# Putting Principles into Practice: Reflections on a Mock Admissibility Hearing on Open Source Evidence

*Dearbhla Minogue, Siobhán Allen, Charlotte Andrews-Briscoe and Yvonne McDermott*

## I. Introduction

Digital open source evidence (that is, evidence on the internet that anyone can access, by observation, purchase or request[1]) plays an ever-increasing role in accountability processes for international crimes. Before the International Criminal Court (ICC), several cases have introduced evidence of this nature, including Facebook posts;[2] videos;[3] images,[4] and satellite imagery.[5] In the domestic prosecution of international crimes, too, several recent cases have relied upon videos found on YouTube;[6] photographs posted to Facebook,[7] and Telegram messages,[8] amongst others.[9] A growing body of scholarly literature examines the relevant legal, ethical, and practical considerations for the discovery, use and admission of such evidence in some detail.[10]

---

[1] Human Rights Center, University of California, Berkeley/UN Office of the High Commissioner for Human Rights, *Berkeley Protocol on Open Source Investigations* ('Berkeley Protocol'), 1 December 2020 6–7.

[2] *Prosecutor v Bemba et al (Decision on 'Prosecution's Fifth Request for the Admission of Evidence from the Bar Table')* ICC-01/05-01/13-1524 (14 December 2015); *Prosecutor v Bemba et al (Prosecution's Fifth Request for the Admission of Evidence from the Bar Table)* ICC-01/05-01/13-1498 (30 November 2015) paras 17–18; *Prosecutor v Yekatom and Ngaissona (Transcript)* ICC-01/14-01/18-T-023 (29 March 2021) 69.

[3] Most notably, *Prosecutor v Al-Werfalli (Warrant of Arrest)* ICC-01/11-01/17-2 (15 August 2017) paras 11–22 and *Prosecutor v Al-Werfalli (Second Warrant of Arrest)* ICC-01/11-01/17-13 (5 July 2018) paras 17–18, but also: *Prosecutor v Gbagbo and Blé Goudé (Transcript)* ICC-02/11-01/15-T-117 (7 February 2017); *Prosecutor v Al Mahdi (Judgment and Sentence)* ICC-01/12-01/15-171 (27 September 2016).

[4] *Prosecutor v Said (Transcript)* ICC-01/04-01/21-T-004 (12 October 2021) 17.

[5] *Prosecutor v Al Hassan (Transcript)* ICC-01/12-01/18-T-027 (21 September 2020).

[6] eg Court of Appeal in The Hague, *Case No 2200128321* (6 December 2022) <www.recht.nl/rechtspraak/uitspraak/?ecli=NL:GHDHA:2022:2421> accessed 19 December 2022; Court of Appeals for Western Sweden, *Chief Prosecutor v Hassan Mostafa Al-Mandlawi and Al Amin Sultan* (Judgment 30 March 2016).

[7] eg Södertörn District Court, *Prosecutor v Mouhannad Droubi* (Judgment 26 February 2015); Örebro District Court, *Prosecutor v Saeed* (Judgment 19 February 2019).

[8] District Court of The Hague, *Prosecutor v X*, Case Nos 09/748012-19 and 09/748012-19-P (joined at the hearing, 29 June 2021).

[9] See further, Karolina Aksamitowska. 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands' (2021) 19 JICJ 189–211.

[10] Amongst many others see: the contributions to a 2019 JICJ Special Issue edited by Daragh Murray, Yvonne McDermott, Alexa Koenig and Emma Irving, entitled 'New Technologies and the Investigation of International Crimes'; Rebecca J Hamilton, 'User-Generated Evidence' (2018) 57(1) Colum J of Transnat'l L 1; Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2018) 41(2) Fordham Int'l L J 283; Sam Dubberley, Alexa Koenig and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability* (OUP 2020); Daragh Murray, Yvonne McDermott and Alexa Koenig, 'Mapping the Use of Open Source Research in UN Human Rights Investigations' (2022) 14 Journal of Human Rights Practice 554.

