COUNTERING MALICIOUS USE OF SOCIAL MEDIA

MALICIOUS USE OF SOCIAL MEDIA: CASE STUDIES FROM BBC MONITORING

Olga Robinson
BBC Monitoring

ISBN: 978-9934-564-41-3

ISBN: 978-9934-564-41-3
Author: Olga Robinson
Project manager: Sebastian Bay
Text editor: Anna Reynolds
Design: Kārlis Ulmanis

Riga, November 2018
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

BBC Monitoring is a specialist unit within BBC News that tracks thousands of international media outlets, including hard-to-reach broadcast sources, to report news from and about the world's media and social media.

CONTENTS

> BBC Monitoring uses a range of tools for social media analysis, and continues to explore ways of using evolving technology to improve its journalists' ability to track multiple sources and spot media manipulation

INTRODUCTION

BBC Monitoring (BBCM) is a specialist unit within BBC News that tracks thousands of international media outlets, including hard-to-reach broadcast sources, to report news from and about the world's media and social media.

Set up at the outbreak of World War II with the primary purpose of informing the War Office about propaganda by Nazi-controlled media, BBCM has a long history of tackling disinformation and misleading reporting. Over the past 79 years, the service has translated, explained, and interpreted media messages, from the broadcast propaganda of the Cold War to the multiplatform campaigns of today. The rise of social networks and instant messaging platforms has ushered in a new and fast-changing era for open-source media monitoring.

Today, BBCM still relies on its detailed knowledge of media sources and behaviour along with linguistic, regional, and cultural expertise to navigate the increasingly complex and muddled information space. In addition, it uses a range of tools for social media analysis, and continues to explore ways of using evolving technology to improve its journalists' ability to track multiple sources and spot media manipulation.

BBCM this year launched a new dedicated disinformation team, whose primary purpose is to spot, collate, and investigate examples of misleading reporting and manipulation, drawing on BBCM's overall monitoring of global media.

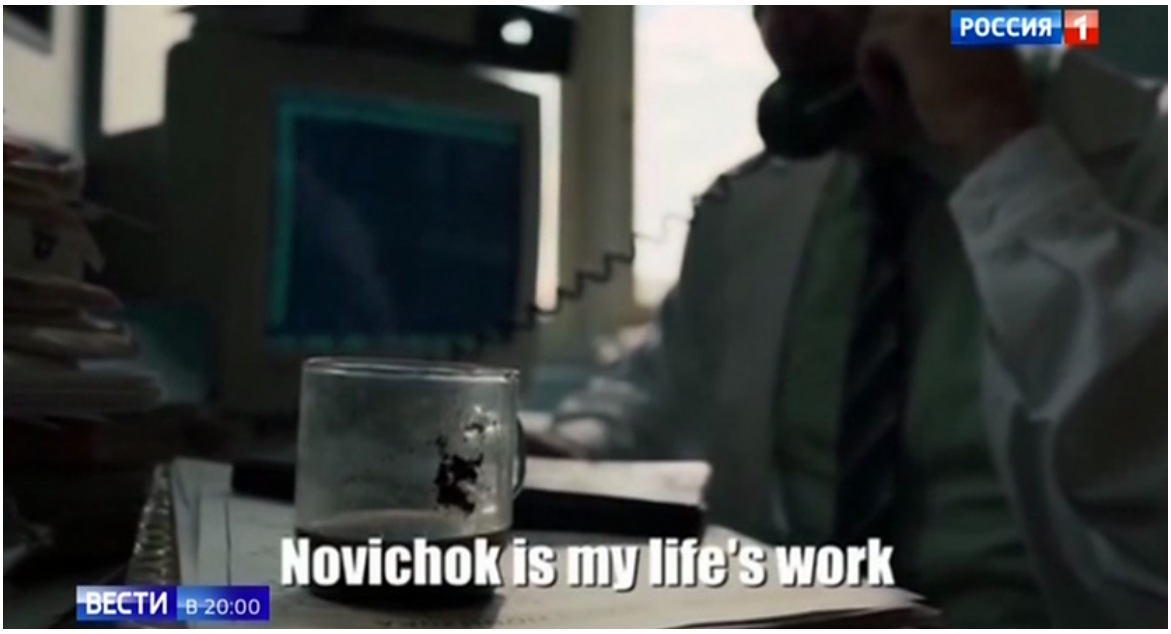
This report shows some of the disinformation techniques and tactics that BBCM journalists have come across in their recent work, and outlines the approach adopted by BBCM to rise to the challenges of disinformation in the 21st century.

WHAT WE ARE SEEING: EXAMPLES AND TACTICS

Confuse and rule

During the Cold War, Soviet propaganda—couched in Communist ideological language—aimed to persuade its audience that the West, primarily the US, was failing and that the USSR was superior to Western democracy. Today, the Kremlin still seeks to discredit Western values and the US. But to do that it no longer relies on ideology and consistency in its messaging. Instead, it pushes multiple, at times competing, narratives through a loose network of officials, state media, and online trolls and bots—automated computer programmes designed to amplify messages and inflate trends.

The aim is to reduce truth to the level of opinion, sow discord, and confuse audiences in order to rally support for the Kremlin at home and hinder the response to Russia's actions in the West. Widely used in the aftermath of the MH17 crash over east Ukraine in 2014, the tactic was also deployed this year in the fallout from the attempted murder of former double agent Sergei Skripal and his daughter Yulia in Salisbury.



