Volume 10 | Spring - Autumn 2021

# DEFENCE STRATEGIC COMMUNICATIONS


The official journal of the
NATO Strategic Communications Centre of Excellence



SPECIAL EDITION

# BELLINGCAT: RAPID ADVANCES, TROUBLING RISKS

## A Review Essay by Tony Esmond

*We are Bellingcat an Intelligence Agency for the People,*
Eliot Higgins. London: Bloomsbury, 2021.

**Keywords**—*strategic communications, strategic communication, intelligence, OSINT, open-source, Bellingcat*

### About the Author

Tony Esmond served as a police detective for 31 years in the United Kingdom. He is currently employed as a researcher at Cardiff University, Wales.

## INTRODUCTION

This review essay uses the lens of an experienced former police detective to examine the history and practices of the non-governmental organisation "Bellingcat", in the conduct of Open-Source Intelligence (OSINT) and investigation. The intention is to compare and contrast both regulated and unregulated practice, and to follow the journey OSINT has been on in the two settings to the present day. Over the past thirty years, law enforcement and intelligence agencies have been subject to increasing oversight of their practice. Some might say, rightly so. Since the explosion in Open-Source Intelligence following its first major use by UK Policing during the 2012 London Olympics, it is now available to anyone with a computer, and is increasingly employed by 'citizen journalists' as a key research practice. While checks and balances are enforced by law and have an increasing trajectory in official roles, the actions of the citizen journalist are subject to little regulation or bureaucratic oversight. In essence, we have seen the rapid move from police surveillance to citizen surveillance with little consideration of the implications or consequences.

To set the scene for this essay, I would like to travel back along the path of my own career. In 1988 I was 'invited upstairs', as it was called, to the Criminal Investigation Department (CID) Office.[1] The role of *Detective* was for most of my career a vocation as much as a job. *Detectives* ran informants, carried multiple heavy caseloads, became part of a competitive community, and produced results. The terms *Detective* and *Investigator* were synonymous with professionalism and a dogged refusal to give up. There were no quibbles about working hours or refreshment breaks in the CID Office. You came in and worked until you finished.

In the years that followed, came radical changes in all areas of police work in the UK. Many were the result of public enquiries and increasing calls for police practice to be regulated to protect the public from injustices. Loosely formulated Judges' Rules[2] for the conduct of investigations were reformed

1 'Criminal Investigation Department', *Britannica* online. The CID Office was set apart from the Uniformed Patrol Officers and led by a different management structure of Detectives.
2 T. E. St. Johnston, 'Judges' Rules and Police Interrogation in England Today', *Journal of Criminal Law & Criminology*, Volume 57, No 1, (1966): 85–92. Judge's Rules were guidelines for police interrogations—now called interviews and evidence needed for arrest.

by Codes of Practice that grew out of the Police and Criminal Evidence Act (PACE) of 1984.[3] Under this legislation, interviews progressed from scribbled contemporaneous notes in a smoke-filled room, to being taped or videoed to show transparency and ensure the rights of the accused. Today we have become familiar with Body Worn Video[4] cameras (BWV) being regularly worn by street level and community officers, and with cameras in police vehicles and all areas of custody suites. For investigators, the Regulation of Investigatory Powers Act (RIPA) of 2000,[5] governing the use of covert surveillance and other similar tactics by public bodies, caused a significant shift in police practice. This Act applies to a long list of public authorities who, when engaged in covert investigation techniques, must show reasoning and oversight.

Thus, in the world of crime and counterterrorism, where I learnt the skills of my craft, much has changed. Investigators are no longer *Detectives* or even necessarily warranted police officers, and their working practices often adhere to a strict eight-hour day and no more. It is now common for much of the research into the most serious moments in human history to be conducted, at least in part, by those with computer skills, rather than people skills. Cases are routinely solved with what can be found on the hard drive of a computer, the memory of a phone, or in the files of a CCTV (closed-circuit television) system. Long hours are spent examining communication and digital devices for that one piece of evidence that will solve a case. Changes in digital media investigation go much deeper than a dusty property bag containing a grubby laptop. The world of Open-Source Intelligence[6] or 'Online Open-Source Investigation' as Eliot Higgins prefers,[7] continues to show a global evidential purpose that is being pursued with imagination and some downright cunning tactics. Except this time, it's not only the police or security services who are making the headlines; it's Bellingcat and other citizen digital investigation groups.