Reflecting on the theme of this volume of international criminal law before domestic courts, it is worth noting that most relevant domestic cases availing of open source evidence have been heard in legal systems broadly hailing from the inquisitorial or Romano-Germanic legal tradition. Whilst the adversarial-inquisitorial dichotomy is an oversimplification, as there is variation within and between countries' individual legal systems,[11] we can note that in the inquisitorial (or civil law) legal tradition, there tends to be a 'free proof' approach to the admission of evidence, whereby there are only certain rare exceptions where evidence will be excluded. On the other hand, legal systems from the common law or adversarial legal tradition tend to have stricter rules on the admission of evidence, designed to prevent prejudicial material with limited probative value from reaching the lay jury.

Three of the authors of this piece are practicing lawyers working for GLAN, the Global Legal Action Network, a non-governmental organisation which has worked extensively on open source investigations in close collaboration with the investigative journalism organisation, Bellingcat. GLAN and Bellingcat's initial collaboration centred on international crimes committed in Yemen,[12] while most recently they have broadened their focus to investigate atrocity crimes in Ukraine.[13] The fourth author is a legal academic specialising in the law of evidence, with a particular interest in evidence as it relates to international crimes.[14] All four are based in the United Kingdom. Given our training in the common law tradition, we were frequently asked about whether open source evidence might be admissible in a domestic case in England and Wales trying international crimes. The simple answer was that we could not be sure, as there had been no case of this kind to date.

Over time, GLAN and Bellingcat had, with input from a wide range of legal and investigative experts,[15] developed a state-of-the-art methodology designed with justice and accountability processes in mind.[16] This methodology, which is still evolving, aims to identify, preserve, and parse content in such a way that investigators and lawyers can examine how it was discovered and the steps that were taken in verifying it. As a result, the idea came about that we could test the methodology through an adversarial mock *voir dire* hearing into the admissibility of a piece of

[11] John Jackson, 'Finding the Best Epistemic Fit for International Criminal Tribunals: Beyond the Adversarial-Inquisitorial Dichotomy' (2009) 7(1) JICJ 17; Antonio Cassese, *International Criminal Law* (2nd edn OUP 2008) 329.
[12] The Yemen Project, <https://yemen.bellingcat.com> accessed 19 December 2022.
[13] See GLAN, 'Methodology for Online Open Source Investigations' <www.glanlaw.org/online-open-source-methodology> accessed 19 December 2022.
[14] See *OSR4Rights,* 'Team' <https://osr4rights.org/team/> accessed 19 December 2022.
[15] See the acknowledgements in Annex X of the Methodology (n 13).
[16] Preamble, Methodology, ibid.

evidence discovered and verified using the methodology, which would also give some insight into how the courts of England and Wales might approach such evidence.

This chapter introduces the mock admissibility hearing exercise and the judgment rendered in 2021, both of which can be found online in full.[17] Part II sets out the exercise itself, briefly outlining the fictional case, evidence, and actors involved, the main arguments put forward by the parties, and the judge's ruling. Part III outlines the main lessons learned from the exercise, including insights on the nature of online open source information as evidence, and whether an open source investigator can be an expert witness under the law of England and Wales. It also reflects on the key insights that shaped later iterations of the methodology, the current version of which was made publicly available in December 2022.[18]

# II. The Mock Admissibility Exercise

## A. Designing the Exercise

### 1. Fictional Underlying Case

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 (fictional) 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. In the fictional scenario, GLAN received a tip-off that credibly suggested that the defendant was the pilot responsible for the airstrike. It is important to note that the incident around which this fictional scenario was framed was real – in other words, the Office of the Presidency was bombed by the Saudi-led coalition on 7 May 2018, and the video forming the subject matter of the exercise is a real video that was posted to social media in the aftermath of that bombing – but the other elements of the scenario were fictional for the purposes of the exercise.

[17] *Putting Principles into Practice: Mock Admissibility Hearing on Open Source Evidence – Part 1, The Hearing*, 19 February 2021 <www.youtube.com/watch?v=dq_m2POiVdw> and *Putting Principles into Practice: Mock Admissibility Hearing on Open Source Evidence – Part 2, The Judgment* (16 March 2021) <www.youtube.com/watch?v=-yVgbKTEtMM&t=3s> accessed 19 December 2022. This chapter is closely based on a public report of the exercise: GLAN, 'Putting Principles into Practice: Testing Open Source Video as Evidence in the Criminal Courts of England and Wales' (2022) <www.glanlaw.org/oosi-reports> accessed 19 December 2022.