Russian TV pushed multiple theories about the origin of the Novichok nerve agent (Rossiya 1)

After the UK authorities found that Russia was 'highly likely' to be the perpetrator of the attack, officials, state TV, and pro-Kremlin actors on social media flooded the information space with numerous narratives and conspiracy theories. They variously questioned the origin of the Novichok nerve agent, dismissed the poisoning as a staged special operation by British or US intelligence, depicted it as an attempt to tarnish Russia's reputation ahead of the FIFA World Cup, and speculated that it was an attempt to meddle in the Russian presidential election.

While in the West the Russian response was widely criticised and questioned, it appears to have been better received by domestic audiences. A recent poll released by the independent Levada Centre polling organisation suggested that only 3 per cent of Russians think that the Russian intelligence services were behind the Skripal poisoning, while 56 per cent think it could have been carried out by 'anyone'.

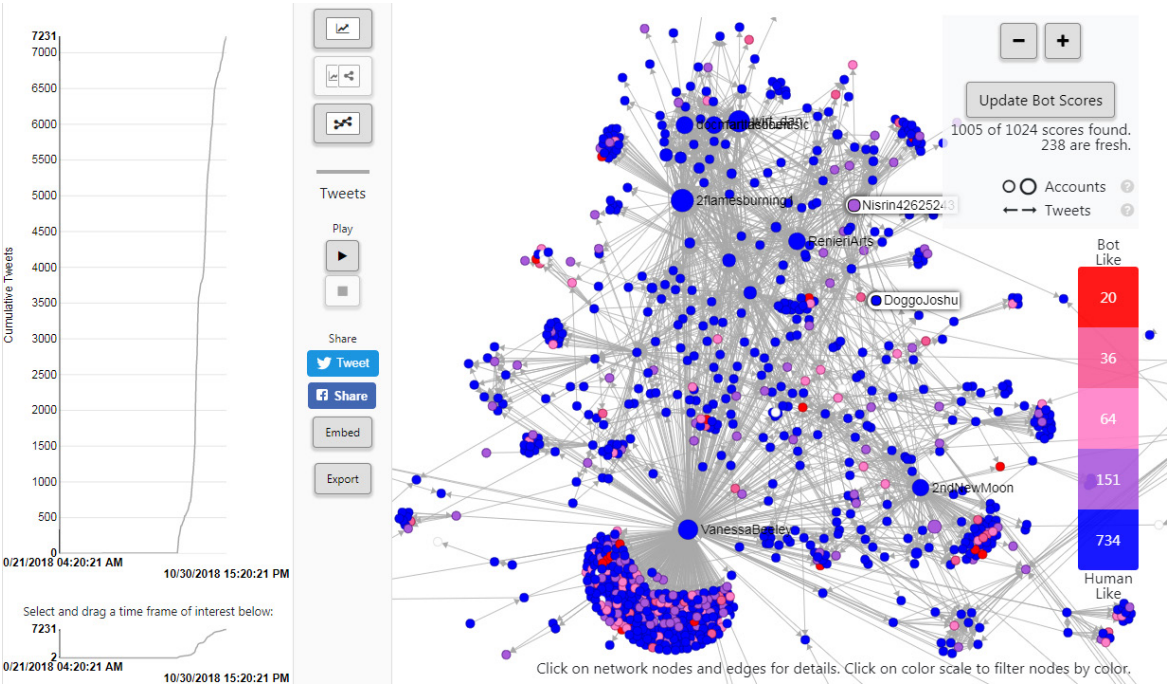
Focus on networks

In countries like Russia, influence operations use a multi-spectrum approach involving various sources—state-controlled TV, state officials, foreign-facing media outlets, and social media accounts—acting in unison as an 'ecosystem'.

Involving both directly controlled resources and ostensibly independent actors, this approach aims to create a semblance of diversity of voices while giving the impression of a consensus and pushing the same talking points.

In a typical example, on Twitter in August 2018 a loose network of state-funded media, apparent trolls, and prominent supporters of Syrian President Bashar al-Assad, sought to promote Russian allegations against Syrian volunteers from the White Helmets civil defence group. The Russian Defence Ministry said that members of the group were planning to stage a chemical weapons 'provocation' in the northern Syrian province of Idlib with the support of Western intelligence.

Accounts that amplified allegations against the White Helmets in August included prominent pro-Assad and pro-Kremlin bloggers, Russian media, and apparent trolls (via Twitter)



