PUTTING PRINCIPLES INTO PRACTICE:
Testing Open-Source Video as Evidence in the Criminal Courts of England and Wales

Lessons Learned From a Mock Voir Dire Hearing

A joint publication from Global Legal Action Network (GLAN) and Bellingcat
PUTTING PRINCIPLES INTO PRACTICE:
Testing Open-Source Video as Evidence in the Criminal Courts of England and Wales
Lessons Learned From a Mock Voir Dire Hearing

A joint publication from Global Legal Action Network (GLAN) and Bellingcat, supported by OSR4Rights

Global Legal Action Network (GLAN) is a non-profit organisation based in London. GLAN works with affected communities to pursue innovative legal actions across borders, challenging powerful actors involved in human rights violations and systemic injustice.

Bellingcat is an independent international non-profit collective of researchers, investigators and citizen journalists that specialises in online investigations, specifically fact-checking and analysing open-source information including audio-visual content.

OSR4Rights at Swansea University was a research project funded by the UK’s Economic and Social Research Council which examined how open source research is currently used in human rights investigations, and interrogated whether and how this evidence can be leveraged more systematically for the discovery and documentation of human rights violations in future.
PUTTING PRINCIPLES INTO PRACTICE: Testing Open-Source Video as Evidence in the Criminal Courts of England and Wales Lessons Learned From a Mock Voir Dire Hearing

In February 2021, the Global Legal Action Network, Bellingcat and OSR4Rights at Swansea University staged a mock hearing to test the admissibility of an online video before the criminal courts of England and Wales.

This report gives an overview of the event and analyses the significance of the outcome. Part I introduces the project and sets out, in narrative form, how the hearing unfolded. Part II enters into a discussion and analysis of the event in terms of evidentiary rules and draws attention to some lessons learned.

Dearbhla Minogue, Siobhán Allen and Yvonne McDermott Rees¹

¹ Dearbhla Minogue and Siobhan Allen are Senior Lawyers with Global Legal Action Network. Yvonne McDermott Rees a Professor in Law at the Hillary Rodham Clinton School of Law at Swansea University and a member of the Legal Action Committee of Global Legal Action Network.
# Table of Contents

**PART I: WHAT HAPPENED**

A. INTRODUCTION AND BACKGROUND ................................................................. 4  
B. DRAMATIS PERSONAE ....................................................................................... 5  
C. DEFINITIONS ....................................................................................................... 7  
D. FICTIONAL UNDERLYING CASE ......................................................................... 9  
E. EVIDENCE ............................................................................................................ 10  
F. MOCK HEARING OVERVIEW ............................................................................. 11  
G. PROSECUTION AND DEFENCE ARGUMENTS ..................................................... 12  
    i. Prosecution ......................................................................................................... 13  
    ii. Defence ............................................................................................................ 14   
H. EVIDENCE PROVIDED BY THE FACTUAL AND EXPERT WITNESSES ............ 16  
I. THE RULING ......................................................................................................... 17  
    i. Open-source Analysis as Expert Evidence ......................................................... 17  
    ii. Admissibility of the Exhibit CG/2 Video ......................................................... 19

**PART II: ANALYSIS**

B. THE CATEGORISATION OF OAVC EVIDENCE AND THE CONCEPT OF AUTHENTICITY .......................................................................................................................... 23  
C. THE IMPORTANCE OF TAILORING WHAT CLAIMS ARE MADE ABOUT THE VIDEO ................................................................................................................................. 26  
D. OSI AS EXPERT EVIDENCE ................................................................................. 29  
    i. How Independent Does the Expert Need To Be? ................................................. 30  
    ii. What Should an OSI Analyst as an Expert Refrain From Commenting On? ..... 31  
    iii. Note on the Witness Statement of Eliot Higgins .............................................. 31  
        iv. Digital Forensic Analysis ............................................................................... 32  
E. THE BELLINGCAT METHODOLOGY ................................................................. 33  
    i. Bias ..................................................................................................................... 33  
    ii. Chain of Custody ............................................................................................... 35  
    iii. Peer Review ..................................................................................................... 36  
        iv. Types of Expertise Within Bellingcat ............................................................ 36  
        v. Duties on Investigators .................................................................................. 37
F. THE EXPERT’S ONLINE SEARCH .................................................................................43
G. THE OTHER VIDEOS ........................................................................................................44

ANNEX I: DETAILS OF WITNESS EVIDENCE AT MOCK HEARING .........................45
  Charlotte Godart: Witness of Fact ...............................................................................46
  Eliot Higgins ................................................................................................................46
  Frank Palmer: Expert Witness ......................................................................................49

CREDITS .................................................................................................................................53
PART I:
WHAT HAPPENED
A. INTRODUCTION AND BACKGROUND

1. GLAN’s work towards accountability for crimes committed in the context of the war in Yemen is comprised of three main strands:

   a. Development of litigation strategies in partnership with Yemeni and international organisations;

   b. Development of a multimedia evidence database of airstrikes causing grave civilian harm; and

   c. Seeking to increase the likelihood of successful litigation through exploration of the use of technology and digital evidence in international and domestic judicial proceedings.

2. As part of the third of these strands, since 2019 GLAN and Bellingcat have partnered in a long-running project to design a methodology for the discovery, collection and preservation of digital open source information (“OSI”). The aim of developing the methodology is to increase the likelihood of this content – in particular audiovisual content such as video – being admitted and given due weight as evidence in criminal proceedings. The project was initiated on the basis of the increasing recognition in the legal community that digital open source information can be a vital addition to traditional forms of evidence, but that there are challenges in utilising it. There is emerging suggested best practice amongst academics and practitioners in this regard, reflected in particular by the Berkeley Protocol on Digital Open Source Investigations.2 However, there is still insufficient predictability as to exactly how open source audiovisual content will in fact be treated when it is presented to a court as evidence. The issue has arisen to a limited extent at the International Criminal Court and some domestic jurisdictions, but issues surrounding the admissibility and weight of online videos and other similar content have not yet been tested in the courts of England and Wales.

3. The purpose of staging a mock hearing was to robustly test the methodology GLAN and Bellingcat designed and to better understand any potential risks or weaknesses in relying on open source evidence in litigation. It was envisaged that lessons taken from the process would be used to anticipate challenges, strengthen the methodology and enable better presentation of findings. With those objectives in mind, GLAN and Bellingcat, together with the OSR4Rights project at Swansea University, hosted a fictional voir dire hearing that emulated a real application before the criminal courts of England and Wales to admit a piece of open source evidence from the conflict in Yemen, before a live online audience.

4. The hearing concentrated on a real airstrike on the Office of the Presidency in Sana’a, Yemen, by the Saudi/UAE-led coalition (the “Coalition”). The video around which the fictional proceedings centred (referred to in the proceedings and this document as “Exhibit CG/2”), was also real and had been posted online via a Yemeni Twitter account. However, other aspects of the evidence were fictionalised, omitted or otherwise differed from real proceedings for the purposes of the exercise. These included:

---

a. The individual who posted the evidence online: The piece of evidence was a video of an airstrike posted by a Yemeni journalist on Twitter. The journalist was not named in the fictional hearing because we wanted to allow for the defence to impugn the source as would likely happen in reality. We also did not want our audience to confuse any fictional, criticised source with the actual online source. It should be noted for completeness that in a real prosecution, an attempt would have been made to find the creator to attend court and authenticate the video, but this is often not possible. This exercise proceeded on the basis that the source could not be found.

b. The individuals in the video: The faces of the people appearing in the video are visible in the online version but were pixelated by GLAN to respect their privacy given that this was a public-facing exercise. As in the case of the Twitter source, in a real prosecution an attempt would be made to find these people. Given that this was not a real hearing (in addition to the intentional focus on the open source nature of the video), no such attempt was made to locate the individuals.

c. Time: In reality, an application like this would have run for much longer with more detailed cross-examination of witnesses and likely additional witnesses and experts called to give evidence, in particular a defence expert witness.

d. The expert, defendant and witnesses: Whilst the witnesses from Bellingcat (Eliot Higgins and Charlotte Godart) are real individuals, the expert ‘Frank Palmer’ (played by Bellingcat’s Nick Waters) was a fictional individual working for a fictional organisation. The defendant and his confession were entirely fictional, as was Dr. Althaibani, the medical doctor who provided evidence in relation to civilian casualties. Further, the witness evidence provided by Eliot Higgins contained a mixture of fact, expert and legal submissions which would, in a real case, be separated out and addressed elsewhere in the materials (see paragraph 88 below). For more discussion as to why fictional evidence was introduced, see Part II.

e. The judge’s ruling: given the fictitious nature of the case and the hearing, the decision reached by HHJ Korner for the purposes of the exercise of course has no legal status in any real proceedings brought in any jurisdiction in respect of the conflict in Yemen or otherwise.
## B. DRAMATIS PERSONAE

<table>
<thead>
<tr>
<th>Real persons</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Legal Action Network (&quot;GLAN&quot;)</strong></td>
<td>A non-profit organisation that pursues innovative legal actions across borders.</td>
</tr>
<tr>
<td><strong>Bellingcat</strong></td>
<td>An independent international non-profit collective of researchers, investigators and citizen journalists that specialises in online investigations, specifically fact-checking and analysing open-source information including audio-visual content. Bellingcat worked with GLAN to investigate the incident and located the Exhibit CG/2 video which was the subject of the mock hearing. For the purposes of the exercise, it was fictional assumed that GLAN and Bellingcat had sent a referral to the war crimes team of the Metropolitan Police Counter Terrorism Command (SO15) notifying SO15 of the details of the 7 May 2018 airstrike and the fact that the defendant was to pass through Heathrow airport imminently.</td>
</tr>
<tr>
<td><strong>Charlotte Godart</strong></td>
<td>Bellingcat investigator, project manager and trainer who conducted the search that located the Exhibit CG/2 video footage on Twitter. Manager and lead investigator of Bellingcat’s Yemen project. Her statement is fictional for the purposes of the exercise but the content of it is true and accurate as it relates to Bellingcat’s expertise and approach to locating and analysing the Exhibit CG/2 video evidence.</td>
</tr>
<tr>
<td><strong>Eliot Higgins</strong></td>
<td>Founder of Bellingcat. His witness statement is fictional for the purposes of the exercise but the content of it is true and accurate as it relates to Bellingcat’s expertise and approach to locating and analysing the Exhibit CG/2 video evidence.</td>
</tr>
<tr>
<td><strong>Judge</strong></td>
<td>Her Honour Judge Joanna Korner CMG QC.</td>
</tr>
<tr>
<td><strong>Prosecution (the Crown Prosecution Service)</strong></td>
<td>Helen Malcolm QC of Three Raymond Buildings and Joshua Kern of 9 Bedford Row.</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Defence</strong></td>
<td>Andrew Cayley QC of Temple Garden Chambers and Shina Animashaun of Garden Court Chambers.</td>
</tr>
<tr>
<td><strong>Fictional persons</strong></td>
<td><strong>Frank Palmer</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Dr Althaibani</strong></td>
</tr>
<tr>
<td><strong>Defendant</strong></td>
<td>‘Saud Al Kahtani’, a fictional pilot with the Royal Saudi Air Force who was piloting fighter jets in Yemen for the Coalition in 2018. He did not appear in the proceedings.</td>
</tr>
</tbody>
</table>
C. DEFINITIONS

5. There are a number of terms which are often used interchangeably in this sphere. This report adopts the following definitions:

• **Open source information (OSI)** encompasses publicly available information that any member of the public can observe, purchase or request without requiring special legal status or authorized access.\(^3\) OSI is thus a very broad term which would incorporate anything from print media to NGO reports to online videos.

• **Open source intelligence (OSINT)** differs from the broader category of OSI in that it refers specifically to intelligence, which is “actionable information with context and value that is provided to government and military officials, usually to assist with immediate policy or strategic decisions.”\(^4\) This term is often used to refer to open source investigations carried out by journalists and human rights researchers, which does not strictly accord with the correct definition of the term and can give the impression of associations with state intelligence services. This report therefore does not use the term OSINT.

• **Online open source investigation (OOSI)** describes the work of Bellingcat and other online investigators. For the sake of accuracy, Bellingcat prefers to use the term OOSI to describe its work, rather than OSINT. OOSI is different exercise to a review (however comprehensive) of traditional materials online, for example written media and NGO reports, but because they both focus on the broad category of content covered by the term OSI, the two activities can be unhelpfully conflated, leading to deprecation of OOSI. To clarify the distinction of OOSI from traditional media review, we suggest loosely dividing open source material (i.e. OSI) into descriptive content and examinable content, with the latter being the substantive material that, due to its granular and/or examinable nature, is capable of being analysed by investigators to draw new conclusions or check existing ones.\(^5\) In other words, examinable content is material whose value is established by an analysis of the substantive content itself, which is to be contrasted with descriptive or ‘narrative’ content, whose contribution is much more contingent on the trust placed in the author or organization that published it.\(^6\) Descriptive content could range from a short news article to a lengthy NGO report containing witness interviews, while examinable content could be anything from a Tweet to an entry on Wikimapia to an aftermath video – there is no presumptive hierarchy between the categories.

---

\(^3\) *Id.*, para. 14.

\(^4\) Lindsay Freeman, in *Digital Witness, Prosecuting Atrocity Crimes with Open Source Evidence*, at Part 1, Chapter 3, p. 48.

\(^5\) See also Daragh Murray, Yvonne McDermott and Alexa Koenig, *Journal of Human Rights Practice, Mapping the Use of Open Source Research in UN Human Rights Investigations*, 2022, at 1-28; in which types of OSI are distinguished based on two key variables: whether the item is a primary or secondary account, and whether the item is a unique piece of data or a report based on an aggregation of data.

\(^6\) According to the methodology, examinable content includes: OA VC, Maritime trackers, aviation trackers, weather logs, and other forms of OSI tools and sources; Social media posts without audiovisual content which can be used to assist with OSI exercises such as chronolocation or initial geolocation enquiries, or those which can be analysed in bulk for text patterns; Sites which record user entries like Google Maps and Wikimapia.
Online audio-visual content (OAVC) – digital content, found online, which contains recordings of sounds and/or photographic images (whether stills or video). This definition is used to differentiate OAVC from other categories of information which would fall within OSI, but which do not have the same evidentiary characteristics – for example Wikimapia entries, text-only tweets or weather logs.

User generated content (UGC): UGC is a sub-set of OAVC in that it tends to refer to content generated or gathered by private individuals in a lay (non-professional) capacity. In contrast, OAVC can include video released by the media (in particular local media) and NGOs.

Digital evidence is “information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.”

D. FICTIONAL UNDERLYING CASE

6. In the fictional scenario devised for the purposes of the mock exercise, the prosecution case was that at approximately 10:30 a.m. on 7 May 2018 the defendant flew his fighter jet above Tahrir Street in Sana’a, Yemen and, in a ‘second wave’ strike, launched two air-delivered bombs at the Office of the Presidency, which is located in a densely populated civilian area. The prosecution alleged that multiple civilians were present in the area, that at least six civilians were killed and that dozens were wounded. GLAN received a tip-off that credibly suggested that the defendant was the pilot responsible for the airstrike.