3 The Police and Criminal Evidence Act aka PACE is the ever-evolving set of rules regarding police arrest, detention, transport, and identification of offenders. 'Police and Criminal Evidence Act 1984', Legislation.gov.uk.
4 Cameras worn by uniformed police for capture of crime and disorder. 'Body Worn Video (BWV)', London Metropolitan Police website.
5 RIPA is legislation that sets out rules for the authorisation and deployment of covert tactics. 'Regulation of Investigatory Powers Act 2000', Legislation.gov.uk.
6 OSINT is the umbrella term for 'any information that can legally be gathered from free, public sources about an individual or organization'. 'What is Open Source Intelligence (OSINT)?', SentinelOne website.
7 'Bellingcat Founder Eliot Higgins on Navalny, Syria and Qanon', YouTube, 5 February 2021.

## A CHANGE IN STEP

'From the outset, we have had two goals: find evidence and spread this field.'[8]

In *We Are Bellingcat,* Eliot Higgins, the founder of the Bellingcat organisation, shows what information about all of us—and where, when, and how we live our lives—is available in the online public domain; and what citizen digital investigators can obtain and then do with that information. The book is laid out as a history of the origins, evolution, and successes of the organisation. It is an amusing read and manages to walk the line between a book that appeals to a casual reader picking up something for a long train journey, and something for those who want to go deeper into Bellingcat's practices.

For a career detective, this book exemplifies just how the world has moved on from the examination of a suspect across an interview table to what they and others have posted online. Is there a need to catch someone in the act of their crime when you can catalogue evidence of their preparation, execution, and getaway using the content of their 'digital dust'?

To rewind, in 2011 Eliot Higgins was doing 'admin and finance work for various companies'.[9] During his day-to-day seemingly unsatisfying and tedious work, he had taken a keen interest in the situation in Libya. Tentatively, he began to blog about it and came upon a technique for the use of still images, video, and satellite imagery to piece together an account of what was happening. Describing his actions as 'stumbling into Geolocation',[10] Higgins had in effect found both a calling and a community: his 'call upstairs' moment had happened.

In recent times, Bellingcat have not been shy of the attention of either the media or the public. But that's not how it started. Higgins describes a process of evolution from a popular BlogSpot[11] written and researched solely by him and named after a Frank Zappa song 'Brown Moses',[12]

8 Eliot Higgins, *We are Bellingcat an Intelligence Agency for the People* (London: Bloomsbury, 2021), p. 22.
9 'Bellingcat Founder Eliot Higgins on Navalny, Syria and Qanon', YouTube, 5 February 2021.
10 The World of Intelligence podcast, 'An interview with Bellingcat founder Eliot Higgins', *Janes,* 11 February 2020.
11 Eliot Higgins, Brown Moses Blog, 6 April 2012. The original Higgins blogspot site.
12 Frank Zappa, 'Brown Moses', YouTube, originally composed in 1984; Higgins, *We are Bellingcat,* p. 18.

to the beginnings of what is now Bellingcat. In fact, the original Blog can still be found online,[13] the last entry dated 15 July 2014 describing the move to the new venture.

When discussing who or what he believes Bellingcat represents, in a recent 'Intelligence Squared' livestream YouTube interview,[14] Higgins gave the answer: 'Everyone who participates with us is Bellingcat'. This is resonant of the catchphrase used by the Anonymous group[15] and reflects the advent of the 'online community' to which he belongs, which is also somewhat 'outside' the mainstream, and counter cultural. He is keen to show that, other than in incidents of serious risk or in dealing with officially required evidence, Bellingcat does not work directly with, and is in a sense uncomfortable with, authorised intelligence agencies and law enforcement. He claims an identity that, despite Bellingcat's massive growth and notoriety, is still positioned as something of an insurgent and disruptor aligned with the world of the independent citizen journalist. To make his point, he gives his Kickstarter crowdfunding origins as proof. A quick search reveals that he has run two successful crowd funders, one in 2014[16] and another in 2017,[17] that between them raised £119,448 sterling. Enough at the time to get up and running, but nothing compared to the size and scope of Bellingcat in 2021. As a reader you sense the tension between Bellingcat's current success and its dearly held identity as an upstart disruptor.

## ESTABLISHING A REPUTATION

After a short anecdotal origin story in the opening chapter, the book goes into the technical/social/political details of the cases Bellingcat has handled. By 2011, Higgins had already covered subjects such as the UK Phone Hacking Scandal[18] as well as the events in Tahrir Square[19] but as the blogger 'Brown Moses', not as Bellingcat.

13 Eliot Higgins, 'What is Bellingcat?', Brown Moses Blog, 15 July 2014. The last entry on the Brown Moses Blog.
14 'Bellingcat Founder Eliot Higgins on Navalny, Syria and Qanon', YouTube, 5 February 2021.
15 'We are Anonymous' is a phrase often used by the anarchist 'hacktivist collective' to indicate their lack of structure and leaders who might be sought by law enforcement. 'We are Anonymous—How to Join Anonymous', YouTube, 12 November 2018.
16 'Bellingcat, for and by citizen investigative journalists', Kickstarter Campaign, Round 1, 2014.
17 'Bellingcat: the home of online investigations', Kickstarter Campaign, Round 2, 2017.
18 'Phone-hacking trial explained', *BBC News*, 25 June 2014.
19 Protests in Cairo in 2011 that led to the fall of Egypt's President Hosni Mubarak. Colin Freeman, 'Ten years on from Egypt's Arab Spring—what has become of the Tahrir Square revolutionaries?', *The Telegraph*, 24 January 2021.

