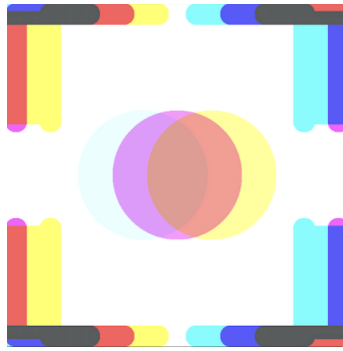


BELLINGCAT GLOBAL LEGAL ACTION NETWORK



JUSTICE AND ACCOUNTABILITY UNIT

METHODOLOGY FOR ONLINE OPEN SOURCE INVESTIGATIONS INTO INCIDENTS TAKING PLACE IN UKRAINE SINCE 24 FEBRUARY 2022

Foreword

Digital media derived from the internet offers significant potential as evidence of atrocity crimes, but carrying out online investigations in a manner that courts will recognise is challenging. This methodology was developed by GLAN and Bellingcat in response to that challenge, to guide Bellingcat’s court-focused investigations. Its aim is to ensure that any material discovered by Bellingcat’s dedicated Justice and Accountability Unit is gathered in accordance with rules on admissibility of evidence so as to make it suitable for use in future legal proceedings and other accountability processes. It is the product of years of testing and development and has benefited from input from legal and investigative practitioners.

This collaboration began during a 2018 [workshop](#) hosted by GLAN, Swansea University and Garden Court Chambers, to consider the potential for digital evidence in the fight for accountability for atrocities in Yemen. Work on this methodology began shortly afterwards when lawyers at GLAN undertook a review of evidentiary principles in consultation with investigators at Bellingcat, with a view to developing a set of simple steps which investigators could take to comply with those principles. This resulted in the drafting of the first version of a methodology, which aimed to strike a balance between being practical as well as robust. Since then, there have been a number of key milestones:

- 2019: To test the investigative workability of the methodology, GLAN and Bellingcat convened an interdisciplinary [“Hackathon”](#) event at which world-renowned open source investigators trialled the methodology to investigate alleged airstrikes in

Yemen. The results of these investigations were completed by Bellingcat and subsequently [published as the Yemen Project](#).

- 2020: GLAN and Bellingcat continued to revise the methodology while conducting further investigations into attacks causing grave civilian harm in Yemen. A project at Harvard University's Advocates for Human Rights led by GLAN's Dr Ioannis Kalpouzou scrutinised the Yemen Project investigations for their significance in assessing international humanitarian law compliance.
- 2021: To test the evidentiary aspects of the methodology, GLAN, Bellingcat and the OSR4Rights project at Swansea University designed and convened a [mock hearing](#) challenging the admissibility of a piece of open source evidence discovered using the methodology. The purpose of this exercise was to have the methodology scrutinised and challenged in as realistic a way as possible in the context of an English court. The draft methodology was then revised again to address the issues raised by the exercise.
- 2022: The methodology was finalised into its current form, and together GLAN and Bellingcat [launched](#) the Justice and Accountability Unit which uses the methodology to conduct online open-source [investigations on Ukraine](#). We also released two [reports](#) addressing the use of open source investigations as evidence in legal proceedings.

This methodology should be thought of as a set of standard operating procedures, providing granular, practical steps for investigators to follow when searching for content online. It should therefore not be seen as an alternative to the Berkeley Protocol on Digital Open Source Investigations or other guiding principles. The Berkeley Protocol sets out high-level guidance on the effective use of OSI as evidence, and anyone wishing to take it into account will need to develop their own standard operating procedures which implement the principles comprehensively articulated by the Protocol. This methodology was reviewed after the Berkeley Protocol's publication in 2020 and we consider that it complies with the principles identified by the Protocol.

This methodology has been tailored to the particular context and objectives of the Justice and Accountability Unit's investigations on Ukraine, but we hope that it may provide a helpful blueprint for other organisations working in Ukraine or other contexts. The methodology assumes that the organisation has sufficient resources to maintain certain aspects that are not without cost, for example the use of dedicated devices; the use of highly secure digital infrastructure, and sufficient budget for dedicated investigators to be allowed to work through investigations quite slowly. Furthermore, it is not trivial to ensure standardised practices among a group of multiple investigators. It therefore may not be compatible with organisations whose objective it is to get through a lot of data quite quickly. It will be a balancing act for each organisation to consider what is workable and achievable in their own particular context. For larger organisations, coalitions and organisations working with volunteers or consultants, a more light-touch methodology could be considered. If they have decided to conduct online investigations, organisations should do what they can to standardise their online investigation procedures, and ensure those investigations are conducted in accordance with legal and ethical requirements, but the absence of a comprehensive bespoke methodology such as this one does not mean that the evidence gathered will be automatically inadmissible. We wish to be clear that this methodology is, in

our view, one way of conducting investigations with accountability processes in mind – it should not be viewed as the only way of doing investigations.

This methodology does not teach online investigation methods such as locating or verifying content; it assumes knowledge of these and instead addresses the surrounding aspects relating to legal admissibility. It also does not cover forensic preservation, since Bellingcat's preservation is carried out by our partners at Mnemonic.

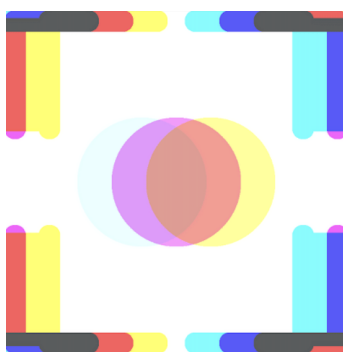
There is a list in the final Annex of people who have contributed in some way – either through direct review or sharing of knowledge – to the development of this methodology. We are extremely grateful to all of them. Any errors remain our own. Bellingcat and GLAN would like to express our gratitude to all our generous funders who have made this project possible. In particular, we would like to thank Avaaz and its supporters for enabling this project.

This methodology is a living document, and we welcome feedback: please contact accountability@bellingcat.com setting out your comments.

Bellingcat
Global Legal Action Network
December 2022

BELLINGCAT

GLOBAL LEGAL ACTION NETWORK



JUSTICE AND ACCOUNTABILITY UNIT

METHODOLOGY FOR ONLINE OPEN SOURCE INVESTIGATIONS INTO INCIDENTS TAKING PLACE IN UKRAINE SINCE 24 FEBRUARY 2022

TABLE OF CONTENTS

I: Systems and resources	7
II: Briefings	8
III: Categories of information	9
IV: Preparation	10
V: Investigation	12
VI: Discovery / Content Gathering	13
VII: Verification & Analysis	16
VIII Roles and responsibilities	19
ANNEX I - BIAS	20
Algorithmic Effects	20
What are algorithms?	21
Why is OOSI's interaction with algorithms different?	22
Virtual Private Networks	24
Browsers and varied searching activities	25
Use of Passive Research Accounts	26
Deletion of Cookies and Browsing Data	27
Access Bias	28
Human Bias	28
ANNEX II: DATA PROTECTION, PRIVACY AND JOINING CLOSED GROUPS	31

ANNEX III: SEXUAL AND GENDER BASED CRIMES	35
ANNEX IV: CRIMES AGAINST AND AFFECTING CHILDREN	44
Overview	44
ANNEX V: LEGAL BRIEFING	48
RULES OF EVIDENCE	48
Why should we take into account legal considerations at this stage?	48
The testing of evidence	48
Admissibility and weight	49
Fairness and exclusion of evidence	50
The requirement to pursue all lines of reasonable enquiry including those leading towards evidence that may explain the attack or suggest alternative attribution	52
Recording your searches and using VPNs	52
Retaining all relevant content and background content for disclosure purposes	53
Preserve all relevant material	54
Presentational considerations	55
IHL: Fundamentals	56
Who and what can be attacked	57
The humane treatment of civilians and persons hors de combat	59
The prohibition on specific methods of warfare	60
The protection of civilians under a force's control	61
ICL: WAR CRIMES, GENOCIDE AND CRIMES AGAINST HUMANITY – RELEVANT KEY POINTS	61
War crimes	62
Crimes against humanity	62
Genocide	65
Mental Element	65
Command Responsibility	67
Translating this into factual inquiries	68
ANNEX VI: FACTUAL INQUIRIES AND THEIR RELATIONSHIP TO THE ELEMENTS OF CRIMES	69
ANNEX VII: STYLE GUIDE AND NAMING CONVENTIONS	75
Neutral Language	75
Date & Time	76
Coordinates	77
Reporting Casualties	77
Images	77
Satellite Imagery	78
Graphic Imagery	79
Footnotes	80
Discovering Earlier Sources	80
Referring to Sources	80

ANNEX VIII: INCIDENT ASSESSMENT TEMPLATE	81
ANNEX IX - UWAZI FIELDS	84
ANNEX X: ACKNOWLEDGMENTS	90

Who is this methodology for?

This methodology has been tailored to guide Bellingcat's investigations into hostilities taking place in Ukraine after a Russian invasion began on 24 February 2022. In response to the Russian invasion and subsequent events, which have led to allegations of international crimes, Bellingcat's analysts will be conducting real-time monitoring for prompt publication, in addition to more formalised investigations undertaken according to a replicable procedure, with a view to ensuring that the information obtained is suitable for use in future accountability proceedings. This document outlines the methodology to be followed by investigators working on the formalised investigations. It will only be undertaken by those who have received the legal training by Global Legal Action Network.

I: Systems and resources

GENERAL

Dedicated Device: You are expected to use a dedicated work device for your Justice and Accountability investigations. It is not for personal use. Ensure the hard drive of your laptop is encrypted and that you have set a very strong password. You will need to use separate user accounts for any other Bellingcat work which is not Justice & Accountability work.

VPN: You will be provided with a virtual private network.

Slack: Application for communicating with other team members.

Cloud: You will be given access to cloud storage in which to create and populate folders as set out below.

IN GOOGLE CHROME

Hunchly: Google chrome plugin which tracks your online activities, preserving essential information about the webpages.

Google Sheets: You will have access to the following spreadsheets:

- Incident Seed Data: Civilian Harm Sheet (CIVHARM)
- Incident Seed Data: Ukraine Witness Sheet
- Device Log Sheet
- Mnemonic Preservation Sheet
- Incident Link Sheet: for recording all relevant links to an investigation.

Google documents: You will create the following documents for each investigation:

- Research Notes: for recording your search terms and generally keeping a log of your activity
- An Incident Assessment for each incident or set of incidents (depending on what is appropriate)

In another browser window that is not running Hunchly

Uwazi: An analysis database for keeping track of and displaying incidents, media content and actors - note that Uwazi does not preserve content.

II: Briefings

Legal: You will be provided with a legal briefing which covers the core evidentiary principles you need to be aware of, along with the substantive law applicable to the situation you are investigating. In this case, the relevant law is international humanitarian law (IHL), serious violations of which, when committed with intent, amount to war crimes under international criminal law (ICL). Other offences under ICL may also be relevant, such as crimes against humanity or genocide. This is provided so that you are aware of what information is relevant to your inquiries and the importance of being able to demonstrate a neutral evidence-gathering process. While it is often necessary to comment on matters *relevant* to a legal assessment, for example whether military personnel could be observed or whether a source seems reliable, it is not the role of the investigators to comment on the legality of an attack. Rather, investigators are required to document the incident to the highest standard possible, providing an in-depth summary and technical analysis of the information uncovered.

Practical: You are provided with a Style Guide and Incident Template, which is designed to ensure consistent and appropriate use of language across written work. You will also build shared resources as a team which will allow you to better understand material you may come across, for example the weapons available to each party, how to identify them and their effects.

III: Categories of information

When collecting and describing information, your sources should be clearly cited and categorized. There are generally two different categories of sources of information or content, but there will necessarily be some overlap:

- i) Examinable or core content:** This describes the granular items of online content (such as individual videos, photographs, Tweets, Wikimapia entries, flight logs) which you, as an OSI analyst, can apply your expertise to in order to draw further conclusions. That is to say, content that can be examined and interrogated for its veracity and/or significance in cross-authenticating other items of content. Examinable content is something which can be analysed and pieced together to form conclusions.
 - Online audiovisual content (**OAVC**), including user generated content (**UGC**) and audiovisual content posted by organisations, such as NGOs or media outlets
 - Satellite imagery
 - Maritime trackers, aviation trackers, weather logs, and other forms of OSI tools and sources
 - Social media posts without audiovisual content which can be used to assist with OSI exercises such as chronolocation or initial geolocation enquiries, or those which can be analysed in bulk for text patterns
 - Sites which record user entries like Google Maps and Wikimapia

- ii) Descriptive content:** This is any content published online, usually written, in which events are described, but which cannot be examined using OOSI techniques. For example, if a reliable NGO publishes witness statements, these are descriptive content, and so too is a media article describing the occurrence of

an event. Such content is not necessarily more or less reliable than examinable content, but it is not the subject matter to which you are applying your skills, and it is therefore to be differentiated. As noted above, some written content could be examinable content (for example, individual Tweets or a photograph of a death certificate) - the issue is whether the item can be interrogated using OOSI techniques. It always helps to review and summarise descriptive content, which can often be very reliable, but strictly speaking it is not the kind of OSI you are interested in.