[18] The methodology is accessible online at (n 13) and Bellingcat, 'What is Bellingcat's J&A Unit?' (15 December 2022) <www.bellingcat.com/what-is-bellingcats-ja-unit-december-2022/> accessed 19 December 2022.

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.

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.[19]

The defence had made an application to exclude the Exhibit CG/2 video evidence located by Bellingcat.

## 2. Evidence

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.

Digital evidence:

a. A video, Exhibit CG/2, submitted by the prosecution to depict the 7 May 2018 airstrike.

[19] Under the ICCA, only UK nationals and residents can be prosecuted. The defendant's residency was therefore invented to meet with this requirement. There is no jurisdiction under the Geneva Conventions Act 1957 due to the classification of the Yemen war as a non-international armed conflict.

b. A video showing that the Coalition had 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.

Further evidence drafted and presented included:

c. Expert report of investigator, 'Frank Palmer' (see part 3 below).

d. Witness statement of Bellingcat founder, Eliot Higgins.

e. Witness statement of Bellingcat investigator, Charlotte Godart.

Evidence not developed or reviewed, but agreed for the purposes of the exercise, included:

f. 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.

g. 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.

## 3. Actors

The relevant actors in the mock exercise were as follows.

Real persons:

- **Global Legal Action Network (GLAN):** A non-profit organisation that pursues innovative legal actions across borders.
- **Bellingcat:** 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.
- **Charlotte Godart:** 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.

- **Eliot Higgins:** 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.
- **Judge:** Her Honour Judge Joanna Korner CMG KC. At the time of the exercise, Judge Korner was serving as a judge at Southwark Crown Court of England and Wales; she is now a judge at the International Criminal Court.
- **Prosecution (the Crown Prosecution Service):** Helen Malcolm KC of Three Raymond Buildings and Joshua Kern of 9 Bedford Row.
- **Defence:** Andrew Cayley KC of Temple Garden Chambers and Shina Animashaun of Garden Court Chambers.

Fictional persons:

- **'Frank Palmer':** A fictional Senior Investigator and Analyst at the fictional 'OSINT Reports', a company providing expert analysis of open source content, online open source investigation training to criminal investigators, and engaging in independent journalism. In the exercise, he had fictionally been engaged by the Crown Prosecution Service as an independent expert to verify the authenticity of the Exhibit CG/2 video; the content and findings of the expert report are, however, a real analysis of the video and set out precisely the techniques that an expert would use in real circumstances. Frank Palmer was played by Bellingcat analyst Nick Waters, and his professional credentials and background were identical to those of Waters.
- **'Dr Althaibani':** Fictional medical doctor who treated civilians injured and killed on Tahrir Street and provided witness evidence to SO15 during its investigation. He did not appear in the proceedings.
- **Defendant:** '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.

## B. The Hearing

### 1. Overview

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.

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 several 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.

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 on whether to allow the evidence into the fictional main proceedings before a jury.

On 16 March 2021, HHJ Korner handed down her reasoned judgment orally in a second live webinar.[20] Given the fictitious nature of the exercise, the decision would, of course, 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 open source information is put before it.

## 2. Prosecution and Defence Arguments

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 video, 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, and the uploading of the video to Twitter stripped it of its original metadata.

### *a) Prosecution*

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.

When interviewed by police, the defendant eventually admitted to carrying out the mission, but claimed that it took place at 7 am 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.

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

[20] *Putting Principles into Practice: Mock Admissibility Hearing on Open Source Evidence – Part 2* (n 17).

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.

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, and that the courts should not decline to admit a particular form of evidence simply because it is new.

The prosecution argued that proof of provenance 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.

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.

Finally, the prosecution argued that pursuant to Section 78 of the Police and Criminal Evidence Act 1984 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, with appropriate warnings if necessary.