The shooting down of Malaysian Airlines Flight MH17[20] on 17 July 2014 over Ukraine served as Higgins' and his colleagues' first significant challenge under the Bellingcat banner. He describes how the missile launcher was tracked across the country after Higgins issued a 'Gold Star challenge'. Essentially, this challenge involved the activation of crowdsourcing, inviting intelligence from the public, the reward for which was a 'gold star'. But he has since moved on to offering financial rewards on Twitter.[21] Already sought out as a media commentator, Higgins would find his own star in the ascendant in a startling trajectory.

Recognising a wealth of investigative opportunities in videos and photographs shared online, Higgins and company looked beyond geolocation into the identification of munitions being deployed.[22] This skill was learnt quickly through the necessity of keeping up with current events and led to the debunking of news items and rumours. Higgins invented a term for a type of unidentified tubular rocket—'UMLACA', standing for Unidentified Munitions Linked to Alleged Chemical Attacks. This use of homemade acronyms shows the lack of a professional background. But a useful hesitancy to jump to conclusions emerges that more broadly benefits the discipline. I was reminded of a Staff Sergeant at Hendon Police College in London in 1988 writing 'Never Assume' on a whiteboard. The core principles of investigation begin to show through in Bellingcat's stated benefits of analysis: 'Identify, Verify, Amplify'.[23]

While sitting at home in Leicester and digging through video footage of inspectors in the suburbs of Damascus, Higgins noticed the use of a measuring tape. He cut and pasted it into another image to show scale and in so doing identified the rocket used as a Soviet 140mm M14 artillery rocket. Reading this description, I was reminded of valuable advice given to me when attending my first-ever murder scene. 'Think Evidence, Evidence, Evidence and never ignore the details.' Here these same principles were being transferred to a whole new digital arena.

That said, the details regarding the locating and tracking of weapons through online techniques can become a little dry on occasions.

20 'MH17 Ukraine plane crash: What we know', *BBC News*, 26 February 2020.
21 Eliot Higgins, 'Bounty Tweet', Twitter, 31 July 2018.
22 Higgins, *We are Bellingcat*, p 73.
23 Ibid, p. 221.

Rocket launchers travelling through Ukraine feel like they are being described at almost every intersection of their journey. Albeit interesting to OSINT users, this section began to drag.

## IMPORTANCE OF RULES AND PROCESSES

One of the briefer sections in Chapter 3 of the book mentions the relationship between Europol's Child Sexual Offences initiative and Bellingcat. Law Enforcement Agencies (LEA) are often cynical towards the involvement of private organisations in criminal investigations and especially in the area of Sexual Contact Offenders. We have all seen the 'Paedophile Hunter'[24] vigilantes on numerous documentaries and Facebook pages. Often well-meaning, their ignorance of procedures of evidence gathering and continuity rules make it easier for suspects to escape prosecution on a technicality, or by using the Agent Provocateur[25] defence.

For decades, Indecent Images of Children (IIOC)[26] have circulated on the internet, finding homes on message boards, websites, and most notably The Dark Web[27] and TOR.[28] Media publicity around arrests that dates back to Operation Ore,[29] and the arrest of Luke Sadowski [30] has made sexual predators both knowledgeable and careful. There is rarely any meta data to be found in the images and videos they share. As a result, investigators are sometimes left only with what can be visually examined, and by close inspection of what is present in an image. Bellingcat researchers were ideally suited to help with the Europol 'Stop Child Abuse—Trace an Object'[31] initiative and continue to assist in solving cases.

24 Stinson Hunter is one of the more famous of these vigilantes. Stinson Hunter's YouTube Channel.
25 *R v Looseley [2001]* clarified the legal term of Agent Provocateur. One cannot instigate, incite, or procure another to commit and express breach of the law that they would not have committed anyway. House of Lords, 'Judgments—Regina v Looseley', parliament.uk, 25 October 2001.
26 There are different levels and types of IIOCs. They are no longer referred to as 'CP' aka Child Pornography. 'About indecent images of children', Bedfordshire Police website.
27 The 'dark web' is that part of the internet that cannot be accessed using surface net search engines. Darren Guccione, 'What is the Dark Web? How to Access it and What You'll Find', CSO: The State of Cybersecurity, 1 July 2021.
28 Tor is an anonymised browser that hosts around 30 000 websites in the unregulated regions of the internet. 'History', The Tor Project website.
29 Operation Ore uncovered a business run in the US that hosted a portal to sites where IIOC could be purchased online by credit card. Many thousands of people worldwide were arrested for downloading IIOC and further contact offences. Jon Kelly & Tom de Castella, 'Paedophile net: Did Operation Ore change British society?', *BBC News*, 17 December 2012.
30 Arrest of Luke Sadowski (aka George Richards): 'Ex-FBI-sting paedophile George Richards jailed for life', *BBC News*, 14 March 2014.
31 'Stop Child Abuse—Trace an Object', Europol initiative launched 2017.