7. Bellingcat investigated the 7 May 2018 incident using the methodology designed by GLAN and Bellingcat. According to the fictional narrative, on 15 June 2020 GLAN and Bellingcat sent a referral to the war crimes team of the Metropolitan Police Counter Terrorism Command (SO15) notifying SO15 of the details of the 7 May 2018 airstrike and the fact that the defendant was to pass through Heathrow airport imminently. The defendant was detained at Heathrow airport that day and interviewed with a solicitor present. He initially denied any involvement in the airstrike in question, but when presented with specifics contained in the GLAN/Bellingcat referral he admitted to carrying out the mission. However, he contended that the airstrikes landed at 7am when no civilians were present and that in any event this was not a civilian location. He claimed that two high-level Houthi leaders were present in the Office of the Presidency, that no damage was done to any surrounding property and that no civilians were harmed.

8. In the fictional proceedings, the defendant was charged with two counts of war crimes under section 51 of the International Criminal Court Act 2001 (“ICCA”); specifically, murder and directing an attack against civilians. The case had come before HHJ Korner in the Central Criminal Court and the judge had ruled that the courts of England and Wales had jurisdiction on the basis of the defendant’s UK residency.8


8. Under the ICCA, only UK nationals and residents can be prosecuted. The defendant’s residency was therefore invented to meet with this requirement.
9. The defence had made an application to exclude the Exhibit CG/2 video evidence located by Bellingcat.

E. EVIDENCE

10. The evidence put forward by the prosecution, as set out below, comprised evidence specifically drafted by GLAN and Bellingcat for the purposes of the exercise and provided to the counsel teams, and other information or documentation not provided but the existence of which was presumed and agreed for the purposes of the exercise.

i. Digital evidence
   a. A video, Exhibit CG/2, submitted by the prosecution to depict the 7 May 2018 airstrike.
   b. A video showing that the Coalition has access to high resolution drone footage, to support the prosecution’s claim that the defendant would have been able to see the civilians in the street prior to the launching of the airstrike.

ii. Evidence drafted and presented to the parties/HHJ Korner
   c. Witness statement of Bellingcat investigator Charlotte Godart.

iii. Evidence not developed or reviewed, but agreed for the purposes of the exercise
   a. Witness statement of Dr. Althaibani who was present at Thawra Hospital, Sana’a, on the day of the incident, where he treated 13 casualties, three of whom died from their injuries: one of the deceased was a girl aged nine, seven patients were young males wearing civilian clothing, and five were women. Dr. Althaibani was told by the ambulance crew and a number of the patients that they had come from Tahrir, near the Office of the Presidency.
   b. An admission in police custody by the defendant that he carried out the strike, but alleging that it targeted a military objective and no civilians were harmed.

There is no jurisdiction under the Geneva Conventions Act 1957 due to the classification of the Yemen war as a non-international armed conflict.
F. MOCK HEARING OVERVIEW

11. The mock hearing, which took place by way of live webinar on 19 February 2021, was a voir dire hearing before HHJ Korner, in the absence of a jury, for the purpose of determining the admissibility of the Exhibit CG/2 video. HHJ Korner heard argument from the prosecution as to why it should be admitted in evidence in the proceedings and from the defence as to why it should be excluded. As noted above, the fictional nature of the hearing meant that it was subject to some constraints, such as the allocated time and number of witnesses called. However, it was conducted in as realistic a manner as possible to illustrate the kinds of issues that may arise in real proceedings.

12. The mock hearing centred around the Exhibit CG/2 video, located by Bellingcat on Twitter during its investigation and put forward by the prosecution on the basis that it captures the airstrike. The video is 2 minutes and 20 seconds in length and depicts the aftermath of a large explosion in which considerable destruction is observed on a street that the prosecution submits is Tahrir Street, Sana’a, Yemen. In the video, a woman dressed in traditional Yemeni black robe can be seen along with some men, one of whom is wearing a blue office suit, attempting to retrieve what appears to be a young man or boy from underneath the rubble. The video shows extensive damage and a number of apparent casualties on the street. At approximately 22 seconds, a large explosion is heard, preceded by a loud whirring, at which point the camera is obscured by smoke and debris for approximately 1 minute. Further screaming and car alarms are heard and the camera begins to pick up the aftermath of the second explosion. At around 1 minute 10 seconds the video cuts to footage that appears to have been taken before the second strike. By the time the second airstrike detonates, smoke and debris from the earlier explosion have apparently cleared, leaving the sky clear.

13. During the hearing, the prosecution and defence each put forward opening statements setting out their position in respect of the admissibility of the video. The prosecution called Eliot Higgins, the Chairman and Executive Director of Bellingcat, and Frank Palmer, the fictional expert witness, to give evidence. Both were cross-examined by the defence and then re-examined by the prosecution. Finally, the prosecution and defence each made a closing statement. As is often the case in real proceedings, the judge did not make a ruling immediately. HHJ Korner instead reserved her judgment, meaning that she went away to consider the evidence that had been presented to her and the arguments made by both sides. She would then reach a decision on whether or not to allow the evidence into the fictional main proceedings before a jury.

14. On 16 March 2021, HHJ Korner handed down her reasoned judgment orally in a second live webinar. Given the fictitious nature of the exercise, the decision of course would have no legal effect in any real proceedings brought in any jurisdiction in respect of the conflict in Yemen or otherwise. However, it was helpful to understand the way in which an English court may approach the issue as and when OSI is put before it.

---

15. The parties agreed that the Coalition carried out an airstrike at the Office of the Presidency on 7 May 2018. In relation to the Exhibit CG/2 video footage, it was not in dispute that: it is made up of two separate segments; it is not the original and it is not known which version of the video it is; the maker of the video is unknown, as is the identity of the individual who uploaded it to Twitter albeit his Twitter account and activity is public; the uploading of the video to Twitter stripped it of its original metadata.

i. Prosecution

16. The prosecution argued that the video is credible, reliable and admissible as real evidence, subject to proof of provenance/retrieval and authenticity. The video was relevant because it captured the two airstrikes in issue in the proceedings and went to the death of, and injury to, civilians, which was at the heart of the dispute between the prosecution and defence.

17. When interviewed by police, the defendant eventually admitted to carrying out the mission, but claimed that it took place at 7am when no civilians were present and that in any event this was not a civilian location. He further claimed that there was no damage to surrounding buildings, that there was no harm to civilians, and that the video was a fake piece of sophisticated propaganda. The issues in dispute between the parties were therefore the time of the attacks, whether there was damage caused to the surrounding area and if so the extent, the presence of civilians, and the defendant’s knowledge of their presence prior to the second strike.

18. If credible and accurate, the Exhibit CG/2 video provided valuable evidence answering each of the positions adopted by the defendant in interview: it shows the time of day at which the strike took place (through chronolocation based on the light and shadows evident in the video), the presence of civilians, widespread damage caused by the first strike, injuries to civilians prior to the second strike, the fact that the pilot’s view of the scene and civilians present would have been clear prior to the second strike, and, finally, it depicts the second strike itself. According to the prosecution, it therefore passed the first test of admissibility in that it provided what was clearly relevant evidence.

19. The prosecution further argued that the Exhibit CG/2 video was admissible because it was not excluded by any rule of law: it is real evidence at common law (therefore falling outside of the rules on hearsay) and admissible subject to the court being satisfied that it is credible and reliable. The prosecution argued that courts are fully experienced in testing reliability, assessing corroboration and giving suitable warnings to jurors; the courts should not set their face against a form of evidence simply because it is new.

---

11. The prosecution referred to a further video submitted in evidence, which had been created and released by the Coalition to show its targeting precision in eliminating specific targets (including people) and which demonstrates the high-resolution sensor technology available to its pilots. The prosecution contended that this video supported its position that, at the time of the second strike on 7 May 2018, the defendant would have been able to see the widespread damage caused by the first strike and would have been able to see that there were civilians on the ground helping those injured in the first strike. For more discussion of this issue, see Part II.
20. The prosecution argued that proof of provenance/retrieval was one aspect of the testing exercise to be undertaken by the Court. The video had been subjected to rigorous analysis in accordance with the Berkeley Protocol on Digital Open Source Investigations by the prosecution expert, Mr. Palmer, who found no reason to doubt its authenticity. He analysed the video using: triangulation of other data confirming an attack on that date and the damage caused; chronolocation to confirm the time of the attack; and geolocation to confirm the place of the attack. He established the place and time it was taken, considered internal consistency, and saw no evidence of manipulation based on what could be seen in the video. The timing of the posting of the video online, mere hours after the attack, further indicated that there was insufficient time for a fake of this sophistication to be produced.

21. The prosecution further noted that the trained Bellingcat investigator, Ms. Godart, likewise considered the video to be genuine and authentic. In addition, the video was corroborated by other pieces of evidence, both as to the event recorded and as to the time and date it was captured, and the expert evidence confirmed that the video had not been repurposed, digitally altered, nor did it contain material omissions. The prosecution contended that the Exhibit CG/2 video therefore satisfied the second test of admissibility in that it was reliable.

22. Finally, the prosecution argued that, pursuant to Section 78 of the Police and Criminal Evidence Act 1984 cited above, it would be fair and appropriate in all the circumstances to admit the video into evidence: given the depth, rigour, and objectivity of the analysis of the experts, there would be no unfairness in putting it before the jury – if necessary with appropriate warnings.

23. In summary, the prosecution response to the defence’s application to exclude Exhibit CG/2 was that:

   i. the video was admissible as real evidence subject to proof of provenance/retrieval;
   ii. the utterances heard on the video were admissible by virtue of Section 118 (4) of the Criminal Justice Act ("CJA") 2003 as res gestae or alternatively under Section 114 (i) (d) as hearsay admissible “in the interests of justice”;
   iii. the examination by Mr Palmer found no reason to doubt its authenticity;
   iv. the events shown in the Exhibit CG/2 video were corroborated by other shorter clips which were uploaded to Twitter, as well as the evidence of the doctor who treated civilian casualties; and
   v. Mr Palmer had the required experience and expertise to conduct such an analysis.

**ii. Defence**

24. The defence submitted that the admission of publicly available digital evidence of questionable origin and authenticity is a new phenomenon in both national and international courts and one which the Court should approach with extreme caution. The defence further submitted that the Court should approach with equal caution well-meaning novel ‘experts’ seeking to authenticate and reassure courts of the reliability of such types of video evidence. The defence argued that both the Exhibit CG/2 video and the expert report of Mr. Palmer should be excluded from evidence.
25. The defence pointed to the law applied by the International Criminal Court on the admissibility of evidence, which requires an assessment of whether the evidence is relevant, whether it has probative value and whether it prejudices the proceedings - the probative value limb requiring an examination of the authenticity, credibility and reliability of the evidence. The defence argued that the Exhibit CG/2 video should be excluded from evidence because it is neither authentic nor reliable given that:

   (i) it is not the original video nor is it known which iteration thereof it purports to be;

   (ii) the identity of the creator is unknown and the person who uploaded it is known from the material he has previously posted to be biased against the Coalition;

   (iii) it has been edited and/or manipulated and the original metadata is not available; and

   (iv) its discovery on the internet was subject to the unavoidable bias of the algorithms of the search engine, such that there could be exculpatory evidence that has been omitted or missed.

26. The defence argued that as the video evidence in question is not authentic or reliable, the conclusions reached by Mr. Palmer in his expert report were based on inherently unreliable real evidence. The defence also submitted that the report and evidence given by Mr. Palmer did not comply with the requirements of Rule 19 of the UK Criminal Procedure Rules ('CPR') and should be excluded in any event on the basis that:

   (i) his opinion and conclusions were based on the data from the video which is fatally flawed because the video is not authentic;

   (ii) he did not confine himself to his area of expertise and therefore commented outside his expertise;

   (iii) he drew conclusions, some of which are for the jury; and

   (iv) he was not independent or objective.

12. We also note that the ICC’s Chambers, when introducing social media videos into evidence, has required that the social media company provide the full packet directly to the Court if it is still available on the relevant site. In this mock hearing, although the original video was still available on Twitter, the Defence did not specifically request this, and no order to this effect was made by the Judge. In general, little was made in this mock exercise of the need to demonstrate integrity, completeness and chain of custody between the extraction of the item from the internet to its presentation as evidence. In reality of course, this is a significant matter which would be given due consideration in a real prosecution.
27. The defence case was that the evidence should be excluded under the provisions of Section 78 of the Police and Criminal Evidence Act (‘PACE’) 1984 which provides that “In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it”.

H. EVIDENCE PROVIDED BY THE FACTUAL AND EXPERT WITNESSES

28. The prosecution relied on the evidence of Charlotte Godart, Eliot Higgins, and the expert report of Frank Palmer. Ms. Godart was not called to give oral evidence at the hearing and her witness statement stood as her evidence. Mr. Higgins and Mr. Palmer both gave oral evidence at the hearing, including cross-examination by the defence.

29. In her witness statement, Ms. Godart detailed the steps of her investigation into the incident, following the GLAN/Bellingcat methodology, and how she located Exhibit CG/2. In his evidence, Mr. Higgins provided further detail about the methods Bellingcat uses to analyse the significance, reliability or authenticity of open source evidence, in respect of both discovery of material and verification of its content, primarily: geolocation and chronolocation. In his expert report, Mr. Palmer set out in detail the step-by-step process he undertook to verify the Exhibit CG/2 video using these two techniques as well as further cross-referencing for corroboration. His evidence also addressed issues of algorithmic bias and the unknown provenance of the video.

30. Full details of the evidence provided by both witnesses of fact and the expert witness, which may help to inform a full understanding of the judgment reached by HHJ Korner and the analysis we discuss in Part II, are set out in Annex I.

I. THE RULING

31. The legal authorities on which both sides relied included national case law and decisions of the International Criminal Court (‘ICC’). The judge noted that whilst the ICC decisions were of assistance, they are not binding upon the English courts.

i. Open Source Analysis as Expert Evidence

32. HHJ Korner acknowledged that analysis of the significance, reliability and/or authenticity of open source video evidence is a relatively new field, composed of the application of technical knowledge (such as understanding of metadata and digital alteration, along with techniques
such as geolocation and chronolocation) as well as training and experience in the examination of such material (such as the use of search engines).