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

a. the video was admissible as real evidence subject to proof of provenance/retrieval;

b. 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";

c. the examination by Mr Palmer found no reason to doubt its authenticity;

d. 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

e. Mr Palmer had the required experience and expertise to conduct such an analysis.

### *b) Defence*

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.

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.[21] The defence argued that the Exhibit CG/2 video should be excluded from evidence because it is neither authentic nor reliable given that:

a. it is not the original video nor is it known which iteration thereof it purports to be;

b. 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;

[21] In this mock hearing, although the original video was still available on Twitter, the defence did not specifically request that the social media company disclose information relevant to the evidence, 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.

c. it has been edited and/or manipulated and the original metadata is not available; and

d. 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.

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:

a. his opinion and conclusions were based on the data from the video which is fatally flawed because the video is not authentic;

b. he did not confine himself to his area of expertise and therefore commented outside his expertise;

c. he drew conclusions, some of which are for the jury; and

d. he was not independent or objective.

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

> [i]n 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.

## 3. Evidence Provided

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.

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.[22]

## 4. The Ruling

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

### *a) Open Source Analysis as Expert Evidence*

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).

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.[23]

The expert must provide an opinion which is objective and unbiased and within his/her area of expertise.[24] In determining the reliability of expert opinion, the Court may take into consideration factors including:

---

[22] Full details of the evidence provided by both witnesses of fact and the expert witness can be found in Annex I of the *Putting Principles into Practice* report (n 17).
[23] Criminal Practice Directions 2015 para 19A.1.
[24] Criminal Procedure Rules 2020 Part 19.

a. the nature of the data on which the expert's opinion is based;

b. the safety or otherwise of inferences drawn;

c. the nature of methods used;

d. the extent to which any material upon which the expert's opinion is based has been peer-reviewed;

e. the extent to which the expert's opinion is based on material falling outside the expert's own field of expertise; and

f. whether the expert's methods followed established practice in the field.[25]

HHJ Korner considered the domestic and international legal authorities relied on by both parties. She briefly addressed the position at the ICC, 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.[26] 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.[27] 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.[28]

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.[29]

---

[25] Criminal Practice Directions 2015 para 9A.5.
[26] Rome Statute of the International Criminal Court (adopted on 17 July 1998, entered into force on 1 July 2002) 2187 UNTS 3 art 69(4); *Prosecutor v Katanga and Ngudjolo (Decision on the Prosecutor's Bar Table Motions)* ICC-01/04-01/07-2635 (17 December 2010) para 15.
[27] Ibid para 24(d).
[28] *Prosecutor v Al Werfalli* (*Second Warrant of Arrest*) (n 3) para 18.
[29] See eg *Prosecutor v Yekatom and Ngaïssona (Initial Directions on the Conduct of the Proceedings)* ICC-01/14-01/18-631 (26 August 2020); *Prosecutor v Al Hassan (Decision on the Conduct of Proceedings)* ICC-01/12-01/18-789 (6 May 2020) Annex A; *Prosecutor v Ongwen (Initial Directions on the Conduct of Proceedings)* ICC-02/04-01/15-497 (13 July 2016); *Prosecutor v Ntaganda (Decision on the Conduct of Proceedings)* ICC-01/04-02/06-619 (2 June 2015); *Prosecutor v Katanga and Ngudjolo*

Turning to English law on the issue, HHJ Korner cited the case of *R v Robb*,[30] 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.[31] 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.'[32] 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.

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'[33] 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'[34]). She concluded that,

*(Directions for the Conduct of the Proceedings and Testimony in Accordance with Rule 140)* ICC-01/04-01/07-1665-Corr (1 December 2009).

[30] [1991] 93 Cr App R 161.

[31] Ibid para 164.

[32] *Myers & others v The Queen* [2016] AC 314 para 58.

[33] Id.

[34] *R v Robb* (n 30) para 166.

with the exception of peer review, Mr Palmer fulfils the criteria set out in Part 19 of the Criminal Practice Directions.[35]

### *b) Admissibility of the Exhibit CG/2 Video*

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.

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.