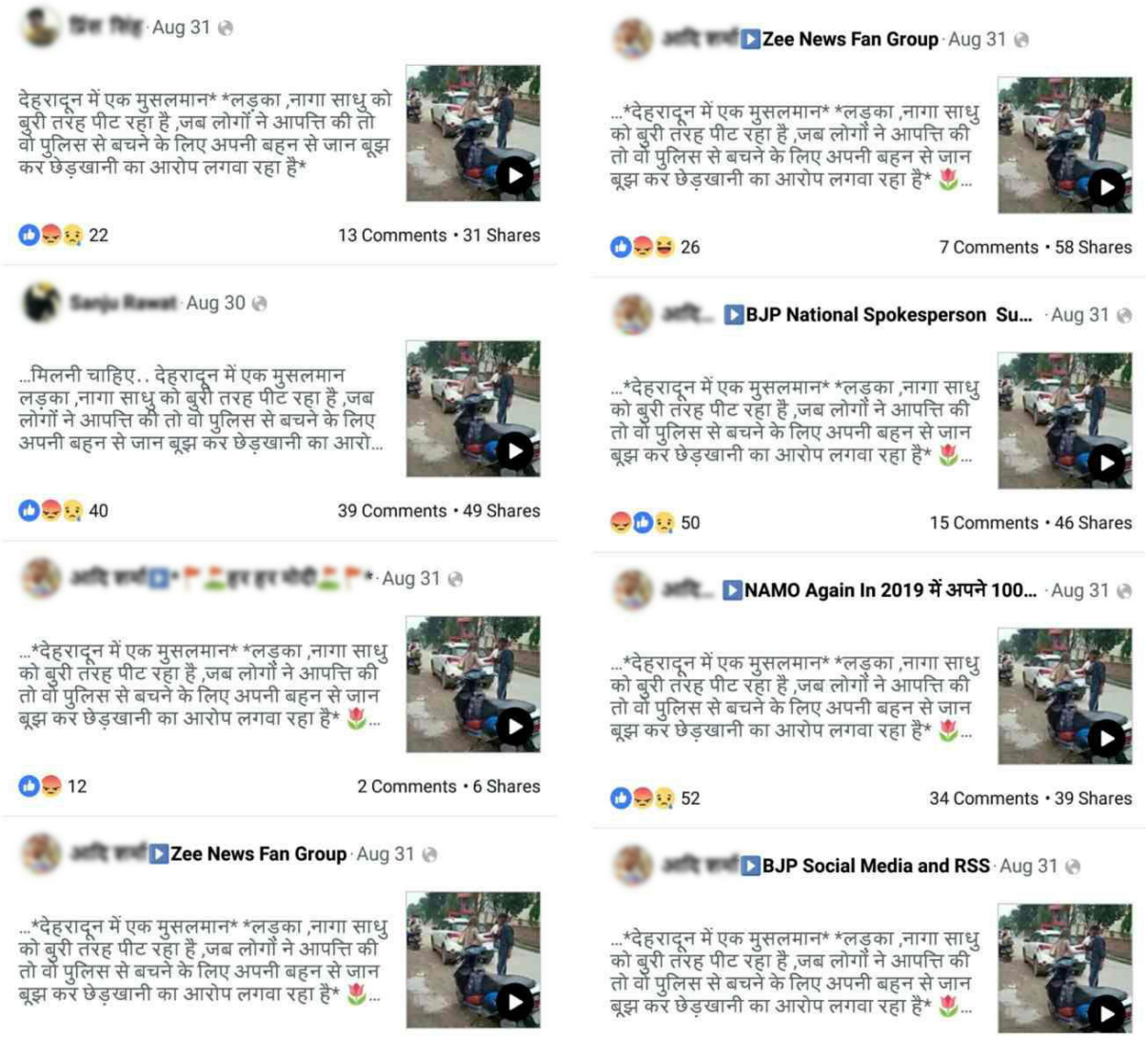
Vanessa Beeley's diffusion network on Twitter, which includes both pro-Assad and pro-Kremlin accounts (via Hoaxy)

The allegations were picked up by leading state TV channels, including Rossiya 1 and Channel One, as well as English-language RT.[1] On Twitter, the Russian warnings and conspiracy theories about the White Helmets, including their alleged links with terrorists and Western intelligence services, were amplified by Russian embassies[2], dozens of influential pro-Kremlin accounts,[3] and pro-Assad accounts,[4] as well as through possible troll activity.[5]

One of the driving forces behind the campaign on English-language social media appears to have been British blogger Vanessa Beeley,[6] who has frequently accused the White Helmets of faking their volunteering work and having links with terrorists. Beeley is a regular contributor to RT on Syria and has been interviewed by Russian state TV. Her posts are also regularly retweeted by some accounts consistently expressing pro-Kremlin views and echoing Kremlin media narratives.

In India, networks affiliated with political forces or religious groups have spread misleading messages, apparently aimed at fuelling community tensions.

In late August 2018, a random act of violence in the northern Indian state of Uttarakhand was cast as a communal incident on social media by right-wing accounts, with the message amplified by influencers and media outlets with the same leanings. It began with a video circulating online which purported to show a 'Naga sadhu'—an ash-smeared naked ascetic, being beaten up by a group of Muslims.



Identical misleading messages about a viral video were circulated on Facebook in India

The police dismissed the rumours,[7] saying that the man was no sadhu and was in fact beaten by local residents, rather than Muslims, for allegedly harassing a woman. But the video went viral. It was shared on Twitter accounts,[8] which called for a Hindu state in their biographies,[9] and in nationalist Facebook groups that support Indian Prime Minister Narendra Modi.[10]

In a sign of coordinated activity, on 31 August, Facebook groups supporting Prime Minister Modi's BJP party and right-wing Hindu nationalist group RSS were

flooded with identical messages saying that in the attached video clip a Muslim man was beating up a Naga sadhu in Dehradun.

