Written Representation 36

Name: Ben Nimmo
Senior Fellow Information Defense, Digital Forensic Research Lab

Received: 22 Feb 2018

Deliberate online falsehoods - methods and responses

Ben Nimmo, Senior Fellow, Information Defense, Atlantic Council Digital Forensic Research Lab (DFRLab)

1. The use of falsehood to achieve influence is older than history. The Arthashastra expounds at length on methods of infiltration, influence and propaganda.[1] The Hittite Empire spread disinformation before the Battle of Kadesh in approximately 1274 BCE, sending agents to convince the Egyptian army that the Hittite forces had retreated.[2]

2. The advent of the internet and, in particular, of social media has had five main effects on this process.

3. First, the number of platforms and channels by which falsehood can be spread has increased radically.[3] On Facebook alone, the number of active monthly users grew from 100 million in Q3, 2008, to over 2 billion in Q4, 2017.[4]

4. Second, the relatively low cost of creating an online platform has made it far easier for purveyors of falsehoods to look like traditional reporting outlets, without adhering to traditional editorial standards.

5. Third, social media have allowed peer-to-peer interactions on an unprecedented scale, allowing malicious actors to bypass traditional editorial verification and spread their falsehoods (literally) unchecked.[5]

6. Fourth, the borderless nature of the internet has made it much easier for foreign actors to impersonate internet users in the target country, and thus to infiltrate target communities.[6]

---

[1] See in particular Arthashastra, books XI and XIII, online at https://en.wikisource.org/wiki/Arthashastra/Book_XI and https://en.wikisource.org/wiki/Arthashastra/Book_XIII

[2] "The Battle of Kadesh. Part I: The Disinformation Campaign," tr. M. M. Bishop, online at http://www.ilefarsiv.com/akildefteri/gorsel/dosya/1046190609Kadesh.pdf

[3] Source: Statista.com, online at https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[4] Source: Statista.com, online at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[5] See, for example, "Inside the Macedonian fake-news complex," Samanth Subramian, Wired.com, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/.

[6] For example, "The fake Americans Russia created to influence the election," Scott Shane, New York Times, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

7. Fifth, modern editorial techniques have made it progressively easier for malicious actors to create false or misleading content, ranging from photoshopped images to doctored videos which can make a speaker appear to say something they did not.[7]

8. Thus the spread of digital publishing technologies has made it easier to *create* false stories. The internet has made it easier to *publish* fake stories, and social media have made it easier to *spread* false stories.

Typology of falsehood

9. Not all online falsehoods are equal: many fail to achieve traction, and vanish into obscurity. Others, however, can have a dramatic effect.

10. A fake tweet about a bomb attack on the White House posted from the account of the Associated Press in 2013 triggered a short-term crash on the stock market.[8] (The AP account had been hacked.) A false claim that South African President Jacob Zuma had resigned in 2018 triggered a brief spike in the value of the rand.[9]

11. Successful falsehoods tend to have four components.[10] They have an instant emotional appeal; they claim authority by referring to an unimpeachable source; they have an insertion point into the information space; and they then have an amplification network which passes them on to a broader public. Stories which lack one or more of these elements tend to fail.

12. For example, a false claim made by Russian state TV in April 2017 that a Russian aircraft had managed to disable a U.S. warship using electronic jamming was pitched as an emotional and patriotic story on the anniversary of a key date in Russia's 1905 war with Japan.[11] Its claim to authority was that it was allegedly based on a social media post from a U.S. sailor. It was published by Russian state TV, and then amplified by a network of supportive websites, and by Western tabloids which had been fooled by the story.

13. The article was a deliberate falsehood, in that the "social media post" on which it rested its claims was a spoof published by a Russian website in 2014. It is therefore a successful example of the spread of a false story.

---

[7] On photos, see for example "#ElectionWatch: Fake photos in Catalonia?", Ben Nimmo, DFRLab, October 23, 2017, https://medium.com/dfrlab/electionwatch-fake-photos-in-catalonia-fe3f045df171. On video, see "Fake Obama created using AI video tool," BBC, July 17, 2017, http://www.bbc.co.uk/news/av/technology-40598465/fake-obama-created-using-ai-tool-to-make-phoney-speeches

[8] "False White House explosion tweet rattles market," Hibah Yousuf, CNN The Buzz, April 23, 2013, http://buzz.money.cnn.com/2013/04/23/ap-tweet-fake-white-house/.