IV: Preparation

Before you begin your investigation, please carry out the following steps:.

1. Ensure your computer is encrypted, has a strong password and has a separate user account for your J&A work.
2. Install Hunchly on Chrome

Download Hunchly [here](#). It will ask you for a licence key that will be provided to you via email.

3. Install a VPN

Make sure that you have a VPN installed. This is necessary for your security and, to a lesser extent, to standardise any risks associated with algorithmic delivery of content based on your real identity or location in your investigations. Mullvad VPN subscriptions are being provided for you by Bellingcat. If you are using a different VPN, the lead investigator must be asked for approval and a memo of the interaction must be made. This must state the decision made as to whether that provider can be used and the reasoning for the decision.

Ensure the exit node is set to the USA, due to some search engine results being restricted in Europe. If an alternate node is used, permission must be sought from the lead investigator and a memo of this decision recorded.

4. Create virtual identities on all major social media platforms

Creating an online identity protects you from revealing who you are in an online investigation while continuing to have access to certain platforms. A fresh **[withheld]** account will be required to conduct research. This will both protect investigators, as well as reduce the potential for algorithmic selection to negatively interfere with search results based on prior history.

For Facebook and Twitter, you will need virtual identities in order to access the information contained there. For Youtube and Instagram, you can access the information without an account. Ensure that you are signed out of your personal Youtube and Instagram accounts.

[detail withheld]

Record all of this information in your tab on the Device Sheet, including information about your research accounts so that they can be traced.

5. When you create a new research account, you will need to conduct investigation-related searches in English, Ukrainian and Russian while signed in so that the algorithms of the search engines learn the content you are interested in. This may take some time.
6. You should never reach out to a source or make any kind of interaction with an account without further authorisation. If you believe that a source would be crucial to reach out to, communicate this to the lead investigator.

Communication

Throughout these investigations, the team will act as one unit, working together. To do so, they must communicate clearly and often about research progress, source evaluation, and any issues that may arise. For communication, there will be a Slack channel for the team members to discuss these issues. For anything particularly sensitive (involving sensitive legal or personal information), the team will use a group chat in Signal. Do not use personal conversation threads or other unrelated threads to discuss the investigations.

V: Investigation

During your investigation, it is important to record every step in your process in order to keep the investigation replicable and traceable. It is equally important to keep your online identity safe to protect yourself and the integrity of the investigation.

1. Turn on your VPN

- Make sure that before you begin any part of your investigation, your VPN is turned on and shielding your online identity

2. Log out and Log in

- Ensure you are logged out of your other accounts on all social media sites and search engines
- Log into your passive research accounts where needed

3. Create the Investigation Folder

- Access our private cloud via your Bellingcat Google account (this will be the Ukraine-specific Google Drive) and create a folder for the incident you are investigating. Name it with the incident ID. This will be a shared folder, so ensure that no one else on the team has created the same folder. This folder should contain the following:
 - A Google Doc for the assessment, titled “CIVXXXX Incident Assessment” - copy and paste the incident template into this document.
 - A Google Doc for your research notes, titled “CIVXXXX Research Notes - INVESTIGATOR NAME”
 - A Google Sheet named “CIVXXXX Links”
 - A folder for Hunchly files named “Hunchly files”
 - A folder for images and videos, titled “Images and Videos”
 - A miscellaneous folder titled “Misc”

5. Switch on Hunchly

- Create a case in Hunchly for the incident and make sure it is selected. Name it your incident ID. Turn on Hunchly in your investigation profile: all pages that you visit in that Chrome window will now be recorded.
 - If you need to do something unrelated to the factual enquiry, use a different browser to reduce the amount of noise in Hunchly.

- **IMPORTANT:** Do not use the same device for personal use and investigations. If you need to do something personal using your investigations device, such as checking your email, messaging with someone, or using your password manager, make sure you do this in a separate browser window so that Hunchly does not record this personal data during the investigation. If you have no option but to use the same device for personal use and investigations, please make a note of the reasons and ensure that your team leader is aware. It is important that investigations remain completely isolated.
- Do not edit your Hunchly dashboard. If you need to remove something (for example, personal information you may have accidentally revealed), consult the lead researcher who can make note of the edit.

Note that some videos on some platforms require proof of identity to view, because of the graphic nature of the content. If this happens, it is permissible to transfer the link and watch it using another account that is sufficiently verified, such as your regular Bellingcat account, as long as all you do while outside the J&A workstream is watch the video.

VI: Discovery / Content Gathering

If necessary, refresh yourself on your legal briefing materials to ensure that you follow all reasonable lines of inquiry. Ensure you are comfortable with the core concepts of international humanitarian law, so that you will recognise all relevant information which points both towards and away from a violation of IHL. This is extremely important so that you do not miss information that could be of assistance to any future defendant. Have your Table of Factual Inquiries ready so that you can familiarise yourself with where your search terms should be going. However, your own common sense is important - your objectives are to uncover all aspects of what happened, considering all possibilities with an open mind and from a neutral starting point, and to find all reasonably relevant content. You should investigate both the immediate acts that gave rise to the harm you are documenting and any surrounding events that are relevant.

In general, your investigative task is to find out everything you can about your incident. The incident assessment template has some key questions, and the Table of Factual Inquiries is there to assist you, but it may help to prepare a list of questions you intend to answer to keep you on track and to discuss this with the legal team if you wish. In

particular, you should remember to actively pursue alternative possibilities and avenues of investigation that will ensure you are not influenced by cognitive biases.

Once you have completed the steps above, you are ready to begin finding content for your investigation.

Make sure to record the key words you search and take note of your most successful advanced searches (both to make your investigation replicable and to ensure that you can pick up where you leave off if it requires more than one sitting to complete the investigation). Do this by maintaining a search log in the Research Notes document. If you search for something that is not obvious, make a note of why you decided to run this search. If you make small variations in searches, record these. Record which search engines you used and, if you used anything unusual, explain why.

Archiving and Sorting Your Work

Throughout the investigation, all your searches and webpages will be archived by Hunchly and the content will be preserved by Mnemonic through the archiving sheet, which Mnemonic has access to. Any link you discover which you consider could amount to relevant information or evidence should be placed in the archiving sheet so that it is picked up by Mnemonic. Mnemonic will be archiving all of the video and photographic material we use throughout these investigations. In the long term, once your investigation is complete, all relevant material will go to them and you/Bellingcat will not be responsible for preservation of the content.

For examinable content, always try to find the earliest online source (the **Original Online Source**) of the full text, video, or image. This earliest user should be the person cited for the content even if their post isn't how you first came across it. The version of the content you decide to send for preservation and refer to in your incident report is the one that will be recorded in the Uwazi database, and the online poster will be recorded as the 'source'. Your Hunchly files should trace how you came upon the earliest version. If a later version of a piece of content is higher quality or of longer length, then this should be preserved too.

Be sure to link to the Original Online Source when possible and cite the user, author, organization as well as the platform or website where you obtained the content. Analysis of the online source can be useful, especially if you are confident they are the first person to post the content or if they claim to have direct knowledge of its veracity. Stay aware of biases

and manipulation-- if you are ever unsure, ask other investigators or the lead researcher. However, this is all separate from verifying the content, which is ultimately the goal. A biased or non-credible source can still post content that can be independently verified, and this material should be assessed on a case-by-case basis.

In addition to preserving the content with Mnemonic, we will be using Uwazi to log the items of evidence you consider relevant for analysis purposes and for case building. Anything that is examinable should be checked as such in the Mnemonic sheet, because that will signpost the system to bring it into Uwazi.

In addition, it is good practice to keep for your own purposes your own copies for reference and save them in your cloud folder. For **pictures**: Download the pictures relevant for your investigation and keep them in your private cloud folder for your incident. Name your picture “incidentID_photox” where x corresponds to a number that is unique for that picture. The legal team will enter the content into Uwazi and notify you when it is ready for your review.

For **videos**: Download the videos relevant for your investigation and keep them in your private cloud folder for your incident. Name your video “incidentID_videox” where x corresponds to a number that is unique for that video.

If you think that a picture or video you have could be helpful for another researcher, contact them about it in our communication channel and then transfer the media content into a shared cloud folder for them to access it.

Once your investigation is complete, the legal team will establish the incident and entities in Uwazi for investigators to review and populate further. This will be done in accordance with the Uwazi Workflow, Uwazi Field Guide and Investigators’ Guide.

Satellite Imagery

Satellite imagery is not considered to be at risk of removal, so it does not need to be preserved, but it can be helpful to download for review purposes, in particular where a subscription to a given service is time limited.

‘Before and After’ satellite imagery can be grouped together in an Uwazi evidence entity and linked to a specific event.

Paid satellite imagery sources available for you to use: **[withheld]**

VII: Verification & Analysis

This phase of your investigation includes geolocation, chronolocation, corroboration, and describing your content. It will inform your verification in your Research Notes and ultimately your Incident Assessment Report, your final product of the investigation. This verification process must be clearly displayed within the Incident Assessment.

The Incident Assessment will be used as a living document which will contain all of your verification work and conclusions and should follow the guidelines in the **style guide**. It is your neutral description of what you have found and your analysis of what it means. It is not a formal expert report and you are free to comment on any matters which you consider are relevant to informing the reader about what happened.

Make descriptive notes of your verification work performed on each item of content, cross-referencing using hyperlinks to other items. This can be done using screen shots to illustrate what is being described. Each investigation has a beginning and an end, but in reality any verification notes are generally a living document. They are not “evidence” in themselves, rather they are a description of the significance of the evidence. The reports should be written in an accessible style, but your target audience is someone who understands the concepts of geolocation, chronolocation and cross-referencing. You may need to write a longer, very detailed geolocation report in the future if the investigation is being considered for use as evidence in particular proceedings, but at this stage that level of detail is not required.

Deaths or Casualties Reported

The process of counting civilian deaths can be challenging and exact numbers are often inaccurate due to contradictory reports. The identification of civilians and members of the armed forces in conflict also poses a problem when investigating civilian deaths and

casualties using OSI. Because of this, team members are advised not to attempt to count casualties.

We will authoritatively report on actual numbers of civilian deaths only where direct evidence is presented through the means of examinable items such as - images/video of death certificates, hospital papers or images of tombstones - that can be reviewed and matched with images or footage of dead bodies or patients with injuries viewed on open source content or reports in the media. The credibility and reliability of the online source will be taken into account. Where a confirmed number is included in a report, it must be made clear that this is only what Bellingcat could confirm using OOSI methods; it is not necessarily contradictory to other NGO reports' figures, which will often be higher since they are on the ground, interviewing families and hospital staff. Investigators will also be aware of the legal status of civilians to take a direct part in hostilities.

Casualty estimate ranges from news reports, INGO reports and other sources should be included as Descriptive Content for completeness, but no comment should be made on their veracity unless it is possible to analyse them using the method outlined above.

When you are describing casualties, use the term "military personnel" if you think someone could be a fighter, and avoid over-use of the term 'civilian'. This is because 'civilian' is both a legal and a descriptive term, and because the Ukrainian conflict has involved civilians taking a direct part in hostilities, which raises legal complexities. It is also preferable to report on casualties without making the distinction of whether the individuals killed or injured are civilian or not, for example by describing "a young male wearing jeans and a t-shirt."

Review the content taking into account the possibility that it may depict or constitute a red flag for sexual or gender-based violence - see Annex III.

We will not attribute formal confidence gradings or degrees of likelihood to any findings or conclusions. It is best to use language terminology in line with the so-called 'language of confidence', such as "appears to be", "suggests", "indicates", or "strongly indicates/suggests." However, you should avoid over-use of the language of uncertainty if you have a basis to conclude something with certainty. An example is "this event must have taken place on or before 12 March" if the item was posted on 12 March; or "this weapon must have been shipped after 25th May based on its serial number."

Logging Off

When you finish your investigation session, go through the following steps to make sure you can pick back up where you left off, without compromising your online security or your investigation.

- Save all important links and leads in your search log and links sheets.
- Enter the links into Mnemonic's sheet. Tag examinable content and anything else you think should wind up in Uwazi.
- Upload all content that you want saved into the Incident folder in the Ukraine Project Google Drive.
- Turn off Hunchly and close all tabs and browsers.
- Delete everything you downloaded off your computer and empty your trash.
- Power off your laptop at night and any time you are travelling or where it is at risk of being stolen. This reduces the risk that a thief will be able to access your data.

VIII Roles and responsibilities

Investigators - ten in total

Lead investigator: Nick Waters

First instance investigators: **[six investigators - names withheld]**

Coordination with legal on design of procedures: **[six investigators - names withheld]**

Reviewing investigators: *[three investigators - names withheld]*

Legal

Lead lawyers: Dearbhla Minogue, Siobhan Allen, with support from Charlotte Andrews-Briscoe

Ad-hoc consultants: Professor Yvonne McDermott (evidence, international criminal law), Dr Ioannis Kalpouzos (international humanitarian law, international criminal law).