To track messages spread across such loose networks and better understand how they operate, BBCM has over the past few years explored and used tools that help its journalists visualise large amounts of data derived from social media. It has also invested in analysis tools that collate information from social media channels in numerous languages.

Tailored messages

Some influence campaigns target specific groups and demographics with carefully crafted content, tone, and messages. Researchers investigating Russian attempts to influence the 2016 election in the US,[11] have found that trolls targeted users in discussions about potentially controversial issues, such as gun rights and the Black Lives Matter movement, to sow discord and stoke anger.

The past two years have seen the rise of several online projects linked to the Russian government-funded RT that focus on the younger generation of voters. ICYMI, or In Case You Missed It, is an online video project that mixes commentary on topical political stories with flashy images, jokes, and catchy graphics. Since its launch in early 2018, the project—which now has 116,000 followers on Facebook—has satirised the Cambridge Analytica scandal, the murder of Saudi journalist Jamal Khashoggi, the Skripal poisoning, and climate change. Its dismissive take on the Russian meddling accusations[12] and the Skripal case,[13] as well as open mockery of Western values, appear to be consistent with Kremlin media narratives.

While ICYMI has a strong focus on politics, a similar online project, In the Now, has a different approach. Its Facebook page, which has more than 3.7 million followers, mixes purely human interest and entertaining stories with occasional political or social stories that push messages similar to those promoted on Russian state television.[14]

Apart from messaging consistent with the Kremlin media line, another feature that makes In the Now and ICYMI stand out from other Russian-linked media projects is their focus on creating highly emotional, sharable, and engaging content full of light-hearted jokes and satire. Judging by their steady following on Facebook, this approach to content production seems to resonate well with internet users.

Projects like In the Now and ICYMI also highlight the importance of understanding the intricacies of media ownership in different parts of the world. BBCM has done a lot of work in this field over the past 15 years, producing regularly updated and detailed media guides that provide essential insight into regional media ecosystems and the way they operate.

Bot or not?

Internet trolls and bots have become a staple of modern information warfare online.

Researchers traditionally identify bots by looking for a set of characteristics that highlight their automated nature, such as anonymity and a high level of activity combined with no original content or no interaction with other users.

During this year's anti-government protests in Iran, dozens of such Twitter bots were deployed to brand widely shared videos of rallies as fake, or to discourage people from joining the demonstrations. Most of the accounts had unusual profile names and pictures,[15] and were created during the protests. They also had only a handful of similar-looking followers and spread the exact same messages below videos of rallies between 1 and 4 January.

But harder to spot are semi-automated accounts, or 'cyborgs', that look more like humans in their online behaviour. In the run-up to this year's midterm elections in the US, some Twitter accounts that promoted highly partisan content in support of US President Donald Trump exhibited some of the tell-tale signs of bots partly moderated by humans. Several accounts analysed by BBCM in late October 2018 posted pro-Trump memes and even 'conversed' with other accounts to appear more natural. But the sheer volume and quality of their output suggested at least some level of automation.

According to the Twitonomy social media analysis tool, one of these accounts tweeted over 500 posts a day between 23 and 29 October. Most of the posts were retweets of Donald Trump, his family, and conservative news outlets such as Breitbart.

The curated content was written in broken English with odd punctuation and looked repetitive; it was heavy with pro-Trump hashtags, emojis, memes, and links to external websites. The quality of the tweets suggested that either English was not the user's first language or that the account used an algorithm to put words together to create rough sentences.

The account also interacted primarily with similar-looking accounts (for example, George Washington's Axe—now suspended) and had large follow-to-follower ratios.

The growing sophistication and proliferation of bot activity points to a need to exercise extra caution in identifying automated social media accounts and avoid labelling. Over the past few years, BBCM journalists have had to revise their approach to spotting and analysing possible bots. In many cases, the process now requires more time, effort and use of analysis tools that detail users' activity patterns in addition to general profile information.

Bot battles

Disinformation is often primarily associated with state-sponsored campaigns. But misleading messages can be disseminated by players on both sides of a political divide.

In October 2018, a BBCM investigation found that both supporters and opponents of the Iranian government had been pushing misleading messages on currency fluctuations on social media for political or financial gain. Exploiting the volatility of the foreign exchange market following a currency crisis, different factions deployed automated and semi-automated social media accounts to either amplify the sense of instability or suggest that the rial was set for more gains against foreign currencies.

Since the campaigns did not use hashtags to disseminate misleading messages, a combination of keywords and advanced Twitter searches were used to analyse online content. An analysis of the search results of two weeks' worth of tweets pointed to an unusual number of previously unknown or lesser-known accounts with vague identities that were spreading identical messages, images, memes, and videos.

One popular meme widely-shared by pro-government users warned that greed 'makes you blind'

A separate linguistic and semantic analysis of tweets suggested that they were pushed by actors from opposing sides. Among the most active accounts promoting the message that the rial would continue gaining against the dollar was a popular account supportive of Iran's political hardliners. It was also one of the most prominent demonstrating automated behaviour.

A close inspection of its activity suggested that the account tweeted an average of 350 tweets per day—or every few minutes. In addition, its timeline consisted almost entirely of retweets, with almost no engagement with other users—another sign of possible automation.

