 per cent), followed by Russian- (13.2 per cent), Dutch- (9.7 per cent), German- (1.4 per cent) and Indonesian-speaking users (0.5 per cent). Our analysis is limited to the highly engaged and cohesive subset of users who are at the core of the predominantly English-speaking debate on the MH17 crash.

Results

In this section, we start by examining the polarization of the MH17 debate in the entire network. We then move on to analyse which type of profile (state, professional media, civil society group or citizen) is most influential in the cohesive core of the network, and what role they play when it comes to spreading different narratives about the MH17 crash.

Polarization and the representation of MH17

To map the information struggle over the MH17 plane crash, we analysed the content of the tweets, how they relate to one another and who spreads them. We randomly sampled 10,000 tweets in English out of the 513,715 English tweets and retweets in the entire corpus. We limited our content analysis to English for pragmatic reasons—simply because it is the dominant language in the entire network as well as in the k-10 core. The tweet texts were manually coded using the following descriptors:

(1) a pro-Ukrainian frame, where the Russian Federation or pro-Russian separatists in Ukraine are explicitly or implicitly portrayed as responsible for the crash (10.3 per cent), for example:

Video - Missile that downed MH17 'was brought in from Russia' @peterlane5news
RT @mashable: Ukraine: Audio recordings show pro-Russian rebels tried to hide #MH17 black boxes

(2) a pro-Russian frame, where Ukrainian authorities, NATO or EU countries are explicitly or implicitly blamed for shooting down the plane (5.5 per cent), for example:

Detailed analysis: MH17 shot down by Ukrainian SU-25 cannon fire and air-to-air missile
Why the USA and Ukraine, NOT Russia, were probably behind the shooting down of flight #MH17

(3) a neutral frame, where neither Ukraine nor Russia or any others are blamed for shooting down the plane (84.2 per cent), for example:

#PrayForMH17 :(
RT @deserto_fox: Russian terrorist stole wedding ring from dead passenger #MH17

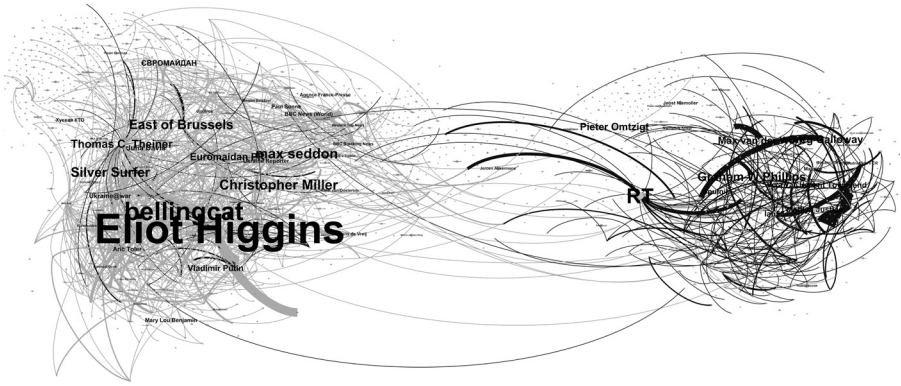
Since this article finds the investigations of the Dutch Safety Board and the JIT to be reliable, we refer to tweets as 'pro-Russian disinformation' in cases where the narrative deflects the blame away from the Kremlin by denying its involvement in the incident and instead blames Ukraine or the West. It is important to note that users spreading pro-Kremlin disinformation about the MH17 crash cannot automatically be assumed to favour the Russian government; they may be critical towards the Kremlin when it comes to other issues or events. Furthermore, curators who spread pro-Russian tweets may not be intentionally misleading, since these users may be fully convinced of the truthfulness of the stories they are retweeting. The real motivation of each user remains unknown to us. Structurally, however, these tweets become part of a larger disinformation campaign, supported by Russian media loyal to the government and by Kremlin officials presumably aware of a situation that involves Russian armed forces. Willingly or unwillingly, Twitter users become part of this campaign by spreading disinformation. The same structural issue holds for users who spread pro-Ukrainian narratives.