33. The relevant procedural rules state that “[e]xpert opinion evidence is admissible in criminal proceedings at common law if, in summary, (i) it is relevant to a matter in issue in the proceedings; (ii) it is needed to provide the court with information likely to be outside the court’s own knowledge and experience; and (iii) the witness is competent to give that opinion.”\textsuperscript{13} The expert must provide an opinion which is objective and unbiased and within his/her area of expertise.\textsuperscript{14} In determining the reliability of expert opinion, the Court may take into consideration factors including:

- the nature of the data on which the expert’s opinion is based;
- the safety or otherwise of inferences drawn;
- the nature of methods used;
- the extent to which any material upon which the expert’s opinion is based has been peer-reviewed;
- the extent to which the expert’s opinion is based on material falling outside the expert’s own field of expertise; and
- whether the expert’s methods followed established practice in the field.\textsuperscript{15}

34. HHJ Korner considered the domestic and international legal authorities relied on by both parties. She briefly addressed the position at the International Criminal Court, where earlier case law suggested that authenticity must be shown at the stage evidence is submitted: in ruling on the relevance or admissibility of evidence, the Court may take into account its probative value and any prejudice it may cause to a fair trial; if evidence is determined to be relevant, its probative value is then evaluated on the basis of reliability and significance, and if the prejudice is disproportionate to the probative value then the evidence must be excluded.\textsuperscript{16} Pursuant to that line of authority, it is for the party tendering the evidence to provide evidence establishing reasonable grounds to believe that an item is authentic which, for video recordings, requires evidence of originality and integrity. Evidence should be provided as to the date and/or location of the recording in order to demonstrate relevance.\textsuperscript{17} HHJ Korner acknowledged that in a 2018 case, when assessing authenticity of a video, the ICC noted in particular an expert report submitted by the prosecution which analysed a video and concluded that there were no traces of forgery or manipulation.

35. We note that more recently the ICC has moved away from this approach toward one where it allows all evidence to be submitted throughout the proceedings and subsequently considers questions of admissibility and weight at the end of the process when reaching its judgment.\textsuperscript{18}

\textsuperscript{13} Criminal Practice Directions 2015, at paragraph 19A.1.
\textsuperscript{14} Criminal Procedure Rules 2020, at Part 19.
\textsuperscript{15} Criminal Practice Directions 2015, Paragraph 19A.5.
\textsuperscript{16} Rome Statute of the International Criminal Court, at Article 69(4) and ICC, Katanga and Cluni (ICC-01/04-01/07), Decision dated 17 December 2010, at paragraph 15 and generally.
\textsuperscript{17} ICC, Katanga and Cluni (ICC-01/04-01/07), Decision on the Prosecutor’s Bar Table Motions, 17 December 2010, at paragraph 24(d).
\textsuperscript{18} See for example, Gbagbo and Goude (ICC-02/11-01/15), Bemba II (ICC-01/05-01/08), al Hassan (ICC-01/12-01/18).
36. Turning to English law on the issue, HHJ Korner cited *R v Robb* [1991] 93 Cr App R 161 in which Bingham LJ confirmed that expert evidence is not limited to the old-established sciences and professions but instead the essential questions are whether study and experience will give a witness’ opinion an authority which the opinion of one not so qualified will lack.\(^\text{19}\) The expert must nonetheless be confined to matters within his/her areas of expertise. HHJ Korner noted the case law cited by the defence in which the Court stated that there must be a sufficiently reliable scientific basis for an evaluative opinion to be admitted. She concluded that the closest analogy in English case law to the present case is that of evidence from police officers of drug prices or gang membership, which the Court has accepted can constitute a field of expert evidence provided the officer has made a “sufficient study, whether by formal training or through practical experience, to assemble what can properly be regarded as a balanced body of specialised knowledge which would not be available to the tribunal of fact.”\(^\text{20}\) HHJ Korner concluded that the two principles of universal application from the UK case law which were of importance to her decision were that employment by an organisation which could be said to have an interest in the outcome of a case is not an automatic bar to providing expert evidence and that expertise may be derived through practical experience.

37. HHJ Korner thus accepted that the field of analysis of video material to establish its significance, reliability or authenticity constitutes a field of expert evidence composed of a number of factors including: the application of technical knowledge such as the operation of metadata and methods of digital alteration; techniques such as geolocation and chronolocation; and training and expertise to use search engines and examine material for evidence supporting or undermining the content of videos, the methodology for which is set out in the Berkeley Protocol. HHJ Korner found that whilst Mr. Palmer does not have technical knowledge of metadata or digital alteration, his other qualifications and his experience make him an expert in the analysis of digital open source information. She ruled that his expert evidence was admissible, on the basis that he is a person who is able to “assemble what can properly be regarded as a balanced body of specialised knowledge which would not be available to the tribunal of fact.”\(^\text{21}\) and he was giving an opinion which is objective and unbiased, and within his area of expertise (noting, in the words of Lord Bingham, that he is not “a quack, a charlatan or an enthusiastic amateur”).\(^\text{22}\) She concluded that, with the exception of peer review, Mr. Palmer fulfils the criteria set out in Part 19 of the Criminal Practice Directions.\(^\text{23}\)

### ii. Admissibility of the Exhibit CG/2 Video

38. HHJ Korner began by noting that that the UK courts have taken the view that the rules which required the exclusion of evidence not strictly proved have had to be amended to take account of modern forms of the creation, storage and communication of evidence, and that it is in the interests of justice that such amendment should take place. However, she also noted that the interests of justice equally require that care is taken before admitting into evidence material adduced for the purpose of convicting a defendant of a crime, particularly where it is obtained from internet searches.

---

\(^\text{19}\) *R v Robb* [1991] 93 Cr App R 161, at paragraph 164.
\(^\text{20}\) *Myers & others v. The Queen* [2016] AC 314, at paragraph 58.
\(^\text{21}\) Id.
\(^\text{22}\) *R v Robb*, *supra* note 19, at paragraph 166.
\(^\text{23}\) Criminal Practice Directions, at paragraph 19A.5.
39. HHJ Korner noted that the factors most pertinent to the admission of such evidence in a
criminal trial are whether the material sought to be adduced is, relevant, authentic and reliable.
She considered the domestic and international authorities relied on by each of the parties.

40. The prosecution submitted that the video constitutes real evidence on the basis that it is “the
evidence afforded by the production of physical objects for inspection or other examination by the
court”, by analogy with a case relating to a mechanically produced film of the echoes made by
colliding ships. HHJ Korner also referred to two further cases which addressed the admission
into evidence of anonymous pieces of evidence. In the first case, relating to video footage, the
Court had held that once the video was found to be relevant and prima facie authentic, it was admissible and any attack thereafter could go only to weight. The Court commented
that weight could be addressed through further enquiries as to the video’s authenticity,
provenance, history, whether it was original and how it came to be copied; authenticity could
be proved, “like most facts” circumstantially including for example by comparing it with films
taken by others of the same event. In the second case, the Court held that documents of
unknown authorship located online were admissible on the basis that they were not relied on
for the truth of their contents but to show that another document (of known provenance)
was derived from a particular source. The Court noted that if any evidence had been put
forward as to the provenance of the open source material, it may only have tempered the
direction given to the jury rather than affected its admissibility.

41. In relation to each of the key elements of the admissibility test, HHK Korner ruled as follows:

a. Relevance: the Exhibit GC/2 video is clearly relevant.

b. Authenticity: the Exhibit GC/2 video suffers from the drawbacks that the creator is
unknown, it is not the original, nor does it have any of the electronic data attached, which
allows for technical checks to be carried out on the time date and location of the content.

c. Reliability: there is the possibility that whoever uploaded the video has edited it to remove
aspects which do not suit his purpose e.g. the presence of military personnel at the scene.

42. However, the Judge ruled that authenticity and reliability of the video were established by
other evidence, namely:

a. the findings of Mr Palmer;

b. other postings on Twitter corroborating that an attack took place on that date time
and place;

c. the evidence of the doctor of the casualties treated;

25. In R. v. Murphy [1990] NI 306, the Northern Irish Court of Appeal dealt with the admissibility of film clips, which were not the original footage, shot
by a cameraman who was not called as a witness. In that case, the defence objected to admission into evidence of the film clips on grounds not dissimilar
to those advanced by the defence in this mock hearing, namely that the footage was only admissible if the cameraman was called or it was an authentic
copy of the original. In R. v. Amjad [2016] EWCA Crim 1618 the Court of Appeal Criminal Division considered the admission into evidence of
documents of unknown authorship obtained from the internet by police officers doing a Google search, in particular one document from Wikipedia.
26. R. v. Murphy, supra note 25, at paragraph 61.
27. Id., at paragraph 61.
d. the evidence of the time at which the video was uploaded to Twitter which did not allow for the kind of sophisticated alteration which would be needed for manipulation of the contents to take place;
e. the content of the video itself i.e. the damage to the area; and
f. the acceptance by the defendant that he took part in an attack that day.

43. HHJ Korner was satisfied that the Exhibit CG/2 video fulfilled the relevant criteria and should be admitted into evidence in the proceedings. The Judge noted that the jury would be given appropriate directions and warnings in respect of the drawbacks of the video that had been identified during the voir dire hearing.

44. In relation to the utterances in the Exhibit CG/2 video, HHJ Korner exercised her discretion to exclude them from evidence on the ground that their admission would be unfair as any probative value they may have was outweighed by their prejudicial effect (and given that Mr Higgins, in his witness statement, had indicated that the prosecution would not intend to rely on those utterances). 29

---

29 The prosecution had relied on Section 118 (4)(a) of the Criminal Justice Act 2003 (headed “rex gestae”) which reads as follows: “Any rule of law under which in criminal proceedings a statement is admissible as evidence of any matter stated if—(a) the statement was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion can be disregarded”. In the alternative they relied on Section 114 (1)(d) which states “In criminal proceedings a statement not made in oral evidence in the proceedings is admissible as evidence of any matter stated if, but only if—the court is satisfied that it is in the interests of justice for it to be admissible. Section 114 (2) then sets out the factors which need to be taken into account when considering admission. For a discussion of hearsay, see Part II.
PART II: ANALYSIS
45. This section analyses the mock hearing exercise for lessons learned that can inform and assist investigators, experts and legal practitioners who use online audio-visual content (“OAVC”)\textsuperscript{30} as evidence in future. In summary, the exercise provided key insights into the following areas, discussed in detail below:

i) The categorisation of OAVC as evidence and the concept of authenticity (and reliability);
ii) The importance of tailoring claims made on the basis of items of OAVC;
iii) OSI analysis as expert evidence; and
iv) The investigative process followed by Bellingcat.

A. INTRODUCTORY REMARKS: THE CONTEXT AND THE PREPARATION OF THE EVIDENCE

46. In legal proceedings where facts are in dispute, the preparation and presentation of evidence plays a decisive role. While this may be an obvious statement, it bears emphasising because there is no area in which it is more important to ensure clear and tailored presentation than in the introduction of OSI as evidence. In particular in jurisdictions where court time is at a premium, it could be easy for novel forms of evidence to be misconstrued or misunderstood due to inadequate allocation of time for comprehensive analysis of its nature and significance. Whether to the detriment of the prosecution or defence, any such misunderstanding is contrary to the interests of justice.\textsuperscript{31} The risk is particularly great in this context because OSI traverses evidentiary categories; raises disparate and complex issues such as chain of custody, digital forensics, expert evidence and hearsay; and can involve third party organisations as sources (such as Bellingcat). Owing to these factors and the inherent impossibility of demonstrating its provenance, in practice OAVC ultimately seems to carry with it a de facto presumption of being unreliable which must be rebutted by the prosecution.

47. The purpose of the mock hearing was to take these real-life factors into account in testing a piece of OAVC and to make that test as realistic as possible so as to obtain an accurate picture of the kinds of issues that could go wrong as well as right. It was anticipated that the exercise would reveal challenges that could not be easily foreseen through desktop analysis of the relevant legal and evidentiary principles alone. As such, perfection was not the objective; and indeed some matters in the fictitious case scenario were consciously left imperfect for the purpose of observing how they would be dealt with in a ‘real-life’ setting. Whilst GLAN and Bellingcat were pleased with the judge’s ruling that the relevant legal principles resulted in the admission of OAVC into evidence for the purpose of the mock hearing, the main purpose of the exercise was to learn from how the event played out.

\textsuperscript{30} As per the definitions in Part I, OAVC is the preferred term to refer to any audiovisual content found online, because it is a broader category than User Generated Content, but narrower than Online Open Source Information.

\textsuperscript{31} Criminal Procedure Rule 1.1. The overriding objective of the Criminal Procedure Code is that criminal cases be dealt with justly, including by acquitting the innocent and convicting the guilty.
B. THE CATEGORISATION OF OAVC EVIDENCE AND THE CONCEPT OF AUTHENTICITY

48. The first thing to say is that OAVC is not in an evidentiary category of its own – after all, it is digital video evidence, which is already very commonly introduced in criminal proceedings (for example in the form of CCTV or police video). The qualities setting it apart are that its creator is not present in court and therefore that it is presumptively unreliable, but the same principles apply to OAVC as apply to all video evidence.

49. OAVC is documentary evidence, and as such, like all documentary evidence, must be authenticated before it can be admitted into evidence. A document is anything in which information of any description is recorded. Authentication is “the process of convincing a court that a “thing” (which may be a document) matches the claims made about it.” In this case, the claim being made by the prosecution was that the video was comprised of genuine clips of footage filmed on Tahrir Street on 7 May 2018 which captured the moments between the two airstrikes and the second airstrike itself. If there was insufficient evidence of authenticity, it would plainly be unfair to admit this video as evidence against the defendant. The requirements for authentication can differ depending on the context, and it is not always as straightforward as showing that an item is the original or has not been changed at all. As shown by this exercise, the video had been edited since its creation but was nonetheless deemed to have met the relevant threshold for authenticity (see paragraph 42 above which lists the reasons given by the judge for her finding in this regard).

50. Authentication of images is commonly achieved through witness testimony from the item’s creator, but the courts have already recognised that anonymous videos can be authenticated “circumstantially,” without the creator being present in court to provide evidence of provenance. For example, in R v. Quinn [2011] NICA 19, an anonymous Youtube video depicting a defendant engaged in criminal acts was admitted without evidence from the creator because the defendant’s failure to deny in interview that he was the person in the video gave rise to an inference that the video was authentic. Despite this precedent, there has been no test of whether a video – in particular one depicting conflict events in a distant country - could be authenticated using open-source analysis techniques. Such videos are markedly

---

32. This is also the case at the international level. See Lindsay Freeman, Digital Evidence and War Crimes Prosecutions, supra note 7, at p.297.
33. For a discussion as to the threshold for admission into evidence, see below and, in this specific context, see O’Flahlin, M. and Ormerod, D., Criminal Law Review, Social networking material as criminal evidence, July 2012, at pp. 486-512.
34. Civil Procedure Rule 31.4. Documents can also be introduced as physical (real) evidence, for example if being introduced to show their physical condition. As noted below, OAVC is documentary evidence containing real evidence, which is not the same as a document being introduced as real evidence in the sense just described.
35. ASIC v Rich [2005] NSWSC 417 at paragraph 118. It can be important to differentiate between claims being made by the party introducing the item in court and, for example, the person on social media who tweeted the video. This definition refers to the former.
36. Some conceptions of authenticity can refer to an item being unchanged since its creation, and others still refer to the need to show an item’s continuity between seizure and presentation in court. Both of these conceptions relate to chain of custody, which is a distinct topic. Possession of the original, unedited footage can be an influential factor in determining authenticity, but it is by no means the whole test. For example, a video could be an original, unedited piece of footage but could be put forward as evidence of the wrong incident (repurposed) or could even have been entirely staged, rendering it wholly unreliable even though the digital item is in its original and unedited form. Thus, key to establishing authenticity is the relationship between the thing and the claims being made about.
38. Id.
different to the example in *Quinn*, because of the Court’s unfamiliarity with the context and the location; the heightened potential for the role of disinformation which increases the plausibility of falsification; the nature of the events being depicted (explosions and their aftermath); the absence of any witness who was present at the scene and could be located to give evidence to the Court; and, most importantly, the nature of the expert evidence required to authenticate them.