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.[36] HHJ Korner also referred to two further cases which addressed the admission into evidence of anonymous pieces of evidence.[37] 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.[38] 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.[39] In the second case, the Court held that documents of unknown authorship located

---

[35] Criminal Practice Directions para 19A.5.
[36] *Sapporo Maru (Owners) v Statue of Liberty* [1968] 1 WLR 739.
[37] 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.
[38] *R v Murphy* (n 37) para 61.
[39] Id.

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.[40] 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.

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

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

b. *Authenticity:* the Exhibit CG/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.

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;

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.

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

[40] *R v Amjad* (n 37) para 35.

appropriate directions and warnings in respect of the drawbacks of the video that had been identified during the *voir dire* hearing.

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.

## III. Analysis and Lessons Learned

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)[41] as evidence in future. In summary, the exercise provided key insights into the following areas, discussed in detail below:

a. The categorisation of OAVC as evidence and the concept of authenticity (and reliability);
b. The importance of tailoring claims made on the basis of items of OAVC;
c. Open source investigative analysis as expert evidence; and
d. The investigative process followed by Bellingcat.

### A. The Categorisation of OAVC Evidence and the Concept of Authenticity

OAVC is documentary evidence,[42] and as such, like all documentary evidence, must be authenticated before it can be admitted into evidence in England and Wales.[43] A document is anything in which information of any description is recorded.[44] Authentication is 'about showing that the document is what it is claimed to be'.[45] 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 were insufficient evidence of authenticity, it would plainly be unfair to admit this

[41] 'Online audio-visual content (OAVC)' is the preferred term to refer to any audio-visual content found online, because it is a broader category than user-generated content, but narrower than online open source information.
[42] This is also the case at the international level. See Freeman (n 10) 297.
[43] For a discussion as to the threshold for admission into evidence, see below and, in this specific context, see Michael O'Floinn and David Ormerod, 'Social Networking Material as Criminal Evidence' (2012) 7(7) CLR 486.
[44] 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.
[45] *ASIC v Rich* [2005] NSWSC 417 para 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.

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.[46] 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 part 4.b above, which lists the reasons given by the judge for her finding in this regard).

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.[47] For example, in *R v Quinn*, 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.[48] 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 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.

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

[46] 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.
[47] *R v Aiden Quinn* [2011] NICA 19 para 48.
[48] Id.

> 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… Kelly LJ stated 'Any attack thereafter could only go to weight. The issue of weight could embrace many things – further inquiries 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…The film may be proved authentic by comparing it with films taken by others of the same event, taken at the same time or even at a different time.'

As was seen throughout the remainder of the ruling, HHJ Korner applied this framework to the Exhibit CG/2 video, subject to the quality of the evidence adduced as to the video's authenticity.[49]

Another issue worthy of discussion is how open source video evidence 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'.[50] 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.*'[51]

The crux of the prosecution's argument was thus that the material could 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 were 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

---

[49] It can be useful to think of authenticity as a fact to be proved. 'Facts in issue' can be differentiated from 'facts relevant to the issue'. The former are 'principal facts' that are necessary by law to establish the claim being made. The latter, sometimes referred to as 'evidentiary' facts, are facts that indirectly go to facts in issue. See *Phipson on Evidence* (20th edn Sweet & Maxwell 2021) paras 7-02 to 7-04. Thus, facts in issue that this video could prove if shown to be genuine are the time of the airstrike, the extensive damage, that there were civilians present at the location of the airstrike when the defendant attacked it; and that the skies were clear. The manner in which open source investigators obtain and store evidence, along with whether the content is authentic, are facts indirectly relevant to the issue of whether the facts in issue took place, because this information is needed to assess the reliability of the evidence establishing those principal facts.

[50] *Phipson on Evidence,* ibid para 1-14.

[51] Id. (emphasis added, footnote omitted).

of its contents.[52] 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 two 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.[53]

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.[54]

---

[52] See also below in respect of hearsay.

[53] Berkeley Protocol (n 1) para 177. 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, Alexa Koenig and Daragh Murray, 'Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations' (2021) 19(1) JICJ 85, 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.