[9] "South African rand rocked by fake Zuma reports," Nicholas Megaw, Financial Times, January 9, 2018, https://www.ft.com/content/1b207d6a-070a-3f86-8992-badbc663844c

[10] This typology expands on a report presented to the "fake news" enquiry launched by the UK Parliament's Committee on Culture, Media and Sport in 2017, online at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/fake-news/written/68987.pdf

[11] "Russia's fake 'Electronic bomb,'" Ben Nimmo, DFRLab, May 9, 2017, https://medium.com/dfrlab/russias-fake-electronic-bomb-4ce9dbbc57f8

14. The "Pizzagate" conspiracy theory, which claimed that U.S. Democratic candidate Hillary Clinton had been complicit in a paedophile ring managed from a Washington, D.C., pizzeria, used emotional and aggressive language on child abuse. It claimed authority through the conspiratorial interpretation of emails hacked from Clinton campaign manager John Podesta.[12] It was initially posted on online forum 4chan, and was amplified by anonymous and automated Twitter accounts ("trolls" and "bots").[13] The story prompted an armed American citizen to "self-investigate" the pizzeria, indicating the impact such stories can have.

15. This taxonomy is significant for the implications it has in governing a response. Each of the four "pillars" of a successful false story should be addressed in a different way; addressing just one of the pillars, without addressing the others, is less likely to succeed. Responses will be addressed from point 47, below.

Motivations and methods

16. Those who spread falsehoods online can broadly be divided into three categories, based on their motivation: mischief, money or political influence.

17. Many fakes appear to begin online as efforts at mischief-making. For example, a forged letter purporting to expose connections between Britain's GCHQ intelligence agency and the Obama administration was first posted on 4chan in June 2017. Users quickly exposed it as a fake, but some suggested sending it to broadcasters anyway, "for the lulz" (i.e. for entertainment). The fake continued to circulate online as a genuine document well into 2018, despite being repeatedly debunked.[14]

18. More common, and more pernicious, are fakes created for money. The aim is to attract internet users to adverts by using sensational, emotional or divisive content ("clickbait"). Much of this content is non-political, but polarising and divisive political themes have been shown to be a potent source of revenue.

19. For example, during the 2016 election campaign in the U.S., multiple reports highlighted how teenagers in Macedonia were profiting from fictional, hyper-partisan "news" stories to earn money from advertising.[15] An American writer called Paul Horner claimed to make US$10,000 per month writing false stories.[16]

20. These stories are written for profit, but profit stems from mass appeal. Writers of such stories therefore target those demographics which they see as most likely to share their stories, and adjust their stories according to the market. The New York

---

[12] "Pizzagate: Anatomy of a fake news scandal," Amanda Robb, Rolling Stone, November 16, 2017, https://www.rollingstone.com/politics/news/pizzagate-anatomy-of-a-fake-news-scandal-w511904
[13] Throughout this paper, a "bot" will be considered as an automated social-media account which attempts to pass as a human user. A "troll" will be considered as an anonymous and aggressive human user who harasses others online.
[14] "Online lies about spies," Ben Nimmo, DFRLab, February 2, 2018, https://medium.com/dfrlab/online-lies-about-spies-b1f5fb86aed4
[15] "The city getting rich from fake news," Emma Jane Kirby, BBC, December 5, 2016, http://www.bbc.co.uk/news/magazine-38168281.
[16] "This person makes $10,000 a month writing fake news," Sally French, marketwatch.com, November 18, 2016, https://www.marketwatch.com/story/this-person-makes-10000-a-month-writing-fake-news-2016-11-17.

Times interviewed a Georgian commercial writer of false stories who said that he had originally written stories praising Democratic candidate Hillary Clinton, but found that stories attacking Clinton and praising her rival, Donald Trump, were far more popular.[17]

21. This commercial content can nevertheless have political consequences. In an interview with the Washington Post, Horner said that "instead of hurting the [Trump] campaign, I think I helped it," by spreading false stories.[18]

22. Commercially-driven information fraudsters can also use fake accounts, instead of false stories, in order to generate revenue. One network of bots masqueraded as supporters of President Trump and posted links to a range of stories, some partisan, others from legitimate news sites. In each case, the link led to a pay-per-click site, generating revenue for the manager of the botnet.[19] In this case, the falsehood lay in the nature of the accounts posting retweets, rather than the information.