51. For the purposes of admissibility, the judge only needed to be satisfied that the video was *prima facie* authentic – that is, that the prosecution had produced enough evidence to create a presumption that it was authentic. If so, the video would be put before the jury, who would then be the ultimate arbiters of whether the video was authentic and what weight should be attributed to it as evidence of the defendant’s guilt.\(^39\)

52. The admissibility threshold and the fact that the creator remains unavailable for the purposes of the proceedings, given that they cannot be brought to Court to authenticate the video itself, were addressed as follows by HHJ Korner in her ruling:

> “The admission into evidence of anonymous pieces of film has been considered in other cases which have come before the UK courts. In *R. v. Murphy* [1990] NI 306, the Northern Irish Court of Appeal dealt with the admissibility of film clips, which were not the original footage, shot by a cameraman who was not called as a witness. It had been included in a BBC news report and evidence was called to verify that transmission. The objections to admission of this evidence by the defence were in terms not dissimilar to those advanced by the defence in this case i.e. that it was only admissible if the cameraman was called or it was an authentic copy of the original. The Court upheld the trial judge’s decision to admit the film stating that once the clips were found to be relevant and *prima facie* authentic, they were admissible. At p.61 Kelly LJ stated “[a]ny attack thereafter could only go to weight. The issue of weight could embrace many things – further enquires into its authenticity its provenance and history and whether it was original and if not how it came to be copied. Authenticity, in our view, like most facts may be proved circumstantially...[T]he film may be proved authentic by comparing it with films taken by others of the same event, taken at the same time or even a different time.””

53. As was seen throughout the remainder of the ruling, HHJ Korner was content to apply this framework to the Exhibit CG/2 video, subject to the quality of the evidence adduced as to the video’s authenticity.

54. Another issue worthy of discussion is how OAVC is characterised as a form of evidence beyond placing it in the general category of documentary evidence. The prosecution in these mock proceedings argued that the video was admissible as real evidence. Phipson on Evidence contains a number of definitions of real evidence, one of which is “evidence from things as distinct from persons”.\(^40\) In particular, it notes that real evidence, “when available, is probably the most satisfactory kind of all, since, save for identification or explanation, neither testimony nor inference is relied upon. *Unless its genuineness is in dispute, the thing speaks for itself.*”\(^41\)

---

39. As was evident from HHJ Korner’s ruling, the witnesses (including the expert) would have to give evidence again before the jury at trial.  
41. Id.
The crux of the prosecution’s argument was thus that the material can be directly analysed as a primary source or “thing” (once verified), rather than being treated as any kind of statement made by a person. If the latter was the case, it would be harder to justify admitting the video given its creator is not available to testify, because it would be hearsay if introduced as evidence of the truth of its contents. This was reflected in the prosecution’s argument, as summarised by HHJ Korner in her ruling (emphasis added):

“In support of the prosecution submission that the video is real evidence I was referred to the authority of Sapporo Maru v. Statue of Liberty [1968] 1 WLR 739 in which a mechanically produced film of the echoes made by 2 ships which collided on the River Thames was objected to by the defendants. Sir Jocelyn Simon ruled that in his view “the evidence is admissible and could indeed be a valuable piece of evidence in the elucidation of the facts in dispute” adding “in my view the evidence in question...has nothing to do with the hearsay rule... [I]t is in the nature of real evidence” which as defined “is the evidence afforded by the production of physical objects for inspection or other examination by the court.” The defence do not seek to argue to the contrary.”

This characterisation is particularly important when it is considered that in many conflict situations it will not be possible to say with any certainty whether the creator or poster of an item of OAVC was affiliated with one party or another. The act of verification of the OAVC itself can dispense with the need to rely on other indicators as to the credibility of its creator or poster, although the identity of the source, if known, is a factor which should be taken into account at all times by an analyst.

It thus appears that both parties agreed that the video was real evidence, albeit it contained depictions of persons making hearsay statements. Images, whether in the form of stills or video, are real evidence introduced within a document (a digital file). It is the document which must be authenticated according to the rules of documentary evidence, and once it has been authenticated, the contents speak for themselves.

See also paragraphs 58 onwards below in respect of hearsay.

When Palmer was giving evidence during the mock hearing, he stated that the credibility or reliability of the source in this case did not affect the degree to which he considered the video to be genuine because he could analyse the video itself and did not have any reason to believe the source was involved in malicious misinformation. For completeness, we add that this would not always be the case, for example if the source was known to be involved in the generation of sophisticated deepfake imagery or if the account was new and had posted the first online iteration of the video. Thus, the source can be a relevant factor going to the degree of confidence that the item is genuine and such consideration would be given as a factor external to the analysis of the actual content. For an example of a falsified video whose inauthenticity was missed due to a failure to consider the source, see: Yvonne McDermott, Alexs Koenig and Daragh Murray, Journal of International Criminal Justice, Open Source Information’s Blind Spot: Human and Machine Bias in International Criminal Investigations, 2021, which addresses an incident where those who were fooled by a staged video had failed to consider the fact that the first iteration of the video had come from a new source that had never posted any content before.

It should be noted here that the definitions of the categories involved are somewhat porous, which can lead to confusion or interchangeable terminology. For example, a hard drive containing videos would be considered ‘physical evidence’, which is a term often used in place of ‘real evidence’, where real evidence is defined as ‘material objects produced for inspection by the court’. As noted above, the definition of real evidence adopted here is ‘evidence from things as distinct from persons.’ (See Phipson on Evidence, para. 1-14). Similarly, documents can be physical evidence if introduced as evidence of their condition (for example if they are bloodstained), and can contain written testimonial evidence, which can constitute hearsay if introduced as evidence of its truth.
58. If OSI is deemed to constitute or contain hearsay evidence, this may have a bearing on its admissibility. In England and Wales, hearsay is defined as a “statement not made in oral evidence that is evidence of any matter stated” \(^{45}\), where the “statement” may be “any representation of fact or opinion made by a person by whatever means” including a representation made in a sketch, photo fit or other pictorial form. \(^{46}\) For example, if person A tells the court that person B told her he had seen the defendant commit the crime, this is hearsay. The court cannot assess the credibility and reliability of person B, since he is not in court, and it would thus be unfair to admit person A’s statement as evidence of what person B saw (i.e., the truth of person B’s statement as recalled by person A), even if person A is credible and reliable. Hearsay is presumed inadmissible unless one of a range of exceptions apply. \(^{47}\) There are thus two questions to ask in respect of OSI in this regard: first, is there a hearsay issue? And second, if so, do any of the exceptions apply? As noted above, video evidence is not of itself hearsay. Hearsay requires a statement to be made, and while the definition of ‘statement’ is reasonably broad, it does not extend to the capture of photographic or video evidence. \(^{48}\)

59. However, online videos and photographs are often accompanied by, or can contain, hearsay. For example, if the Tweet posting the video contained claims that the Coalition was responsible for the airstrike and that it had killed and injured 66 people. These are statements which, if introduced as evidence of the truth of their contents, are hearsay. Such statements would not be introduced into evidence by the prosecution without an application to the Court as they would be inadmissible absent such an application.

60. However, there are also statements made within the video itself which, although hearsay, may have been admissible under one of the exceptions to the rule against hearsay. A woman depicted in the video can be heard shouting “I could have been killed with them by the presidency office...” and, later, referring to the young casualty seen throughout the video, the man filming says “...and this child...”. These are statements which are clearly relevant to the issues in dispute in the proceedings given that they assert both the location of the airstrike and the possibility that one victim is a child. As such, the prosecution sought to introduce the statements, or utterances, for the truth of their contents in support of its case that this video depicted an attack at the Office of the Presidency which killed civilians. \(^{49}\) In so doing, the prosecution relied on re gestae, a common law exception to the rule against hearsay which is preserved by Section 118 of the Criminal Justice Act (emphasis added):

\[
4 \quad \text{Any rule of law under which in criminal proceedings a statement is admissible as evidence of any matter stated if—}
\]

\[
(a) \text{the statement was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion can be disregarded.}
\]

\(^{45}\) Criminal Justice Act 2003, Section 114(1).
\(^{46}\) Criminal Justice Act 2003, Section 115(2).
\(^{47}\) The exceptions are set out starting at Section 116 Criminal Justice Act 2003 and include situations where it is in the interests of justice to admit evidence where the relevant person is dead, outside the United Kingdom, cannot be found, or cannot give evidence due to fear. Some of these exceptions would potentially be relevant but this was not developed in the preparation of this case.
\(^{49}\) Note that it could also have been introduced as evidence of other matters that would not engage the hearsay principle, such as the Arabic dialect spoken by the woman, which would have supported claims that the video was made in Yemen.
(b) The statement accompanied an act which can be properly evaluated as evidence only if considered in conjunction with the statement, or

(c) The statement relates to a physical sensation or a mental state (such as intention or emotion).

61. Because only two hours were allocated for the mock hearing, it was agreed in advance that the prosecution should not place substantial focus on these statements to ensure that the issue did not take time away from the more important (for the purposes of this exercise) issue of whether the video could be authenticated through OSI analysis. After all, if the video was not established to be genuine then the utterances would not be admissible either, so admissibility of the video itself was the primary concern of the exercise. In any event, in her ruling HHJ Korner noted that Mr Higgins, in his witness statement, had indicated that the prosecution would not intend to rely on the utterances and in her view they would not be admissible on the ground that their admission would be unfair. ⁵⁰

62. One additional issue in this regard relates to the background content used in the verification of the Exhibit CG/2 video, some of which contained hearsay. For example, the tweet which Palmer used to assist with his geolocation stated, alongside a photograph, that an airstrike was ‘happening now.’ Given that this was only one factor in Palmer’s chronolocation, it does not appear to us to raise a fairness issue, however the idea that hearsay could be introduced through the ‘back door’ in this way is potentially problematic. In jurisdictions where hearsay is not presumed inadmissible, this is less concerning because it can simply be established that the judge does not place weight on that item but rather views it as part of the evidential picture that the expert relied on. In England and Wales, it would technically have to be introduced by way of an exception, which did not happen in this case. This is connected to the ‘corroborative jigsaw’ point discussed at paragraph 117 below in relation to the other videos that were used to verify the Exhibit CG/2 video – namely that all of the evidence, from the central video to the other items which are more unreliable individually, need to be presented as a package, in which the evidentiary value (and therefore fairness) of the introduction of each is only clear by reference to the package as a whole.

63. A further point of interest which draws together some of the above discussion is that in some circumstances an item of video could be authentic and yet its contents could still be unreliable. ⁵¹ Whether an authentic video is also reliable depends on what claims are being made about what it proves. For example, an authentic video of an interview with a person about whom nothing is known of their credibility might be considered authentic as a depiction of what the person said, but nevertheless unreliable as evidence of the truth of what the person is saying. Another example might be a video which, while authentic, depicts an item that can be very easily planted, such as a weapons fragment. In other situations, however, the authentication of the video is one and the same as an assessment of reliability where the claims being made on the basis that the video can be clearly evaluated by the fact finder on the face of the video alone.

⁵⁰ Ruling, para. 63 This issue may have played out differently in a real scenario, because more time may have been given to establishing that the res gestae exception justified the inclusion of the utterances.

⁵¹ Lindsay Freeman, Digital Evidence and War Crimes Prosecutions, supra note 7, at p.296, citing ICC, Bemba, Case No. ICC-01/05-01/08-3343: Judgment, 21 March 2016, at paragraph 39.
64. In the case of the Exhibit CG/2 video, the claims being made by the prosecution included that civilians were present when a second explosion took place; that extensive damage was done; and that the skies were clear at the time of the attack. The trier of fact (the jury in this case) would be able to judge for themselves the damage, whether the people appeared civilian and whether the sky was sufficiently clear to allow for reconnaissance sensors to capture them. These contents could be relied upon because they were readily apparent and verifiable from the video itself; there was no statement being made within the video which may have been itself unreliable – in other words, the natural conclusion of the authentication was that the video was reliable as to what some of the people present looked like, and as to what the sky and the street looked like. Many items of OA VC will present a mix of reliable and less reliable content. As already noted, in the case of Exhibit CG/2 HHJ Korner ruled that the video was admissible as evidence of the facts outlined above but that other contents, namely the utterances made by the people in the video, were not admissible.

65. Like authenticity, the final analysis of reliability is a matter for the jury, but the question is important at the admissibility stage because, even once an item has been determined to be authentic, the ultimate test then applied by the judge is an analysis of fairness based on weighing the item’s overall probative value against any prejudicial effect it may have on the jury. If its prejudicial effect outweighs its probative value, fairness will dictate that the item is excluded from evidence despite its authenticity.

C. THE IMPORTANCE OF TAILORING WHAT CLAIMS ARE MADE ABOUT THE VIDEO

66. To create scope for argument both in favour of and against admission of the video, other fictional evidence was introduced by the organisers alongside the real Exhibit CG/2 video. This was because it would be unlikely for a video such as this to be allowed into evidence if there was no other admissible evidence of the event it depicts. More realistically, a trial would likely not take place at all on such an evidentiary basis, given that the prosecution will only proceed if satisfied that there is a reasonable prospect of conviction.

67. For the purpose of facilitating the exercise, the organisers introduced evidence from a fictional MSF doctor who received injured patients that he believed had come to his hospital from the Office of the Presidency. Because the video on its own would not necessarily link a particular party to the attack, let alone a specific pilot, the organisers also included in evidence the defendant’s ‘admission’ in police custody to having carried out the airstrike. The additional

---

52. Subject, as noted elsewhere in this report, to further fact and witness evidence on this point.
53. Haw Tua Tau v Public Prosecutor [1982] A.C. 136 PC, at 151: “Matters such as the reliability of evidence and resolution of disputed evidence are generally matters for the jury”.
54. Probative value is a qualitative assessment of the degree to which a piece of evidence is capable of proving a significant fact. Thus, if a document was authentic and highly relevant but ultimately unreliable, it would still be of little probative value and would fall to be excluded on the basis of its unreliability, as opposed to its inauthenticity.
55. In reality, the Coalition does accept responsibility for this attack, but the online report to this effect could raise hearsay questions that might distract from the issues we wanted to test, and in any event our fictional proceedings needed the defendant to have personally carried out the attack. For the Coalition’s version, see Saudi Press Agency, Joint Incidents Assessment Team Issues Statement Regarding Allegations against Coalition Forces 2, 19 August 2020, available at: https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2123609.
Insofar as objects are concerned, “military objectives” are defined according to a two-stage process, pursuant to Article 52(2) of Additional Protocol II.