Which is revealing with regard to their credibility with law enforcement agencies.

Nothing is more rewarding than recovering a child from sexual abuse. Every photograph is a crime scene. The smallest detail on a rocket launcher can be a useful identifier, as in the MH17 case, and so too are everyday items in Child Sexual Offences cases, such as the type of wood used in the headboard of a bed, the wristwatch of a suspect, or plants that can be seen through the small portion of a window. It is gratifying that Bellingcat have entered this field of work so that their techniques in image examination might yield positive results.[32] However, I worry about the level of publicity they then give to each success. For the victims and their parents, this may feel like an unnecessary reminder of traumatic events.

## POLICIES OF NON-INTRUSION IN CHARLOTTESVILLE

Higgins writes extensively about the far-right demonstration in Charlottesville in 2017, the public disorder, violence, and subsequent murder of Heather Heyer.[33] Bellingcat trawled through footage and identified many of those involved in the violence on the day.[34] Bellingcat's investigation was distinguished by innovation and originality—they logged birthmarks on the neck of one rioter that led to his identification. Higgins does, nevertheless, pose important questions about OSINT and the responsibilities attached to it: Does the investigation revolve around people who could have committed a serious crime? Who holds a public position of power and may be directing the disorder? Who is threatening criminal acts on the ground and online? These are important questions in any criminal investigation and especially in public disorder.

This is an important point in the narrative and shows Bellingcat were beginning to grapple with the ethical question—Why are we doing this? Are there groups or organisations for whom we should not be working? Higgins goes on to state that he and Bellingcat had no intention of bullying people because they attended a political rally. There would be

32 Carlos Gonzales, 'Creating Impact: A Year On Stop Child Abuse—Trace An Object', *Bellingcat*, 22 April 2020.
33 Minyvonne Burke and Marianna Sotomayor, 'James Alex Fields Found Guilty of Killing Heather Heyer During Violent Charlottesville White Nationalist Rally', *NBC News*, 8 December 2018.
34 Aric Toler, 'Database of August 12 Charlottesville Videos', *Bellingcat*, 29 August 2017.

no doxing of people merely for being with the wrong groups, or in the wrong place at the wrong time. In stating this, he was, in effect, beginning to apply aspects of the RIPA principles to his work in OSINT; namely, the principles of unnecessary collateral intrusion; and only intruding on those subjects when it was a serious case involving human rights principles of *necessity* and *proportionality*. In creating an embryonic, ethical framework for his new discipline, he was in proxy applying similar standards to those applied to public bodies. But with one key difference: no regulatory body exists for OSINT to check that such standards are being applied. Furthermore, Higgins and his collaborators could cease to apply them whenever they please.

Bellingcat make it clear that they do not consider themselves to be traditional journalists. Nevertheless, they decided to create ethical guidelines that allowed them to work in good conscience as 'internet sleuths'. They declared that their first responsibility was to the victims, and only when their safety had been established would they act to protect the identities of anyone appearing in criminal evidence. But they bear no criminal responsibility regarding the safety of the victims.

Perhaps it is a bridge too far to suggest what might be in the minds of men and women near to those acting illegally. Can we prove *mens rea*[35] and *actus reus*[36] from a short video extract on Snapchat? We return to the question of the human element: How can we examine what is in the hearts of people through a computer screen? It is a question that becomes more relevant with every case and especially if there is a requirement then or later in a criminal case.

The second half of the book describes wider far-right movements in the US, UK, and beyond, showing the influence that online forums and videos have on actors in the real world. Higgins describes the online outrage at Gamergate,[37] and the move from 4chan[38] to 8chan[39]—sites that increasingly became breeding grounds for hate speech and racism.

35 The legal term for criminal intent. 'Mens Rea', Legal Information Institute website. Cornell Law School.
36 The legal term for the act or omission that makes up the physical part of the crime. 'Actus Reus', Legal Information Institute website, Cornell Law School.
37 Jay Hathaway, 'What Is Gamergate, and Why? An Explainer for Non-Geeks', *Gawker*, 10 October 2014.
38 Emma Grey Ellis, '4Chan Is Turning 15—And Remains the Internet's Teenager', *Wired*, 1 June 2018.
39 Mike Wendling, 'What is 8chan?', *BBC News*, 5 August 2019.

