

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

<https://www.e-ir.info/2019/01/21/hacking-westphalia-ict-infrastructures-fake-news-and-global-politics/>

ANDREA PAVÓN-GUINEA, JAN 21 2019

Digital platforms and other internet services have opened the way for people to connect, debate and gather information; yet they have also increased the spread of fake news which, in turn, has become a key problem for the functioning of our democracies, affecting people's understanding of reality. Despite being an old phenomenon, the term fake news has gained increasing importance due to the rise of digital platforms online. Today, the term refers to false or misleading information made to look like fact-based news stories in order to influence public opinion or earn advertising money (Kalsnes, 2018). The salience of the term 'fake news' nowadays stems from a confluence of events, namely, the election of Donald Trump as US President and its use of the term 'fake news' for retaliation against critical reporting. Secondly, both the Brexit vote and other European elections and the role of the Russian disinformation military strategy in them. Finally, it is also necessary to take into account the crucial role of social media for news consumption nowadays (Nelson and Taneja, 2018). Taken together, these circumstances have contributed to a media environment where fake news spreads faster, deeper and further than genuine information (Vosoughi, 2018).

Furthermore, in the contemporary world, we find ourselves increasingly surrounded by prominent material forces: from climate change-fueled storms to a ubiquitous computational infrastructure where the social world is constantly intermingling with the material world in complex and diverse ways (Srnicek et al., 2013). Following the 'material turn' in International Relations, this article points to the importance of the Information and Communications Technology (ICT) infrastructure that incentivizes the production, circulation and consumption of fake news. Instead of looking at fake news through a national security lens, this article argues that disinformation campaigns take advantage of industry-standard digital advertising and marketing tools (Ghosh and Scott, 2018): the spread of disinformation and fake news is strongly linked to the nature of social media as advertising platforms.

Taking up David Beer's call for the need to explore and describe 'power through the algorithm' (2009: 999), this article thus attempts to analyze the technological facets of fake news by focusing on the ICT materiality that allows and sustains contemporary forms of digital circulation.

The Intimate Relationship Between Fake News and The Media

Fake news is not a new phenomenon but its history is parallel to that of real news: they began to circulate widely after the printing press was invented in 1439. However, as it has above mentioned, social media and their personalization tools have accelerated its spread and the use of the term that gained visibility during the final months of the 2016 United States presidential election, when viral fake news prompted more engagement on Facebook than real news.

Notwithstanding the above, there is no universally agreed upon definition of what fake news constitutes. Authors such as Conroy et al. (2015), O Klein and Wueller (2017) or Shu et al. (2017) have adopted a definition of fake news based on 'authenticity' and 'intent'. This way, 'fake news is news articles that are intentionally and verifiable false and could mislead readers'.

Fake news, propaganda and disinformation are three terms that recently have been used interchangeably despite the

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

differences in their meaning. For the purpose of this article, propaganda is considered as the 'systematic dissemination of information in a biased or misleading way in order to promote a political cause or point of view', and has been often associated with political persuasion and psychological warfare (Bentzen, 2017).

On the other hand, disinformation can be defined as the 'dissemination of deliberately false information, supplied by a government or its agent to a foreign power to the media, with the intention of influencing the policies or opinions of those who receive it' (Bentzen, 2017).

Milosevich-Juaristi (2017), has argued that the term has its origins in Russian 'dezinformacija' and goes on to explain that what distinguishes Russia from other 'cyber actors' and disseminators of lies is the use of information warfare as a military strategy defined by and integrated into the most recent Military Doctrine of the Russian Federation, official since 2014. In light of the illegal referendum taking place in Catalonia, the author defines the Russian disinformation strategy as 'combination' (kombinaciya) to refer to the operation which integrates diverse instruments such as cyberwarfare, cyber-intelligence, disinformation, propaganda and collaboration with players hostile to the values of liberal democracy.

Disinformation, in this sense, is different from misinformation to the extent that the latter is considered as 'erroneous and incorrect information' that, contrary to 'disinformation', is intention-neutral.

In regard to fake news, it can be fabricated for two main reasons: to mislead publics or to generate traffic ('clickbait'). In the former case, fake news falls under the categorization of disinformation. Taking all of this into account, this article understands fake news as news that is intentionally and verifiable false and could have either been designed for political or economic and commercial purposes (Kalsnes, 2018). This way, by following this definition this article rules out other conceptions of fake news such as satire, rumours, conspiracy theories, misinformation and hoaxes.