ANNEX I - BIAS

1. As set out in the legal briefing, any investigation leading to the collection of evidence needs to be as impartial and comprehensive as possible so as to be fair to the person against whom the evidence is ultimately used. This methodology thus takes measures to mitigate against bias.

Algorithmic Effects

2. The effects of search engine and social media algorithms are a consideration in OOSI. To the extent that these algorithms pose a threat to the comprehensiveness of investigations, the use of advanced and varied search terms is the most appropriate remedy. Additionally, we have found that algorithms becoming familiar with a particular OOSI research account is a necessary part of online investigation.
3. [McDermott et al., \(2020\)](#) define algorithmic bias as “*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.*” The Berkeley Protocol has the following to say about technical bias:

“The browser, search engine, search terms and syntax used may lead to very different results, even when the underlying query is the same. Inherent biases in the Internet’s architecture and algorithms employed by search engines and websites can threaten the objectivity of search results. Search results may also be influenced by a number of technical factors, including the device used and its location, and the user’s prior search history and Internet activity. Open source investigators should counterbalance such biases by applying methodologies to ensure that search results are as diverse as possible, for example, by running multiple search queries and using a variety of search engines and browsers. Investigators should be aware that search results may also be influenced by other factors, including as a result

of the discrepancy in the digital environment whereby online information may be unevenly available from certain groups or segments of society.”

What are algorithms?

4. **Search engine algorithms** are sets of instructions that describe how the search engine should perform a search, and in what order and format it should display the results. These instructions incorporate complex methods for evaluating the relevance and quality of potential search results for each individual search query, so that the search engine can display first the results that are most likely to be relevant to the user. Such algorithms are necessary for search engines to function. These algorithms may consider, among other factors, complex inferences about the semantic meaning of the search terms provided, as well as inferences about what the user might have been looking for based on other user information (search history, location, language, etc). The search engine might also make inferences about the quality and recency of the web pages, along with their estimated relevance to other users performing similar queries. This information is used by the search engine to predict which search results are most likely to be relevant to the user, and to provide a satisfactory answer to the query. **Social media algorithms** are sets of rules that dictate the type of content a user sees in their feed, and in what order, based on the algorithm’s prediction about the content’s relevance to the user. Both types of algorithms will use general characteristics about the user (location, device, browser, cookies, etc as well as specific details (search history, accounts followed, videos watched, etc) to highlight or surface content predicted to be interesting to the user. In other words, these algorithms are what make searches useful for most people most of the time.
5. Search engine algorithms are unlikely to inject overt, explicit political bias of their own into search result evaluation. But algorithms may group content based on similarities and likelihoods that two pieces of content containing similar words and phrases will interest the same person. In addition, because the algorithms will make assumptions based on where the person is located and what language they search in, among other factors, the search results may reflect the interests of a larger population, including that population’s political preferences. In other words, the algorithms may show a user what it thinks the user will want to find, rather than what

a theoretical, more “objective” user might have wanted to find. Take the example of the delivery of BBC search results by Google to a searcher believed to be in the UK whereas the same search terms from Russia might return a Russian state media article. The algorithms have delivered the content based on what most people in those regions are interested in.

6. There is thus a reality that if users perform surface level searches (in the case of search engines) or passively scroll on social media, the algorithms will decide what to offer the user. If the user does nothing else, and takes no measures to perform additional research or to discover information in different ways, the user may, in some circumstances, see, at least at the top of the feed or results, contents that favours one party to a conflict over another, for the reasons outlined above. However, such simple searches and scrolling are unacceptable for investigation or verification activities. For example, no online investigator will merely scroll through a feed, passively looking at what content appears in the same way that a casual user would. Online investigators must understand and deploy an investigation methodology that is calculated to surface relevant content.

Why is OOSI’s interaction with algorithms different?

7. As outlined, search engine algorithms offer results based on what they assume search terms to mean to the user and objective criteria about quality of web pages. Such default functions are substantially interfered with by the active nature of, and levels of specificity involved in, OOSI searches. The use of **targeted and sophisticated search terms** has a dual effect: if the search query is very specific, it can indicate to the algorithm the meaning of the query and assist with connection to the most relevant page. However, the largest effect is simply that it dramatically lowers the number of indexed web pages that the algorithms have to rank. The use of a combination of neutral and partisan search terms in multiple languages further limits the scope for algorithmic delivery ‘choices’ which have the effect of suppressing potentially relevant content. Nevertheless, there will always be some algorithmic decision-making.

8. Algorithmic tracking of user preferences is an **advantage** for OOSI purposes. Search algorithms' main audience (insofar as searches concerning current affairs are concerned) are people who wish to find relatively mainstream content of a certain quality; a reputable article without undue amounts of spam pop-ups which has been cross-cited by many other sources, for example. Online investigators are not necessarily interested in this largely Descriptive Content; from search engines they want local content, small blog posts with first hand Examinable Content; partisan material on both sides, showing insider knowledge, message boards, and other material that the average searcher is not looking for. From social media they want niche accounts such as aggregator accounts and ultimately individual members of the public who are posting about their first-hand experiences. Thus, in the case of OOSI, it is actually a significant advantage that a profile is built up of the researcher based on their past activity. This was demonstrated by a Ukraine investigator's difficulty in finding any relevant content when he had just created his research account - the algorithms took about a week to learn the fact that he wanted local Ukrainian and Russian content, low-traffic and/or granular content. Before this, he was being shown mainstream content such as BBC.
9. In light of the above, Bellingcat recommends caution in characterising the selective delivery of content as *necessarily* involving "bias". "Bias" suggests unfairness, which does not always flow from the delivery of differing content depending on the factors noted above. Indeed, the algorithms in question are necessary to assist with online investigations, since without them, researchers could not find relevant content at all.
10. While it is not possible to be absolutely certain that 100% of the relevant content in existence on the internet has been returned reasonably near the top of the search results for a single query, good investigations incorporate many methods to surface relevant content. It is this, and not (for example) the use of country node selection or the clearance of cookies, which will have a significant effect on the comprehensiveness of search results. See further below in relation to VPNs. However, to the extent that Bellingcat's searches could be impacted by bias associated with the factors outlined in the Berkeley Protocol, we take some measures to mitigate, or at

the very least to randomise, any technical bias. Their underlying rationale is set out below.

11. To summarise, the methodology employed by Bellingcat allows investigators to work with the reality of algorithmic selection in a controlled fashion, mitigating any potential biases and benefiting from selective delivery of search results and taking advantage of algorithms to reach niche content.

Virtual Private Networks

12. VPNs are used to disguise the IP address and protect the traffic of the user. They create an encrypted tunnel through which the user's information will pass, eventually exiting at a given node with an IP address different from that of the original user. This has the effect of giving the relevant website or search engine the impression that an IP address other than the user's is conducting a search or accessing a site.
13. In addition to being necessary for security purposes, VPNs affect algorithmic delivery because a user's IP address can influence search results. However, it is far from clear exactly how algorithms would influence results based on IP address; and the general considerations concerning algorithms set out above apply.
14. Additionally, the IP address of the exit node of the VPN will likely have been used by other people, all of whom would have their own browsing habits which would influence the algorithm of the search engine. This influence is impossible to quantify. As such, using them involves effectively swapping a somewhat known factor (the user's true IP Address) for an entirely unknown one. The use of a VPN may therefore mitigate bias, but in theory it could also swap it for a different kind of bias.
15. Ultimately, because the algorithms of search engines are proprietary and essentially 'black boxes,' it is extremely difficult to demonstrate precisely what measures can effectively ensure the returning of all relevant content and prevent. However, the decision was made to use VPNs, because they are necessary for the security they provide to the researcher, and because they would at least eliminate any algorithmic effects directly associated with activity from IP addresses used by Bellingcat's

investigators. It is noted here for completeness that J&A investigators use research accounts whose data are not cleared before every session - so the search algorithms will be accessing other information that can identify the researcher's past activity. The use of VPN therefore disguises the user's real IP address but not their browsing habits and history as an investigator.

16. VPNs allow the user to select an 'exit node' (i.e. the IP address of the exit node detectable by the search engine or website) in a particular country. It is not possible to select a country which would attract more or less hypothetical bias than another. In order to avoid introducing other unintended biases by actively selecting an exit node in a given country, a preliminary decision was to select the country in which the researcher is based while using the VPN. However, given that almost all of the time the researchers will be in jurisdictions for which some data is filtered out for GDPR purposes, it was decided that the exit node will be set to the United States. In addition, since the beginning of the conflict, some results, such as from Russian state media, [will not be served](#) to European users on social media sites such as Twitter. However, these accounts are still available in the United States.

Browsers and varied searching activities

17. The Berkeley Protocol recommends alternative **browsers**, however due to Bellingcat's use of Hunchly in Google Chrome, a decision has been taken not to use additional browsers. Bellingcat considers that the influence of the browser involved could not affect the delivery of results to such an extent as to outweigh the disadvantages associated with having searches conducted outside the Hunchly collection or the inconvenience of using multiple browsers running Hunchly (which would then have to be cross-referenced).
18. Investigators will be searching in English, Ukrainian and Russian using terms that are as standardised as possible relative to the investigations. Russian- and Ukrainian-speaking investigators are on hand to assist English-only investigators and to ensure that search results when conducted by these investigators are not problematically limited due to these investigators' inability to vary their search terms naturally in response to what they find. They will also be using Google and Yandex, in addition to any other search engines they see fit.

Use of Passive Research Accounts

19. Research accounts are needed to gain access to social media platforms by logging in.
20. Bellingcat investigators do not use their true identifies for a number of reasons, namely:
 - a. The use of a passive research account protects the identity of a researcher. If a researcher were to use their personal account and accidentally, for example, “like” a post by a subject of interest, that would alert the subject that a member of Bellingcat was viewing their profile. This could result in potential evidence being deleted, or even attempts to surveil the researcher.
 - b. In the same way, the use of passive research accounts protects subjects of interest and potential sources. If a person who posted a video is stopped at a checkpoint and a soldier checks their phone, if they have posts that have been “liked” by a member of Bellingcat, this could represent a risk to that person.
 - c. Finally, the use of a fresh social media account may help mitigate potential algorithmic selection based on the profile that a researcher has developed on their personal account.
21. While the ideal may be for a fresh passive research account to be generated for each new investigation, in reality this is not feasible for the following reasons:
 - a. Social media platforms have processes to detect bots or inauthentic behaviour and as such it is necessary to go through a certain process in order to generate stable accounts that will not be deleted. This **[process is time-consuming - detail withheld]**. If the social media platform believes the account is inauthentic, it will be deleted and the process must start from the beginning.
 - b. Continually generating new social media accounts appears extremely inauthentic to social media platforms. Although it may be possible to avoid some scrutiny by using a VPN, it is likely that a social media platform may still be able to identify the fingerprint of a user from other pieces of information,

such as the version of the browser, the language, the time settings of the machine, the window size, their cookies, and even the fact that they're using a VPN. Some platforms, such as banks, can even identify fraudulent users based on how they interact with the website. There is a small risk that if a platform identifies a fingerprint of a user continually creating inauthentic accounts, that platform may permanently prevent that user from creating more accounts.

Deletion of Cookies and Browsing Data

22. Cookies are small pieces of data placed upon a user's browser by a website. They help to track the user across various sites and help to uniquely identify a user. This could, in theory, affect the kind of information that is displayed to a user. As such, all cookies, and other browsing data, could be removed before the start of an investigative session in order to mitigate any potential algorithmic selection which makes assumptions about the user. However, the deletion of cookies presents a red flag to social media platforms and frequently leads to rapid deletion of research accounts when done in combination with the other steps being taken.
23. In any event, deleting cookies would not eliminate the information that a website will collect based on searches conducted while a user is signed in to various platforms, including Google, Facebook and Twitter. Therefore, while logged in using a passive research account - which is unavoidable - the investigator will carry some information with them even while using a VPN and deleting cookies.
24. For these reasons - and because, as noted above, our researchers have found algorithmic tracking helpful - it has been decided not to systematically remove cookies and browsing data before an investigative session. To do so would result in the repeated deletion of passive social media accounts that are often essential to access information on particular platforms. Although this will allow for algorithmic tracking, we believe this is justified relative to the need to access social media platforms and taking into account the types of searches investigators would be carrying out.

25. Privacy Badger is a plugin which is designed to prevent third party trackers track the websites that an individual user visits. This is primarily installed for security reasons in order to make it more difficult for websites to identify the user.