In March 2018, Brenton Tarrant[40] posted his final remarks on 8chan before committing mass murder at two mosques in Christchurch, New Zealand. With widespread exclusion from or de-platforming on Twitter,[41] Facebook, YouTube, and even TikTok,[42] the far right have scrambled to secure a foothold on any commonly used platform. Even Russia's Facebook-style VK site (VKontakte) became a brief home for Tommy Robinson and Britain First before their Group Pages were deleted. When Parler lost its servers,[43] the UK and US far right continued with the messaging app Telegram,[44] but also looked to move to other sites such as Gab[45] and MeWe. Bellingcat's activity on these much smaller sites is intriguing, where hiding in a crowd becomes more difficult. Might they be using False Persona Profiles[46] or — commonly known in OSINT fields as 'Research Accounts'?

## THAT'S A PRETTY SPIRE

Following the Salisbury Novichok poisonings in the UK in 2018, Bellingcat seems to have taken more chances and resolved to 'own' their growing reputation. Identifying two Russian agents[47] involved in the attack catapulted the organisation into the mainstream media, who were reporting extensively on Bellingcat's successes. No longer could they be dismissed as amateurs or laptop detectives. They were beginning to be noticed by the 'right' and 'wrong people'; and they played up to this. Even their podcast 'Bellingchat' would adopt a satirical introduction with a Russian accent.[48] Chapter 4 of the book reveals working practices of the Russian Secret Services and the deployments of their undercover assassins. Focus is placed on how the agents created a false identity, then on what Bellingcat did to prove the Russian Undercover Unit's tactics were flawed in our modern information age—an age where backstories and legends can be researched from a laptop.

40 Florence Keen, 'After 8chan', Centre for Research and Evidence on Security Threats, 4 December 2020.
41 'Twitter suspends Britain First leaders', *BBC News*, 18 December 2017. Twitter bans Britain First and Paul Golding.
42 'TikTok bans Britain First and Tommy Robinson for hate speech violations', *TellMAMA*, 23 April 2020.
43 Russell Brandom, 'These are the violent threats that made Amazon drop Parler', *The Verge*, 13 January 2021.
44 'Kevin Collier, Anna Schecter and Ezra Kaplan, 'Telegram, a recent haven for the far right, purges extremist content', *NBC News*, 14 January 2021.
45 Danielle Abril, 'Trump supporters flock to MeWe, Gab, and Rumble after Parler goes offline', *Fortune*, 12 January 2021.
46 False Persona Profiles are faked user profiles that can be used to penetrate closed groups and allow for the obfuscation of the true person at the keyboard. Alex Aronovich, 'How to Detect Fake Profiles—Understanding Phishing', Cybint website, 14 August 2018.
47 Elliot Higgins, How Bellingcat uncovered Russia's secret network of assassins, *Wired*, 4 February 2021.
48 Bellingchat Podcast, Episode 3, 'Hunting the Salisbury Poisonings Suspects', *Bellingcat*, 16 June 2020.

What is surprising is Bellingcat's move away from image investigation to using informants who received payments from the organisation for information supplied. A Russian Government worker, referred to as a 'babushka',[49] insists on payment in roubles for providing personal details of Russian citizens. Bellingcat took a chance—it proved successful. The account makes for gripping reading, but I worry about the ethics. The use of paid informants is widespread in policing and journalism, their payments scrutinised and handled with the utmost security.[50] It is a process that occasionally goes wrong with serious risks and consequences, particularly to the informant. The method of payment is not described in this book but leaves a few questions dangling. How were these payments explained and how great was her risk of exposure? Who else saw the payment or bank account? Was the staff member subject to a style of vetting that would have revealed the payment? Informants are often not the most honest of people, but they do deserve a duty of care. Had Bellingcat fully explored the serious risk this informant would face? The necessary considerations for running the babushka informant are explored further in the next section. Have Bellingcat and Higgins at this point moved outside the working sphere of 'Open Source' and into something more dangerous?

## WELFARE

Bellingcat were becoming victims of their own success and were facing various threats. Robert Evans, one of their lead investigators, found a photoshopped 'Wanted' poster on 8chan offering a large reward for his head. Cyberattacks from unidentified actors were also commonplace and had been an active tactic against Higgins from his Brown Moses days. But the biggest threat came from psychological damage. Higgins describes in heart-breaking detail how Andrew Carvin, a senior fellow with Higgins at the Atlantic Council's Digital Forensic Research Lab, suffered with Post-Traumatic Stress Disorder (PTSD) from the imagery he had viewed online. Higgins describes it as 'a slow-drip effect of repeated exposure'. To Bellingcat's credit they attempted to address the problem by publishing a guide on identifying and preventing PTSD.