23. The authors of such false stories and accounts vary. In the Macedonian and Georgian cases, they were people of student age; Horner was 34. The common feature was a realisation that emotionally-charged false stories could monetise internet users' attention by generating advertising revenue.

24. The third category of authors of false stories and accounts is the politically-motivated group. These can be either internal to a country, or external.

25. Internally, the best example is the "alt-right" movement in the United States. This is largely homegrown, although it was infiltrated very successfully by Russian operatives in 2016. It is not a homogeneous group; indeed, after the election, the movement split into acrimonious sub-groups.[20]

26. The alt-right drove a number of major false narratives during the election campaign, notably "Pizzagate" (see 14, above), and the claim that Clinton's adviser, Sidney Blumenthal, had blamed her for the death of U.S. diplomats in Benghazi (in fact, Blumenthal had merely been flagging up a Newsweek article which made that claim).[21]

---

[17] "Inside a fake news sausage factory: 'This is all about income,'" Andrew Higgins et al, New York Times, November 25, 2016, https://www.nytimes.com/2016/11/25/world/europe/fake-news-donald-trump-hillary-clinton-georgia.html

[18] "Facebook fake-news writer: 'I think Donald Trump is in the White House because of me,'" Caitlin Dewey, Washington Post, November 17, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/?utm_term=.cf11258faab8.

[19] "Portrait of a botnet," Ben Nimmo, DFRLab, February 21, 2017, https://medium.com/dfrlab/portrait-of-a-botnet-12fa9d5d6b3

[20] "Alt-right movement descends into civil war after leading figure is booted from Trump inauguration event," Allan Smith, Business Insider, December 27, 2016, http://uk.businessinsider.com/alt-right-civil-war-twitter-cernovich-milo-alaska-2016-12

[21] "Russia was not behind Donald Trump's false Blumenthal-Benghazi claim," Aric Toler, Bellingcat, October 12, 2016, https://www.bellingcat.com/news/americas/2016/10/12/russia-not-behind-donald-trumps-false-blumenthal-benghazi-claim/

27. These false stories appear to have been driven by the political desire to harm the Clinton campaign and boost that of Trump. They were largely generated and spread by local citizens for local, partisan reasons.

28. However, thousands of Twitter and Facebook accounts which appeared to belong to members of the alt-right, and to the opposed Black Lives Matter campaign, were in fact run from the so-called "troll factory" or Internet Research Agency in St Petersburg, Russia, an organisation which employs people to manage large numbers of false social-media accounts.

29. According to Twitter, the "troll factory" managed at least 3,814 troll accounts and 50,258 bot accounts; so far, 1.4 million American users are known to have interacted with these accounts in some way.[22] According to Facebook, the "troll factory" ran at least 470 accounts and spent $100,000 on advertising.[23] Facebook later admitted that troll-factory posts reached at least 126 million Americans.[24]

30. Some of these accounts appear designed to inflame local tensions by focusing on divisive issues, including LGBT rights, gun control, race and immigration.[25] In the most notorious case, troll-factory Facebook groups triggered a standoff between supporters and opponents of an Islamic centre in Texas.[26]

31. Others appeared designed to target the election directly, posting content which lauded then-candidate Trump and demonised candidate Clinton. One such account alone gained over 70,000 followers and was quoted voice by dozens of high-profile media outlets.[27] Another had over 130,000 followers and was retweeted by senior members of the Trump campaign.[28]

32. These false accounts, which shared a mixture of true, partisan and false stories (such as "Pizzagate"), were generated by foreign actors in order to create division and handicap one candidate in the election. They were thus a tool of both generic political interference, creating tension, and specific interference, targeting the election. They performed both functions simultaneously.

