Background

Bellingcat is an online open source investigation collective, initially staffed by volunteers from across the world and now employing 16 staff members with a head office in The Hague. Bellingcat is best known in the UK for its work revealing the true identities of the two suspects in the Skripal poisoning.¹

Internationally, Bellingcat’s work on the downing of MH17 in Ukraine on July 17th 2014 has brought it a great deal of attention in the Netherlands, Ukraine, and Russia. Bellingcat’s MH17 investigation tracked the missile launcher used to shoot down MH17 back to the 53rd Air Defence Brigade in Russia, identified key suspects, and other revelations linking the Russian Federation to the downing of MH17 that the official Joint Investigation Team investigation would later confirm.²

Since Bellingcat’s launch, the Bellingcat Investigation Team has won a number of prizes and awards, both by itself, and in partnership with other organisations. Bellingcat has won The Hanns Joachim Friedrichs Prize in 2015, the European Press Prize for Innovation in 2017, the Ars Electronica Prize for Digital Communities in 2018, the European Press Prize for Investigation in 2019, and the London Press Club award for Digital Journalism in 2019. Bellingcat has also been involved with award winning collaborative projects, most recently the BBC Africa Eye investigation, Anatomy of a Killing, which has won multiple major journalism awards, including a Royal Television Society Award and Peabody Award.

Bellingcat has also written extensively about the conflicts in Syria and Eastern Ukraine. These investigations into the Skripal poisonings, the downing of MH17, Ukraine, and Syria are often critical of the Russian Federation, and in response the Russian Federation and its supporters have responded harshly. This response has included relentless criticism and attacks in the Russian funded media, criticism and false allegations made by Russian government officials, and cyber-attacks linked to Russian intelligence services.

Russian Government Funded Media

Since 2015, following multiple articles published by Bellingcat about Russia’s involvement with the downing of MH17 and its involvement in the conflict in Eastern Ukraine, the Russian government funded news agencies Sputnik and Russia Today have published dozens of articles and videos critical of Bellingcat’s work. For example, these are some of the article titles from 2018 from RT.com:

Despite mainstream glory, questions raised about Bellingcat authenticity and Skripal poisoning case
Moscow slams Bellingcat for ‘leaking misinformation’ on Salisbury suspects from special services

¹ Skripal related articles on the Bellingcat website - https://www.bellingcat.com/?s=skripal
‘Fantasy gone wild’ – Moscow sighs as Bellingcat claims FSB tried to influence UK visa process

Bellingcat blogger slammed on Twitter for refusing to debate MIT professor on Syria claims

Bellingcat & Atlantic Council join to award exploited Syrian child & American mass murderer

The coverage is relentlessly negative and is willing to use any source to justify negative coverage of our work. For example, in a September 2016 report, ‘Untenable claims’: Russian activists raise more questions about Bellingcat MH17 investigation cites an “investigation carried out by a team of bloggers, journalists, aviation experts and volunteers calling themselves ‘Anti-Bellingcat’.”

This investigation attacks various aspects of Bellingcat’s MH17 investigation, although the report itself is full of errors which shows those attacks are unfounded. For example, it is implied in the Anti-Bellingcat report satellite imagery used by Bellingcat must be from a foreign government or intelligence service because the authors of the report are unable to find it online. What in fact happened is the authors were unable to correctly use the search interface on the Digital Globe catalogue, which was the source of the imagery used in the Bellingcat report and assumed Bellingcat was lying about the source of the imagery. The same imagery from Digital Globe used by Bellingcat is now freely available for anyone to view on Google Earth, further undermining the claim made in the Anti-Bellingcat report.

Despite these many errors, RT appeared to make no attempt to validate the contents of the report before reporting on it, and quotes Mikhail Malyshevsky, an adviser to the chief designer of Almaz-Antey about Bellingcat and the report:

“That’s an information war, [Bellingcat’s] version [of the tragedy] is evidence-free. They do not build a version based on facts, but trim the facts to fit their version. Just to give an example, the Dutch, at the suggestion of Bellingcat, claim that the missile flew toward the plane. This has been refuted by all our data, both mathematical and experimental.”

Almaz Antey is the Russian Buk missile manufacturer who had published their own claims relating to the launch site of the Buk missile that shot down MH17, contradicting the official investigations by the Dutch Safety Board and Joint Investigation Team. What RT fails to mention is Mikhail Malyshevsky was the key technical expert to the Anti-Bellingcat group, which also included Yury Kotenok as a lead co-author. Kotenok was the head of the press department of the Russian Institute of Strategic Studies (RISS), which was founded by Vladimir Putin as a government think tank and is also, according to the New York Times, linked to Russian foreign intelligence, a fact RT also fails to mention in its reporting.