The offence of attacking civilians requires an active intention to kill the civilians – the defendant must have been aware of who is targetable in non-international armed conflicts, of which Yemen is one, is less straightforward than in international armed conflicts, but it offers a definite military advantage.

Therefore, mere awareness would need to be accompanied by direct or circumstantial evidence (which could come through inference) that the defendant intended to kill the civilians. This would require:

- Evidence that the defendant was responsible for the attack and carried it out on purpose;
- Evidence that the people killed and injured were protected from attack under the law of armed conflict (i.e. that they were civilians); and
- Evidence that the defendant was aware of the civilian nature of the targeted people and was aiming the attack at them, as opposed to a military target.

The need to establish these elements means that one particularly relevant factual inquiry was whether there were any legitimate military targets in the vicinity of the airstrike. For example, if there were military personnel present at the Office of the Presidency, it could support an argument from the defendant that those personnel were the military target of the strike and/or that their presence rendered the Office of the Presidency itself a military target at the time of the attack; thus impacting the prosecution’s ability to prove that the defendant intended to kill the civilians.

It was not impossible, as agreed by Palmer and Higgins under cross-examination, that the original video contained footage showing military personnel or objects which was omitted from this iteration of the video to increase the propaganda value of the video for the Houthis. Thus, the fact that the video had admittedly been edited could well have been a strong countervailing factor in the judge’s assessment of whether it was fair to allow it into evidence.

68. Very broadly, a prosecution of this nature would need to convince the jury that the defendant intentionally killed people he knew to be civilians. This would require:

- Evidence that the defendant was responsible for the attack and carried it out on purpose;
- Evidence that the people killed and injured were protected from attack under the law of armed conflict (i.e. that they were civilians); and
- Evidence that the defendant was aware of the civilian nature of the targeted people and was aiming the attack at them, as opposed to a military target.

69. The need to establish these elements means that one particularly relevant factual inquiry was whether there were any legitimate military targets in the vicinity of the airstrike. For example, if there were military personnel present at the Office of the Presidency, it could support an argument from the defendant that those personnel were the military target of the strike and/or that their presence rendered the Office of the Presidency itself a military target at the time of the attack; thus impacting the prosecution’s ability to prove that the defendant intended to kill the civilians.

70. It was not impossible, as agreed by Palmer and Higgins under cross-examination, that the original video contained footage showing military personnel or objects which was omitted from this iteration of the video to increase the propaganda value of the video for the Houthis. Thus, the fact that the video had admittedly been edited could well have been a strong countervailing factor in the judge’s assessment of whether it was fair to allow it into evidence.

---

56. These bullet points are intended to loosely condense the requirements of murder and attacking civilians under the Rome Statute of the International Criminal Court. The full offences and elements can be found in the Rome Statute and Elements of Crimes available at: https://www.icc-cpi.int/nr/dononlyres/336923d8-a6ad-40ec-ad7b-45b9de73d56e/0/elementsofcrimeseng.pdf. Article 8(2)(e)(i) of the Rome Statute makes an offence of “Intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities.” The relevant elements for this offence are: 1. The perpetrator directed an attack. 2. The object of the attack was a civilian population as such or individual civilians not taking direct part in hostilities. 3. The perpetrator intended the civilian population as such or individual civilians not taking direct part in hostilities to be the object of the attack. Article 8(2)(e)(i) creates an offence of serious violations of Article 3 common to the four Geneva Conventions of 12 August 1949, namely, “any of the following acts committed against persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention or any other cause: i) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture; (…).” The relevant elements of the war crime of murder are: 1. The perpetrator killed one or more persons. 2. Such person or persons were either hors de combat, or were civilians, medical personnel, or religious personnel taking no active part in the hostilities. 3. The perpetrator was aware of the factual circumstances that established this status. There are other elements which relate to the existence of an armed conflict, but those are not controversial in this setting.

57. The offence of attacking civilians requires an active intention to kill the civilians – the defendant must have been trying to kill them. Incidental harm arising out of an attack intended for a military target, even fully anticipated and unlawfully disproportionate, would not meet this threshold. Therefore, mere awareness would need to be accompanied by direct or circumstantial evidence (which could come through inference) that the defendant had the necessary intention. There is an argument that the threshold for murder is lower – but that is beyond the scope of this document.

58. Insofar as objects are concerned, “military objectives” are defined according to a two-stage process, pursuant to Article 52(2) of Additional Protocol I to the Geneva Conventions and Article 50 of Additional Protocol I. The definition is: “… those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.” In relation to people, the definition of civilians is “persons who are not members of the armed forces.” The question of who is targetable in non-international armed conflicts, of which Yemen is one, is less straightforward than in international armed conflicts, but it is not necessary to elaborate as part of this exercise. It is sufficient to note that military objectives or members of the armed forces would have been legitimate targets (subject to the rule against disproportionate and indiscriminate attacks).
To avoid this potential pitfall, it was agreed in advance that the prosecution would make clear that the video was not being introduced as evidence that no military target was present; and the judge decided that the video was still admissible even taking into account the possibility that it could have omitted images of a potential military target. Indeed, ‘proving this negative’ is notoriously difficult even where first-hand witness evidence is available, because the attacker could counterclaim that civilian witnesses or others might not have known about the existence of a military target.

71. The presence of the civilians and the fact that the video shows clear skies at the time of the second attack is also relevant to the second and third ‘elements’ set out above. The Coalition is known to have access to very high-resolution reconnaissance imagery which is capable of distinguishing adult men from women and children, in addition to identifying weapons and observing behaviour. The clear skies aspect was thus introduced as a fact potentially relevant to a prosecution claim that the defendant knew civilians were present in the street. On the facts as prepared for this mock exercise, there was not enough information to make this link, but the purpose of introducing the subject was to introduce facts that made the clear skies relevant for the purposes of the fictional voir-dire hearing.

72. Thus, the video was introduced by the prosecution only to show the time of the attack, the condition of the street, the presence of civilians and the clearness of the skies, all of which are material in establishing the second and third parts of the condensed ‘elements’ as set out above. The prosecution disavowed any suggestion of reliance on the video as evidence of any wider claims. In that sense, the claims being made about the video were tailored and the prosecution did not ‘over-reach,’ allowing it to freely accept that omissions could have been made from the video without affecting its reliability. Significant time was devoted to the potential for omissions during the hearing, highlighting that the outcome may have been different if the prosecution had made unrealistic claims about what the video proves or had failed to properly anticipate the defence’s attacks on the video.

59. It is worth re-stating here that this was just a test of the admissibility of the video; convicting the defendant would, of course, entail a different analysis.

60. See, for example, Iona Craig and Shuaib Almosawa, The Intercept, U.S.-Backed Saudi Airstrike on Family With Nine Children Shows “Clear Violations” of the Laws of War, 2 August 2018, available at: https://theintercept.com/2018/08/02/saudi-airstrikes-yemen-war-laws/, in which a leaked US report describes a drone feed depicting the aftermath of a Coalition bomb on a tent: “multiple personnel, to include at least 1 female and 4 children, exited the tent and fled towards a road”.

61. In reality, there would need to be evidence of what reconnaissance camera was carried on the specific jet being flown by the defendant, his angle and distance from the location and more.
D. OSI AS EXPERT EVIDENCE

73. One of the most instructive parts of the exercise was examining the issue of OSI investigation and analysis as expert evidence.

74. Testimony given in court is divided into evidence of fact and expert evidence, and there are key differences between these forms of witness evidence. Witnesses of fact, who comprise the majority of witnesses, can give evidence of factual matters within their knowledge but are not permitted to give their opinion. Experts have a specific status in the context of legal proceedings – they can only give evidence with the permission of the court in defined circumstances and are allowed to give their opinion. Expert opinion evidence is admissible when:

\[(i) \text{it is relevant to a matter in issue in the proceedings;} \quad (ii) \text{it is needed to provide the court with information likely to be outside the court's own knowledge and experience;} \quad \text{and (iii) the witness is competent to give that opinion.}\]

75. As to the application of these criteria to the Exhibit CG/2 video, criterion (i) is uncontroversial – the question of whether the video is genuine, if it can be answered by an expert, is clearly relevant to a matter in issue. The judge heard submissions bearing on criteria (ii) and (iii) in some detail. While she ultimately decided that an OSI analyst could meet the criteria, the discussion is very instructive and provides guidance for the future use of OSI analysts as expert witnesses.

76. The kind of analysis that OSI investigators perform broadly consists of geolocation, chronolocation, checks for internal consistency within a video and source analysis, checks for consistency across multiple items purporting to depict the same event, and other, ad-hoc, methods. Since Bellingcat’s creation, its executive director, Eliot Higgins, has propagated the consistent position that OSI analysis can be performed by anyone - it is easy to learn how to do. Indeed, this is one of the reasons the field of practice, whether in a journalistic or evidentiary setting, is seen as democratizing and transparent, a notable benefit being that any person with an internet connection can critically assess a whole investigation and its underlying data for themselves without relying on the trustworthiness of the journalist. During the mock hearing, Palmer also confirmed that this was his view. The defence’s questioning explored the position that, given that anybody can take up OSI analysis without formal training, it is not appropriate subject matter to form the basis of expert evidence. Citing the case of _R v. Robb_, defence counsel echoed the Court of Appeal’s warning of the need to avoid “tenuous qualifications” leading to an unfair shifting of the burden of proof onto the defence to displace an assertion that should never have been put before the jury on such a tenuous basis. The answer to these criticisms lay in a review of the trajectory of the court’s attitude to what specialisms can be treated as expert evidence. Certain paragraphs from HHJ Korner’s ruling on the admissibility of Palmer’s evidence are worth quoting in full – she recognised that the categories of practice which are capable of forming the basis of expert evidence are by no means closed:

---

63. _R v Robb_, supra note 19.
36. “English law is “characteristically pragmatic” as to the test for establishing expertise: Bingham LJ (as he then was), in R v Robb [1991] 93 Cr App R 161 stated “This appeal raises questions touched on but not discussed in depth in the authorities: what characterises a field as one in which expertise may exist, and what qualifies, or disentitles, a witness to give evidence of his opinion as an expert? The old-established, academically-based sciences such as medicine, geology or metallurgy, and the established professions such as architecture, quantity surveying or engineering, present no problem. The field will be regarded as one in which expertise may exist and any properly qualified member will be accepted without question as expert. Expert evidence is not, however, limited to these core areas. Expert evidence of fingerprints, hand-writing and accident reconstruction is regularly given. Opinions may be given of the market value of land, ships, pictures or rights. Expert opinions may be given of the quality of commodities, or on the literary, artistic, scientific or other merit of works alleged to be obscene... Some of these fields are far removed from anything which could be called a formal scientific discipline... Thus the essential questions are whether study and experience will give a witness’s opinion an authority which the opinion of one not so qualified will lack.” (p.164)

77. Reflecting the arguments made by the defence, HHJ Korner continued:

37. “That said, by whatever method the expertise is acquired, the expert must be confined to matters within his area/s of expertise. In Robb, Bingham LJ stated (at p.166): “We are alive to the risk that if, in a criminal case, the Crown are permitted to call an expert witness of some but tenuous qualifications the burden of proof may imperceptibly shift and a burden be cast on the defendant to rebut a case which should never have been before the jury at all. A defendant cannot fairly be asked to meet evidence of opinion given by a quack, a charlatan or an enthusiastic amateur...”

78. The defence had argued that the practice of OSI had not evolved into a discipline with sufficiently scientific characteristics to qualify as expert evidence. HHJ Korner’s ruling continued:

38. “The Defence rely upon what was said by the President of the QBD in R v Dlugosz & Others [2013] EWCA Crim. 2. These were conjoined appeals dealing with the admissibility of Low Template DNA evidence. At para 8. he stated “It was the primary submission of the appellants in each case that unless statistical evidence of match probability could be given, then evaluative evidence should not be admitted. That was because the jury needed to have a firm basis on which they could evaluate the significance of the evidence given. In the absence of statistical evidence it was not possible to do so.” He continued in the next paragraph: “We cannot accept that argument. As is clear from the judgments in Atkins and Atkins (paragraph 23) and T (Footwear Mark Evidence). (at paragraph 92) the fact that there is no reliable statistical basis does not mean that a court cannot admit an evaluative opinion, provided there is some other sufficiently reliable basis for its admission”.

39. “Para. 11, on which the defence place emphasis, stated “It is essential to recall the principle which is applicable, namely in determining the issue of admissibility, the court must be satisfied that there is a sufficiently reliable scientific basis for the evidence to be admitted. If there is then the court leaves the opposing views to be tested before the jury.”"
40. “At para 14 the President went on to say “In our view, an expert is not bound to express an evaluative opinion by reference to the hierarchy; he can use other phrases. The real significance of the expert’s inability to use the hierarchy might be that it is indicative of the lack of a proper basis on which to express an opinion. In our view, it can be no more than that. It is a matter to be taken into account in an assessment of whether there is a sufficiently reliable scientific basis for such an evaluative opinion to be given.””

79. HHJ Korner made reference by analogy to evidence of gang practices given by police officers, which is admissible although not a scientific discipline, provided “… the officer must have made a sufficient study, whether by formal training or through practical experience, to assemble what can properly be regarded as a balanced body of specialised knowledge which would not be available to the tribunal of fact.” On this point, HHJ said:

43. “The defence in their written submissions on this authority, argue that Mr Palmer does not possess the same level of expertise as was apparently possessed by the police officer who gave evidence at the trial. That may or not be the case, but it is the principles which appear to me to be of universal application which are of importance namely:

• That employment by an organisation which could be said to have an interest in the outcome of a case is not an automatic bar to providing expert evidence
• That expertise may be derived “through practical experience, to assemble what can properly be regarded as a balanced body of specialised knowledge which would not be available to the tribunal of fact.”

80. HHJ Korner then ruled as follows:

44. “The field of analysis of video material to establish its significance, reliability or authenticity, is one which appears to be of relatively recent origin and is one which is composed of a number of factors.”

45. “One is the application of technical knowledge e.g. an understanding of the operation of metadata and methods of digital alteration. Another is knowledge of techniques such as geolocation and chronolocation. However much of the analysis relies upon factors, such as the use of search engines for obtaining satellite imagery and evidence which supports or undermines the content of the video, which do not require specialist expertise but are derived from training and experience in the examination of such material. The Berkeley Protocol, referred to by Messrs Higgins and Palmer, sets out the methodology required to conduct proper investigations into open-source material.”

46. “Whilst Mr Palmer has no technical knowledge in respect of metadata or digital alteration, his other qualifications and more to the point his experience in this kind of analysis make him a person who is able to “assemble what can properly be regarded as a balanced body of specialised knowledge which would not be available to the tribunal of fact.”
47. “Having heard him give evidence I am satisfied that he is giving an opinion which is objective and unbiased, and within his area of expertise. In the words of Lord Bingham he is not ‘a quack, a charlatan or an enthusiastic amateur.’”

48. “I find that, with the exception of peer review, he fulfils the criteria set out in Part 19 of the CPD.”