Four coders were responsible for the coding, among them two of the authors. Prior to coding, coders went through a training phase where they could discuss and resolve conflicting interpretation of tweets. Because the randomly sampled, coded tweets appear in the total corpus multiple times (as duplicates and retweets), our final coded corpus consisted of 128,423 tweets, of which 10,000 were coded as 'pro-Ukrainian' and 3,442 were coded as 'pro-Russian'. By transferring these codes from the entire dataset to the limited subset, we were able to categorize 10 per cent of the retweets in the k-10 core. The connection between two users was labelled either pro-Russian or pro-Ukrainian if at least one of the retweets connecting the two contained the relevant framing.[45] Figure 1 illustrates the results of our analysis. It clearly reflects a polarization of the MH17 network into two opposing clusters. In the k-10 core (counting 2,434 members), the pro-Russian disinformation frames (black) are concentrated in the cluster to the right, where the users with highest in-degree centrality predominantly blame Ukraine or the West for the deaths of civilians in the MH17 crash. The pro-Ukrainian counter-disinfor-

[45] We saw no instances of two users being connected simultaneously by 'pro-Ukrainian' and 'pro-Russian' retweets.

mation frames (grey)—representing users who blame Russia or Russian separatists for the downing of the flight—are concentrated on the opposite side. Both disinformation and counter-disinformation are concentrated in their respective opposing poles, with relatively few direct links between them.

Figure 1: K-10 core retweet network: disinformation (black) and counter-disinformation (grey)



Note: Nodes represent profiles. A connection between two nodes is established if one profile has retweeted the other profile at least once. Connection weight reflects number of retweets. The graph includes only those connections where the retweets have been annotated as either 'pro-Ukrainian' (grey) or 'pro-Russian' (black). Node and profile name size reflect impact (in degree). The metric is computed using all 47,229 retweets and is therefore not limited to manually annotated English tweets. The full profile names do not reflect real names. For instance, 'Vladimir Putin' is a 'pro-Ukrainian' troll account under the handle name @DarthPutinKGB.

Which users are most influential?

We then moved on to examine which type of profile was most influential in the network. To do so, the 2,434 profiles in the cohesive core had to be manually coded by two coders into the subcategories of 'state', 'civil society' and 'media'.[46] Our coding was based on the profiles' self-description, reflecting how the users choose to portray themselves online. Some users might describe themselves as 'journalists' even if they have not been formally educated as such and are not employed by any media entity in this function. Going by Twitter names, current 'avatars' and the self-descriptions of the profiles, the following codes were used to identify the profiles with these results:

1 *state institutions* (1.6 per cent): governmental or intergovernmental institutions
2 *public officials* (1.2 per cent): ministers, governmental advisers, and public officials working in intergovernmental institutions
3 *politicians* (0.6 per cent): members of, or candidates for, national/local parliaments, and politicians in international or supranational bodies

[46] The coding process is fully described in the codebook for manual annotation available on our project website: https://disinfo.ku.dk/.

4 *commercial and state media* (6.6 per cent): commercial or state-owned newspapers, radio stations, TV channels or news websites
5 *journalists* (6.2 per cent): journalists, editors, correspondents, columnists, etc. (excludes profiles who describe themselves as 'citizen journalists' as well as bloggers and journalists working for non-profit volunteer news sites)
6 *civil society groups* (2.5 per cent): NGOs, grassroots organizations, social movements, non-profit research centres, non-profit volunteer news sites, and citizen journalist groups
7 *citizens* (74.4 per cent): individual users who are not journalists, politicians or public officials (includes users whose profiles lack self-description)
8 *other* (1.1 per cent): profiles that fall outside any of the categories listed above (e.g. universities, think-tanks and political parties)
9 *removed from Twitter* (5.8 per cent): profiles no longer available on the platform.