On the other side, an account set up in July appeared to be one of the most active in spreading anti-regime tweets. Similar to accounts used in the pro-government campaign, it also exhibited some signs of automated behaviour. Since its creation, it has tweeted 24,000 times, almost 185 times a day. Its timeline also mostly consisted of retweets and showed no engagement with other users.

Inflated trends

Twitter trends can be a litmus test of changing sentiments, growing discontent, or the level of support for a country's authorities. But in some states viral hashtags and campaigns are designed to create a semblance of popular consensus around sensitive issues.

Following the disappearance of Saudi journalist Jamal Khashoggi in Istanbul on 2 October 2018, suspected bot accounts attempted to shape the social media narrative around the rapidly developing story. Arabic hashtags expressing support for de facto Saudi leader Crown Prince Mohammed Bin Salman, condemning news organisation Al Jazeera and urging users to 'unfollow enemies of the nation' were among those amplified by bot networks, alongside genuine users.

Routine monitoring of social media trends on 14 October suggested that the top global topic was the Arabic 'We all have trust in Mohammed Bin Salman' with some 250,000 tweets. The second trend, also in Arabic and referencing Saudi Arabia, was 'We have to stand by our leader' with over 60,000 mentions.

Traffic analysis showed hundreds of postings per second for 'We all have trust in Mohammed Bin Salman', suggesting that large numbers of those posting were bot accounts. While some of the traffic was undoubtedly from genuine Twitter users, analysis suggested large numbers of brand new users, mixed with previously inactive accounts that had suddenly burst into life, all of which pointed to an artificially inflated trend.

Hijacking existing campaigns

Fake online campaigns are often designed to give the appearance of popular consensus on a topic. But there are times when genuine campaigns can be manipulated in order to mislead audiences.

In late August, pro-Kremlin media in Russia actively promoted and distorted a relatively partisan #BBCSwitchOff campaign on UK Twitter to boycott BBC output over its alleged support for the government, presenting it as a general revolt against the broadcaster among the wider British public. Commenting on the campaign, one of the leading state TV channels, Rossiya 1, alleged that 'the BBC's main audience has united against it'. Despite the impression given by the channel, an examination of the tweets generated by the hashtag made it clear that it was overwhelmingly driven by online supporters of Labour leader Jeremy Corbyn.

There was some evidence of possible Russian troll involvement in promoting the #BBCSwitchOff hashtag too. A British journalist known for promoting pro-Kremlin views tweeted a link to a YouTube clip in which he accused the BBC of propaganda under the hashtag. The post was retweeted by several accounts that showed a combination of some of the hallmarks usually associated with Russian trolls, such as the presence of the Russian language, an unusually high level of tweets or 'likes', anonymity, and a near total preponderance of retweets over active tweeting.

Comment manipulation

While comment and 'like' manipulation is well-documented on platforms such as Twitter, Facebook, and Instagram, there is evidence to suggest that it is also used on lesser known, indigenous platforms in some parts of the world. For example, in South Korea, a recent opinion-rigging scandal showed how online comments could be manipulated on popular web portal and search engine Naver.

In April, a group of individuals led by influential blogger 'Druking' was accused of artificially boosting the number of clicks on 'agree'—Naver's equivalent of 'like'—for comments on political news stories. The portal, one of the most popular news outlets in South Korea, automatically promotes comments with the most 'likes' to the top of its comments section, giving them more public exposure.

According to South Korean media reports, it was revealed that multiple—mostly fake—IDs were used to boost a certain keyword search and to agree with comments, by means of a programme that allowed thousands of 'likes' to be registered at once. The aim was reportedly to lead people to believe that certain comments about the actions of President Moon's administration reflected popular opinion. The scandal provoked a mass outcry and pushed Naver to introduce several changes in its design and operation to prevent comment manipulation from happening in the future.

Fake jihadist propaganda

When it comes to jihadist media, the proliferation of fake content and accounts presents a considerable challenge that requires constant vigilance and verification.

Since the team's launch in 2006, BBCM's jihadist media specialists have seen a range of apparent attempts by both governments and anti-jihadist activists to spread fake propaganda purporting to be issued by a particular jihadist group. Militant groups, particularly in Syria, are also reportedly behind the spread of some bogus material. The aim of such actions is to undermine the credibility of the 'official' media outlets of the targeted group, to sow confusion and mistrust among its supporters, and in some cases to encourage infighting between militant groups.

In one recent example, on 28 June 2018, at least three fake editions of Islamic State's (IS) flagship newspaper *al-Naba* surfaced online around the same time of *al-Naba's* expected release time. What caused further confusion was that the publication was disseminated by Telegram channels that mimicked IS's official outlets.

Faced with such challenges, BBCM has developed a variety of ways to ensure it is dealing with authentic material, including careful verification techniques, attention to detail, language expertise, and extensive background knowledge.

State control

In some parts of the world, governments use the concept of fake news as an excuse to crack down on freedom of speech and tighten control over the internet.

This year Egypt has seen independent journalists, activists, and bloggers critical of the government being arrested on charges of 'spreading false news'. The authorities have also adopted a controversial law that allows them to block social media accounts and punish journalists for spreading false information. The legislation does not, however, make it clear what exactly it means by 'fake news'.