81. The key passage is at paragraph 46, in which HHJ Korner concluded that Palmer is an expert for the purposes of Part 19 of the Criminal Procedure Rules because although his experience could be gained by any person on the jury, it has not been – and thus it “would not be available to the tribunal of fact.” In this way, it is comparable to the other types of non-traditional expert evidence of the many and varied categories listed by Bingham LJ (as he then was) in R v Robb.

82. There were thus two main lessons in this respect – the first is that the court was persuaded that OSI is a field of practice capable of forming the basis of expert opinion. The second, which is equally important, is that the judge will expect the analyst to have certain competencies and significant, demonstrable experience. In debrief, the judge stressed that Palmer’s academic qualification was important; but it was also clear that the breadth and calibre of his prior work, in addition to his ability to respond robustly to questioning, had carried a lot of weight. Additionally, one particular strength was that he was capable of speaking just as fluently about what OSI could not tell the court (for example when asked about forensic analysis and detecting omissions), which, in the organisers’ view, reassured the court that he was not an “enthusiastic amateur.”

i. How Independent Does the Expert Need To Be?

83. As noted above, in her assessment HHJ Korner concluded that

“... Employment by an organisation which could be said to have an interest in the outcome of a case is not an automatic bar to providing expert evidence...”

on the basis of Myers & others v. The Queen [2016] AC 314 in which the Privy Council held that police officers can give expert evidence provided that the ordinary threshold requirements for expertise are established and the ordinary rules as to the giving of expert evidence are observed.

84. When preparing the papers for the exercise, the decision was made that it would be preferable for the prosecution to have instructed an independent expert – hence, the creation of ‘Frank Palmer’ of ‘OSINT Reports.’ Given that in the fictional scenario Bellingcat had gathered the information for the original referral to SO15, the organisers were concerned that a Bellingcat analyst may not be deemed sufficiently independent by the court as an expert witness. However, HHJ Korner’s finding that the principles derived from Myers have universal application, and her statement as quoted above, indicates that this concern was perhaps unwarranted.

85. However, it is worth noting that neither Myers nor the mock hearing directly addresses the precise question of whether the same OSI analyst who uncovered the video could be the expert witness, as opposed to another individual from the same organisation. Indeed, it is a somewhat
unique feature of OSI that the investigators and analysts could be both fact and expert witnesses, which is not a situation that is usually seen. In a traditional situation, for example, a blood sample would be taken from a crime scene by a member of the police and analysed by a DNA expert. The police officer would give fact evidence as to how they encountered the evidence, and the DNA expert would testify as to their analysis on its contents.

86. Finally, an OSI analyst, if giving evidence solely as the individual who sourced the particular item, could be a witness of fact. This was seen in the case of Charlotte Godart in these proceedings: Godart is a trained OSI analyst with practical and academic expertise but in this context was merely introducing the video and confirming the circumstances of its discovery, without any opinion or technical analysis. As such, this witness, although she happens to also be an OSI expert, is a fact witness.

ii. What Should an OSI Analyst as an Expert Refrain From Commenting On?

87. Defence counsel raised the important issue of the need for experts such as Palmer to remain disciplined in the scope of the matters on which they opine – that is, opine only on matters properly requiring expert opinion and avoid commenting on matters that properly fall to the jury to assess. This principle is of course of general application in respect of expert evidence but is particularly important to bear in mind in the context of OSI given that it may be counterintuitive to OSI analysts. OSI analysis is often conducted in a journalistic or other analytical context (as distinct from the strict confines of evidentiary rules) where a comprehensive review of items of OSI is undertaken to establish the whole picture and any written commentary tends to involve the OSI analyst describing and commenting on an item’s content in a way that would not be appropriate in the context of an expert report prepared for a court. For example, in the mock hearing the defence pointed out that the expert report made reference to “a number of casualties,” visible in the video which is something that could be assessed by the jury on viewing the video. Defence counsel pointed out that Palmer should have restricted himself to his description only of content that was relevant to his verification process (i.e. the geolocation, chronolocation and cross referencing). In her ruling (at paragraph 49), HHJ Korner acknowledged that the delineation between what matters are for the expert and what matters are properly for the jury can also be dealt with in other ways, for example the prosecution and defence could agree this in advance of Palmer’s evidence going before the jury or it could be dealt with prior to Palmer giving evidence in front of the jury in the main proceedings.

iii. Note on the Witness Statement of Eliot Higgins

88. The witness statement of Eliot Higgins was prepared by the organisers with the aim of providing to the court and counsel teams the necessary explanation of certain characteristics of OSI. However, it contained a mixture of evidence of fact, expert evidence and law, which would not be permissible in real proceedings. In reality, the information conveyed in Mr. Higgins’ statement would have likely been split across the statement of Charlotte Godart (as to the methodology followed by Bellingcat, its origins); Frank Palmer (as to the parts concerning what OSI analysis comprises generally, and the authenticity of the CG/2 video in particular); and the legal submissions (as to the evidentiary qualities of OSI).
iv. Digital Forensic Analysis

89. While rigorous evidence of chain of custody from creation to presentation can assure the court that no manipulation has taken place since its collection and preservation, in the sphere of digital evidence there are other ways of checking for manipulation and editing, which involve analysis of the digital file itself. This warrants a brief discussion about the difference between the kind of analysis performed by Palmer and how it compares to the discipline commonly called digital forensics. The hearing addressed in detail the difference between a digital forensics expert and an OSI expert, which provided guidance useful to both practitioners and investigators wishing to ensure controlled presentation of their material.

90. Misleading videos can be created with varying degrees of sophistication. For example, a real video could be miscontextualised or edited using relatively crude steps such as cutting out undesirable parts of the clip before posting it online. However, much more difficult to contend with are so-called 'deep fakes' - sophisticated videos in which a computer takes images of a real person and, using artificial intelligence, uses those images to generate very convincing fake footage of that person doing or saying something. Somewhere in the middle, there are doctored videos in which the contents of a piece of audio-visual information are digitally altered. The familiar example is a photoshopped image, but there are far more sophisticated technologies available which can create convincing computer-generated imagery capable of deceiving the untrained eye. In the mock hearing, Palmer differentiated these concepts by drawing a distinction between ‘editing’ and ‘manipulation,’ recognising a core difference between simply using genuine digital content misleadingly (whether or not maliciously) and digitally inserting or removing content. An example of manipulation in this case would be if someone had altered the contents of the video to actually remove or insert a person or object, such as a military target, by tampering with the individual images. When asked by HHJ Korner to give an example of what would be a sign of manipulation, Palmer used the example of rudimentary attempts to allege that the Beirut explosion of 4 August 2020 was caused by a missile: some Twitter accounts had shared a version of real footage of the explosion, but with a cartoon missile inserted in two frames, which appears to be falling on the location just prior to detonation.

91. Digital forensics is a separate discipline to OSI analysis (although there is some overlap). Digital forensics methods range from technical, computational tests which analyse the files themselves for anomalies or unnatural repetitions, to visual inspection of the content depicted in the file, including by separating the frames into stills and searching for so-called ‘artifacts of manipulation.’ The computational tests are most effective at detecting such features when performed on an original file, as opposed to a downloaded file. This is because when videos are posted on social media, the platforms make various changes to the videos to reduce their size, which include compression, reducing the frame rate, and reducing pixel resolution. Further, as noted elsewhere, these sites remove embedded metadata from files as a privacy measure. All of these are changes which detract from the degree to which a file can be forensically analysed, because key information has been stripped out, introducing an inherent complication for digital forensics. That is to say, the process of uploading to a social media platform and downloading from the internet effectively creates a new file which is not the
same as the original file. Thus, the technical methods used by digital forensics experts can be applied to open source files, but because they contain less information, their work is more limited on such files.

92. The overlap between digital forensics and OSI analysis lies in the visual inspection aspect of digital forensics. HHJ Korner clarified this difference with Palmer when she asked for him to define what his expertise covered, following which Palmer made clear he was not a digital forensics expert. HHJ Korner’s chosen phrasing was to ask Palmer whether he was an expert in “verifying whether or not what appears in a piece of film is genuine.” This was a very fitting descriptor which, although simple, can take into account the overlap between what a digital forensics expert and an OSI expert can do, albeit the fields are otherwise distinct both in content and the background and training of the expert. Thus, Palmer confirmed that he can separate a video into its individual frames and analyse them sequentially, which allows him to perform his regular checks aimed at geolocation, chronolocation and consistency, but also to check for artifacts of manipulation such as the kinds of glitches that appear on close scrutiny of manipulated videos or deepfakes.

93. Further, HHJ Korner asked Mr Higgins about his assertion that, given the complex and chaotic nature of the contents of the video, it is highly unlikely that it could have been fabricated in the short time between the alleged event and the upload of the video online. This is an opinion on the question of whether the item could be a deepfake and is a judgment of a different nature to the bulk of an OSI technical/granular analysis. However, it is an issue that does arguably fall within the field of expertise of a Bellingcat analyst given their vast experience of watching hundreds, if not thousands, of conflict videos. These are matters which do not pertain to the file itself but visual inspection of ‘what appears,’ set against the analysts’ experience. In that sense, OSI analysts, while they may not be technical experts in digital forensics, can apply their vast experience of watching conflict videos to give their opinion on whether – even putting aside their other verification processes – a video is likely to be a fake.64

94. However, given that a digital forensics expert could comment on technical issues that an OSI analyst could not, and potentially also on visual appearance with greater expertise than some OSI analysts, it would be advisable for the prosecution and defence to instruct such experts in any event. Indeed, it was argued by the defence in the mock hearing that the correct expert proffered by the prosecution should in fact have been a digital forensics expert – but it is clear there is a role for both, given that a digital forensics expert would not have the same experience as an OSI analyst.

95. One point made by Palmer which is of relevance here is that metadata is not always accurate. He stated that he had encountered files whose metadata suggested a given time and date of creation, whereas his OSI analysis of what the file depicted showed otherwise. He thus considered that OSI analysis was in some ways more reliable than such metadata.

E. THE BELLINGCAT METHODOLOGY

96. The organisers had intended that the methodology followed by Bellingcat be tested by the proceedings. This lean methodology was designed after a review by lawyers at GLAN of the core evidentiary principles – it was developed as a ‘light touch’ methodology which unofficial investigators such as Bellingcat could follow with the objective of increasing the likelihood that evidence located in the course of those investigations would be admissible in court. The methodology and legal components involve, among other things:

- Training on the core principles of international humanitarian law;
- The requirement to follow all lines of inquiry, including those which point away from a violation of IHL;
- The requirement to take steps to counteract technical biases;
- The requirement to track all searches and website visits;
- The requirement to preserve all key evidence; and
- Standardising the language and style of the written reports on the incidents.

97. For a number of years, lawyers and technologists coordinated by the Human Rights Center at the University of California, Berkeley had been drafting what is now known as the Berkeley Protocol. The Berkeley Protocol was published in December 2020 after an extensive consultation which involved reviewing principles and practice across many jurisdictions and disciplines, giving rise to a guidance document which could be used to standardise the use of digital investigations for human rights and accountability purposes. While the GLAN/Bellingcat methodology was not ‘based’ on the Berkeley Protocol (which had not yet been published when the GLAN/Bellingcat methodology was developed), the organisations wished to make the legal teams in the mock hearing aware of its existence so that the methodology could be tested ‘against’ the standards the Berkeley Protocol sets. Given the restricted timeframe, this issue was not wholly explored, but the defence did ask some probing questions which gave rise to interesting issues, as discussed below. The judge did not explicitly address the issue of compliance with the Protocol, save for two references to the Protocol which appeared to suggest that she viewed its existence as a factor weighing in favour of treating online digital investigations as a legitimate field of practice.

i. Bias

98. Objectivity is a fundamental requirement of all fair and accurate investigations, including OSI investigations. Thus, the question of the potential for bias in OSI investigations was raised in argument. The key biases that present risks to the objectivity of an investigation are: 1) access bias, i.e. missing information, due to some relevant parties not having access to the internet or the platforms used in the search, 2) technical bias, and 3) cognitive (human) bias.

---

66. Berkeley Protocol, supra note 2, at para. 27.
99. Access bias did not arise in the context of the mock hearing.

100. All of the parties appeared to accept that the use of internet searches could be affected by unavoidable technical bias. McDermott et al. have highlighted that technical bias can take the form of so-called algorithmic bias: “the bias embedded in the design of algorithms and their use, often due to already-biased training data. Algorithmic bias can impact what results users see when they conduct a search, and the order in which results are presented.”

101. As the defence highlighted in closing submissions, this is a potentially serious issue simply because these biases could theoretically cause exculpatory evidence to be missed. Palmer accepted under cross examination that there is no such thing as a ‘neutral’ search but stressed that measures are taken by OSI investigators to mitigate any bias that might be connected to information specific to that researcher (such as their IP address or their previous search history, to the extent that that is possible to erase). This reflects the recommendation in the Berkeley Protocol and in legal practice more generally to be aware of the potential for algorithmic bias and be able to state the measures put in place by the investigator to minimize the risks. Dealing with the unavoidable existence of algorithmic bias raises the logical difficulty that a ‘counterfactual’ cannot be demonstrated. That is, the defence would be unlikely to be able to show to the court an example of an unbiased search, in order to highlight what the algorithms may be causing OSI researchers to miss out. There is, perhaps, a certain relationship between the acceptance of algorithmic bias and refraining from ‘over-reaching’ – the prosecution in this case asserts that it is fair to introduce the video as evidence of the positive facts already summarised elsewhere – not as evidence that there were no military targets at the location. That absence of a claim that OSI can ‘prove a negative’ can be extended to take into account the fact that it is theoretically possible the investigators were not presented with exculpatory content over the course of their searches. However, it is noted at this juncture that Palmer suggested that rather than withholding certain results, the algorithms simply display them in a particular order – and some practitioners interviewed by GLAN do not consider that algorithmic bias necessarily presents fairness issues given the specialised nature of the searches conducted. It seems clear that conversations as to the risks and consequences associated with the algorithms run by private companies, about which very little is known, is an evolving conversation.

102. Cognitive bias refers to “any distorted evaluation of information by humans.” There are a number of forms of general cognitive bias which any investigator, whether online or offline, must actively resist. For example, confirmation bias is the tendency to seek out or pay attention to information that supports an investigator’s hypotheses while “disregarding, avoiding or

---

67. McDermott et al., *Open Source Information’s Blind Spot; Human and Machine Bias in International Criminal Investigations*, supra note 44. The Berkeley Protocol has the following to say about technical bias: “The browser, search engine, search terms and syntax used may lead to very different results, even when the underlying query is the same. Inherent biases in the Internet’s architecture and algorithms employed by search engines and websites can threaten the objectivity of search results. Search results may also be influenced by a number of technical factors, including the device used and its location, and the user’s prior search history and Internet activity. Open source investigators should counterbalance such biases by applying methodologies to ensure that search results are as diverse as possible, for example, by running multiple search queries and using a variety of search engines and browsers. Investigators should be aware that search results may also be influenced by other factors, including as a result of the discrepancy in the digital environment whereby online information may be unevenly available from certain groups or segments of society.”