---

[22] "Update on Twitter's review of the 2016 U.S. election," Twitter, January 31, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html

[23] "An update on information operations on Facebook," Alex Stamos, Facebook, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/

[24] "Facebook says some 126 million Americans may have been influenced by Russian political posts," ABC Australia, October 31, 2017, http://www.abc.net.au/news/2017-10-31/facebook-says-126-mln-americans-may-have-seen-russia-posts/9102736

[25] Facebook update; see note 23.

[26] "Russian Facebook trolls got two groups of people to protest each other in Texas," Lorenzo Franceschi-Bicchierai, Motherboard, November 1, 2017, https://motherboard.vice.com/en_us/article/3kvvz3/russian-facebook-trolls-got-people-to-protest-against-each-other-in-texas

[27] "Jenna Abrams, Russia's clown troll princess, duped the mainstream media and the world," Ben Collins and Joseph Cox, The Daily Beast, November 2, 2017, https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world

[28] "Twitter ignored this Russia-controlled account during the election. Team Trump did not." Luke O'Brien, Huffington Post, November 1, 2017, http://www.huffingtonpost.co.uk/entry/twitter-ignored-this-russia-controlled-account-during-the-election_us_59f9bdcbe4b046017fb010b0

33. Fake accounts on social media (i.e. those which either do not have a human user behind them, or are run by a human who pretends to be someone else) are the footsoldiers in this form of warfare. They can be used to amplify messaging and force hashtags into the trending lists.[29] On occasion, they can be used to intimidate or block other users.[30]

34. As with false stories, some bots and botnets generate revenue by steering users to pay-per-click sites. Many more are created by bot herders who hire them out, and thus sell retweets, likes and follows.[31] Some businesses are on a very large scale, counting thousands or tens of thousands of accounts.[32] Others are known to have worked through vending machines.[33]

35. Other botnets are created and managed for political reasons, and focus on political content. Such botnets, counting thousands of accounts, were especially active during the U.S. election, pushing divisive, partisan and false content.[34]

36. However, the use of bots can change: after all, a bot is an account run by an algorithm, so whoever is behind the algorithm can change it at any point. For example, during the German election campaign in September 2017, a botnet which had formerly retweeted Russian-language commercial content (such as advertisements for cars, Bitcoin and plastic windows) began retweeting posts supporting the anti-migrant Alternative für Deutschland party.[35] During the ANC leadership contest in South Africa, a botnet which posed as American and had largely posted commercial content began posting political South African messaging.[36]

37. One Russian bot herder interviewed by BuzzFeed news claimed to have made his commercial botnet available to the far right in Germany "for free (mutually beneficial)", without elaborating.[37] This illustrates the murky crossover between bots

---

[29] "Why bot makers dream of electric sheep," Ben Nimmo, DFRLab, June 27, 2017, https://medium.com/dfrlab/why-bot-makers-dream-of-electric-sheep-76588977072e
[30] "BotSpot: The intimidators," Ben Nimmo, DFRLab, August 30, 2017, https://medium.com/dfrlab/botspot-the-intimidators-135244bfe46b
[31] "I bought a Russian bot army for under $100," Joseph Cox, The Daily Beast, September 13, 2017, https://www.thedailybeast.com/i-bought-a-russian-bot-army-for-under-dollar100
[32] "The follower factory," Nicholas Confessore et al, New York Times, January 27, 2018, https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html
[33] "Russian vending machine sells Instagram likes and followers in shopping centres," news.com.au, June 8, 2017, http://www.news.com.au/technology/online/social/russian-vending-machine-sells-instagram-likes-and-followers-in-shopping-centres/news-story/c28302752dcbae11bd10a34284cc83a4
[34] "Never mind the Russians, meet the bot king who helps Trump win Twitter," Joseph Bernstein, Buzzfeed, April 5, 2017, https://www.buzzfeed.com/josephbernstein/from-utah-with-love?utm_term=.vt4j7r60l#.pfbzmQjvL
[35] "#ElectionWatch: Russian botnet boosts far-right German posts," Ben Nimmo, DFRLab, September 21, 2017, https://medium.com/dfrlab/german-election-russian-botnet-boosts-far-right-posts-45f170bc2321
[36] "#ElectionWatch: American bots in South Africa," Ben Nimmo, DFRLab, December 21, 2017, https://medium.com/dfrlab/electionwatch-american-bots-in-south-africa-1487a537bf59
[37] "This Russian hacker says his Twitter bots are spreading messages to help Germany's far right party in the election," Henk Van Ess and Jane Lytvynenko, BuzzFeed, September 24, 2017, https://www.buzzfeed.com/henkvaness/these-russian-hackers-say-theyre-using-twitter-bots-to-help?utm_term=.glxWY37Qq#.eg05Ywv48

which are created for political purposes and bots which are created for commercial uses, and then hired out or otherwise made available to political users.