Access Bias

26. All actors do not have equal access to the mainstream social media platforms. This includes victims or witnesses, for example elderly people, those who have been affected by internet shutdowns, and those who may be coerced into not using social media by occupying forces. Russian online critics may be increasingly silenced on Western and Russian platforms due to the wave of arrests and prosecutions taking place there. It is also important to consider accessing the viewpoint and evidence of Russian forces or supporters, given that Western social media has commenced measures to stop the proliferation of Russian state-backed information campaigns. It is therefore possible that platforms such as Twitter could be regarded as 'pro-Ukraine' in the context of the representation of viewpoints. Any or all of the above could mean that some relevant content, whether pro-Ukraine or pro-Russia, may be less likely to be uploaded to the mainstream platforms.
27. Bellingcat can only search for what is actually present on these platforms and cannot influence the underlying causes of access bias. However, Bellingcat remains aware of these forces and mitigates against all potential biases by ensuring that neutral and varied search terms are used and by searching both Russian and Ukrainian social media and groups where possible.

Human Bias

28. [Cognitive bias](#) refers to a wide variety of inadvertent mental tendencies that can impact perception, memory, reasoning and behaviour. There are numerous types of cognitive bias, each leading to the same problematic outcome: investigators placing undue focus on some information and not enough on other information. Cognitive biases cannot be eliminated - they have evolved to allow the human brain to function and take decisions in the face of otherwise unmanageable amounts of information.

However, bias can be very harmful in criminal investigations, and can undermine the search for truth.

29. As noted elsewhere, Bellingcat is not an official investigatory body, but the J&A Unit seeks to emulate standards expected of official investigators to the extent that that is possible given its size and nature as a non-profit investigative collective. Bellingcat's work on Russia to date and Russia's engagement with Bellingcat in retaliation has led to an extremely antagonistic relationship involving public displays of hostility from both sides. Indeed, Bellingcat has been classified by Russia as a 'foreign agent' and an 'Undesirable Organisation' This antagonistic relationship cannot be erased retrospectively and continues to be played out online today.

30. Bellingcat's investigators must be aware that this could lead to accusations that its justice and accountability investigations cannot be relied upon, due to Bellingcat's inherent bias against Russia. In order to mitigate against any real or perceived cognitive bias, Bellingcat takes the following steps:

- Beginning an investigation with no settled hypothesis as to what happened or what party was responsible;
- Actively pursuing all lines of inquiry in the case of every investigated incident, for example by searching for a military justification for each Russian attack;
- Searching all platforms, including pro-Russian social media and groups;
- Performing intensive verification on each piece of content whether it is posted by pro-Ukraine or pro-Russian sources;
- Working through a list of questions in the methodology to ensure that no relevant lines of inquiry are skipped due to bias;
- A separation of 'inducted' investigators, who work on justice and accountability (J&A) investigations, from non-inducted investigators and leadership. The latter category will not work on J&A investigations; and
- Separate review of investigations by the team leader and legal team.

Use of social media

- Because there is overlap between the personnel and the J&A investigators will also work on journalistic content, it is not feasible to impose a prohibition on the J&A investigators using social media. However, they are encouraged to

take a measured tone if they choose to post. Issues of perceived bias may be raised if members of the J&A Unit post about the situation in Ukraine if their posts are considered imbalanced.

31. Ultimately, the real issue or question that needs to be addressed is whether any hypothetical bias renders investigators incapable of carrying out objective and exhaustive investigations. The team leader and legal teams are satisfied that the inducted investigations team are more than capable of taking the risk of cognitive bias into account and actively taking steps to be aware of the risk and to correct for it through the steps outlined above, such that there is no risk of unfairness associated with the use of Bellingcat's work against a Russian defendant.

ANNEX II: DATA PROTECTION, PRIVACY AND JOINING CLOSED GROUPS

1. Compliance with data protection obligations, respecting social media users' right to privacy and refraining from gaining unauthorised access to online information are all issues which are important in their own right. However, adherence to the relevant rules is doubly important due to their potential relationship with the admissibility of evidence at national or international levels.
2. GLAN and Bellingcat have instructed specialist data protection lawyers to advise on the project's data protection compliance and any other privacy-related risks. The project must comply with the letter and spirit of the GDPR, and we do this by adhering to the general data protection principles and by maintaining a controlled data management system, which includes all relevant risk assessments. The relevant written policies and agreements with external organisations are being developed on an ongoing basis in light of the advice of counsel.

Joining Closed Groups

3. Some social media platforms allow users to create groups among themselves, which are not open to any user of that platform without the owners' permission. Such groups are interchangeably referred to as 'private' or 'closed' groups - Bellingcat adopts the term 'closed', rather than 'private', for the reasons outlined below.
4. Closed social media groups can hold crucial evidence relating to suspected atrocity crimes, ranging from usefully collated UGC to perpetrator content. There are many reasons to be careful about joining closed social media groups. This project defines closed groups as groups for which there are any criteria for entry, for example where a request has to be made or where an invitation is required (and that this process is not automated or simply used to screen for bots.). This project does not extend to joining Whatsapp or Signal groups as they are not considered open source.

5. Online closed groups occupy a grey area in respect of the definition of open source information, which is, according to the Berkeley Protocol: **publicly available information that any member of the public can observe, purchase or request without requiring special legal status or authorised access.** While closed groups have some threshold for entry and thus require ‘authorised access’, some are so large and undiscerning that they *effectively* have no authorisation requirement of entry. This project takes the position that some closed groups are so large as to effectively represent open source information.
6. In the United Kingdom, where the lead investigator is based, it is *prima facie* a criminal offence under the Computer Misuse Act 1990 (CMA) to join closed groups through deception, because the act of gaining entry by deception renders the accessing of the information “unauthorised” for the purposes of the Act. There is no public interest defence under the CMA. There are also related offences under the Data Protection Act 2018 and the Investigatory Powers Act 2016. The specifics of other offences in European jurisdictions are not known, but it is safe to assume until advised otherwise that there are similar or equivalent offences.
7. Under GDPR, there are also reasons to be very careful about joining groups through misrepresentation (see separate GDPR policies and guidance).
8. Taking into account all of the above, Bellingcat J&A investigators should therefore be careful not to gain **unauthorised** entry to closed groups.
9. We will be operating according to the following policy of passive research only:
 - No joining of groups through active deception, for example by pretending to be pro-Russian, pro Ukrainian or by otherwise lying about one’s identity, affiliations, or objectives;
 - No engaging with individuals directly, e.g. through befriending people or exchanging messages.
10. However, closed groups can be joined in some circumstances, if we consider that effective authorisation has been achieved. It will be assessed on a case by case basis, taking into account in particular the legal regime in which the investigation is

expected to be ultimately used. The following are examples of when it may be permissible:

- The requirement to be “invited” is no more than a device to screen for bots. These are not considered ‘closed.’
- The size and membership of the group is such that there are effectively no criteria for membership
- The group can be joined with a benign and neutral account, such as one with a picture of a car or a cartoon as a profile picture;
- The group may be discerning about its membership but you disclose through your request to join that you are a ‘western’ based open source investigator with an interest in accountability. By doing this, you are gaining effective authorisation even if you do not use your actual identity;
- Groups will not be approached using your actual identity, nor the fact that you work for Bellingcat. This is in line with our policy of using research accounts across all platforms, for your own protection and the protection of people you might interact with. If you are concerned that being part of Bellingcat might materially affect whether you are otherwise admitted to a group (even if you disclose that you are investigating for accountability purposes), you can either not enter the group or, after discussion with the lead investigator so that a risk assessment can be performed, attempt to join using an expressly labelled ‘Bellingcat Research Account’ dummy account or an actual Bellingcat account. If that account is given access, you can then join with your alias account, withdrawing the Bellingcat-associated account that was granted access, because you can be satisfied that you would not be gaining ‘authorisation’ by deception.

11. This project maintains a list of the closed groups which have been joined and the rationale for which they have been joined. They are:

Group name and link	Platform	Number of members	Justification
---------------------	----------	-------------------	---------------

12. The project will develop a procedure to be followed where a particularly important closed group or private group is discovered but cannot be joined without deception. This would involve coordination with official authorities to pass the account to them without delay or to otherwise facilitate their access to the account using Bellingcat's accounts or contextual knowledge.

ANNEX III: SEXUAL AND GENDER BASED CRIMES

Definitions

1. The following definitions are to establish clarity when speaking about the concepts in this annex:
 - a. *Gender* within this context follows the Rome Statute definition referring “to the two sexes, male and female, within the context of society”, but also with the understanding that individuals can hold other gender identities. Further, “this definition acknowledges the social construction of gender, and the accompanying roles, behaviours, activities, and attributes assigned to women and men, and to girls and boys.”¹
 - b. *Gender-based violence* within this context follows the definition of the Office of the High Commissioner for Human rights in that it “is considered to be any harmful act directed against individuals or groups of individuals on the basis of their gender”.²
 - c. *Sexual violence* is a type of gender-based violence³; it can comprise of any “sexual act, unwanted sexual comments or advances, or acts to traffic, or otherwise directed against a person’s sexuality using coercion, by any person regardless of their relationship to the victim, in any setting , including but not limited to home and work.”⁴ Examples of sexual violence can include, but is not limited to, rape, sexual assault, threats of sexual violence, mutilation of

¹ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.3.

² United Nations Office of the High Commissioner for Human Rights, ‘Sexual and gender-based violence in the context of transitional justice’ (October 2014), p.1.

³ UN OHCHR, ‘Integrating a Gender Perspective into Human Rights Investigations’ (2018), p. 9; International Protocol on the Documentation and Investigation of Sexual Violence in Conflict (2017) U.K. Foreign and Commonwealth Office (‘International Protocol’ hereafter) p.18; United Nations Office of the High Commissioner for Human Rights, ‘Sexual and gender-based violence in the context of transitional justice’ (October 2014), p.1.

⁴ International Protocol, p.18; United Nations Office of the High Commissioner for Human Rights, ‘Sexual and gender-based violence in the context of transitional justice’ (October 2014), p.1; World Health Organization, ‘Violence against women: Intimate partner and sexual violence against women’ (2016), p.2.

sexual organs, sexual slavery, forced prostitution, forced pregnancy, forced nudity, trafficking, forced abortion or sterilization, and sexual torture.⁵

- d. *Gender-based crimes* follows a similar definition and “are those committed against persons, whether male or female, because of their sex and/or socially constructed gender roles. Gender-based crimes are not always manifested as a form of sexual violence. They may include non-sexual attacks on women and girls, and men and boys, because of their gender.”⁶
- e. *Sexual crimes* are “physical and non-physical acts with a sexual element”⁷ which constitute crimes as defined broadly by international laws or progressive national legal systems
- f. *Gender perspective*, within this context, “requires an understanding of differences in status, power, roles, and needs between males and females, and the impact of gender on people’s opportunities and interactions.”⁸
- g. *Gender analysis* is a tool to examine, analyse, and understand power dynamics and interactions, inequalities, and differences between different genders and how they impact societal norms.⁹ It can be used to understand and think about whether and how crimes were impacted by gender.¹⁰
- h. *Intersectional approach* takes into account the intersection of discriminatory qualities faced by individuals such as age, race, gender identity, sex, socio-economic status, religion, culture, sexual orientation in order to contextualise acts and understand how they are sexual in nature and their gravity.¹¹

Overview

- 2. Sexual and gender-based violence (SGBV) is frequently observed in armed conflict. SGBV has been criminalised by the international legal community under international criminal law, in addition to being prohibited under international human rights law and international humanitarian law. This annex outlines the steps taken by Bellingcat and GLAN to identify and properly handle information suggestive of the occurrence of SGBV, with a view to facilitating investigations into sexual and gender based crimes (SGBC).

⁵ International Protocol, p.18; United Nations Office of the High Commissioner for Human Rights, ‘Sexual and gender-based violence in the context of transitional justice’ (October 2014), p.1.

⁶ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.3.

⁷ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.3.

⁸ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.3.

⁹ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.4.; UN OHCHR, ‘Integrating a Gender Perspective into Human Rights Investigations’ (2018), p.7.

¹⁰ ICC OTP, ‘Policy Paper on Sexual and Gender-Based Crimes’ (October 2014), p.4.

¹¹ The Hague Principles on Sexual Violence, p.108.

3. Bellingcat and GLAN recognize that as open source investigators, the Justice and Accountability Unit (“J&A Unit”) is not equipped to fully investigate an incident involving SGBV and that open source information alone will not be sufficient for investigating these crimes. However, due to the nature of the conflict, it is highly likely that there will be incidents of SGBV encountered in the material reviewed during online open source investigations (“OOSI”) or indicators that SGBV may be happening or have happened. As such, a system for approaching these crimes separately and in a manner that provides dignity for the victim must be established. The J&A Unit takes a “do no harm”¹² approach to all investigations, but particularly relating to SGBV, taking into account the additional sensitivities and ethical considerations surrounding SGBV.¹³
4. In order to make sure that no acts of SGBV present in open source material reviewed by the J&A Unit go unidentified, the J&A Unit will adopt the practice of conducting a gender analysis¹⁴ for each major investigation. It is intended that the team will integrate a gender perspective into investigations as a whole rather than as a separate exercise. By integrating a gender analysis into each major investigation, the J&A Unit hopes to mitigate the reinforcement of gender norms through individual investigators' own gender biases as well as allow for an intersectional approach to investigations.¹⁵
5. If an incident specifically involving SGBV becomes one of the incidents selected through the J&A triage process, a separate investigation plan will be created - including a list of search terms that may be used colloquially to refer to SGBV.
6. Specific content relating to SGBV and crimes against children will be held in a highly secure manner to protect the identity of the victims and alleged perpetrators. As set out below, the UWAZI database will be arranged so that this content can be filtered out if this is deemed necessary. Content the viewing of which would further erode the

¹² See International Protocol pp.85-102.; OHCHR, Manual on Human Rights Monitoring, Chapter 14, p. 8; UN OHCHR, ‘Integrating a Gender Perspective into Human Rights Investigations’ (2018), p. 25.