68. The exception to this is results that are withheld due to GDPR concerns. Investigators could consider setting their Virtual Private Networks to have their exit nodes in a non-EU country, so that search results are not filtered.

rejecting information that counters them.”70 This would clearly occur where, for example, an investigator has decided in advance that an attack intentionally targeted civilians and may cause them not to devote resources to following other lines of inquiry, such as those which might reveal evidence of a military target. This kind of bias was referred to by Eliot Higgins under cross examination, which he described as “consciously or unconsciously” shaping an investigation to suit a preconceived notion of what will be found.

103. Even where an analyst is not motivated by something as powerful as confirmation bias, there remains the potential for other influences on their work. While in this case Bellingcat had conducted the ‘discovery’ phase of the investigation and saved all of the content they considered important, it would not be realistic to expect an expert to confine their analysis to the files provided by the prosecution – they would expect to have free rein to search online for anything which could help them to verify the video. This raised the interesting question of what happens when an online investigator cannot avoid seeing the results of another investigation. Indeed, this situation is likely to be very common where an expert is asked to geolocate a video of a well-known event and, given the precise and objective nature of geolocation, the conclusions reached by separate independent experts are likely to be not just similar but identical. In such circumstances it would likely suffice simply for the expert to acknowledge that they are aware that another report exists containing the same analysis and conclusions but confirm that their exert report is the result of their own independent analysis. The situation is no different to other areas of expert evidence which is scientifically precise and where other similar or identical analyses may exist.

104. One factor which can go some way to mitigating against confirmation bias in respect of geolocation is the fact in most cases unique reference points can be objectively corroborated which, combined, make it extremely unlikely that the location is wrong. This is particularly true in cities, where recognisable landmarks can be found in sufficient numbers to confirm a location. However, this alone is not a watertight safeguard against confirmation bias, for example given the risk that where several main markers have been corroborated the analyst may subconsciously disregard small anomalies. This may particularly be a risk in respect of more rural locations where geolocation is based on less clear markings such as unpaved roads, trees or mountain topography. Therefore, other complementary mitigating actions such as peer review remain important given the assurance that can be taken from more than one person conducting the same exercise and reaching the same result. This also highlights the need for equality of arms between the prosecution and defence, as if there is plausible doubt about a geolocation, a defence OSI analyst will be able to robustly contest it.

105. The risk of cognitive bias applies to any conclusion arising from an analysis, including the overall assessment of whether or not a video is genuine. An expert may be unconsciously influenced by the fact that other investigators have decided that a video is genuine, particularly if they are reputable. This further highlights the need for active steps to be taken to ensure objectivity and peer review.

70. McDermott et al., *Open Source Information’s Blind Spot; Human and Machine Bias in International Criminal Investigations*, supra note 44, which sets out a range of the most prevalent cognitive biases, of which confirmation bias is one.


### ii. Chain of Custody

106. Prosecutors must be prepared to present evidence to the court with an accompanying record of where it has been stored since its seizure, who has accessed it and any changes that have been made to it, and this very much applies to digital evidence.\(^1\) This chain of custody record is essential to showing that evidence has not been tampered with by law enforcement or other parties, with the familiar examples being the planting of DNA on physical evidence such as weapons. Where a police officer captures a video of a crime scene, there will be a clear chain of custody showing exactly where the video had been stored between the moment of its creation and its presentation in court. This would include an audit trail of any access to the original file and any changes made, even if they make no difference to the substance of the file (for example re-naming a file). In contrast, by definition the chain of custody from creation is non-existent in the case of open source files because they are posted, often anonymously, online. Thus, any chain of custody record will only flow from the point of download by the police or a third-party referring organisation. In this sense, the point of download is comparable to the point of ‘seizure’ of pre-existing files on a physical device found at a crime scene. Post-download metadata may not reveal anything about the creation of the file, because it may not contain the uploaded metadata; it will more likely only reveal the circumstances of the download and any changes made thereafter. Therefore, in an OSI context, preservation and chain of custody are of relevance only to show that the file as presented to the court is identical to the file that was downloaded from the internet.\(^2\)

107. In many cases, the video in question will still be available online at the time of the hearing, rendering this issue less important. However, videos depicting violent events are notoriously vulnerable to automated take-downs by the algorithms operated by social media platforms. Additionally, creators of content may take it down for a variety of reasons, for example because it is incriminating, where it was filmed by the perpetrators themselves. Non-governmental organisations such as Mnemonic (Syrian Archive, Yemeni Archive), Syria Justice and Accountability Centre and others have developed the technology to preserve videos of this kind, which includes storage on multiple servers, audit trails, generating unique numerical values (hash values) from each file and time-stamping those values using blockchain technology. If a video preserved in this manner were to be introduced as evidence, there would likely be a need for lengthy evidence on a range of advanced technological issues to demonstrate the chain of custody. Given that the mock hearing was only designed to last two hours, the decision was taken not to raise the issue of chain of custody. This was in any event appropriate for the video in question, which was still online in the location where it was sourced by Bellingcat.

108. The methodology prepared by GLAN and Bellingcat includes steps to maintain records of the investigative process (using the Hunchly software tool) and to ensure the appropriate preservation of files which investigators consider might need to be used as evidence. Any

---


\(^2\) There was a reference to this kind of file analysis in the papers and in the course of the hearing. Palmer had stated that he had checked for manipulation of the file, which gave the legal teams the impression that he had performed forensic analysis on the file. In fact, what he meant was that he had simply checked that the file he was “given” by Bellingcat was identical to the one he found online.
organisation which envisages that its OSI investigations might be used as evidence could take these steps at a minimum, but it is recommended that they consult a legal practitioner to ensure their methods are adequate. If a third party organisation became the only remaining source of a piece of key evidence, their practices (including their credibility, independence and reliability as an organisation, as well as their documentation practices) would come under scrutiny and they may need to give disclosure of all relevant material to the defence.

iii. Peer Review

109. The Berkeley Protocol recommends peer review to ensure the integrity of written reporting and the conclusions drawn from the available data.\(^{73}\) Although Bellingcat’s Yemen Project investigators work in teams, the GLAN/Bellingcat methodology does not provide for formal peer review of a project’s conclusions. This was raised in the mock hearing by the defence as a potential line of attack and is clearly a point worth bearing in mind going forward wherever OSI analysis and conclusions might be used as evidence in legal proceedings.

110. As outlined by HHJ Korner in the ruling (at paragraph 29), the Criminal Practice Directions list the factors which the court may take into account in determining the reliability of expert opinion, which includes “the extent to which any material upon which the expert’s opinion is based has been peer-reviewed.”\(^{74}\) HHJ Korner’s ruling found that Palmer had met all of the requirements set out therein “with the exception of peer review.”

111. In the debriefing session following the mock hearing, this issue was discussed among the lawyers and investigators. It presented an interesting question because in the normal course of events, Bellingcat’s written reports are generated as a public information source, which could constitute evidence but would more likely be treated as lead information from which expert analysis would be generated on specific items of content, as took place in these mock proceedings. Bellingcat’s reports could thus be strengthened from the outset by building peer review into the process but this would have to be repeated in the event that a distinct expert report is subsequently prepared for legal proceedings, whether by Bellingcat or another OSI analyst. This raises the question of what stage it is best to seek peer review of an analyst’s work.

112. The participants in the debrief accepted that because this is a small field of expertise, experts are likely to need to either draw on peers from within their own organisation or with whom they already have a relationship. It is not uncommon for those seeking experts in legal proceedings to encounter this problem and to have to work within such constraints - the key is to take such steps as would be considered reasonable in the circumstances of the individual case.

---

\(^{73}\) Berkeley Protocol, infra note 2, at para. 209.

\(^{74}\) Criminal Procedure Rule 19A.5.
iv. Types of Expertise Within Bellingcat

113. Eliot Higgins was asked under cross examination whether Bellingcat had sought the assistance of weapons experts or technical experts in satellite imagery. Weapons expertise was not an effective area of challenge for the defence, given that the claims made by Palmer in his report did not extend to the cause of the damage. Satellite imagery is a field of expertise beyond the scope of this exercise, but it is perhaps sufficient to say that there are aspects of satellite imagery analysis in which Bellingcat could be considered to have the requisite expertise, and others in which they do not. This would have to be explored based on the individual circumstances of a case. In every case, the scope of the expertise of the OSI analyst expert should be carefully assessed and additional experts engaged if necessary to ensure a comprehensive expert analysis is presented to the court.

v. Duties on Investigators

114. Questioning by the defence repeatedly raised the question of whether any ‘duties’ or contractual obligations exist requiring investigators to undertake certain actions, such as to follow the Berkeley Protocol or keep records of any systems failures on a given day. Similarly, the defence established through questioning that Bellingcat is not regulated as an investigative organisation (as distinct from a journalistic one). This line of questioning highlights a potential line of challenge in future cases to the credibility and/or consistency of investigations and therefore may prompt organisations like Bellingcat to ‘lock in’ their methodologies by formalising requirements to adhere to the methodology. In relation to regulation, prosecution counsel’s point about the Berkeley Protocol being an attempt to set industry standards may be borne in mind. However, what is ultimately key is whether the principles of evidence are observed, and reference to useful practice guides such as the Berkeley Protocol are only one route to ensuring that this takes place.

115. In this regard, it is noted that the judge and counsel teams recommended that the witness statement of the Bellingcat investigator (in this case, Charlotte Godart) should contain a very detailed, step by step account of the practical application of the methodology, including explanations of the meaning of certain steps where they would not be understood by lay people.

F. THE EXPERT’S ONLINE SEARCH

116. One point worth addressing, is the extent of what the expert would or should look at in the course of their work. This of course will depend on what the expert has been instructed to do – whether the instruction is simply to verify a defined data set or whether they are being asked more widely to confirm whether disproving or contradictory information exists. Generally speaking, as noted above, while the expert would be given formal instructions including a set of the relevant files located by the investigators working with the instructing party, it would not be realistic to expect them to remain offline in verifying the content. This raises the important question of whether the expert witness, in the process of their verification, must themselves
maintain a log of their searches and essentially follow a methodology similar to that used by Bellingcat or envisaged by the Berkeley Protocol. On one hand, if the underlying discovery phase has been exhaustive and objective, it could be said that there is no need for the expert to be so rigorous because they are only likely to uncover material that the investigators have already seen. However, it is also theoretically possible that an expert analyst could discover a new file and wish to refer to it in their report. In that case, it could be problematic if they have not maintained a log of how they came upon the file. This was not tested in these proceedings but is rather raised as a matter for consideration. If possible, it seems prudent for experts to employ their own replicable methodology.

G. THE OTHER VIDEOS

117. As was made clear by the expert report of Frank Palmer and the questioning by the defence, there were other online videos that were used to cross-reference and corroborate the verification of GC/2, including to aid with geolocation. The organisers were unsure how to deal with these extra videos – that is, whether they should have all been introduced as items evidence with equal prominence to CG/2 (and thus subject to the same admissibility test), or otherwise introduced as background or corroborative evidence. There could be risks associated with giving undue prominence to these videos, which were presumptively less probative individually for a range of reasons\textsuperscript{75} and therefore could have been undermined individually more easily by the Defence. This could create a ‘domino effect,’ culminating in a persuasive argument that since the videos being used to assist the geolocation are themselves so unreliable, none of the authentication can be relied on. However, this risk could be mitigated by setting out clearly the same arguments that apply to circumstantial and corroborative evidence more generally. That is, even if individual pieces can be impugned, the judge can be asked to consider the chances of multiple pieces of evidence independently appearing on the internet which support each other, being fabricated. In conclusion, it was recommended that the extra videos be introduced by the investigator (not the expert), and be presented to the Court as a ‘corroborative jigsaw’ in which the weaknesses of the corroborative videos are acknowledged.

118. Logically, this would lead to an individual admissibility decision having to be made about each video, or about the bundle of corroborating videos (depending on the nature of objections by the defence). Given that their probative value is lower individually, there may be scope for some videos to be considered disproportionately prejudicial, for example if they contain violence to civilians. However, such issues could be dealt with, for example by artificially blurring content that is not needed to show the corroborative value of the video.

\textsuperscript{75} For example, one was filmed from further away (Video 1/CG5); another had been posted by overtly Houthi sources (Video 2/CG6).
ANNEX I:
DETAILS OF WITNESS EVIDENCE AT MOCK HEARING
Charlotte Godart: Witness of Fact

1. In her witness statement, Ms. Godart set out how she investigated the incident in question, adhering to the methodology developed by Bellingcat and GLAN as detailed by Mr. Higgins in his statement, and discovered the Exhibit CG/2 video which depicts the moments between the first and second attacks.

2. Ms. Godart described how she conducted her investigation over the course of three days. She detailed the search terms through which she discovered the video and exhibited to her statement a full list of the sources she uncovered. She explained that she entered the link to the Exhibit CG/2 video into Bellingcat’s preservation system and proceeded to analyse its content. She determined that it depicted the location of the airstrike on the day in question and assessed that it captured the aftermath of one large explosion and the occurrence of another. She also determined that the video was genuine and did not identify any signs that it had been embellished. Ms Godart also introduced through her statement a video released by the Coalition which demonstrates some examples of its reconnaissance capabilities.

3. Ms. Godart cross-referenced Exhibit CG/2 against other videos she located that depicted locations in the vicinity of the incident and concluded that the Exhibit CG/2 video depicts an airstrike at the Office of the Presidency in Tahrir, Sana’a City at 15.348216, 44.204964 on 7 May 2018 in the mid-morning; specifically, that it is in two segments, split at 01:10 minutes, and depicts the moments immediately after an airstrike and captures the effects of a secondary airstrike.

Eliot Higgins

4. In his witness statement, Mr. Higgins explained that ‘open source’ evidence is evidence which is available to the public and that ‘online open source investigation’ refers to the collation of pieces of open source evidence so as to arrive at conclusions that would not arise from consideration of the individual pieces of evidence. He explained Bellingcat’s online methods to analyse the significance, reliability or authenticity of open source evidence, namely: (i) discovery, being advanced methods for finding and filtering online content; and (ii) verification, being methods for analysing the significance, reliability or authenticity of the content. He stated that the focus of Bellingcat’s investigations is principally to establish the location and time of specific attacks, and to attempt to establish what occurred by examining the digital evidence.

5. Mr. Higgins explained that audio-visual evidence does not replace witness evidence but is compelling and, once authenticated, speaks for itself. Footage filmed in the aftermath of an attack can capture crucial evidence such as the resulting damage, the cause of the damage, the presence of civilians and civilian items and/or military targets, follow-up airstrike(s) and the location of the airstrike(s).