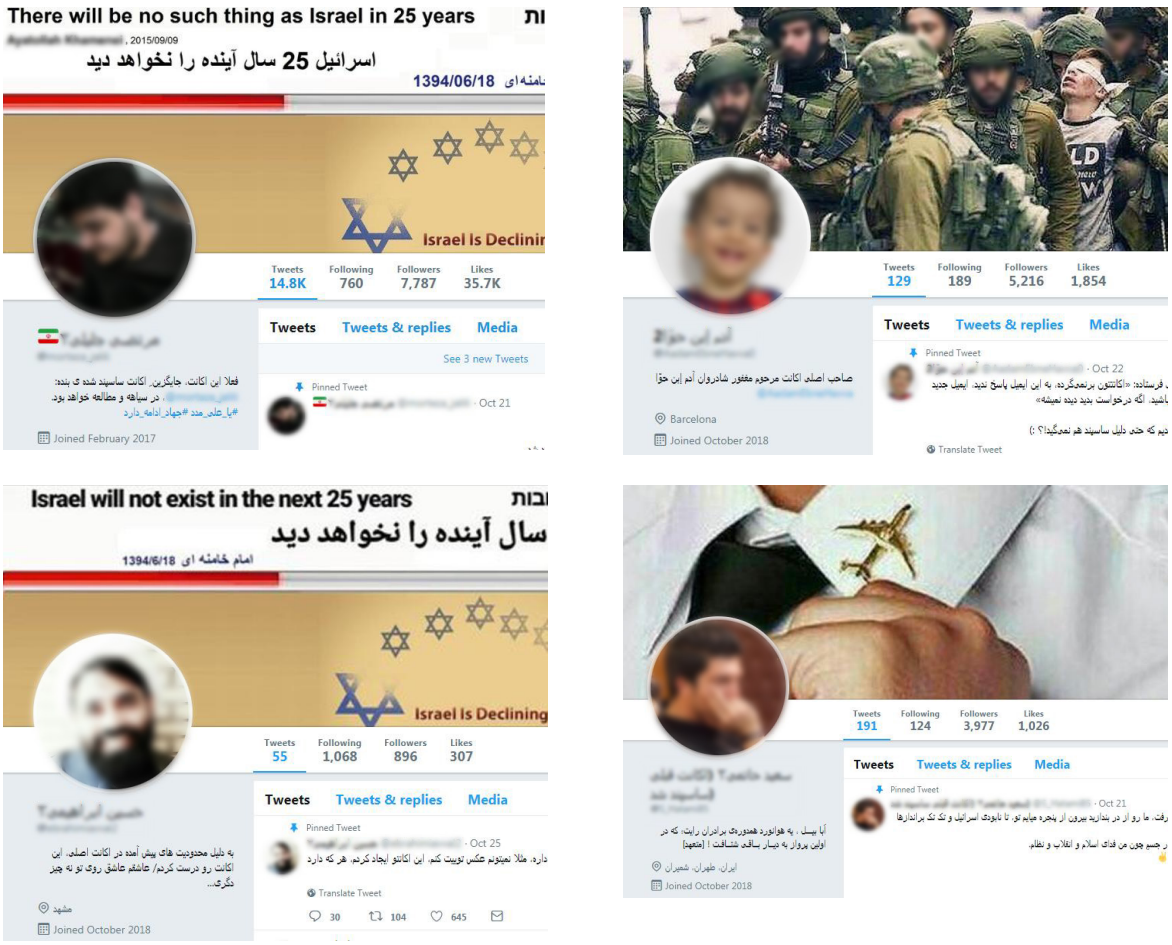
In China, media and social media are tightly controlled, with the government seeking to determine what people see and comment on. Government censors routinely monitor online discussions and ban terms and phrases—even seemingly innocuous ones—they consider could be critical of the authorities. In justification of this, the government's stance is that it deletes and takes action where it feels that there is evidence of disinformation or fake news. It will sometimes publicise how it has fined companies or individuals who have propagated fake or misleading news, but without providing much in the way of detail.

CHALLENGES AHEAD

Cat-and-mouse account blocking

Over the past two years, Twitter and Facebook have intensified their efforts to stop the spread of disinformation on their platforms, leading to hundreds of accounts and pages being suspended for disseminating hate or exhibiting inauthentic behaviour.

Although suspensions may help decrease the overall volume of disinformation at a certain point in time, the effect in most cases appears to be temporary. For example, most of the Iranian users who were suspended as part of Twitter's concerted efforts to stop the spread of malicious misinformation ahead of the US midterms, simply switched to new accounts.



Some of the suspended Iranian bloggers switched to new accounts following the ban (Twitter)

The new Twitter profiles made it clear who they were and openly said that they had been among the suspended accounts. Some profiles were even set up months before, which fuelled analysts' suspicions that the suspended users ran multiple accounts.

The effect of account suspensions on instant messenger services appears to be equally temporary. After Facebook and WhatsApp moved against what they saw as misuse of their platforms during the 2018 presidential campaign in Brazil, daily newspaper *Folha de Sao Paulo* reported that many supporters of then front-runner Jair Bolsonaro had migrated to Telegram,[16] another secure messaging app.