49 Higgins, *We are Bellingcat*, p. 165.
50 The payment of police Covert Human Intelligence Sources is often a subject for conspiracy theorists and Freedom of Information requests. Sally Murrer, 'Revealed: How much money is paid out to informants by police force looking after Milton Keynes', *MKCitizen*, 30 January 2020.

As Higgins found, when searching the internet there are rarely warnings. A brief surf through certain channels on most platforms will produce upsetting material. RIPA deals with this and appoints officers whose job it is to specifically deal with the welfare of operatives and supervisors.[51] In law enforcement and at the UK's National Crime Agency, those viewing extreme material are regularly screened by Occupational Health and/or independent psychologists. For those viewing material every day for long hours these appointments may be as often as each month.[52] Discussing the IIOC Operation with Europol, Higgins mentions tweeting cropped images of the scenes of child abuse to 'a base of thousands of amateur sleuths'. The images showed rooms with the child cropped out, so they were not in themselves indecent. But my experience with victims suggests that even small details can cause anxiety, depression, and flashbacks. As Bellingcat grows, the welfare issue will continue. Others outside of law enforcement have recognised the importance of this too. Significantly, the Human Rights Centre has been working on protocols for Open-Source Investigations. They include references to safety, peer review, and respecting the dignity of operators. Perhaps not perfect and not yet conforming to the standard of Law Enforcement Agency welfare mandates, this is an excellent step forward.

## PUBLICITY

Coming from a working environment where successes are rarely discussed—other than over a pint after work with colleagues—this book could be seen as 221 pages of public backslapping. However, these successes are not from police work; they don't belong to an old-fashioned age of pagers, phone boxes, and meeting with informants in the park. Rather, they take place in the modern internet age. Revealing exposés can be very damaging for someone like President Putin. When the GRU agents in the Salisbury poisoning case were revealed, the public interest required the full facts be put in front of a global audience: 'People who are making the most noise are getting the least attention', writes Higgins.[53]

51 This documentary series goes as far as to show interactions between Child Sexual Offence investigators and their welfare officers. 'Undercover Police: Hunting Paedophiles', *Channel 4*, n.d.
52 Neil Ralph, 'Dealing with the personal impact of crimes against children', College of Policing, 21 August 2020. Report on the implications of officers having to view IIOCs and the treatment they are offered.
53 The World of Intelligence podcast, 'An interview with Bellingcat founder Eliot Higgins', *Janes*, 11 February 2020.

## PRACTICAL CONSIDERATIONS

Coming from a law enforcement background, I am particularly concerned with one aspect of Bellingcat's operating procedures—surveillance. The following definition comes from the Parliament.uk website:[54]

> A literal definition of surveillance as "watching over" indicates monitoring the behaviour of persons, objects, or systems. However, surveillance is not only a visual process which involves looking at people and things. Surveillance can be undertaken in a wide range of ways involving a variety of technologies. The instruments of surveillance include closed-circuit television (CCTV), the interception of telecommunications ("wiretapping"), covert activities by human agents, heat-seeking and other sensing devices, body scans, technology for tracking movement, and many others.

Is what Bellingcat do surveillance? They certainly monitor the behaviour, movements, and contacts of individuals. In recent years, the concept of 'more than two looks make it an act of surveillance' circulated. This was arbitrary and excused the actions of many. But for anyone in an organisation covered by RIPA who decides to surveil a person in the real world or attempts to obtain evidence online, then that constitutes surveillance and requires the appropriate authority signed by a senior officer, and in certain cases a high-ranking government minister. As 'citizen journalists' Bellingcat do not currently fall under RIPA legislation. Is that badge enough to protect them when they fail to balance their work interests against the harm it may do to others?

RIPA doesn't differentiate between 'intelligence' and 'evidence'. And neither should we. To go to someone's social media account to see what they are doing, whom they are speaking to, and what they are posting, represents surveillance—what you learn constitutes evidence. Bellingcat are compiling a list of best working practices and protocols to deal with emerging threats. They are also applying themselves to the evolution of Artificial

54 House of Lords, Chapter 2: Overview of Surveillance and Data Collection, Surveillance: Citizens and the State—Constitution Committee, parliament.uk.

Intelligence[55] and 'Deepfakes'—no doubt numerous other areas too. These protocols feel like the first steps in replicating the checks and balances that RIPA, PACE, and other important legislation dictates in the public sector. As Bellingcat grows and learns, these will hopefully become a set of guidelines they can quote in court and public inquiries. To be clear, today the law that applies to the police and other agencies does not apply to them or to journalists. Or to you or me. Maybe that's a good thing, maybe not?

## VIEW FROM UPSTAIRS

As a retired detective, I always observe other people's motivations, techniques, and abilities carefully, and often with cynicism. There is, however, no denying the many successes of Bellingcat and their refreshing enthusiasm for attacking each challenge. If only more coppers had the same attitude!