6. In his statement, Mr. Higgins introduced the methodology developed by Bellingcat and GLAN to increase the reliability of OSI as evidence in courts of law - the methodology followed by Ms. Godart which led her to discover the Exhibit CG/2 video. During the mock
hearing, Mr. Higgins provided further detail about how Bellingcat’s investigators conduct their investigations and, in particular, the methodologies adopted in this case. He explained that the Bellingcat methodology seeks to comply with the Berkeley Protocol on Open Source Investigations and which was developed specifically by reference to international humanitarian law ("IHL") and the use of open source evidence in legal proceedings. The Bellingcat methodology was developed with GLAN to devise a systematic process for both discovering and also archiving OSI. Bellingcat uses a web browser extension called Hunchly which records step by step what the investigator is doing in his/her browser and records it in a case file. Bellingcat also works with Mnemonic to preserve and archive particular links.

7. In his statement and during the mock hearing, Mr. Higgins explained two of the primary analysis techniques used by Bellingcat to authenticate open source material:

- **Geolocation**: the process or technique of identifying the geographical location of a person, object or event through the examination of photographs or videos, and the identifiable buildings or landscape features (mountains, roads) and other stationary objects (e.g. signposts, telephone poles, trees) in them. These objects can be compared with other photographs or videos, satellite imagery and GPS coordinates to confirm where the photograph or video in question has been filmed. Geolocation helps to verify that a piece of footage is authentic and depicts what it claims to depict, by helping to eliminate the possibility that the footage has been staged elsewhere, has been repurposed from another event or has been digitally generated. Geolocation can lead to the identification of satellite images which can show evidence that is relevant to the assessment of whether a violation of IHL has occurred, such as: the extent of damage or destruction of structures, clear signs of civilian activity (for example, cars or market coverings) or other contextual information.

- **Chronolocation**: once the geolocation has been determined, the investigator can use the technique of chronolocation to identify the exact or approximate time at which an incident occurred or at which a piece of audio-visual content was created. One method of chronolocation uses the shadows cast by objects or individuals as a kind of sun dial to measure the length of the shadow to establish the approximate time of day that an image was recorded. Chronolocation helps to verify that video is authentic, matches other information concerning an incident and is internally consistent. It can also be used to narrow down dates of attacks using satellite imagery of changing landmarks because shadow analysis can be used not only to identify the time of day but also the time of year by reference to the path of the sun.

8. During the mock hearing, Mr. Higgins further explained that once geolocation and chronolocation have been completed, the investigator then undertakes further checks to determine whether the video has been staged or repurposed (whether it is from a different time or location), to confirm that there has been no obvious digital alteration and to assess whether parts omitted might mislead the viewer as to its content.
9. In his statement, Mr. Higgins explained the factors relevant to an analysis of the reliability of a piece of video evidence and applied each of them in turn to the Exhibit CG/2 video. He concluded that in his view the video has not been staged or re-purposed (i.e. the footage set up or representing a wholly different incident), nor has it been digitally altered. Accepting that it is possible that the maker deliberately omitted relevant information, he noted that, even if so, that could not affect the fact that the video evidences that civilians were present and that the “skies were clear” at the time of the attack.

10. During the mock hearing, the defence cross-examined Mr. Higgins on the Bellingcat methodology and certain of the issues relating to the reliability of a piece of video evidence. Mr. Higgins stated that Bellingcat is regulated by the Independent Monitor for the Press (IMPRESS) but accepted that there is no independent regulatory body for open source analysis specifically. He stated that no specific qualification is required to undertake open source investigation, instead one can be trained ‘on the job’, and that the methodology remains the same regardless of who is conducting the investigation. Mr. Higgins agreed that there is no ‘industry standard’ in Bellingcat’s particular form of investigation and, as such, there is no duty on Bellingcat investigators to use any particular software in any particular investigation but agreed that the Berkeley Protocol is precisely an attempt to create an objective, properly regulated industry standard for open source intelligence gathering.

11. Defence counsel took Mr. Higgins through the introductory section of the Berkeley Protocol, which states that it adopted an inter-disciplinary approach in its preparation. Mr. Higgins agreed that no assistance was sought from weapons analysis experts during the development of the Bellingcat methodology; he noted that Bellingcat themselves are the requisite experts in satellite imagery software. Mr. Higgins agreed with the Berkeley Protocol’s emphasis on foundational principles of objectivity and accuracy, agreeing that investigations should be free from bias, including expectation bias, which Mr. Higgins described as preconception of what the investigation will show and building the investigation around that, either consciously or unconsciously. As to accuracy, the Berkeley Protocol notes that this can be improved by peer review, which can lead to the identification of weakness in analysis by an investigator. Mr. Higgins accepted that Bellingcat’s open source investigators are under no contractual duty to follow the Berkeley Protocol. He further agreed that the Bellingcat methodology does not impose a duty on investigators to record online system failure(s) on the day(s) they conduct their investigation nor does it provide for mandatory peer review of findings made.

12. In his witness statement, Mr. Higgins noted that the reliability of a video may be affected by parts of the scene which are omitted, for example the omission of a military target when a video is filmed for propaganda purposes, depending on what the video is being adduced to prove. During the hearing, Mr. Higgins agreed that Bellingcat only knows where the video was posted online (on Twitter) and does not know the creator of the video. He agreed that it is possible that the video was filmed by someone connected to the Houthi movement and possible that certain favourable information may have been edited or not filmed. However, Mr. Higgins noted that the video was not being offered as evidence that there were no military

---

76. As noted at paragraph 88 above, in real proceedings this aspect of his analysis would not be included in a witness statement but would instead be addressed through expert evidence.
personnel present, and if there were in fact military targets in the vicinity of the Office of the Presidency which cannot be seen in the video, that would have no impact whatsoever on the reliability of the video as it relates to what it shows of the extent of the damage to the street, the second explosion, weather conditions and the presence of civilians in the vicinity.

13. In his witness statement Mr. Higgins also stated that as part of Bellingcat’s investigation the Exhibit CG/2 video had been cross-referenced with other online material and was found to be consistent with that content. During the hearing, Mr. Higgins explained that this statement referred to satellite imagery online and/or other videos and images from the scene that show details that match the video. The prosecution confirmed that these corroborative videos which formed part of the Bellingcat investigation were exhibited to Ms. Godart’s witness statement. Finally, Mr. Higgins clarified that his statement that, in his opinion, it is not realistic that the Exhibit CG/2 has been fabricated, is based on his knowledge of the level of complexity that would be required to fabricate a video of this kind, which would be immense in Mr. Higgins’ experience of examining several thousand of these types of conflict videos since 2011.

Frank Palmer: Expert Witness

14. Mr. Palmer was engaged as an independent expert by the prosecution, instructed to assess the location and time of the events depicted in the Exhibit CG/2 video and to make an assessment of its authenticity. His expert report set out in detail the step-by-step process he undertook to verify the Exhibit CG/2 video, demonstrating how he used online open source investigation analysis methods to ascertain the location and time of the filming of the video. The prosecution did not provide Mr. Palmer with the suspected date, time or location of the incident for him to confirm in his analysis; he was only provided with the suspected date range and the time and location of the events depicted in the video were left to him to ascertain through his analysis.

15. Mr. Palmer’s expertise and qualifications to undertake this analysis were set out at the beginning of his expert report and were addressed in further detail during the mock hearing. In summary:
   a. Since 2016, Mr. Palmer has conducted investigations for ‘OSINT REPORTS’, first as a volunteer and, since 2018, as a full-time senior investigator and analyst;
   b. Mr. Palmer has two further years’ of investigations experience (2016 to 2018) in cyber threat intelligence analysis specialising in the use of OSI to identify and assess threats, with Digital Shadows.
   c. Mr. Palmer has conducted such investigations for over five years, including as a consultant to national police forces and for United Nations investigative mechanisms.
   d. Mr. Palmer has a background in the military, including three years as a regular infantry officer and four years as a reservist and including an operational tour, which experience has given Mr. Palmer an understanding of the effects of small arms. Mr. Palmer also has a background as a Class 3 Operational Engineer during which he received training
in demolitions and explosives. Mr. Palmer accepted during the hearing that bombs and missiles launched from aircraft were a specialist topic in the military which he had not undertaken, but noted that he does have experience of this from his work examining similar videos.

e. Mr. Palmer has a Masters degree in Conflict Security and Development from Kings College London. In particular, one module lasting 6 months focused on the use of open source material and identification of whether an image was genuine.

f. Mr. Palmer was introduced to techniques such as geolocation whilst in the army and now teaches them himself.

16. In giving evidence, Mr. Palmer accepted that, as an expert witness, he owed a duty to the court and not to the party instructing him, that he had a duty to be objective, and that he had a duty to disclose any material relied upon in his analysis and any which might undermine his conclusion.

17. Mr. Palmer’s expert report detailed his analysis of the Exhibit CG/2 video, including:
   a. the sequence of events (illustrated with stills taken from the video);
   b. his use of “chronolocation” i.e. “the technique of identifying the exact or approximate time at which an incident occurred or at which a piece of audio-visual content was created”;
   c. his use of “geolocation” i.e. “the process or technique of identifying the geographical location of a person, object, or event”; and
   d. cross-referencing with other content for corroboration and consistency including internal consistency.

18. Mr. Palmer concluded in his expert report that the strike took place no earlier than 10.24 a.m. and no later than 10.44 a.m. in the vicinity of the Office of the Presidency. During the hearing, he described in further detail his use of chronolocation and geolocation techniques to establish this conclusion. He explained that as the sun moves through the sky the length of shadows change, such that it is possible to establish approximate time by analysing the length of the shadow as proportionate to the object that is casting the shadow, as well as analysing the angle of the shadow. In order to mitigate the effects of variable factors such as the type of lens used for filming or rubble on the ground that may affect the length of the shadow, the analysis was carried out eight times and a mean estimated time calculated. Mr. Palmer testified that he is confident that the mean estimated time of 10:33 a.m. contained in his report is correct because if the analysis is conducted using a time 30 minutes earlier or 30 minutes later the shadow is either too long or too short to be commensurate with the shadow depicted in the Exhibit CG/2 video. Mr. Palmer confirmed that his analysis also included comparison with other online material published around the same time, including a tweet at 10:44 a.m. stating that a strike was occurring “now”.

---

77. Criminal Procedure Rule 35.3 dictates that (1) It is the duty of experts to help the court on matters within their expertise; and (2) This duty overrides any obligation to the person from whom experts have received instructions or by whom they are paid.
19. The location of the strike was not disputed by the defence but was in any event analysed by Mr. Palmer. By looking at the buildings in the video and cross referencing them against buildings in satellite imagery, Mr. Palmer was able to satisfy himself as to the location of the events depicted in the video, being the Office of the Presidency in Sana’a.

20. During the hearing Mr. Palmer also testified that in his view there was no indication of manipulation of the video. He accepted that he is not a digital forensic expert, which he defined as “looking at, say for example the manipulation of the metadata of an image or the image itself.” However, he explained that when Bellingcat downloaded the video from Twitter they ensured that a ‘hash’, or digital fingerprint, was produced which could then be compared against other hashes of the same video at a later date, which would identify whether any changes had been made. Mr. Palmer was able to confirm that no changes had been made to the Exhibit CG/2 video that was presented to him for analysis. In his statement, Mr. Palmer referred to the metadata and EXIF, (Exchangeable Image File) of the video but clarified during the hearing that he was referring to the video provided to him by Bellingcat; any such metadata from the original filmed video would have already been stripped when it was uploaded online and was thus not available to him. However, Mr. Palmer explained that EXIF and metadata are only one part of the verification process and are in fact not always reliable. Certain aspects of geolocation and chronolocation are in fact more reliable: some of the information that would be contained in such metadata, such as the time and location at which the video had been filmed, is precisely the information that can be verified through open source analysis such as geolocation and chronolocation, as set out in his report. He testified that his geolocation analysis showed nothing standing out in the video itself as evidence of manipulation, comparison with other videos of the incident showed no inconsistencies, nor in his view was there sufficient time to perform manipulation on the video between the attack taking place and the video being uploaded to Twitter, which occurred at 7.45 p.m. on the same day.

21. The defence addressed the provenance of the video including how Ms. Godart of Bellingcat located it. Mr. Palmer accepted that algorithms outside of the searcher’s control are built into search engines which can control what the searcher uncovers, for example the number of views a site has already had or the number of viewers on a particular Twitter account. He explained that Google will display the results that its algorithms have determined to be the most relevant to the particular searcher based on the data Google has collected about that person. Mr. Palmer therefore accepted that there is no such thing as a “neutral” search but emphasised that open source investigators carry out measures to mitigate this as set out in the Berkeley Protocol, (a reference to that part of Section VI entitled “Bias”). Mr. Palmer emphasised that algorithms do not edit or change the content of each result itself, nor do they omit results, as distinct from displaying them in a particular order.

22. Mr. Palmer accepted during the hearing that we do not know who filmed the video and so do not know what biases may have been in the mind of that person. Mr. Palmer stated that he would note during investigation if the uploader appeared to only upload material supportive of one side of a conflict or unreliable material or have made inaccurate claims. However, regardless of any bias of the person who filmed the video, the content of the video itself can be verified through geolocation and chronolocation such that Mr. Palmer would still consider
the video to be relevant to the proceedings. He confirmed in giving evidence that even if
the original poster of the video to Twitter is biased in favour of the Coalition or against the
Houthis, or had in the past exaggerated casualties in earlier tweets, that does not make the
video less likely to be an accurate depiction of the events of 7 May 2018.

23. In giving evidence, Mr. Palmer testified that the Exhibit CG/2 video appears to contain two
separate pieces of video that have been spliced together and uploaded in one video. He accepted
that it was possible the video had been altered and that, given the reverse order of events,
it had by definition been edited. However, he clarified that there is a qualitative difference
between editing, which he defined as chopping and changing the video, and manipulation,
which he defined as malicious intent in changing the video to alter what it shows for example
the addition of computer-generated imagery. Mr. Palmer reiterated that while the video has
been edited, he does not believe it has been manipulated.
CREDITS

Expert report of Frank Palmer:
   Nick Waters

Underlying investigation:
   Charlotte Godart, Nick Waters

Live witness evidence:
   Eliot Higgins, Nick Waters

Preparation of papers:
   Dan Robinson (Red Lion Chambers)

Student researchers:
   Lucy Brown, Casey Gilroy, Rhiannon Smith, Ryan Lysycia and Eleanor Proctor

Legal teams:
   Helen Malcolm QC of Three Raymond Buildings, Andrew Cayley QC of Temple Garden Chambers, Joshua Kern of 9 Bedford Row and Shina Animashaun of Garden Court Chambers

Judge:
   Her Honour Judge Joanna Korner

Legal research and advice underlying the methodology:
   Thanks to Dan Robinson, Emilie Pottle, Yvonne McDermott, Ioannis Kalpouzos, Paul Clark

Live interpretation:
   Hanady Assaf and Daniele Meouchy

Video editing and miscellaneous written translation:
   Rabie Mustapha

Written Arabic translation:
   Rabie Mustapha

GLAN, Bellingcat and Swansea University thank the following people for their review of this analysis:
   Alexa Koenig
   Wendy Betts
   Yvonne Ng
   Keith Hiatt
   Joshua Kern

Special thanks to Tara Vassefi, Raja Althaibani, Rawan Shaif