Private chat apps

As a recent report from the Reuters Institute for the Study of Journalism highlighted, audiences increasingly use private messaging apps to share and discuss news 'away from the toxicity of political debate' on social media.[17]

On the one hand, according to the BBC's Social Media Editor Mark Frankel, this offers journalists an opportunity to 'seek out new stories and forge essential new community relationships'.[18] But the closed nature of these services can also turn them into fertile ground for disinformation and misleading rumours. This is exemplified in India and Mexico,[19] where rumours shared on WhatsApp about child kidnappers have resulted in multiple deaths.

In Iran Telegram has been used to spread misleading messages about currency rates, despite a recent ban by the authorities. In September, pro-Kremlin Russian accounts on Telegram spread near-identical CCTV images of the Skripal poisoning suspects from Gatwick airport wrongly claiming they were identical.

For journalists, the privacy and end-to-end encryption of messaging apps present significant challenges, as well as complex editorial and ethical questions. Journalists can, of course, monitor open-source platforms and public channels on such platforms as Telegram to see if misleading claims surface there, and can seek tip-offs from members of the public. This approach was successfully used by journalists from Comprova (Prove it), a Brazilian verification project, during the 2018 presidential election campaign and resulted in numerous wrong claims and rumours being debunked.

BBCM is considering the challenges of working with closed conversations, whilst also paying close attention to local media and social media reporting of misleading claims spread via messaging services.

Deepfake technology

Deepfake technology uses machine learning and Artificial Intelligence, or AI, to create convincing videos of events that never happened.

In response, engineers from the BBC's 'Blue Room' team and Research and Development department are looking at how machine learning can help journalists spot manipulated digital media.

So far BBCM has only observed instances of this technology being used for entertainment and amusement purposes. But it may be only a matter of time before such sophisticated fakes start cropping up as part of influence campaigns. To stay abreast of developments, BBCM maintains close contact with BBC engineers and researchers working in the field.

Proliferation of sources

The huge growth in the number of sources spreading false information represents a major challenge. In Russia, for example, it is no longer enough to routinely monitor news bulletins on the main state TV channels, as misleading narratives are also widely pushed through popular political talk shows.

Monitoring such programmes, which may last up to four hours, on a daily basis, requires significant effort and resources. BBCM is looking at ways of automating the transcription of long programmes that could potentially contain disinformation, using speech-to-text software.

> Russia, in particular, is now widely seen as a key exponent of a new kind of information warfare

CONCLUSION

In a rapidly changing digital world, disinformation is a truly global problem, as no country appears to be immune from false claims and manipulation. It challenges democracies across the globe and affects societies where reliable information is in short supply. From Egypt to India and from Iran to Mexico, an increasing number of players use new media platforms and communication technologies to sow discord and manipulate public opinion.

Russia, in particular, is now widely seen as a key exponent of a new kind of information warfare, which relies on loosely-defined networks of pro-Kremlin actors using traditional and social media to influence opinions both at home and abroad.

Long-established methods of censorship and propaganda are still in evidence, but disinformation is becoming more sophisticated in terms of coordination, use of networks and advanced technology. Proliferation of sources, and the use of automation and closed communication channels by various actors also present new challenges to journalists and societies.

To operate successfully in such an environment, it is no longer enough to simply debunk individual claims. It is also important to raise awareness of disinformation tactics and manipulation techniques to help the public navigate and understand the increasingly complex and crowded information space.

The BBC—which has a long history of tackling misleading claims and verifying social media content—sometimes in collaboration with other independent open-source investigators, reports on these issues and helps bring them to the public's attention. In one recent example, the BBC's Africa Eye in September uncovered the truth behind the killing of women in Cameroon through

forensic analysis of open-source data.[20] By also describing in detail how this was done, an awareness of what to look for when coming across such stories was simultaneously promoted. As well as this sort of forensic reporting and open source analysis, the BBC is helping to promote media literacy in the UK and internationally through initiatives such as its Young Reporter scheme.

The role of BBCM, as a specialist unit observing hundreds of media each day, reporting on misleading narratives and providing the context necessary to understand them, is perhaps now both more necessary and more challenging than ever. BBCM's specialist journalists will need to continue to deploy both their linguistic and cultural expertise honed by constant observation of the sources, and technical expertise and support to help them cope with the complexity and scale of the challenge, which ultimately has the potential to undermine the very concept of truth.

ENDNOTES

1 RT. "MORE: After Attack People Dressed as White Helmets Members Planning to Film Themselves Helping 'Victims' to Be Shown in Intl Media - Russian Defense Ministry https://On.Rt.Com/9d3g #Syria." Tweet. @RT_com (blog), August 26, 2018. https://twitter.com/RT_com/status/1033653777239298048.

2 UK, Russian Embassy. https://twitter.com/EmbassyofRussia/status/1034793520706539521

3 Мордора, Голос. "Американцы предупредили Асада, что если в Идлибе их подопечные 'Белые каски' по приказу ЦРУ устроят провокацию с химическим оружием, то Асад будет немедленно и жёстко наказан." Tweet. @spacelordrock (blog), August 25, 2018. https://twitter.com/spacelordrock/status/1033250045267779584.

4 Pujji, Nardeep. "Dozens of Children in #Idlib and #Aleppo Kidnapped to Be Involved in Chemical Attack False Flag Snuff Movies by US UK Sponsored #WhiteHelmets Stop White Helmets from Sacrificing Children Again for Staged #ChemicalAttack in Order to Pin Blame on Assad #BreakingNews @mfa_russiapic.Twitter.com/0221DaftJB." Tweet. @AWAKEALERT (blog), August 28, 2018. https://twitter.com/AWAKEALERT/status/1034664350324326400.