Social Media is not just the home of noisy teenagers at the back of the bus bragging about how many friends they have on Myspace. Those days are long gone. It is now an evolving source for both news and opinion. The complications described in this book regarding misinformation and disinformation, influence operations, counter-factual cyber hand grenades, and deepfakes make for an invigorating reading experience, but they also show how vulnerable we are as individuals to being manipulated. Extrapolate that beyond the single person to the town, city, organisation, and state, and you can see what a pernicious weapon the internet and social media have become. Daily headlines prove how unguarded we have allowed ourselves to be. The recent infiltration of AstraZeneca staff by North Korean cyber spies through the previously untouched networking site LinkedIn came from left field.[56]

With the responsibility of welfare to operatives and the investigative processes comes the necessity to organise carefully and catalogue all evidential material. Currently, according to Law Enforcement protocols, material is stored for six years and often longer. A good researcher

55 AI claims to borrow concepts from Darwinian evolution and develop before our eyes. Ed Gent, Artificial Intelligence is Evolving All By Itself, *Science*, 13 April 2020.
56 North Korean agents managed to infiltrate workers at AstraZeneca during the development of their COVID vaccine using LinkedIn. Jack Stubbs, 'Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca—sources', *Reuters*, 27 November 2020.

will keep digital copies of their evidence and should be able to find it in minutes, no matter how long ago it was discovered. The testing of this ability to produce older work should be closely monitored by the supervisor. The extensive details that Higgins explains in his book regarding each crisis they have investigated indicates that their evidential bookkeeping is well handled.

However, numerous questions remain. How well do Bellingcat realise the importance of evidential continuity?[57] Or identification case law such as *R v Turnbull*,[58] which is as relevant to video identification as to the 'Street ID' it was originally designed to address? Or contemporaneous note-keeping, time-stamped notes, and processes of corroboration of evidence in English and especially Scottish law?[59]

Running a team of operators, who may be using False Persona Profiles[60] is a sensitive sphere of operations. While not falling under RIPA legislation specifically, Bellingcat are still a group who tangentially are tasked by LEA (see the IIOC operation at Europol). If so, then oversight of psychological and logistical support is maybe not legally required, but certainly much preferred in case there are future complications. 'I wasn't given enough support' comes the scream of the operator caught doing something wrong/unlawful. A requirement protects the operator and their supervisor.

Verification of 'hands on keys',[61] and seeking to confirm whose fingers were responsible for typing is tricky without the human element. Image verification is a desirable descriptor but ultimately a video can be evidentially useless if you can't prove who took it, present it in a manner acceptable to a court of law, and confirm that the video has not been tampered with.

57 'Continuity' is the evidential principle required by a criminal court of law that can show where and with whom an exhibit is at all times. 'Continuity', Health and Safety Executive website.
58 *R v Turnbull* [1977] is important identification case law quoted in Code D of the Codes of Practice within PACE. 'Identification', The Crown Prosecution Service (CPS) website, updated August 2018.
59 'Corroboration of evidence' has been an important aspect of Scottish law for centuries but also impacts covert case law in England; *R v Birtles* [1969] is an example. 'Corroboration of Evidence in Criminal Trials (Law Com. No. 202)', The Law Commission, 1991.
60 False Persona Profiles are not the same as 'Takeover Accounts' or accounts owned by criminals that are used as fishing tools by investigators. '35200 POLICY – Open Source Investigation and Research', Hampshire Constabulary, updated 8 January 2018.
61 'Hands on keys' is a phrase used in relation to proving who actually typed an online comment or posted a video. Questions such as—Who had access to the computer? Was it ever left unlocked?—are used by the defence in court.

'Lateral thinking' is something Higgins raises. He reflects on how to use it and remain unhindered by the paperwork generated by the heavy bureaucracy of law enforcement, so allowing him to act tactically and more rapidly to catch that early prize. This achieves spectacular results. Nevertheless, it's hard not to compare Bellingcat to my previous employers. They share many techniques and intentions. However, they are not analogous. Higgins grew up on a staple of John Pilger and Noam Chomsky[62] and not early mornings of marching, saluting, and learning the Road Traffic Act 1972, by rote. This allows for imaginative thinking and brilliant out-of-the-box innovation but may also cause complications when producing their work in a way acceptable to the law courts or to future public opinion.

Using informants and the tactic of paying for information are still troubling. Not from an ethical point of view (people have been paid like this for centuries) but from that of Bellingcat's duty of care to their sources. A payment is the easiest thing in the world to discover. There is also a distance that can be easily explained when using OSINT techniques, which does not equate to dealing with Human Intelligence (HUMINT). Officers train for years to keep individuals safe. These individuals may be at extreme risk. Acting like this moves Bellingcat from being an OSINT company into something resembling an espionage agency. They are entering into territory that implicates them in what could be a criminal conspiracy or assisting, if not encouraging, a crime to obtain protected information.[63] This is no longer the world of research but rather an unlawful interaction where corruption of an official is occurring. This book may represent an admission of guilt.