On both the disinformation and the counter-disinformation sides, we found many citizen and civil society group profiles. To further ensure that the citizen profiles we identified were not bots, we used the Botometer API.[47] The Botometer tool assigns a score between 0 and 1 to a user profile reflecting the likelihood that the profile is a bot. The score is calculated on the basis of a wide range of parameters, including information about the network, tweet content and activity patterns.[48] Only 2 per cent of these citizen profiles in the k-10 core had a bot score higher than 0.6. While the Botometer's predictions are far from perfect, the bot score distribution on the k-10 core suggested that a majority of the users classified as 'citizens' were indeed likely to be humans.[49] What we found more difficult to determine was whether the citizen accounts were covertly managed by government agents to manipulate the public. However, in 2017 Twitter provided the US Congress with a list of 2,752 human-controlled Twitter profiles linked to Russia's Internet Research Agency (IRA), popularly known as the 'Russian Troll Farm'.[50] Interestingly, none of these trolls appeared in the k-10 core. Although it is impossible to determine with complete certainty, we found no indication that any of the citizen profiles in our sample were managed by the IRA.

Media profiles, including media outlets and individual journalists, represented 13 per cent of the users in the k-10 core. The media cluster appeared to be divided into two opposing poles: a group of western media, dominated by a pro-Ukrainian framing of the crash, on the one hand, and the pro-Russian RT on the other hand. As reflected in table 1, commercial and state media in the k-10 core tend not to pass on information by retweeting other users. Instead, individual journal-

[47] See the Botometer website: https://botometer.iuni.iu.edu/#!.
[48] Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer and Alessandro Flammini, 'Online human–bot interactions: detection, estimation and characterization', *Proceedings of the International Conference on Web and Social Media (ICWSM)*, March 2017, https://arxiv.org/abs/1703.03107.
[49] Only 8.8 per cent of citizen profiles have a bot score of above 0.5. The low proportion could be caused by Twitter systematically removing bots. We can only categorize a profile if it has not been removed during the manual coding. Many of the removed accounts may have been bots. The removed profiles do not play a central role in the network.
[50] The US Congress has publicized the IRA list: see https://democrats-intelligence.house.gov/uploadedfiles/exhibit_b.pdf.

ists may play a bridging role in the network as indicated by their high betweenness score, offering a potential flow of information between the two opposing poles of disinformation and counter-disinformation. However, further research is needed to conclusively establish the role of individual journalists as bridges between opposing views on MH17.

Table 1: Profile type ranked by normalized betweenness centrality

Profile type	No. of profiles	In-degree mean	Out-degree mean	Betweenness mean
Civil society groups	62	32.4	8.1	0.00145
Journalists	151	30.6	4.8	0.00074
Citizens	1,811	9.6	15.6	0.00073
Public officials	29	29.5	3.9	0.00058
Removed from Twitter	141	9.4	14.0	0.00043
Politicians	15	23.5	3.9	0.00042
Commercial/state media	160	29.4	2.9	0.00023
State institutions	39	22.5	3.1	0.00014
Other	26	12.0	10.4	0.00014
All	2,434	13.4	13.4	0.00068

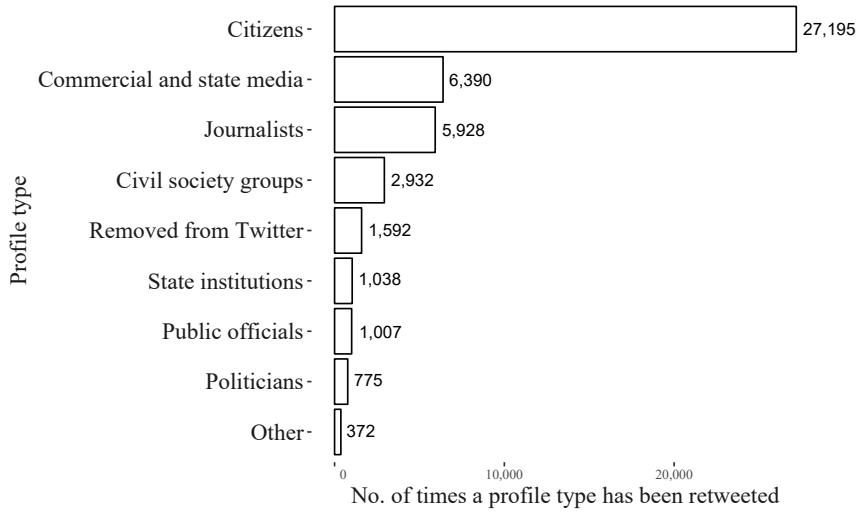
Note: The metrics are based on all 47,229 retweets in the k-10 core – including non-English retweets that have not been included in the content analysis.