5 Евгения. "Так они ж 'эвакуировали' белые каски. Кто им про 'химическую атаку' докладывать будет? Кто за финики с рисом 'пострадавших людей' ледяной водой поливать будет на камеру? Может они туда Скрипалей на разведку заслали?" Tweet. @hasenbraut1 (blog), August 25, 2018. https://twitter.com/hasenbraut1/status/1033251191516536832.

6 Beeley, Vanessa. "1. Staging of Chemical Attack in #Idlib Reportedly Prepped by Olive Grp Who James Le Mesurier Used to Work for, Founder of #WhiteHelmets, OG Merged Wth Constellis in 2015 Who Hve Blackwater in Portfolio., August 25, 2018. https://twitter.com/VanessaBeeley/status/1033292865517105152.

7 Dehradun, S. S. P. "सोशल मीडयिा पर एक व्यक्तजिसि नागा साधु बताते हुए कुछ लोगों द्वारा पीटने का एक वीडयिो वाइरल कयिा जा रहा है। उक्त संबंध में ज्ञात हो कि उक्त व्यक्तएिक बहुरूपयिा है, जसिके वरिुद्ध नशे की हालत में छेड़छाड़ की एक घटना में संलप्ित होने की शकिायत पर वैधानकि कार्यवाही की गयी है। pic.twitter.com/GB9uoDlsMs." Tweet. @DehradunSsp (blog), August 30, 2018. https://twitter.com/DehradunSsp/status/1035195417758056449.

8 Shaikh ✌, Afra. "Indian Muslim in Poor Bager Hindupic. Twitter.Com/OrUS3fktCN." Tweet. @Afraoo7 (blog), September 1, 2018. https://twitter.com/Afraoo7/status/1036107281492889600.

9 परविारशाखा. "देवों और ऋषमिुनयिों की भूमउित्तराखंड के देहरादून में एक नागा साधू को एक मुस्लमि युवक बेरहमी से पटिता रहा बाबा:"मुझे क्यों मार रहे हो," "मुझे माफ़ कर दो...)" वो दया की भखि मांगता रहा, भीड़ तमाशबीन बनी रही !! तसवीर और वीडयिो बनाना याद है, इंसानयित भूल गए !!pic.twitter.com/xdmzoRT0Uf." Tweet. @sakhaparivar (blog), August 30, 2018. https://twitter.com/sakhaparivar/status/1035232706760650752.

10 "Rajeshwar Dubey." Accessed December 4, 2018. https://www.facebook.com/groups/1277876175606583/permalink/1922380411156153.

11 @DFRLab. "#TrollTracker: Twitter Troll Farm Archives." DFRLab (blog), October 17, 2018. https://medium.com/dfrlab/trolltracker-twitter-troll-farm-archives-8d5dd61c486b.

12 "ICYMI." Accessed December 4, 2018. https://www.facebook.com/ICYMIvideo/videos/960971037436435.

13 "ICYMI." Accessed December 4, 2018. https://www.facebook.com/ICYMIvideo/videos/177623516129431.

14 "ICYMI." Accessed December 4, 2018. https://www.facebook.com/inthenow/videos/1914191838659398.

15 UlτrαRεbεl. "طقف ایربیاس راک شور زا نوتعالطا تهج دینک کالب pic.twitter.com/mFQ5ADOjzi." Tweet. @Amirhoseen_ (blog), January 2, 2018. https://twitter.com/Amirhoseen_/status/948196533475954689.

16 "Apoiadores de Bolsonaro começam a migrar grupos do WhatsApp para o Telegram." Folha de S.Paulo, October 19, 2018. https://www1.folha.uol.com.br/poder/2018/10/apoiadores-de-bolsonaro-comecam-a-migrar-grupos-do-whatsapp-para-o-telegram.shtml.

17 "The Changing Face of Social Media and the Rise of Messaging Apps for News | Reuters Institute for the Study of Journalism." Accessed December 4, 2018. https://reutersinstitute.politics.ox.ac.uk/risj-review/changing-face-social-media-and-rise-messaging-apps-news.

18 Frankel, Mark. "Journalists Have an 'Open Invitation' to an Interesting and under-Used Beat." Medium (blog), July 10, 2018. https://medium.com/@markfrankel29/journalists-have-an-open-invitation-to-an-interesting-and-under-used-

beat-5c3d739e16ae.

19 Martínez, Marcos. "Burned to Death Because of a Rumour on WhatsApp," November 12, 2018, sec. Latin America & Caribbean. https://www.bbc.com/news/world-latin-america-46145986.

20 Africa, BBC News. "THREAD July 2018, a Horrifying Video Began to Circulate on Social Media. 2 Women & 2 Young Children Are Led Away by a Group of Soldiers. They Are Blindfolded, Forced to the Ground, and Shot 22 Times. #BBCAfricaEye Investigated This Atrocity. This Is What We Found...Pic.Twitter.Com/OFEYnTLT6z." Tweet. @bbcafrica (blog), September 24, 2018. https://twitter.com/bbcafrica/status/1044186344153583616?lang=en.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org