¹³ Koenig, A and Egan U, ‘Power and Privilege: Investigating Sexual Violence with Digital Open Source Information’, Journal of International Criminal Justice, Volume 19, Issue 1(2021), pp.60-62; UNPF, ‘Reporting on Gender-Based Violence in Humanitarian Settings: A Journalist’ Handbook’ (2020) Second Edition, p. 14.

¹⁴ See UN OHCHR, ‘Integrating a Gender Perspective into Human Rights Investigations’ (2018), pp. 36-49. See also Koenig, A and Egan U, ‘Power and Privilege: Investigating Sexual Violence with Digital Open Source Information’, Journal of International Criminal Justice, Volume 19, Issue 1(2021), pp. 67-68.

¹⁵ See Koenig, A and Egan U, ‘Power and Privilege: Investigating Sexual Violence with Digital Open Source Information’, Journal of International Criminal Justice, Volume 19, Issue 1(2021), pp. 62-63, 67-68.

dignity of those depicted will be restricted to a need-to-access basis. And as with all other investigative content, J&A Unit investigators should not publicly post/repost this content.

7. **A note on consent and respect for victims:** due to the circumstances surrounding the nature of SGBV in OOSI, it will not be possible for the J&A Unit to obtain informed consent from the victim or those depicted in the content. However, to mitigate any negative impacts this might incur, the J&A Unit will only share information relating to SGBV with prosecutorial/international bodies or partners after considering any relevant policies they have in place which are designed to protect the sanctity and dignity of victims.

Practicalities

8. As mentioned, while open source investigations will never be able to fully investigate an act of SGBV the way traditional investigations can, OOSI has promise in identifying key red flags, locations, and contextual information surrounding such crimes. However, unlike other crimes, SGBV may not be as obvious to an investigator while conducting an open source investigation. This section is intended to provide practical guidance to investigators of what factual information may be relevant to SGBV in the material being reviewed.
9. It is important to note that SGBV can be committed against anyone of any age or sex, including men, women, girls and boys. Groups with certain characteristics that attract discrimination more generally, such as LGBTQI persons and persons with disabilities, should be considered at risk.¹⁶ Understanding the intersectional forms of discrimination is particularly important when approaching SGBV.¹⁷
10. Any photograph or video depicting possible direct evidence of SGBV (“**Direct SGBV**”)¹⁸ will be tagged as “possible SGBV” in Uwazi and any additional tagging systems that the J&A Unit uses. The idea of this being that when information sharing with international/prosecutorial bodies occurs, these incidents, including those identified as having SGBV Red Flags (see para. 11 below), would be easily identified

¹⁶ International Protocol (2017), p. 21

¹⁷ International Protocol (2017), p. 56.

¹⁸ Direct SGBV within this context, is defined as SGBV that can be obviously seen by visual imagery. For example, a video of rape or a photograph of a nude prisoner.

and transferred even if not much other information is available. This will allow international/prosecutorial bodies to have “leads” or supplementary information to additional cases they may be investigating.

11. The Hague Principles of Sexual Violence also set out several *indicia* for an act being sexual in nature which can better define content that investigators should be aware of and looking for:¹⁹

“1) The act involved exposing a ‘sexual body part’ or physical contact with such a body part, including over clothing; 2) The act was intended to be sexual by the perpetrator or was perceived as such by the affected person or their community as being sexual in nature; 3) The perpetrator or a third party derived sexual gratification from the act, or intended to do so; 4) The act, while not necessarily sexual in itself, was intended to impact: a. the affected person’s sexual autonomy or sexual integrity, including their capacity to engage in sexual activity, feel sexual desire, or have intimate relationships; b. the affected person’s sexual orientation or gender identity; or c. the affected person’s reproductive capacity or reproductive autonomy; 5) The act involved sexual innuendos or language with implicit or explicit sexual connotations for the affected person, the community, or the perpetrator; 6) The act involved use, interference, control, or degradation of fluids or tissue associated with sexual and reproductive capacity, including semen, vaginal fluids, menstrual blood, breast milk, or placenta.”

12. Example forms of direct SGBV may include:

- a. Rape - following the Rome Statute, is the invasion “of an part of the body of the victim or of the perpetrator with a sexual organ, or of the anal or genital opening of the victim with any object or any other part of the body”.
- b. Acts of a sexual nature - there is no specific definition of “sexual violence” in international law, however, for the purposes of the J&A Unit’s investigation, this should be taken to mean acts that can be seen or interpreted as being sexual. For example:

¹⁹ The Hague Principles on Sexual Violence, Civil Society Declaration on Sexual Violence, Part 2: Indicia of an act is sexual in nature, paras 1-6.

- i. Anything related to a “sexual body part”²⁰ or genital regions, such as:
 - 1. Beatings/attacks/torture;
 - 2. Touching;
 - 3. Injuries.
 - ii. If nudity/partial nudity is present - note: not just victims, but alleged perpetrators or third parties as well.
- c. It is important to note that [as is clear from the Hague Principles of Sexual Violence indicia set out above] sexual violence does not need to be physical violence - an act of sexual violence “can be sexual in nature even in the absence of physical contact”.²¹
- i. For example, a video of perpetrators joking about committing acts of sexual violence in front of detainees may be categorized as sexual violence.²²
- d. Gender-based violence can also be non-sexual. For example, the killing of those belonging to a certain gender, because they belong to that gender group (see gender persecution below).
- e. Within the Rome Statute, SGBV crimes are included as part of potential crimes against humanity, genocide, or war crimes, including:
- i. “Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity;” “or any other form of sexual violence also constituting a grave breach of the Geneva Conventions.”
 - ii. Gender persecution is another crime identified in Article 7 (h), it is “committed against persons because of sex characteristics and/or because of the social constructs and criteria used to define gender”.²³ Groups that may be targeted for gender persecution could be women, men, girls, boys, and members of the LGBTQI+ community.²⁴

13. Not all pieces of content reviewed by the J&A Unit will contain material depicting Direct SGBV. Pieces of content that have indications or “red flags” for SGBV, but do

²⁰ The Hague Principles on Sexual Violence, Civil Society Declaration on Sexual Violence, Part 2: Indicia of an act is sexual in nature, para. 1.

²¹ The Hague Principles on Sexual Violence, Civil Society Declaration, para. 5.

²² See example given in Koenig, A and Egan U, ‘Power and Privilege: Investigating Sexual Violence with Digital Open Source Information’, *Journal of International Criminal Justice*, Volume 19, Issue 1(2021), pp. 66-67.

²³ ICC OTP, ‘DRAFT Policy on Gender Persecution’ (November 2022), p. 3.

²⁴ ICC OTP, ‘DRAFT Policy on Gender Persecution’ (November 2022), p. 3.

not contain Direct SGBV mentioned above (see para 10), will be tagged with “**SGBV Red Flag**” in both Uwazi and any additional tagging systems the J&A Unit uses.

14. Common red flags can occur within a variety of contexts and have been separated for investigator use:

a. Attacks,& Occupation²⁵

- i. Takeover or occupation of homes or entire villages;
- ii. Taking over, occupying, raiding or placing military checkpoints in/near hospitals, schools, religious centres, and other public places;
- iii. The targeting of specific groups, such as men and boys of “fighting age” (14-65), women/girls, children, or members of the LGBTQI+ community;
- iv. Distinct, separate, or different treatment of men/older boys from women/girls/younger children;
- v. Presence of elderly people, particularly women, living alone;²⁶
- vi. Indications or reports that groups of women/girls may have been held for a period of time in a private location by occupying forces;²⁷
- vii. Verbal or written sexual threats/harassment;
- viii. Humiliating treatment;
- ix. Incidents when a woman/girl or small group of women/girls are found dead and alone/in small groups may be indicative of rape prior to death;
- x. Burnt bodies.

b. Arrests & Detentions

- i. Mass detentions of any one sex/gender/age;
- ii. Strip or body searches;
- iii. Humiliating treatment of detainees;
- iv. Interrogations/torture while in detention;
- v. Targeting of women/girls or men/boys separately for arrests;

²⁵ Note: Women, including elderly women, girls, and other marginalised communities are especially at risk for SGBV in occupied territories. See NGO Working Group on Women, Peace, and Security, ‘Gender Analysis of the Situation in Ukraine’ (April 2022).

²⁶ Ukraine has a large population of elderly women, for example, in Luhansk and Donetsk oblast 71% of the households in government-controlled areas were headed by females, 88% of which were over the age of 60. CARE and UN Women, ‘Rapid Gender Analysis of Ukraine’ (May 2022),p.11.

²⁷ For example, there have been reports that in Bucha, 25 women and girls were raped in one house’s basement. See BBC, ‘Ukraine conflict: ‘Russian soldiers raped me and killed my husband’ (11 April 2022).

- vi. Housing male and female prisoners together;
 - vii. Detaining women and girls, in particular under male, rather than female, guards;
 - viii. Injuries as the result of a detention may be indicia of SGBV, especially if there are related to sexual or reproductive organs;
 - ix. Reports/images of any form of nudity (by detainees or other) during arrest/detention.
- c. Recruitment & Training
- i. Recruitment targeted of women and girls by parties engaging in armed conflict (militaries, militias, etc.);
 - ii. Forced conscription by men/boys in occupied areas;
 - iii. Performance of sexual acts/forced nudity as part of training;
 - iv. Civilian women and children living, working, or present in military camps or barracks;
 - v. Social media posts depicting members of armed forces engaging in discriminatory behavior, condoning, inciting, or joking about SGBV.
- d. Campaigns against SGBV
- i. Reports by people on the ground/civil society organisations/media of SGBV;²⁸
 - ii. Advocacy or social media campaigns against SGBV;
 - iii. Statements by parties involved condemning SGBV.
- e. Humanitarian Situation - while the humanitarian situation is something more overarching rather than distinct red flags, investigators should be aware of increased risk for SGBV in areas where there is:
- i. Lack of internet or mobile connection;
 - ii. Poor security (economic, physical, or other)/infrastructure;
 - iii. Presence of vulnerable populations;
 - iv. Discrimination faced when seeking shelter/housing including by men, boys, transgender persons, members of the LGBTQI+ community, the elderly, and persons with disabilities;²⁹

²⁸ See for example, NGO Working Group on Women, Peace, and Security, 'Gender Analysis of the Situation in Ukraine' (April 2022); CARE and UN Women, 'Rapid Gender Analysis of Ukraine' (May 2022).

²⁹ See CARE and UN Women, 'Rapid Gender Analysis of Ukraine' (May 2022), pp. 24-25.

- v. “Informal or unvetted shelters” for displaced peoples;³⁰
- vi. Increased number of displaced women/girls/children, or women/girls/children travelling by themselves³¹;
- vii. Reports of healthcare providers may provide insight into the situation (increased numbers of women and girls, increased sexual health inquiries), though access to healthcare within Ukraine has significantly decreased, and there are barriers to access healthcare outside of Ukraine;³²
- viii. Discrimination or reports of discrimination against women and girls.

15. Notably this list is not exhaustive, but it provides a basis on which investigators may be able to flag should they come across a piece of content that is not on its surface direct SGBV. There will be a text box to explain your reason for tagging an item either as Possible SGBV or SGBV Red Flag.

³⁰ CARE and UN Women, ‘Rapid Gender Analysis of Ukraine’ (May 2022), p.24.

³¹ Note: currently the majority of refugees from Ukraine are women and girls. NGO Working Group on Women, Peace, and Security, ‘Gender Analysis of the Situation in Ukraine’ (April 2022), p.2.

³² NGO Working Group on Women, Peace, and Security, ‘Gender Analysis of the Situation in Ukraine’ (April 2022), p.2.

ANNEX IV: CRIMES AGAINST AND AFFECTING CHILDREN

Overview

1. Crimes against and affecting children (“CAAC”) concern crimes committed against all people below the age of 18 years. As with SGBV, CAAC is a particularly sensitive topic and must be approached with the utmost care, privacy, and dignity for the child. The same approach involving do no harm, protection of data, and consent that has been adopted for SGBV in Annex III above shall be adopted with regards to CAAC. As with SGBV, an intersectional approach is crucial to understanding how crimes may have an impact on children. This annex is intended to be read in conjunction with Annex III.

2. All the crimes covered under the Rome Statute and international law may affect children as well as adults. The United Nations has identified “The Six Grave Violations Against Children During Armed Conflict”³³:
 - a. Recruitment and use of children;
 - b. Killing or maiming of children;
 - c. Sexual violence against children;
 - d. Attacks against schools or hospitals;
 - e. Abduction of children;
 - f. Denial of humanitarian access.