On the other hand, Vosoughi et al. (2018) investigated the differential diffusion of all of the verified true and false news stories distributed on Twitter from 2006 to 2017 and found that false news spread farther, faster, deeper and more broadly than the truth. There are various theories and statistics that shed light on the symbolic and material factors that have contributed to this spread. Those are the following:

Firstly, fake news is today of growing importance due to various reasons among which stands out the fact that barriers to entry in the media industry have dropped precipitously, both because it is now easy to set up websites and because the increasing ability to monetize web content through advertising platforms (Allcott and Gentzkow, 2017). Fake news outlets, in turn, lack the news media's editorial norms and processes for ensuring the accuracy and credibility of information.

Secondly, a growing number of European Union's citizens (around 46%) follow news on social media (Newman et al. 2018). Moreover, a recent study confirmed that 59% of all links shared on social networks are actually clicked on and past on without having read them. This means that the majority of people are sharing articles without reading past the headlines. The reasons are mainly twofold: the economy of attention (attention spans are low) and the fact that it's effortless and more rewarding to give the impression you have read and shared something that the intrinsic value of having read it (Gabelkov et al. 2016). This is in line with the postulates of social identity theory and normative influence theory (Tajfel and Turner, 1979; 2004). Moreover, according to the Information theory and Bayesian decision theory, novelty attracts human attention and encourages information sharing and false information is often significantly more novel than the truth (Vosoughi et al., 2018).

Thirdly, and following the latest Reuters Institute Digital News Report (2018), 53% of the respondents prefer to access news through search engines, social media or news aggregators, interfaces that use ranking algorithms to select stories, rather than interfaces are driven by humans (homepage, email and mobile notifications). By contrast, only a third say they trust the news they find in search engines, while news in social media is seen as even more unreliable (just 23% trust them) (Newman et al. 2018).

In this sense, winning consumer trust is becoming a central issue in today's digital world as businesses compete for

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

attention. The results explain that just 44% of the people surveyed have reported to actually trust the news. This may be due to the fact that the greater the sources, the greater the variety of perspectives on an issue and therefore this can lead to confusion, scepticism and ultimately to a lack of trust.

Related to trust, the report has also researched the public concern over fake news. More than half of the global sample (54%) expresses concern or strong concern about 'what is real or fake' when thinking about online news.

Lastly, despite the shift towards reader payment models, it is worth noting that the majority of online news consumption still happens through free websites, largely supported by advertising.

The main argument of this article is that despite the theories that point to the heuristics and social processes behind the spread of fake news, we need to pay attention to the digital infrastructure that enables the production, dissemination and consumption of fake news.

ICT infrastructure and Fake News: Ethical and Political Implications

The conversation I am trying to begin in this article looks at the ICT infrastructural elements that enable the spread of fake news; that is to say, it focuses on how fake news is governed by concrete material contexts and assemblages (Bucher, 2012a).

The main argument of this article is that the spreading of this type of news is dependent on a number of different technologies and their related business models; the algorithms that are embedded in social media platforms have intrinsically many editorial implications: they are designed to favour sharing certain kinds of contents, with a strong incentive towards encouraging engagement with the system (Fernandez, 2017; Mejías, 2013). This way, this article follows up on Susan Leigh Star's (1999) calling for taking infrastructures seriously (Bucher, 2012b: 2).

In this regard, Ghosh and Scott (2018: 3-4) argue that the interconnected tools of behavioural data collection, digital advertisement platforms, search engine optimization, social media management software and algorithmic advertising technology is 'a brilliant technological machine' that serves to align the economic interests of advertisers and social media platforms. This way, it is necessary to study the entire marketplace of digital advertising while disentangling this alignment of economic interests that lie at the heart of the digital platforms' infrastructure that ultimately fuels the spread of fake news. That is to say, this article argues that the infrastructure of advertising technology perfectly suits the function of disinformation and fake news operations: 'A successful disinformation campaign delivers a highly responsive audience that drives forward engagement on the platform and ultimately delivers more revenue for all parties'. In other words, the central argument of this article is that the spread of fake news today partly succeeds because it follows the infrastructural logic of social media platforms. Following Ghosh and Scott (2018), this article will subsequently analyze the tools that enable the spread of fake news.

The first tool under consideration is the collection of behavioural and location data through web cross-device and tracking technologies for advertising purposes: firstly, the more behavioural data collected on users, the better companies can create targeted ads; secondly, by showing the most relevant content to the user, companies keep those consumers on the platform for a longer time (Ghosh and Scott, 2018). Kirkpatrick (2016) explains that the business has rapidly evolved from conventional ad placement to the use of algorithmic technologies that determine the consumer audience for the delivery and display of online advertising. Disinformation propagators seek thus to collect as much data about potential audiences as possible in order to tailor content across media channels and target advertisements on internet platforms: the more information they know about the potential publics, the easier is to manipulate them through the spread of disinformation (Ghosh and Scott, 2018).