## WHAT CAN WE EXPECT IN YEARS TO COME?

The use of videos and livestreaming linked to the internet is one of the business successes of the last few years. How long before something like a doorbell camera becomes hackable and part of a larger spy network? How long before this becomes an exploitable product by people on both sides of the legal fence? Being able to tell when someone isn't home is of interest to both criminals looking to steal and spies looking to creep… and so much more.

62 'Bellingcat Founder Eliot Higgins on Navalny, Syria and Qanon', YouTube, 5 February 2021.
63 'Inchoate offences', The Crown Prosecution Service (CPS) website, updated 21 December 2018.

The COVID pandemic is influencing all areas of life across the world. But it can also profoundly affect covert operations. There were no doubt a few phone calls shooting between Whitehall (government) and Vauxhall (secret services) when 'Test and Trace'[64] was announced. Perhaps a voice was heard to ask: 'There's a new phone app that can tell you where someone has been and who they have been speaking to? Are you mad!' Monitoring of public and private life may open the door to further avenues of investigation and abuse in the coming years.

As Big Tech moves people considered undesirable off their platforms, we will see the rise in closed niche communities. Society and those active online have become tribal as evidenced by the far-right movements that have been gaining momentum since the US 2020 elections.[65] At the same time, COVID deniers and anti-vaccination activists[66] are being pushed off traditional platforms. A narrative is fed to people in a bubble and when applied to individuals in closed and polarised networks may prompt paranoia, activism, and conspiracy theories.[67] Infiltrating such groups necessitates moving beyond OSINT to a more involved and interactive infiltration mode, beyond simply constructing False Persona Profiles, as is done currently, and into building credible back stories and financial histories. In so doing, the field of investigation will inevitably take many dangerous turns and risk the revelation of operators.

At what point does this become fraud by impersonation? How far does a private organisation push the pretence of being someone else online before their acts become illegal? And how will we really know whom we are talking to? How will it affect our duty of care to operators and those who become involved accidentally? If the only way to monitor and capture evidence on certain sites and groups is by joining under a false name, what can prevent an operator from being arrested under a conspiracy charge? And once arrested, how can the operator mount a defence in court? How is transparency to be measured and managed? This will fundamentally affect the way research can successfully be undertaken. Throughout this book Bellingcat have shown an ability to adapt.

64 UK Health Security Agency, 'NHS Test and Trace: what to do if you are contacted', gov.uk website, 27 May 2020.
65 E.J. Dickson, 'Proud Boys Channels Are Exploding on Telegram', *Rolling Stone*, 14 January 2021.
66 Cristina Criddle, 'Coronavirus: YouTube bans misleading Covid-19 vaccine videos', *BBC News*, 14 October 2020.
67 Michael Butter, John Cook and Stephan Lewandowski, 'Identifying conspiracy theories', European Commission.

The challenges ahead will be yet another testing ground for them, as I'm sure we will discover in a second volume.

## CONCLUSIONS

*We are Bellingcat: An Intelligence Agency for the People* is a book that tells a history that expands beyond its own evolution. In only a few years, the Bellingcat team have gone from a group of online operators to a global brand, highlighting those working behind the scenes to manipulate world events and our interpretations of them in the process. The answer remains to be seen. Bellingcat will change their approach and operational style now that they are recognised as market leaders. Their popularity has been used to spread news of the injustices they have uncovered and advertise the training they organise.

A familiar and personable style permeates Higgins's writing so that, while at moments he belabours 'then we did this, then we did that' sequences, these moments are nevertheless explained for any reader lacking in-depth technical ability. For those short on computer science or conspiracy video background, the amount of information uncoverable by those with a keen investigative nose is shocking. What we do, who we are, and where we live appears to be forever imprinted and available on the web—just occasionally for a charge. What does this mean for the balance of power? If we can't trust our governments, should we trust our neighbours with often very personal data? In Bellingcat's world view does a red line divide what they *can* do from what they *should* do? How do they distinguish between the two? And how do they decide when action is required and who gives that advice/makes that call? How will that view develop in the face of technological change?

Regulation is a tricky area. If this form of OSINT is regulated in the UK there will be another country or authority that does not fall into lockstep. And those who object to some form of registration will flock to it. Numerous parallels can be drawn with law enforcement, and also with the freedom of the press. The ability to operate in an unregulated arena has both a good side and a risky side. The passing of information from one hand to another can be accompanied by genuine peril. Bellingcat are finding out that you can learn from your successes and that you can also learn from your mistakes. Only time will tell which affects them most.