Implications

38. The online falsehoods and false accounts detailed above can be used in short-term and long-term ways.

39. Short-term uses focus on a specific event, such as a vote, demonstration, natural disaster or security incident, and attempt to achieve an effect by the massive and sudden deployment of false stories or accounts. For example, immediately before the second round of the French presidential election in 2017, a 9 GB file of emails hacked from the campaign of now-President Emmanuel Macron was dumped on 4chan and spread by a combination of far-right activists and bots, in an attempt to undermine Macron's candidacy.[38]

40. After the murder of Russian opposition leader Boris Nemtsov in 2015, tens of thousands of bots began spreading conspiracy theories about his death, in an apparent attempt to drown out conversation about the murder on Twitter.[39]

41. Such large-scale actions are only realistically possible in the short term, given the likelihood that the accounts involved will be exposed and suspended. However, the short-term effect can be to spread a false story, or to drown out accurate information, on a very large scale.

42. For Singapore, political debates, moments of tension between ethnic, religious and political groups, demonstrations and security incidents are all events which are at risk of large-scale false information or false accounts by domestic or foreign actors.

43. Longer-term operations typically focus on promoting or attacking a particular point of view. This can range from partisan and one-sided coverage, through hate speech, and into incitement to violence. In extreme cases, online hate speech can be a contributing factor in individuals' decision to commit terrorist acts. This was the case of British citizen Darren Osborne, who drove a van into a crowd outside a North London mosque in 2017, and who was found by a judge to have been "exposed to racists and anti-Islam ideology" via Twitter.[40]

44. Such operations rely on remaining covert as they infiltrate a particular community, as in the case of the Russian troll accounts which masqueraded as far-right Americans in 2015-16. They often use a stepwise approach, first ingratiating

---

[38] "Quelle surprise! Alt-right Americans and internet bots are spreading #MacronLeaks," Akshat Rathi, Quartz, May 6, 2017, https://qz.com/977718/macron-email-leaks-alt-right-americans-and-internet-bots-are-spreading-macronleaks-on-twitter-to-skew-the-french-presidential-election/

[39] "Social network analysis reveals full extent of Kremlin's Twitter bot campaign," Lawrence Alexander, Global Voices, April 2, 2015, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

[40] "Finsbury Park attacker Darren Osborne jailed for minimum of 43 years," BBC, February 2, 2017, http://www.bbc.co.uk/news/uk-42920929

themselves with genuine members of the community, then using the approval of those members to take a stance as a representative member of the community.[41]

45. State-sponsored operations of this nature will typically use multiple platforms, both overt and covert, in a coordinated campaign, creating the impression of a spontaneous movement to cover what is actually an orchestrated action. Russia's use of deniable websites, troll-factory accounts, official media and diplomatic missions to attack U.S. actor Morgan Freeman is a case in point.[42]

46. For Singapore, election campaigns and tensions between different social, religious, political, economic and ethnic groups are likely to be the main targets of any such attempts, as the campaigns tend to gradually inflame tensions and hollow out the political centre at the expense of the fringes. Relations with neighbouring countries can also be the focus of targeted disinformation or influence campaigns.

Responses

47. A number of responses are needed to deal with this challenge. They are based on the four-pillars model of falsehood, described above in points 11-15, above, by which a successful falsehood requires emotional impact, an appearance of authority, an insertion point and an amplification network.

48. In all responses, legislation should be the last resort. As far as possible, information, even false information, should remain outside the purview of government. This is essential for the health of democracy.

49. **Amplification networks** are best dealt with by the social platforms. Governments should therefore engage with platforms, especially Facebook and Twitter, to find a means by which networks of false, automated or inauthentic accounts, can quickly be shut down.