As a matter of fact, in 2017 digital ad revenues surpassed television for the first time and Facebook, Google and Twitter are considered the most desirable publishing outlets (Bucklin and Hoban, 2017). It is worth mentioning that these advertising platforms are typically powered by algorithm technologies so targeted advertisement can be dispatched automatically across thousands of websites and social media platforms simultaneously. This way, the search algorithm sits at the center of the internet economy (Ghosh and Scott, 2018).

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

Another important tactic of disinformation campaigns is the manipulation of commercial search algorithms in order to disrupt results. The importance of Google on this topic is of crucial importance since the entire internet content industry is organized in response to its algorithm (Dash, 2007). This has a direct impact on democracy since search results on news topics play a role in shaping public opinion and therefore has a role in the integrity of the public debate. Manipulation here is key since, for instance, 95% of web traffic goes to sites on page 1 of Google search results (Kaye, 2013). Furthermore, there is evidence of the use of 'black hat' SEO (Search Engine Optimization) tactics by disinformation campaigns. Those tactics consist of putting a particular webpage in the top ranks for a short period of time by tricking the Google search algorithm into assigning a search rank that 'does not correspond to quality content, source reputation or topic relevant responsiveness to the query' (Ghosh and Scott, 2018: 17-20).

On the other hand, at the intersection between machines learning algorithms and advertising technology lie the social media management services, which draws on behavioural data analytics, engages in real-time social media listening to place the message and coordinates across multiple channels simultaneously and automatically. Given the current importance of social media, advertisers can use this technology with the purpose of creating content and sharing it in just a few clicks through social media management platforms like Hootsuite, which supports social network integrations for Twitter, Facebook, LinkedIn, YouTube, Instagram, Tumblr, Google+, etc. These social media management services are weapons of disinformation propagators since they allow them to map sentiment on social media, promote content distribution based on that and coordinate across multiple platforms and sites simultaneously: this way, 'all parties in the ecosystem benefit financially from successful advertising campaigns, [yet] opening the door to abuses that harm the public by weakening the integrity of democracy' (Ghosh and Scott, 2018: 25).

All in all, this analysis has attempted to focus on how relevant is the digital ICT infrastructure to disinformation operations. By investigating the materiality of fake news, one could arguably conclude that the economic incentives of the digital platforms and the political or commercial objectives of disinformation operators are aligned: they take advantage of the digital market infrastructure and how it is designed to deliver targeted messages to millions of people at a low cost and with little transparency. However, this lack of transparency and accountability have the potential to progressively weaken the integrity of democracies by separating citizens from facts and polarizing the political culture of a given country (Ghosh and Scott, 2018). Such conclusions have led a number of commentators to claim that we are now entering an era of widespread algorithmic governance, wherein algorithms will play an increasing role in the exercise of power by disciplining and controlling societies (Kitchin, 2017: 15). In a similar spirit, Shirky (2009) has put forward the concept of 'algorithmic authority' and warned against the dangers of its lack of accountability and transparency. Algorithms suffer from a serious transparency deficit: their process of construction and the specific way in which they work are secret and protected and therefore not open to public scrutiny. Despite being a question that directly goes against the tech giants' business models, the public should have a say on the question as towards what ends are algorithms programmed.

Fake news possesses both symbolic and material characteristics, and in this sense, this article has argued that it is important to focus on the ICT infrastructure that incentivizes the production, dissemination and consumption of fake news online. It has also drawn attention to the fact that algorithms are built in unaccountable practices of selection and encoding and often disguised under the veil of objectivity (Livingstone, 2014).

As a result, these sets of practices have a deep claim on democratic life (Anderson, 2011) because they shape our possibilities to political action. This way, the politics of algorithms should become a question of ethical responsibility in our democratic world and traditional 'theories of freedom should accommodate this new media infrastructure' (Turner, 2014: 255).

All in all, the discussion put forward in this article has been highly speculative and it is important now to ask new questions aimed at uncovering the nature and extent of disinformation and the spread of fake news online. In this sense, future research should look at the conditions under which disinformation can be overcome. In particular, are there any forms of algorithm architecture that could incentivize the circulation of accurate beliefs and punish false stories when they arise? As Lessig (1999) has put forward: 'Different Internet-based technologies have different architectures, encouraging or discouraging different kinds of behaviour' (Farrell, 2012).