Citizens and informational impact

Interestingly, citizens as a combined group have the highest impact when it comes to generating popular content in the core of the retweet network. Out of the total 47,229 retweets that connect the k-10 core group, 27,195 are retweets of posts that have been uploaded by citizens. This is illustrated in figure 2. As a group, citizens are 4.3 times more likely to be retweeted than commercial and state media profiles.

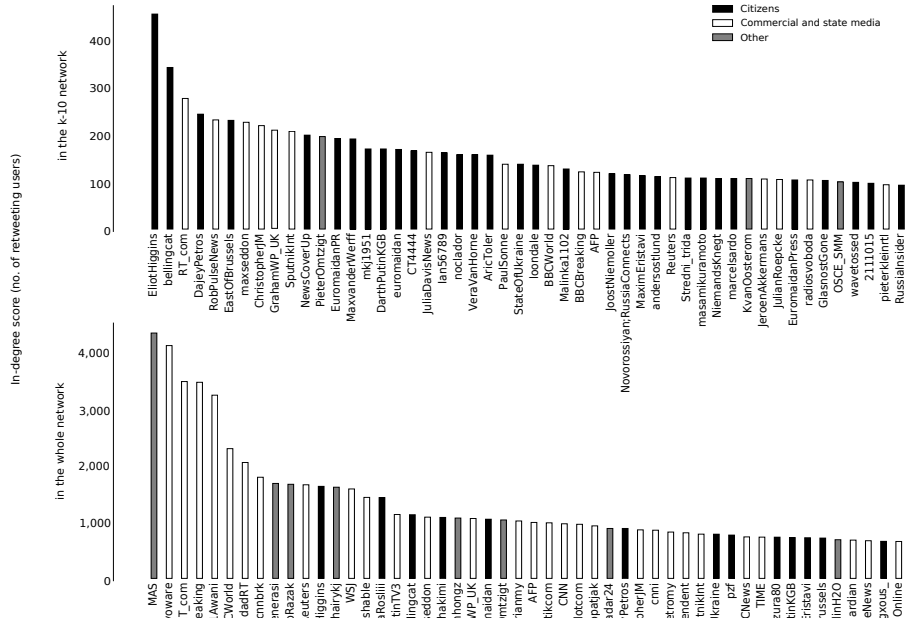
While a citizen profile is retweeted by only 9.6 users (on average)—compared to 32.4 for journalist profiles—citizens have the highest impact of any group. The highly central role of citizens and civil society in the network core cannot be attributed to the large number of citizens alone. The central role of citizens is surprisingly high even when the overall number of citizens is taken into account. Figure 3 provides an overview of the top 50 profiles with the highest in-degree scores—i.e. the number of users who have retweeted the relevant profile in the k-10 core and in the entire retweet network as such. Of the top 50 profiles in the k-10 core, 31 portray themselves as 'civil society' accounts, including 6 'civil society groups' and 25 'individual citizens'. If the sheer number of citizens alone drove the centrality of citizen and civil society accounts, we would see the same pattern in the entire retweet network, where the proportion of citizen profiles is likely to be even higher than in the core. Yet, surprisingly, when we looked at the entire network, we saw that the number of citizen profiles in the list of the 50

Figure 2: Number of times a profile type has been retweeted in the k-10 core



Note: The numbers include all 47,229 retweets in the k-10 core—including non-English retweets that have not been included in the content analysis.