[54] 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

If open source evidence was 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',[55] 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.[56] For example, if person A tells the court that person B told her he saw 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.[57] There are thus two questions to ask in respect of open source information 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 whilst the definition of 'statement' is reasonably broad, it does not extend to the capture of photographic or video evidence.[58]

However, online videos and photographs are often accompanied by, or can contain, hearsay. For example, a Tweet posting a video may also contain claims about fatality numbers or about which party was responsible. 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.

Nevertheless, 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

---

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* n 50 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.

[55] Criminal Justice Act 2003 Section 114(1).

[56] Criminal Justice Act 2003 Section 115(2).

[57] 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.

[58] *Dodson* [1984] 1 WLR 971; *Fowden* [1982] Crim LR 588; *Grimer* [1982] Crim LR 674; as per Blackstone's Criminal Practice 2021 F.16.11.

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.[59] In so doing, the prosecution relied on *res gestae,* a common law exception to the rule against hearsay which is preserved by Section 118 of the Criminal Justice Act. Under this provision, a hearsay statement is admissible where it 'was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion can be disregarded'. Eliot Higgins had suggested in his witness statement that Bellingcat had not relied on the statements made in the video, which suggested a limited probative value. The judge accepted that the statements in the video did fall within the *res gestae* provisions but declined to admit them on the basis that any probative value they may have would be outweighed by their prejudicial effect.

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 did not appear 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 Part III.E.2 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 fairness of the admission) of each is only clear by reference to the package as a whole.

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.[60] 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,

[59] 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.
[60] Freeman (n 10) 296, citing *Prosecutor v Bemba (Judgment)* ICC-01/05-01/08-3343 (21 March 2016) para 39.

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.

In the case of the Exhibit CG/2 video, the claims 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.[61] 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 OAVC 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.

Like authenticity, the final analysis of reliability is a matter for the jury,[62] 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[63] 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.

## B. The Importance of Tailoring What Claims Are Made About the Video

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

[61] Subject, as noted elsewhere in this report, to further fact and witness evidence on this point.
[62] *Haw Tua Tau v Public Prosecutor* [1982] A.C. 136 PC 151 'Matters such as the reliability of evidence and resolution of disputed evidence are generally matters for the jury'.
[63] 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.

because it would be unlikely for a video such as this to be allowed into evidence if there were 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.

For the purpose of the exercise, the organisers introduced evidence from a fictional 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,[64] the organisers also included in evidence the defendant's 'admission' in police custody to having carried out the airstrike. The additional evidence introduced by the organisers to supplement the central open source evidence was purposefully left incomplete, so that the video could not be said to be purely corroborative of facts already established by the witness evidence (which might have made the prosecution's task too easy). The intention was for the evidence as a whole to be balanced and create room for an arguable case on both sides.

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:[65]

a. Evidence that the defendant was responsible for the attack and carried it out on purpose;
b. Evidence that the people killed and injured were protected from attack under the law of armed conflict (i.e. that they were civilians); and
c. 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.[66]

[64] 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 'Joint Incidents Assessment Team Issues Statement Regarding Allegations against Coalition Forces 2' (Saudi Press Agency, 19 August 2020) <www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2123605> accessed 19 December 2022.

[65] 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 <www.icc-cpi.int/nr/rdonlyres/336923d8-a6ad-40ec-ad7b-45bf9de73d56/0/elementsofcrimeseng.pdf> accessed 19 December 2022.

[66] 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.

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.

## C. Open Source Investigative Analysis as Expert Evidence

One of the most instructive parts of the exercise was examining the issue of whether open source investigation and analysis could constitute expert evidence.

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) 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.[67]

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 open source information (OSI) analyst could meet the criteria, the discussion is instructive and provides guidance for the future use of OSI analysts as expert witnesses.

[67] Criminal Practice Directions 2015, part 19 para 19A.1.

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 has propagated the consistent position that OSI analysis can be performed by anyone – it is easy to learn. Indeed, this is one of the reasons the field of practice, whether in a journalistic or evidentiary setting, is seen as democratising 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,*[68] 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. Some 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:

> 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

[68] *R v Robb* (n 30).

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)

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….'

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.'

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 Korner 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.

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.

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* have been gained by any person on the jury, it had 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*.