Despite the obvious errors in the report, the severity of the accusations, and the political biases of the authors of the report, RT still uses it as valid criticism of Bellingcat.

Shortly after Russia began its bombing campaign in Syria in September 2015 Bellingcat demonstrated that the Russian Ministry of Defence was lying about the locations of airstrikes it shared on YouTube, claiming airstrikes were targeting ISIS when in fact they were

4 Kremlin Unleashes Attack Dogs on MH17 Investigation, DFRLab, September 19th 2016 - https://medium.com/dfrlab/kremlin-unleashes-attack-dogs-on-mh17-investigation-64e5df174b24
targeting non-ISIS territory. A few days later a journalist, Nimrod Kamer, contacted me via direct message on Twitter and asked if he could interview me. I was busy that day, and suggested he arranged to interview me at a later date. He responded by claiming he was in Leicester, my home town, with a cameraman on that day to film something about the Leicester Diwali Festival. As Diwali was 4 weeks away, I became suspicious, and quickly discovered he had filmed a piece about the Syrian Observatory of Human Rights (SOHR) for RT where he had tried to track down the person who ran it in their home town of Coventry. This was presented as a humorous piece by RT, but the man behind the SOHR has legitimate concerns for his own safety.

On that same day I then began to receive calls from my office building’s reception, my accountant’s office, and then my mother, who had all received visits from Nimrod Kamer. The encounter had upset my mother and made the others who had to deal with him rather unhappy, especially as they have virtually nothing to do with me on a day to day basis.

The following day RT broadcast Clerk promises ‘truth’ about MH17 ahead of official report which was clearly intended to attack my work and the work of Bellingcat, and made out I was avoiding Nimrod Kamer even though I had made it clear I wasn’t available that day and would have been happy to arrange an interview later.

A year later, RT produced a video broadcast on RT, shared on their website, and published on YouTube, titled Debunking ‘arm chair blogger’ Bellingcat. This video included criticism of our work, partly sourced from the Anti-Bellingcat report, and included selectively edited video footage of one of my presentations on Bellingcat’s MH17 investigation to make it appear if I was vague about evidence that indicated Russia’s involvement in the shooting down of MH17 in Ukraine. This was published on the same day as the first major press conference by the Joint Investigation Team, which confirmed many of the findings of our MH17 investigations, including that the missile launcher that shot down MH17 came from, and returned to, the territory of the Russian Federation. This video appears to have been an attempt to attack the work of Bellingcat and my own personal credibility ahead of this press conference.

False Allegations by Representatives of the Russian Federation

Negative reporting by the Russian media about Bellingcat is often fuelled by statements made by representatives of the Russian Federation. Russian Foreign Ministry spokesperson Maria Zakharova has made various statements and accusations against Bellingcat, including claiming Bellingcat is tied to special services and leaking misinformation, our evidence for our Skripal investigations was provided by Western intelligence services, and other claims.

---

6 Clerk promises ‘truth’ about MH17 ahead of official report, RT, October 8th https://www.youtube.com/watch?v=PR_b048IfBs
7 Eliot Higgins, Twitter, October 7th 2015 https://twitter.com/EliotHiggins/status/651767399591636992
8 Debunking ‘arm chair blogger’ Bellingcat, RT, September 28th 2016 https://www.youtube.com/watch?v=V3lwPS_1E2w
9 Russian diplomat accuses Bellingcat of leaking special services’ misinformation, September 15th 2018 https://tass.com/politics/1021728
10 No probe was conducted into Salisbury incident by Bellingcat, says Russian diplomat, TASS, October 14th
Usually, no evidence is provided to support these claims, but in April 2016 Zakharova made the following statement about Bellingcat’s work on MH17:  

“We understand the purpose of this group’s activities. Acting jointly with the current Ukrainian authorities, they continue to use all possible “fakes,” to create quasi-evidence to blame Russia.”

Following this claim I contacted the Russian Foreign Ministry and asked for evidence to support their allegations. In their initial response they failed to provide the requested information, so I asked again, and they provided a report which listed 4 ways in which our reporting was false. However, similarly to the Anti-Bellingcat report, the analysis in their report made multiple errors and proved to be incorrect.