Figure 3: Top 50 profiles in the k-10 core and the whole retweet network (ranked by in-degree centrality)



Note: In this figure, 'citizens' refers to both individual citizen accounts and civil society group accounts. 'Commercial and state media' includes group accounts as well as individual journalists.

most central users had dropped from 25 to 10, whereas the number of commercial and state media profiles had increased from 7 to 23.

This suggests that citizens are a central source of information at the core of the online debate about MH17, where many highly engaged users interact with each other. Established media profiles, on the other hand, are more dominant outside the network core—on the periphery of the full network. Media profiles have a stronger reach among the more isolated and less active profiles, who are connected to only a few other users.

This finding leads us to the question of which profiles are the most significant in spreading disinformation and counter-disinformation. We analysed the disinformation network (the network based only on tweets coded as pro-Russian) and the counter-disinformation network (the network based only on tweets coded as pro-Ukrainian) separately. Not surprisingly, we found RT to be the most important profile among the top 50 profiles (the profiles with the highest in-degree scores) in the disinformation network—when all non-disinformation tweets were filtered out. Interestingly, however, 39 out of the 50 most central profiles in the disinformation network were citizens. Apart from the citizens' profiles, the top 50 profiles included three commercial and state media profiles (RT, Sputnik and Ruptly); six journalist profiles; and two profiles that had been removed from Twitter at the time of coding. This suggests that individual citizens are much more central as *sources* of disinformation stories than we would expect to be the case from the literature on information warfare. Thus, civil society is not just a target for information warfare, but appears as the most central *producer* of disinformation—even in a social media network like Twitter, biased towards established media. Of course, users might still have been manipulated prior to tweeting disinformation; even so, while civil society might be 'weak', our study clearly shows that citizens are very active in the online debate, and create many of the most popular tweets themselves.

When we looked at which profiles were most active in spreading counter-disinformation (i.e. information that supports the findings of the JIT), we found that citizens also play an important role (19 out of the top 50 profiles). This means that citizens are not only the most central profiles when it comes to spreading disinformation; they play an equally important role when it comes to countering disinformation. The most important profile in the counter-disinformation network is the journalistic civil society group 'Ukraine Reporter'. This is followed by the individual account of Eliot Higgins, the founder of the citizen journalist group Bellingcat, together with that group's own account, @bellingcat. Among the top 50 profiles in the counter-disinformation network are 19 citizen profiles; 11 journalist profiles; 10 commercial and state media profiles; 6 civil society group profiles; and 4 public official / state institution profiles. This leads us to conclude that citizens dominate the core of the online debate over the MH17 crash.

Discussion: citizen curators of (dis)information

Our analysis shows that neither disinformation nor counter-disinformation is as strongly state-driven as is often assumed in the case of the Ukraine conflict. Our analysis also points to the grey zones between citizen comments and journalism, as well as to the methodological problem of labelling different profiles over time. For example, the second most retweeted pro-Kremlin profile (after RT) belongs to Graham W. Phillips, a British self-styled journalist who travels around eastern Ukraine and Russia. Phillips was employed part-time by RT until 2014, and from 2014 to 2015 by Zvezda,[51] but he operates as an individual. Nevertheless, we have chosen to label him a journalist, to ensure that we do not overestimate the number of citizens.[52] Interestingly, the most retweeted profile in the entire dataset is Eliot Higgins, a central member of the Bellingcat citizen journalist group that conducts open-source investigations on social media. Over time, Bellingcat has become professionalized, but it started out as a small civil society group. Drawing on Google satellite imagery and geo-tagged photographs, Higgins's tweets have become a key source of information in the public debate about what happened to flight MH17 and have helped official investigations into the downing of MH17. According to Higgins, this would not have been possible without 'social media posts from local citizens in Eastern Ukraine and the Russian border region with Ukraine'.[53]

Both Higgins and Phillips, operating on two different sides of the Twitter sphere, are representatives of the quasi-professional role that some individuals assume in the battle for truth about the MH17 crash. They also illustrate that in the case of the MH17 incident both disinformation and counter-disinformation are, to a large degree, carried out not only by professional journalists and governments, but also by individuals. To reduce these profiles to passive purveyors of state interests would be to ignore the fact that they produce and curate the most influential pieces of information about the incident, whether this information is false or not.