50. However, the platforms are not the only ones to bear responsibilities in this area. Major media outlets are known to have repeatedly quoted troll accounts run from the "troll factory" in St Petersburg; everyday users shared or liked their posts thousands of times. *Every* social-media user has a duty of awareness in this regard.

51. It is therefore important to educate internet users in the basic principles of digital awareness and hygiene, and to work with the platforms on solutions, rather than against them. Essential skills such as how to identify a bot or a troll can be taught without recourse to sophisticated software or analytical techniques.[43] Such skills are vital for normal users, and particularly for media outlets, which can otherwise amplify fraudulent accounts. As the government is responsible for education policy, it is best placed to lead such educational efforts.

---

[41] See note 27.

[42] "Russia's full spectrum propaganda," Ben Nimmo, DFRLab, January 23, 2018, https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970

[43] See, for example, "#BotSpot: Twelve ways to spot a bot," Ben Nimmo, DFRLab, August 28, 2017, https://medium.com/dfrlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c

52. Online **insertion points** are best dealt with by civil society, researchers and the platforms, working in combination. Researchers can identify websites or social media accounts which repeatedly post information which is demonstrably false; these can then be flagged to the platforms. Given the sheer size of the platforms, it is not practical for them to monitor their content unaided.

53. For example, Facebook suspended a reported 30,000 accounts in the build-up to the French election;[44] Google introduced rules which would block sites falsely claiming to be in a different country from the Google News service.[45] Working more closely with analysts would greatly increase the platforms' ability to identify suspect sites.

54. Governments should not seek direct involvement in this process; however, they have a valuable role to play in bringing the tech and analytical communities together to facilitate cooperation.

55. The **appearance of authority** is best countered by fact-checking groups, which have proliferated in recent years. These have the expertise to expose the various techniques of falsehood, and the reputation to make their work more credible. Many fact-checking and verification operations now exist, such as First Draft, [46]Snopes[47] and Politifact[48] in the U.S., Maldito Bulo in Spain,[49] Les Décodeurs of Le Monde in France,[50] the Bellingcat group,[51] the Atlantic Council's Digital Forensic Research Lab,[52] and numerous units within major broadcasters such as the BBC.[53]

56. In this area, above all, governments should play a hands-off role. Depending on local sensitivities and needs, financial or technical support for fact-checking initiatives could be considered, but government intervention in fact-checking projects is more likely to impair their credibility than otherwise.

57. The exception to this is if a large-scale attack on the information environment is detected - either a short-term burst, such as false stories surrounding a demonstration or debate, or a major attempt to inflame social tensions. In such circumstances, governments can appropriately show leadership by exposing the attack in as much detail, and with as much attribution, as possible, to contribute to overall social awareness of the threat.

58. Governments should also be aware that independent fact-checking organisations will also check government statements. It is vital that officials both recognise and

---

[44] "Facebook cracks down on 30,000 fake accounts in France," Eric Auchard and Joseph Menn, Reuters, April 13, 2017, https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G
[45] "Google purges shady overseas sites in latest blow to fake news," Jeff John Roberts, Fortune, December 18, 2017, http://fortune.com/2017/12/18/google-news-fake/
[46] https://firstdraftnews.org/
[47] https://www.snopes.com/
[48] http://www.politifact.com/
[49] https://maldita.es/malditobulo/
[50] http://www.lemonde.fr/les-decodeurs/
[51] https://www.bellingcat.com/
[52] https://medium.com/dfrlab. The author of this paper works for DFRLab.
[53] http://www.bbc.co.uk/news/topics/cp7r8vgl2rgt/reality-check

emphasise the importance of such work, even when it challenges their own narratives. Attacking the media further empowers online falsehood.

59. The **emotional targeting** of online audiences by false stories can only realistically be addressed through education. Users need to be aware of the tricks and techniques which authors of falsehoods use to make their stories more attractive; they also need to become more aware of how such falsehoods can be used to create either political impact or financial gain. This is an area in which, again, governments should take the lead, through educational curricula.

60. Online falsehood is a complex challenge which requires complex solutions. Various actors in civil society, academia, the tech industry and the media are already working on solutions. Governments can best play a role by facilitating and supporting such initiatives, and providing a grounding in media and information literacy with the aim of increasing society's resilience to falsehood online.