3. In addition and overlapping with these crimes, there are several child-specific crimes listed in the Rome Statute, namely³⁴:
 - a. Conscription, enlistment and use of children under the age of fifteen years to participate actively in hostilities;
 - b. Forcible transfer of children and prevention of birth;
 - c. Trafficking of children as a form of enslavement;
 - d. Attacks against buildings dedicated to education and health care;
 - e. Torture and related crimes;

³³ Office of the Special Representative of the Secretary-General for Children and Armed Conflict, ‘Working Paper No.1 The Six Grave Violations Against Children in Armed Conflict: The Legal Foundation’ (October 2009, Updated November 2013).

³⁴ See ICC OTP, ‘Policy on Children’ (November 2016).

- f. Persecution;
 - g. Sexual and gender-based crimes.
4. A similar system for tagging material will be used as per that set out above in respect of material relevant to SGBV, namely:
- a. Any photograph or video depicting possible direct evidence of crimes against children – meaning the person affected is obviously a child – will be tagged in Uwazi as having “**children visible**” and any additional tagging systems that the J&A Unit uses. As with SGBV, the idea of this being that when information sharing with international/prosecutorial bodies occurs, these incidents, including those identified as having CAAC Red Flags (see below), would be easily identified and transferred even if not much other information is available. This will allow international/prosecutorial bodies to have “leads” or supplementary information to additional cases they may be investigating.
 - b. Pieces of content that have indications or “red flags” for CAAC, but do not depict direct violence or endangerment of children will be tagged with “**CAAC Red Flag**” in both Uwazi and any additional tagging systems the J&A Unit uses. There is a large overlap with red flags for SGBV. Investigators will be briefed to take a restrictive approach and to only select the CAAC Red Flag option if it is not already covered by another tag. This is to avoid too many incidents being tagged as CAAC, which would be unhelpful. Some situations which might amount to a CAAC Red Flag would include:
 - i. Attacks, & Occupation
 - 1. Presence of children in conflict zones;
 - 2. Presence of children in occupied areas;
 - 3. The targeting of schools, playgrounds, or child care facilities;
 - 4. Taking over, occupying, raiding or placing military checkpoints in/near hospitals, schools, religious centres, other public places, or other places children may frequent;
 - 5. Presence of children when violence is perpetrated against their family members;

6. The targeting of specific groups, such as boys of “fighting age”, girls, marginalised children³⁵, or other groups of children;
7. Groups of children being transported³⁶;
8. Children being born during occupation and/or as the result of rape.

ii. Detention

1. Detention of children;
2. Interrogation/torture of children while in detention.

iii. Recruitment & Training

1. Use of child soldiers;³⁷
2. Recruitment aimed at young audiences;
3. Forced conscription of children under 18 in occupied areas;
4. Children living, working, or present in military camps or barracks.

iv. Campaigns Against CAAC

1. Reports by people on the ground/civil society organisations/media of CAAC;
2. Advocacy or social media campaigns against CAAC;
3. Statements by parties involved condemning CAAC.

v. Humanitarian

1. Increased presence of children travelling alone.

5. As with the SGBV annex above, this list is not exhaustive, but it provides a basis on which investigators may be able to flag should they come across a piece of content that could be CAAC. There will be a text box to explain your reason for tagging an item either as Children Present or CAAC Red Flag

³⁵ For example, there is a large Roma minority group in Ukraine (approximately 400,000), the concern for children Roma women surveyed by CARE and the UN was “particularly pronounced”. CARE and UN Women, ‘Rapid Gender Analysis of Ukraine’ (May 2022), pp. 11, 41.

³⁶ For example, there have been reports of over 120,000 Ukrainian children being abducted to the Russian Federation. CBS News, ‘Almost two-thirds of Ukraine’s 7.5 million children have been displaced in six weeks of war, U.N. says’ (April 2022).

³⁷ Note: under the Rome Statute, this applies to those under age 15 - however, the presence of those aged 15 to 18 may be a red flag for younger ages participating as well. See UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998, Article 8, para. xxvi.

ANNEX V: LEGAL BRIEFING

FAO: BELLINGCAT INVESTIGATORS
UKRAINE INVESTIGATIONS

RULES OF EVIDENCE

Why should we take into account legal considerations at this stage?

1. If the material collected as part of this project is ever used in a court case, the defence will ask about the circumstances in which it was obtained, processed and stored. Investigators may have to testify in court as to how they discovered the content and be cross-examined by defence lawyers.

The testing of evidence

2. Fair trials give the defendant(s) the opportunity to challenge the evidence against them. Where the defence disagrees with the evidence of a witness, they can require that witness to attend court to give evidence and have their account challenged. This may include testing their evidence through cross-examination. The defence might examine that witness's credibility, memory, motives, and anything else that could cast doubt on their account.
3. A piece of digital evidence (for example, a video), raises important considerations for the fairness of a trial. Generally, evidence in a criminal trial is 'produced' by a witness who can speak to its provenance and reliability. A familiar scenario is a crime scene photographer who is available to attend court if necessary; if the defence say the photographer has been biased and presented the scene unfairly, the defence have the opportunity to cross-examine the photographer about their actions. Another example is CCTV footage, which can be produced by a police officer who has checked the timing of the CCTV to ensure its accuracy, or

produced by its owner who can speak to how the collected footage is stored. Challenges to the integrity or continuity of the digital material can, in these circumstances, be responded to by a witness. No such option is available in the case of information obtained online.

4. Challenges to evidence obtained online could be made by alleging that its use is inappropriate for a number of reasons, most likely:
 - **Impartiality:** It was collected as part of a biased investigation. This is where the **methodology** comes in.
 - **Authenticity:** It has been tampered with, doctored or edited (either before it came into the possession of Bellingcat or after). This is where both **preservation** and **verification** come in. Preservation, of course, takes place so that no such allegations can be made about manipulation while the file is held by Bellingcat. The authenticity of the video at the point of discovery would ultimately be proven by an expert witness in court, which could be a Bellingcat analyst or someone who was not involved in the investigation. Other experts could also be called, for example digital forensics experts, image science experts or image comparison experts..
 - **Reliability:** Its contents are unreliable, for example because it depicts a partial picture or because it depicts things which cannot be further tested, like hearsay evidence or the presence of moveable items like bomb remnants. An analysis of the first online source of the item will be relevant to reliability (as well as authenticity).
5. This is why it is possible that Bellingcat's investigators could be asked to give evidence about how the evidence was obtained, processed and stored. Participation in the J&A Unit assumes willingness to appear as a witness.

Admissibility and weight

6. Specific rules on admissibility will differ from jurisdiction to jurisdiction but there are principles of broad application that it is helpful to have in mind. By way of examples, this note touches on common practice in England and Wales in addition to the International Criminal Court's rules of evidence.

7. An admissibility assessment decides whether evidence can be put before a court at all in a given proceeding. For example, in England and Wales, decisions on the admissibility of evidence are based on a two stage test. The first stage is **relevance**. Evidence is relevant if it is logically probative or disprobative of some matter which requires proof. Probative means “serving to test or try.” The next step is whether any exclusionary rules apply. All relevant evidence is presumed admissible; but the court has a discretion to exclude otherwise admissible evidence if it renders the proceedings unfair. If a piece of evidence is admitted into proceedings, the jury will then decide what ultimate weight to afford to it after hearing all of the evidence, including evidence from witnesses about how the item was found and analysed.

9. At the level of the International Criminal Court, the admissibility threshold is lower, with greater focus instead placed on what weight the judge will attribute to the content. Much the same analysis of authenticity and reliability will be involved, but in a slightly different procedural order. Weight will be attributed according to common sense. Just as it can influence admissibility, very methodical investigations and verification work can significantly increase confidence in the authenticity and reliability of a piece of content, resulting in increased weighting.

Fairness and exclusion of evidence

10. The overarching exclusionary rule in England and Wales is that judges have a discretion to refuse to admit evidence if in their view it would have an unacceptably adverse effect on the fairness of the proceedings. In making such a decision, the judge will take into account all of the circumstances, including the circumstances in which the evidence was obtained. This can often translate into a balance between the probative value of an item and how prejudicial the item would be to the defendant. At the level of the ICC, evidence can be similarly excluded if its prejudicial effect outweighs its probative value.

11. Applying these concepts to online audiovisual content such as a video depicting an attack:

- Stage 1, Relevance: A video which depicts the events being tried is relevant, because it serves to test or try parts of the allegations which need to be proven. If the video is manifestly and wholly fake or repurposed, it will be irrelevant, since it has no potential to prove anything.
 - Stage 2, Admissibility: If the video’s authenticity and reliability is then contested, the evidence of authenticity and reliability will be weighed against the adverse effects on the judge or jury of seeing the video.
12. Often, nothing can be said about the reliability or authenticity of open source evidence until some analytical work is done on it (whether that be into the source, the file or the content itself). Verification of OAVC essentially increases the degree to which it is fair to introduce that evidence, because it speaks to its authenticity and reliability and therefore its probative value.
13. **Hearsay evidence** is any statement not made in court by a live witness, if it is being introduced as proof that such a statement is true. A classic example would be a witness who tells the court “X told me he saw Y take the car.” X is not present in court for their statement to be challenged so this cannot be relied on as proof that Y took the car; it can only establish that X said so to the witness.³⁸ It makes sense, then, that hearsay is generally inadmissible in England and Wales, because it often cannot be tested at all, and is therefore more likely to be unfair to the defendant. Hearsay is not automatically excluded at the ICC and other international tribunals but is treated with caution. OSI content often contains or is accompanied by hearsay evidence, but this should not deter the collection of the content, because it can be verified and tested in other ways. Not all speech or writing will be hearsay – this can be discussed further with the legal team if required.

³⁸ An OOSI example could be a tweeted video of an explosion accompanied by the text “school full of children bombed today in Sa’ada, Yemen”. This effectively contains the statement that “this video depicts a bomb hitting a school while the children were inside”, but that statement is clearly not being made in court by a witness. Unfairness to a defendant might arise out of any inability to question the maker of the statement on fundamentals such as: Are they the maker of the video? When did they film it? Has it been altered? Could anybody else have altered it? How do they know there were children in the school? Are they a credible and reliable witness? Therefore the video could be submitted as evidence of what it actually shows, but not as evidence that the statement accompanying it is true.

PART II: KEY STEPS OUTLINED IN THE METHODOLOGY

14. The principles and concepts outlined above are what informs the methodology, in particular the following key steps.

The requirement to pursue all lines of reasonable enquiry including those leading towards evidence that may explain the attack or suggest alternative attribution

15. The role of an investigator is to try to establish, with an open mind, what happened in respect of a particular incident. For example, if a police investigator ignores, or doesn't notice, evidence that would exonerate a suspect, that is clearly not fair. The same principle applies to online investigations, which should pursue all evidence that points away from, as well as towards, a violation of international law or a particular suspect's guilt. Essentially, you should ensure to investigate *all possible explanations* for the incident you are investigating. Examples of lines of inquiry that are relevant for the crimes you are investigating are set out in your Table of Factual Inquiries.
16. Exculpatory evidence is evidence that excuses or explains the incident and suggests that it did comply with IHL or was not a criminal offence, or otherwise may point to innocence if there is an Accused. A key example in this context is evidence that shows the presence of military targets in the area before or during the attack (e.g. fighters from the opposing side, checkpoints, military bases, weapons stores, sites of production of materials to support the war effort). Exculpatory evidence could also include evidence that casts doubt on accepted presumptions about who was responsible for an attack. However, because these investigations are taking place long before any specific charges are being brought against a particular person, the use of the term 'exculpatory' is a little premature. Because of this, we state that investigators must actively search for information which could explain an attack or suggest alternative attribution.

Recording your searches and using VPNs

17. In order to demonstrate to an observer how you found certain relevant content, the methodology requires that you maintain a log of search terms in addition to using Hunchly, which tracks your online activity. This has the function of recording whether you did carry out an unbiased search and did pursue all possible lines of inquiry.
18. Similarly, the use of VPNs and the clearance of cookies before the creation of a new research account is to create a standardised starting point in respect of information available to search algorithms. However, the extent to which algorithms would affect searches of the type carried out by Bellingcat is questionable (see Annex I); these measures are taken out of an abundance of caution.