More significantly, as we reviewed their report, we discovered that it had been entirely plagiarised from a popular Russian Livejournal blogger. Along with addressing the faulty claims made in their plagiarised report, we sent the Russian Foreign Ministry the following:

“Your specific examples are a summarization of two blog posts from the LiveJournal “albert-lex.” In some cases, the phrasings in your letter to us are lifted almost verbatim from this blog. In any future responses regarding evidence in the downing of MH17, we would appreciate if you formulated your own responses, or cited the sources for your claims. As your ministry accurately said in its previous response, this topic is “very sensitive” and we would also call on you to refrain from, in your words, “blatant falsifications and provide only verified, sound information.””

The Russian Foreign Ministry responded some weeks later asking us not to contact them again.

The Russian Foreign Ministry is not alone in making unevidenced accusations against Bellingcat. In an October 2018 press conference, the Russian ambassador to the UK repeatedly claimed Bellingcat was part of the British “deep establishment”, stating, among other things, that “Bellingcat is not the media. This is the tool of the deep establishment to leak certain things”.

---

2018 https://tass.com/politics/1025924
11 Briefing by Foreign Ministry spokesperson Maria Zakharova, April 6th 2016 http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2211888#21
However, when asked by journalists what evidence he had to support his accusations against Bellingcat he said “I can’t present you anything, but we have a feeling. No, I cannot present it to you.”

Cyberattacks

Bellingcat has also been targeted by a number of cyberattacks originating from the Russian Federation. Two Russian government linked groups have been connected to these attacks, the Cyberberkut, and Fancy Bear, who have been linked to Russia’s GRU intelligence service.

In February 2016 hackers accessed the personal emails of Ruslan Leviev, used that to gain access to his contributor account on Bellingcat, and defaced the Bellingcat website with images from his private emails and a message from the CyberBerkut claiming responsibility. The UK’s National Cyber Security Centre has linked the CyberBerkut with Russia’s GRU intelligence service.

From February 2015 to July 2016 three Bellingcat investigators, including myself, were targeted by emails that were part of a Fancy Bear phishing campaign. This campaign involved targeting thousands of Gmail accounts, and eventually would result in the leak of emails belonging to John Podesta, chair of Hillary Clinton's 2016 U.S. presidential campaign. While Bellingcat members received many of these phishing emails, Fancy Bear was unsuccessful in their attempts to access our accounts.

Two and a half years after this initial phishing campaigns, in late 2017, the same Bellingcat staff members were targeted by another phishing campaign. Cyber security company ThreatConnect again linked these attempts to Fancy Bear, this time noting the attacks targeted a wider range of accounts, including our DropBox and Skype accounts in addition to our Gmail accounts.

In July 2019 we’ve had further attempted phishing attempts against our investigator’s email accounts. This time, a ProtonMail account belonging to a researcher investigating the Skripal poisoning suspects was targeted. At the same time his account was targeted, ProtonMail accounts belonging to researchers outside of Bellingcat who were collaborating with us on the same investigation were also targeted. In a statement ProtonMail said:

---

16 Russian Ambassador to UK Yakovenko comments on UK-Russian relations, Ruptly, October 12th 2018 https://youtu.be/3_v0Twm04M?t=2733
17 Who is FANCY BEAR (APT28)?, CrowdStrike, February 12th 2019 https://www.crowdstrike.com/blog/who-is-fancy-bear/
18 Belling the BEAR, ThreatConnect, September 28th 2016 https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/
20 Belling the BEAR, ThreatConnect, September 28th 2016 https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/
23 Statement on the attempted phishing attack against Bellingcat, ProtonMail, July 27th 2019
“The resources used in this phishing attack (such as the domain registrars and resellers) are also resources that have been used in the past in other cyberattacks conducted by Fancy Bear (also known as APT28), a Russian cyber espionage group which may be affiliated with the GRU. Thus, while it is not conclusively proven, the evidence (along with independent third-party assessments) seem to suggest an attack of Russian origin.”

They also noted the sophistication of the attack:

“Furthermore, the attackers attempted to exploit an unpatched vulnerability in an open source software that is widely used by email providers in an effort to bypass spam and abuse filters. We were previously aware of this vulnerability and have already been watching it for some time, but we will not disclose it here because the software in question is not developed by ProtonMail, and it has not yet been patched by the software maintainers. This vulnerability, however, is not widely known and indicates a higher level of sophistication on the part of the attackers.”

While initially it appears less than a dozen accounts were targeted, further investigation has identified at least 3 dozen individuals targeted by the same phishing campaign, and all the targets are involved with investigating Russia in some way or another. This includes journalists, campaigners, activists, and fact checking organisations.

Summary

As a result of our investigations related to Russia we have been targeted with misinformation, smear campaigns, and cyber-attacks over a period of nearly 5 years by agents and representatives of the Russian Federation.

July 2019

https://protonmail.com/blog/bellingcat-cyberattack-phishing/