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

Lastly, future empirical research should focus on how can the algorithm serve the public's necessity to be well informed in a democracy for its ultimate survival; for, as stated by Senator Daniel Patrick Moynihan, in a democracy, 'everyone is entitled to his own opinion, but not to his own facts' (Lewandowski et al., 2017: 365).

References

- Allcott, H and Gentzkow, M (2016) "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspectives*, 31(2): 211-236
- Anderson, C.W. (2011) "Deliberative, Agonistic and Algorithmic Audiences: Journalism's vision of its public in an age of audience transparency", *International Journal of Communication*, 5: 529-547
- Beer, D. (2009) "Power through the algorithm? Participatory web cultures and the technological unconscious", *New Media Society*, 11(6): 985-1002
- Bentzen, N. (2017) "Understanding disinformation and fake news", available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA%282017%29599408 [accessed 29 August 2018]
- Bucher, T. (2012a) "Want to be on the top? Algorithmic power and the threat of invisibility on Facebook", *New Media and Society*, 14(7): 1164-1180
- Bucher, T. (2012b) "A Technicity of Attention: How Software Makes Sense", *Culture Machine*, 13: 1-23
- Bucklin, R.E and Hoban, P.R. (2017) "Marketing Models for Internet Advertising", in Wierenga, Berend and van der Lans, Ralf (eds.) *Handbook of Marketing Decision Models* (Springer International Publishing)
- Dash, A (2017) "Underscores, Optimization and Arms Races", *Medium*, available at <https://medium.com/humane-tech/underscores-optimization-arms-races-b34f0dfa4357> [accessed 26 August 2018] Farrell, H. (2012) "The Consequences of the Internet for Politics", *The Annual Review of Political Science*, 15(32): 35-52.
- Fernandez, P (2017) "The Technology behind Fake News", *Library Hi Tech News*, available at <https://doi.org/10.1108/LHTN-07-2017-0054> [Accessed 29 August 2018]
- Ghosh, D. and Scott, B. (2018) "The technologies behind precision propaganda on the Internet", *Public Interest Technology*, available at <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/> [accessed 23 August 2018]
- Kalsnes, B. (2018). *Fake News*, Oxford Research Encyclopedia of Communication, Oxford: Oxford University Press
- Kaye, L (2013) "95 Percent of Web Traffic Goes to Sites on Page 1 of Google Serps", *Brafton*, available at <https://www.brafton.com/news/95-percent-of-web-traffic-goes-to-sites-on-page-1-of-google-serps-study/> [accessed 23 August 2018]
- Kirkpatrick, K. (2016) "Advertising via Algorithm", *Communications of the ACM*, available at <https://cacm.acm.org/news/198460-advertising-via-algorithm/fulltext> <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/> [accessed 23 August 2018]
- Kitchin, R (2017) "Thinking critically about and researching algorithms", *Information, Communication & Society*, 20(1): 14-29
- Lewandowsky, S; Ecker, U.K.H and Cook, J. (2017) "Beyond Misinformation: Understanding and Coping with the Post-Truth Era", *Journal of Applied Research in Memory and Cognition*, 6: 353-369

Hacking Westphalia: ICT Infrastructures, Fake News and Global Politics

Written by Andrea Pavón-Guinea

Nelson, J.L and Taneja, H. (2018) "The small, disloyal fake news audience: The role of audience availability in fake news consumption", *New Media & Society*: 1-18

Newman, N.; Fletcher, R; Kalogeropoulos, A; Levy, D. and Nielsen, R. (2018) Reuters Institute Digital News Report, available at <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475> [accessed 16 January 2019] Shu, K; Sliva, A.; Wang, S; Tang, J; Liu, H. (2017) "Fake News Detection on Social Media: A Data Mining Perspective", *ACM SIGKDD Explorations Newsletter*, 19(1): 22-36

Srnicek, N; Fotou, M and Arghand, E. (2013) "Introduction: Materialism and World Politics", *Millennium: Journal of International Studies*, 41(3): 397

Vosoughi, S; Roy, D and Aral, S. (2018) "The Spread of True and False News Online", *Science*, available at <http://science.sciencemag.org/content/359/6380/1146> [accessed 30 August 2018]

About the author:

Andrea Pavón-Guinea is a PhD Candidate at the Department of Public Communication at the University of Navarra, where she currently teaches a course on international communication and public opinion. She holds an M.Sc. in media and communications (research) from the London School of Economics and Political Science, as well as a B.A. in Politics from the University of Essex, and a second B.A. in Journalism from the University of Navarra. Her research mainly focuses on the intersection of public communication and international politics.