Retaining all relevant content and background content for disclosure purposes

19. A defendant is usually entitled to ask for disclosure of all of the relevant background information that could assist them with their defence. The disclosure threshold is anything which *“can reasonably be considered capable of undermining the prosecution case against the accused or assisting the defence case and will include anything that tends to show a fact inconsistent with the elements of the case that must be proved by the prosecution.”* The [War Crimes and Counter Terrorism Command](#) of the UK’s Metropolitan Police (SO15) define relevant material as *“any material that appears to have some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances unless it is incapable of having any impact on the case.”* Examples from the UK’s War Crimes/Crimes Against Humanity Referral Guidelines for third party referring organisations include:

- any information which casts doubt on the reliability of a prosecution witness or on the accuracy of any prosecution evidence
- any motives for the making of false allegations by a prosecution witness
- any material which may have a bearing on the admissibility of any prosecution evidence
- the fact that a witness has sought, been offered or received a reward
- any material that might go to the credibility of a prosecution witness

- information that a person other than the accused was or might have been responsible or which points to another person whether charged or not (including a co-accused) having involvement in the commission of the offence.
20. Examples given by SO15 of relevant background material in the context of traditional evidence that would need to be retained and potentially disclosed to the defendant are “*any rough drafts of statements from victims, notes of telephone conversations with witnesses, medical notes, legal documents, emails, case notes etc.*”. In the context of open source digital evidence this would include all work relating to the investigations given that the test for disclosure is whether the information could undermine the prosecution’s case or assist the defence’s case. An example of a record that may need to be disclosed would be a conversation between investigators in which they agree to ignore a piece of information which points away from a particular suspect, or comments suggestive of an inability to remain unbiased. Note that not all relevant content needs to be disclosed – only content that meets the undermine/assist threshold does. At the relevant time, all of the records could be handed to the prosecution for them to go through and select the disclosable parts, or else Bellingcat could – likely with the assistance of external counsel – perform a disclosure review in-house and then turn over the disclosable materials to the prosecution.
21. This requirement is addressed in the methodology through the requirement to use Hunchly throughout the duration of your investigation which will create a record of your online activity. Google Docs retains information about changes in drafts, which can be of interest to the Defence if changes meet the undermine/assist threshold.
22. Note also that your records may contain a lot of irrelevant content. For example, Hunchly will collect a range of information that could never have a bearing on any matter in any criminal trial.

Preserve all relevant material

23. Digital evidence should be preserved in a manner that will enable a robust chain of custody to be demonstrated. This will be done through Mnemonic (see

methodology). Mnemonic will take care of the immutable preservation of the content. If you are unsure of whether to enter an item into the preservation sheet, either enter it just to be safe or consult one of the legal team.

24. Uwazi is an analysis database and does not perform preservation. However, for the reasons outlined in this document and in the methodology, anything that could be relevant to an offence will be e logged in Uwazi.

Presentational considerations

25. It is much more helpful to an official investigator or prosecutor that the information you obtain is set out in neutral language, free from legal or moral commentary. In addition to reinforcing your objectivity, it helps to provide a uniform and comprehensive basis for Bellingcat to pass this information on to the relevant authorities or for private lawyers to use it. Following the style guides and language recommendations ensures uniformity. Remember that at this stage, you are not giving expert opinion, so it is not necessary to arrive at a view on anything. However, if you do have opinions on the authenticity or significance of information, it is best to follow the language guidance..
26. Having a uniform presentational style also increases the trustworthiness of the content to outsiders. Note that because your writing is not for journalistic output, there should be no impulse to truncate analysis or descriptions.
27. Another very important function of your write-up and research notes is to trace back through your analysis if you ever are required to appear in court. They should therefore be comprehensive enough so that you or another person could retrace your steps.

PART III: WHAT FACTS ARE RELEVANT TO THE INVESTIGATION?

28. This is a reference document for you to consult whenever you need to refresh your understanding of the legal framework. The legal team is always available for individual queries, large or small, on Slack and Signal. Please read this section with your Table of Factual Inquiries.
29. The objective of your investigations is to seek out information relevant to whether violations of international law are taking place in Ukraine. This requires investigators to have a basic understanding of the relevant international laws and offences so as to be aware of what factual information is relevant. This will enable you to apply your knowledge to develop lines of inquiry using common sense.
30. The project has a very broad remit, which includes:
- International humanitarian law (**IHL**) – the law governing parties' conduct during armed conflict; Serious violations of IHL are war crimes.
 - International criminal law (**ICL**): war crimes, crimes against humanity, genocide;
31. Many events will have the potential to relate to both bodies of law and, as such, we have decided to extract the relevant factual questions that are common to a range of IHL and ICL rules and offences. What follows is a short overview of the two areas of law so that the relevance of the factual inquiries will be clear. Although ICL is the main focus of this project, it makes sense to start with IHL, because IHL needs to be understood before war crimes can make sense.

IHL: Fundamentals

32. IHL covers a wide range of categories of conduct with the ultimate aim of balancing the requirements of military necessity against the need to minimise unnecessary suffering in war. It covers:

- Who and what can be attacked;
- The humane treatment of civilians and persons *hors de combat*;
- Prohibitions on specific methods of warfare, including specific weapons;
- Requirements for forces operating in civilian areas to take steps to keep them safe.

Who and what can be attacked

33. Given the overall purpose of IHL as stated above, not all attacks will be unlawful. Regardless of the lawfulness of the fact of the invasion itself, now that a conflict is ongoing, the Russian army is entitled under IHL to carry out attacks against Ukrainian forces and vice versa. However, they are only permitted to attack certain targets.

34. Attacks during hostilities are governed by the principle of distinction. The principle dictates that only military objectives can be attacked, and not civilians or civilian objects. The definition of a civilian object is any object which is not a military objective. A military objective is defined according to a two stage test:

*“In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action **and** whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”*

35. This means that investigators should consider whether there is evidence of the nature, location, purpose or use of the affected object which may have made it a military objective. Military occupation of civilian locations such as schools or hospitals is a common claim made by attacking forces – such possibilities should be thoroughly investigated where possible.

36. In addition to protecting civilian objects generally, IHL affords specific protection to a range of objects, including medical facilities and cultural and religious property. All of these prohibitions are subject to the objects becoming military

objectives, but in some cases the threshold is higher before they can be attacked. The main investigatory questions would remain the same no matter what kind of ostensibly civilian object has been attacked.

37. The following actions are violations of IHL:

- deliberate targeting of **civilians and civilian objects**;
- the launching of **indiscriminate** strikes (which includes attacks that are not directed at a military target or which use a weapon that cannot distinguish between the target and surrounding civilians or civilian objects).
- Attacks aimed at military objects but which would cause excessive civilian harm relative to the military advantage anticipated (**disproportionate** attacks);
- failure to take all feasible **precautions** before launching a strike;

38. The principle of precautions in attack includes the following obligations, which are important to distinguish from one another:

- “to do everything feasible to **verify** that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection”, e.g. cultural objects;
- “to take all feasible precautions in the **choice of means and methods** of attack” in order to **avoid or minimize civilian harm**;
- to “**refrain** from deciding to launch any attack which may be expected to” violate the principle of proportionality;
- to **cancel or suspend** an attack “if it becomes apparent that” the principles of distinction or proportionality may be violated; and
- to offer “effective advance **warning**...unless circumstances do not permit”.

39. Compliance with IHL is assessed based on the decision made by the commanding officer or pilot **at the point when the attack was launched**. It is not assessed based solely on the consequences of an attack. Therefore, in addition to analysing what took place, you should inquire about what information could have been available to the attacker *before* they launched the attack. An intuitive example is a

clearly visible red crescent on the roof of a facility which has been targeted. The presence of such a symbol could indicate that the attacker knew, or would have known had they taken precautions, that the location was protected. Similarly, if a crowded market is attacked, it can be relevant to assess what the location looked like from above, so as to assess whether the location appeared civilian to a pilot or commander (e.g. from the presence of market stalls) or even what the attacker might have anticipated in terms of civilian harm even if a military vehicle had just driven into the market, which is relevant to proportionality.

40. A civilian is anyone who is not a member of the armed forces. IHL prohibits attacks against civilians generally, however if a civilian takes a direct part in hostilities, they can be targeted. Such civilians who are not formal members of the armed forces are targetable only “*and for such time as they take a direct part in hostilities*”. This has been held to require a civilian directly to cause harm of a military nature, above a certain threshold, specifically designed to support a party to the conflict. Therefore, some civilians working to make soldiers’ uniforms in a factory³⁹ or making camouflage netting in their homes would be unlikely to reach the threshold of taking a direct part in hostilities, but civilians preparing Molotov cocktails for imminent use might.
41. This means that it is relevant to investigate whether there is any information about what people, even if wearing civilian clothes, were doing at the time of an attack.
42. A fuller list of relevant information to seek out concerning attacks between belligerents is listed in the Table of Factual Inquiries. Please use your judgement to expand or contract your inquiries on a case by case basis.

The humane treatment of civilians and persons *hors de combat*

43. This is a large part of the body of IHL. Civilians are as defined above, while persons *hors de combat* may be members of the armed forces who cannot fight because they are captured, in ill health or have surrendered. Such persons must

³⁹ In this case, the factory might be targetable but not the civilian workers. If so, it should be targeted at night when they are not present.

be treated humanely, and the following are prohibited by IHL: (list not exhaustive)

- Violence to life (including murder)
- Torture and cruel, inhuman or degrading treatment
- Rape and other forms of sexual violence
- Hostage-taking
- Discrimination
- The use of human shields
- Arbitrary deprivation of liberty
- Collective punishment

44. There are a series of rules relating to the dignified treatment of the dead, missing persons, persons deprived of their liberty and displaced persons. These can be explored if it appears they become relevant.

The prohibition on specific methods of warfare

45. Some specific kinds of munitions are prohibited absolutely. Investigators should take note of these weapon types, which are listed at Rule 71 of The ICRC Customary IHL Database. Cluster munitions are not automatically prohibited by customary international law, only under the Convention on Cluster Munitions, to which Russia and Ukraine are not parties. However, they are always of interest to document because of their extremely wide areas of coverage and the longevity of the life of the submunitions, making them effectively indiscriminate when used in areas inhabited by civilians.

46. In general, weapon type is important to identify if possible because it not only goes to the questions above relating to whether an attack was indiscriminate and/or proportionate and/or whether the attacker took feasible precautions, but it can also link an attack to a particular party, as well as providing information about anticipated destruction levels, whether the attack hit its intended location or could be directed at a specific location (if it was a precision-guided missile), and more.

47. There are also many specific methods of warfare which are prohibited, including:

- Starvation of as a weapon of war;
- Destruction or seizure of the enemy's property without military necessity;
- Pillage and looting;
- Attacks against objects indispensable to the survival of the civilian population;
- Refusing to allow humanitarian access.

The protection of civilians under a force's control

48. IHL requires that belligerents take steps to ensure they protect civilians and civilian objects in areas they control. The relevant rules are:

- The requirement to take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks. This means doing things like constructing shelters and the withdrawal of the civilian population to safe places.
- The requirement to avoid (to the extent feasible) locating military objectives within or near densely populated areas
- The requirement to remove (to the extent feasible) civilian persons and objects under [the party's] control from the vicinity of military objectives. This is related to the rule against the use of human shields.

ICL: WAR CRIMES, GENOCIDE AND CRIMES AGAINST HUMANITY – RELEVANT KEY POINTS

49. This briefing focuses on the Rome Statute of the International Criminal Court (ICC) as the basis for its outline of international crimes, but it should be noted that this is not the only source of international criminal law. The three categories of atrocity crimes under the Rome Statute that could be relevant in this context are war crimes, crimes against humanity and genocide. Each crime or group of crimes is listed in the Rome Statute and further broken down into the Elements of Crimes, each of which needs to be satisfied before a person can be found guilty.

War crimes

50. Serious violations of the IHL provisions set out above are war crimes, which are itemised in Article 8 of the Rome Statute. A relevant **selection** of war crimes for the purposes of this project is:

- Grave breaches of the Geneva Conventions, including murder, torture or inhuman treatment, wilfully causing great suffering, or serious injury to body or health, unlawful deportation or transfer or unlawful confinement;
- Other serious violations of IHL, including attacking civilians, attacking civilian objects and other protected objects, disproportionate attacks, attacking undefended towns, killing or wounding a combatant who has surrendered, the transfer into occupied territory of the population of the occupier, the transfer of the local population within or outside the territory, pillaging, using certain prohibited weapons, rape and other sexual violence, outrages on personal dignity, in particular humiliating or degrading treatment, using civilians as ‘human shields’, and intentionally using starvation of civilians as a weapon of war.

51. Note that failure to take precautions and indiscriminate attacks are missing from this list. This is because the ICC has a high culpability threshold for intent – reckless or negligent attacks are not war crimes under the Statute (see below). However, the ICC will be interested in indiscriminate attacks or attacks conducted without precautions because judges could *infer* the intention to attack civilians from some such attacks, in certain circumstances. The types of factual inquiries that will be relevant to the above selection of war crimes are set out in the Table of Factual Inquiries.