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'.

## D. The GLAN/Bellingcat Methodology

The methodology followed by Bellingcat (which this exercise was designed to test) was created in collaboration with lawyers at GLAN with knowledge of the core evidentiary principles. It was developed as a 'light touch' methodology that investigators 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:

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

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.[69] 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.

[69] Berkeley Protocol (n 1).

## 1. Bias

Objectivity is a fundamental requirement of all fair and accurate investigations, including OSI investigations.[70] 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. Access bias did not arise in the context of the mock hearing.

All of the parties appeared to accept that the use of internet searches could be affected by unavoidable technical bias. McDermott and others 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.'*[71]

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

---

[70] Berkeley Protocol (n 1) para 27.

[71] McDermott and others (n 54). The Berkeley Protocol (n 1) 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.'

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,[72] 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. Indeed, the draft methodology published in December 2022 refers to 'algorithmic effects' rather than 'algorithmic bias', reflecting the fact that algorithmic amplification can have positive effects in enabling skilled online investigators to find the relevant material they need. 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.

Cognitive bias refers to 'any distorted evaluation of information by humans'.[73] 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 rejecting information that counters them'.[74] 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.

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. Nonetheless, 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.

---

[72] 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.

[73] McDermott and others (n 54) citing Dan Simon, *In Doubt: The Psychology of the Criminal Justice Process* (Harvard University Press 2012) 38.

[74] McDermott and others, ibid, set out a range of the most prevalent cognitive biases, of which confirmation bias is one.

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.

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.

## 2. Chain of Custody

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.[75] 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.[76]

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 takedowns 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

[75] See, eg, Association of Chief Police Officers, 'ACPO Good Practice Guide for Digital Evidence', in particular Chapter 2: 'Principles of Digital Evidence' (March 2012) <www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf> accessed 19 December 2022.

[76] 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.

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.

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 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.

## 3. Types of Expertise Within Bellingcat

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.

## 4. Duties on Investigators

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.

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.

## E. Final Remarks

### 1. The Expert's Online Search

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. 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. 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.

### 2. The Other Videos

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 CG/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 of 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[77] 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. Ultimately, 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.

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.

## IV. Conclusion

This chapter presented the background to a mock admissibility exercise on a piece of online open source information, which was designed to test an innovative methodology created by Bellingcat and the Global Legal Action Network through a rigorous adversarial process. While the findings of the exercise are by no means binding on any court or judge in any jurisdiction, the exercise did

[77] For example, one was filmed from further away (Video 1/CG5); another had been posted by overtly Houthi sources (Video 2/CG6).

provide some fascinating insights on how two key questions might be approached in future cases trying international crimes in the courts of England and Wales.

The first question was whether an OSI analyst could be an expert witness under the English law definition, and whether their evidence could constitute expert evidence, as such. While the techniques of verification do not require a particular academic degree or membership of a professional organisation, the judge in this exercise determined that the investigator could be an expert witness. Through practical experience, an OSI analyst can assemble what can be properly regarded as a body of specialised knowledge that would not otherwise be available to the tribunal of fact, and thus may serve as an expert.

The second question concerned the nature of online audio-visual content, which was determined to be in the nature of real evidence (i.e. it did not constitute hearsay). As such, the judge determined that there were concerns about the authenticity and reliability of the video introduced in the exercise. Nevertheless, she ruled that the authenticity and reliability of the video were established by other evidence on record including the expert report. The judge was therefore satisfied that the video fulfilled the criteria for admission into evidence, but noted that, in a real case, she would give the jury instructions and warnings in respect of the drawbacks to the evidence that had been identified and how they should treat it. A mock jury study would be a logical next step to examine how lay factfinders might reason about this type of evidence in conditions of uncertainty.

Ultimately, the exercise proved instructive in strengthening the GLAN/Bellingcat methodology, by providing key insights on issues of bias, chain of custody, peer review, and investigators' duties, which were incorporated into a later iteration of the methodology. We hope that it will be useful to investigators, legal professionals, and others in considering how open source investigations might be challenged and scrutinised in future international criminal trials, be it in domestic or international courts.