Our findings resonate with, and add greater nuance to, research within communications and media studies on digital misinformation. For several years, media scholars have explored the way citizens make editorial judgements on social media, concluding that social media websites and blogs, which allow for the bypassing of traditional gatekeepers, contribute to the dissemination of misinformation.[54] Yet, as we have shown here, citizens are as active in correcting disinformation online as they are in spreading disinformation.

[51] A channel owned by the Russian Ministry of Defence.

[52] Max Seddon, 'How a British blogger became an unlikely star of the Ukraine conflict—and *Russia Today*', BuzzFeed News, 20 May 2014, https://www.buzzfeed.com/maxseddon/how-a-british-blogger-became-an-unlikely-star-of-the-ukraine?utm_term=.ielXOd7Ea#.jpBz9n4aO.

[53] Eliot Higgins, 'A new age of open source investigation: international examples', in A. Babak Akhgar, P. Saskia Bayerl and Fraser Sampson, eds, *Open source intelligence investigation: advanced sciences and technologies for security application* (Cham: Springer, 2016), p. 189.

[54] Jane B. Singer, 'User-generated visibility: secondary gatekeeping in a shared media space', *New Media and Society* 16: 1, 2014, pp. 55–73.

The data do not offer a decisive answer to the question *why* citizens play such an important role in spreading disinformation and countering it at the core of the MH17 network. Staying with the concept of curation, the distinct credibility attaching to citizens may be the driving mechanism. Historically, intelligence services and propaganda institutions have posed as ordinary citizens to assume a credibility that they lack in their own roles.[55] Moreover, credibility is becoming an increasingly scarce commodity for governments around the world. According to Pew Research, levels of trust in the government are declining in the United States.[56] Gallup polls also indicate that trust in mass media among Americans has been trending downwards during the last two decades, reaching a historical low in 2016, when only 32 per cent of respondents replied that they had 'a great deal' or 'a fair amount' of trust in the mass media.[57] Seen from this perspective, the lack of trust in government institutions and mass media organizations may strengthen civil society actors as an alternative source of information. During international conflicts, when national media and governments from competing countries seek to weaken each other's credibility, we would expect online audiences to contest not only competing 'truths' about political or military events, but also the credibility of well-known civil society actors, including their relation to the less credible government and media institutions. And indeed, there are many instances in the MH17 case where key civil society actors accuse each other of being funded by government institutions such as the CIA or the Kremlin.

Why do citizens curate information in ways that amplify or counter pro-Kremlin disinformation? There are many possible reasons why ordinary citizens may engage in spreading false news. For instance, Vosoughi and colleagues argue that false news spreads faster and more broadly on Twitter because it appears more novel and enticing than true news.[58] While we cannot compare our results directly to this study owing to differences in research design, the argument resonates with the MH17 case, where many of the tweets are hyper-sensational. Some of the pro-Kremlin tweets claim that the CIA set up the crash to delegitimize Russia; that the flight was shot down by Ukrainian Nazis; or that the flight was filled with corpses before take-off in Amsterdam. However, the sensational character of these stories does not itself explain why some individuals engage in spreading false news and others actively counter the stories.

One of the main driving factors behind citizen engagement in (dis)information on the MH17 incident could be users' political alignment. A growing body of literature suggests that people are more likely to believe or engage with informa-

[55] Garry King, Jennifer Pan and Margaret E. Roberts, 'How the Chinese government fabricates social media posts for strategic distraction, not engaged argument', *American Political Science Review* 111: 3, 2017, pp. 484–501; Franziska Keller, David Schoch, Sebastian Stier and Jung Hwang Yang, 'How to manipulate social media: analyzing political Astroturfing using ground truth data from South Korea', *Proceedings of the Eleventh ICWSM Conference*, Palo Alto, California (The AAAI Press, 2017), pp. 564–67.

[56] *Public Trust in Government: 1958–2017* (Washington DC: Pew Research Center, 14 Dec. 2017), http://www.people-press.org/2017/12/14/public-trust-in-government-1958-2017/ .

[57] Art Swift, *Democrats' confidence in mass media rises sharply from 2016* (Washington DC: Gallup, 21 Sept. 2017), https://news.gallup.com/poll/219824/democrats-confidence-mass-media-rises-sharply-2016.aspx.

[58] Soroush Vosoughi, Deb Roy and Sinan Aral, 'The spread of true and false news online', *Science* 359: 6380, 2018, pp. 1146–51.

tion that aligns with their pre-existing knowledge, experience or political views, a mechanism described as politically motivated 'selective exposure'.[59] The term refers to a well-documented phenomenon, namely that individuals often tend to expose themselves to information sources that match their own political views more than to politically discordant sources.[60] Accordingly, we would expect highly conservative users—e.g. those with anti-globalist or anti-EU convictions—to be more engaged in producing and disseminating (false and true) pro-Russian content, because the Kremlin is ideologically aligned with these users, promoting itself as a challenge to global elites and the EU. In contrast, the Ukrainian government brands its country as an aspiring progressive nation set on a course towards joining the EU. Similarly, users with political views that are discordant with the Kremlin's brand of conservatism and anti-globalism may be more likely to spread (true or false) information that contests the Kremlin's legitimacy. These expectations need to be tested empirically by future studies.

Conclusion

Information warfare is not what it used to be. In the age of social media, individual citizens can be more influential than states and professional mass media in spreading information. Analysing the opposing 'truths' about who was responsible for shooting down flight MH17 over Ukraine in 2014, we have explored which Twitter profiles were most active in spreading (dis)information about the crash. While it is not surprising that many citizens are highly engaged on Twitter, we show that individual citizens are the most influential *curators* on Twitter in the polarized debate over MH17, in spreading *both* disinformation *and* counter-disinformation among the most engaged users.

Even during international conflicts such as the one in Ukraine, where regime-controlled media and information campaigns compete over particular narratives, a citizen profile is 4.3 times more likely to be retweeted than a commercial and state media profile. Of the top 50 most central accounts, 31 belong to either individual citizens or civil society groups. A proportion of the tweets posted by citizens contain links to external sources that propagate the Kremlin's or western governments' opposing portrayals of reality. By retweeting these narratives, ordinary citizens actively help produce, select and edit the vast stream of contradicting narratives. Importantly, this pattern is limited to the network core of users who are most engaged in the discussion of MH17. Established media maintain a dominant role at the periphery of the retweet network—among individuals who are more isolated and less engaged in the debate.

[59] Stephan Lewandowsky, Ullrich K. H. Ecker and Colleen M. Seifert, 'Misinformation and its correction: continued influence and successful debiasing', *Psychological Science in the Public Interest* 13: 3, 2012, pp. 106–31; Andrew Guess, Brendan Nyhan and Jason Reifler, *Selective exposure to misinformation: evidence from the consumption of fake news during the 2016 US presidential campaign*, 9 Jan. 2018, https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf.

[60] Kelly R. Garrett, 'Echo chambers online? Politically motivated selective exposure among internet news users', *Journal of Computer-Mediated Communication* 14: 2, 2009, pp. 265–85.

If the concept of 'information warfare' is not fully adequate in the case of the MH17 crash and the conflict in Ukraine, we need to adopt new approaches. Any meaningful attempt to fight digital disinformation will need to engage citizens and civil society groups, not just by raising awareness, but by mobilizing them—acknowledging that they are now *curators* of information. Moreover, to explore how truths about international conflicts are fought over in the digital age, it is not enough to analyse particular narratives. It is crucial to analyse the entire online conversation, using methods such as social network analysis. By turning our attention to not just *what* is said, but also to *how* information flows and *who* spreads it, we can begin to understand how digital disinformation—and attempts to counter it—succeed. Such understanding will ultimately allow us to identify the most influential agenda-setters.