Crimes against humanity

52. Crimes against humanity are a collection of grave acts which, when carried out as part of a widespread or systematic attack against a civilian population, amount to an offence under Section 7 of the Rome Statute. A relevant selection of the acts is:

- Murder;
- Extermination;

- Deportation or forcible transfer of population;
- Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law;
- Torture;
- Rape and other forms of grave sexual violence;
- Persecution of certain groups of people, including on national or gender grounds;
- Enforced disappearance;
- Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

Meaning of “widespread or systematic attack”

53. According to Art. 7(2)(a) of the Rome Statute, an “attack” is a “course of conduct involving the multiple commission of acts against any civilian population, pursuant to or in furtherance of a State or organisational policy to commit such attack.” The “policy” that underpins the attack, which is referred to in Art. 7(2)(a), can be one adopted either by the State or by some other organised group. **It does not have to be a formal programme, and its existence can be inferred from the totality of the circumstances, including events, political platforms, public statements, propaganda programmes, and the creation of political or administrative structures.** However, the policy must contemplate the general type of act of which the individual perpetrator is accused and must be actively promoted or encouraged by the State or organisation in question. Note also that the ICC’s Elements of Crimes indicate that *inaction* can amount to implementation of a policy if there is evidence that the inaction was consciously aimed at encouraging the attack.

54. The attack must be either widespread or systematic — it need not be both. The former refers to the scale of the attack and/or the number of victims, while the latter refers to the organised nature of the acts and the improbability of their having occurred randomly:

- An attack is “widespread” if there is “massive, frequent, large scale action, carried out collectively with considerable seriousness and directed against a multiplicity of victims”. The attack’s widespread character can be derived

either from its extension over a broad geographical area, or from there being a large number of victims.

- An attack is “systematic” if it was organised and planned. The ICC generally requires evidence that the acts of violence comprised a pattern and their repetition was non-accidental. In *Blaškić*, the ICTY held that a systematic attack has the following ingredients:
 - a) There is a political objective, i.e. a plan pursuant to which the attack is perpetrated or an ideology that aims to destroy, or persecute, the attacked community. That plan does not need to be expressly declared or formally adopted by the State, but can be inferred from circumstances like the political background and political programmes, media messaging and incendiary propaganda, the imposition of discriminatory measures, and the scale of acts of violence;
 - b) Crimes are perpetrated on a large scale against a civilian group;
 - c) Significant public or private resources are prepared and used; and
 - d) High-level political and/or military authorities are implicated in the definition and establishment of the plan.
55. Therefore, if it appears that some particular kind of conduct is happening on a repeated basis and/or appears organised, it may be necessary to focus on certain patterns of attack or to direct your inquiries to establishing whether there is evidence that the repeated conduct is in fact part of a coordinated attack or whether the incidents are isolated. You can see from the above that there are plenty of objective lines of inquiry which can be pursued online, for example tracking and preserving public statements by the relevant people and groups, and logging any incident which appears relevant to the potential attack (whether it is consistent or inconsistent with the existence of a policy or organised system). To establish a pattern analysis or to develop a working hypothesis as to crimes against humanity, discuss this with the legal team.
56. Your Table of Factual Inquiries has some guidance as to what you can look for in individual attacks which could help to assess whether there is evidence that an individual attack formed part of a coordinated, larger attack.

Genocide

57. Genocide is set out in Section 6 of the Rome Statute and is committed when one or more of a series of acts is carried out with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such. The acts are:

- Killing members of the group;
- Causing serious bodily or mental harm to members of the group;
- Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part;
- Imposing measures intended to prevent births within the group;
- Forcibly transferring children of the group to another group.

58. The “as such” part of the crime of genocide is crucial and is what elevates this crime above other offences. The attempt to destroy must be conducted out *because the people belong to the group in question* – it is not enough if a large population belonging to a certain group are harmed for another reason (such as to achieve a military advantage), no matter how egregious the act is. Your Table of Factual Inquiries has some information about what might be indicative of genocidal intent.

59. War crimes can only occur in the context of an armed conflict, whereas crimes against humanity and genocide can occur in peacetime or during war.

Mental Element

60. The mental elements of the crimes are often the most complex and the hardest to evidence, let alone using open source information. All investigators can do is to gather as much information as possible to allow an assessment of the mental element of each alleged crime. The main bulk of your investigations are likely to be taken up with documenting the objective events that have taken place, as opposed to finding direct evidence in open sources of the attacker’s intent, but clues as to the latter might appear online. It is therefore important to be familiar with the requirements of the mental element of Rome Statute offences so that you recognise any such clues as they may arise in the course of your investigation.

61. Under Article 30 of the Rome Statute, the mental element of crimes is established “only if the material elements are committed with intent and knowledge”. This means that the person carried out the relevant *conduct* on purpose (i.e., they did not accidentally discharge their weapon or miss their target) and that in respect of the consequences, they either *actively intended* the consequence – e.g., death - to occur, or *knew* it would happen in the ordinary course of events. The Rome Statute offences cannot be committed recklessly – a belief in a *risk* that a consequence will occur, however high, is not enough. In respect of superiors only, there can be criminal liability where the superior *should have known* what their subordinates were doing - see below on command responsibility.⁴⁰
62. To a large extent there is a common sense element to assessing intent. For example, if people have been found shot in the head, it is unlikely to be questioned that the person who shot them intended to cause their deaths. Where it becomes complicated is in the context of the law of armed conflict, where aerial attacks have harmed civilians and the evidence cannot definitively establish what the *main aim* of the perpetrator was, or where additional mental requirements need to be satisfied to establish crimes against humanity or genocide.
63. That being said, whatever crime you are investigating, the most relevant questions will be the following:
- What did the perpetrator **know**? This can be ascertained either directly or through inference. For example, where an extremely large red crescent is visible on the roof of a building at the moment it was bombed, an inference could be drawn that the attacker knew they were targeting a facility ordinarily dedicated to medical treatment.
 - What was the perpetrator actually trying to do? For example, in the case of an airstrike on civilian apartment block, if there is evidence that their aim was to kill civilians, this is evidence of criminal intent to attack civilians. If there is evidence that they thought a military unit was sleeping there, this would suggest that the aim was to attack the fighters. This would not

⁴⁰ However, please note for completeness that in some jurisdictions, crimes can be committed recklessly because the customary international law standard or domestic standards are applied, which can include recklessness.

necessarily be determinative of whether the strike was lawful, but it illustrates the relevance of finding out the attacker's **actual objective**.

- **Why** did the perpetrator do what they did? Is there evidence of their reasoning? Examples would include:

- i) Reports of intercepted calls in which troops tell their superiors that it's impossible to spare civilians and that the only way to win is to destroy everything. This would be suggestive of a widespread policy of attacking all targets indiscriminately as a means of ensuring that the military ones are struck;
- ii) Reports of soldiers in Tigray [telling a woman](#) that they were raping her and making her infertile because they believed no Tigrayan womb should give birth. This is evidence of an intent to destroy Tigrayans as a group through birth prevention, and of an intent that an individual rape be committed as part of a widespread or systematic attack against Tigrayan civilians;

64. The crime of genocide requires additional, “special” or “specific” intent – in addition to the requisite intent for the underlying acts: an *“intent to destroy, in whole or in part, a [protected] group, as such.”* If murder is carried out without that intent, it could still be a war crime or even part of a crime against humanity, but will not amount to genocide.

65. To attract criminal liability, individual acts forming part of crimes against humanity must be committed with the knowledge or intention that the act is being done as part of a widespread or systematic attack against a civilian population.

Command Responsibility

66. Commanders or superiors who are actively involved in the offences in some way, for example through ordering them or aiding and abetting them, can be convicted on that basis. It is for this reason that mapping of command and control lines and activities of the various army structures is very important.

67. Another reason is that superiors bear criminal responsibility for crimes committed by those under their control, where they have failed to prevent those crimes from being committed, or failed to punish those who have committed crimes. Under this command responsibility framework, superiors can be held responsible even if they did not know *but should have known* (or consciously disregarded information indicating) what their subordinates were doing. This is also particularly important in contexts that do not necessarily have a “formal” military structure - what would need to be demonstrated is that the forces were “under his or her effective authority and control”. Note that this is an exception to the high intent threshold for the core acts as described above.

Translating this into factual inquiries

68. Although the three categories of crimes have different structures, in many cases the same underlying harm type will be common to all of them. For example, if a large number of civilian bodies are discovered, it could be evidence of war crimes, crimes against humanity, genocide or all three. Similarly, if significant destruction of property is caused by shelling, the destruction is necessary to document whether the crime alleged is a direct attack on civilian property, a disproportionate attack, or an attack on a protected object. It could also indicate that the forces who were the object of an attack unlawfully stationed themselves beside a civilian target. Therefore, rather than exhaustively list the elements of each crime, we have decided to identify factual enquiries common to all or most of the relevant Rome Statute crimes and to set those out in the Table of Factual Inquiries (in addition to adding some sparingly used tags in the database).

ANNEX VI: FACTUAL INQUIRIES AND THEIR RELATIONSHIP TO THE ELEMENTS OF CRIMES

Please note: this is a guide to what is relevant. You do not need to go through these questions sequentially - use your own judgement

Factual inquiry	Relevance	Comments
GENERAL		
Where was the incident?	General relevance to establish objective facts of incident.	Locate this incident in space. If there are multiple locations, such as in a MLRS barrage, then describe the relevant locations.
When was the incident?		Try to establish the time of the incident, using any method that you can.
Who and what was present?		Was any military activity observed in the area, including vehicles? Are there people carrying weapons? Are there individuals with military uniforms? Are there badges on these uniforms? Are they wearing control measures such as coloured tape around their arms or legs? Who is in the background of the content? If there are interviews from the scene, who is being interviewed? What languages are they speaking? What are they saying?
KILLING		
Who was killed? Where were they when they were discovered?	Core conduct for a range of crimes under the RS including genocide, crimes against humanity and war crimes.	This encompasses their status as civilians or members of the armed forces and their nationality or membership of any particular group. Also include the sex of the person if identifiable, and age if applicable (particularly if they appear to be below 18).
How were they killed? (incl. weapon type)		This relates to linkage but also is relevant to a range of other factors such as the lawfulness of the attack if it occurred in an armed conflict.
Who killed them?		
What were they doing when they were killed?		This relates to whether civilians may have been targetable under IHL because of their direct participation in hostilities.

Is there any evidence of why they were killed?	Relevant to questions of intent and the question of whether a widespread or systematic attack may be taking place.	For example, reports of what killers said (as recalled by survivors), or any public statements. If the killing was caused by an aerial attack, the justification by the attacking party is relevant (even if you do not know whether it is credible).
SGBV (Directly shown, or red flags?)		Are there any signs that SGBV could have been committed? (See SGBV annex)
INJURY, SERIOUS HARM		
Who was harmed?	Core conduct for a range of crimes under the RS including genocide, crimes against humanity and war crimes.	As above (for killing).
How were they harmed?		
Who harmed them?		
Is there any evidence of why they were harmed?	Relevant to questions of intent and the question of whether a widespread or systematic attack may be taking place.	
SGBV Red Flags?		Are there any signs that SGBV could have been committed? (See SGBV annex)
RAPE AND OTHER SEXUAL ASSAULT OR SEXUAL AND GENDER-BASED VIOLENCE (SGBV)		
Who experienced SGBV ? How many people?	Core conduct for a range of crimes under the RS including genocide, crimes against humanity and war crimes.	
How did they experience SGBV?		See SGBV Annex for definitions and indicators.
Who perpetrated the SGBV ?		
Is there any evidence of why they were targeted?	Relevant to questions of intent and the question of	E.g. the example of soldiers in Ethiopia explaining to a woman that they did so so because no Tigrayan womb should give birth. Other examples could be things soldiers said about rape being an entitlement

	whether a widespread or systematic attack may be taking place.	or a spoil of war, or because of a particular attitude to the women of the group to which the victims belong.
PROPERTY DAMAGE		
What was damaged?	Core conduct for a range of war crimes under the RS and could be relevant to, for example, the creation of unliveable conditions as a basis for crimes against humanity.	Including extensive inquiry into the use of the location at the time of attack, if possible, to establish whether the property was a military objective or civilian object.
If applicable, whose property was damaged?		Is there evidence of who lived in the area in terms of membership of particular ethnic or social groups?
How extensive was the damage?		This is relevant to proportionality, among other things.
How was it damaged? (incl. weapon type)		This is relevant to linkage and other issues like proportionality and whether the attack discriminated between civilian objects and military objectives.
Who caused the damage?		This could mean which forces or which individual battalion.
EXPLOSIONS / AERIAL ATTACKS [In addition to the above questions in relation to harm to people and property]		
What kind of munition detonated?		This is of general relevance to many areas, including identifying the perpetrator, identifying the accuracy of the munition, identifying its blast area, which is relevant to IHL considerations, and more.
Is there any evidence of the direction the munition came from?	Linking the attack to the perpetrator	
What did the location look like from above?	Relevant to the mental element of knowledge in cases of attacks which harm civilians	
Was there anything relevant about the		

scene which would have been visible from above?		
Were there military structures, installations or other assets in the area?		Conduct a search in the immediate vicinity (using 200m radius as a guide, but please vary according to the situation) for any military installations on satellite imagery using Google Maps, Wikimapia and other relevant sources. Be clear to differentiate between military structures and military activity.
Was there any crater or remnants?		
Are there any indications of what the location was being used for? What was happening at the time of the incident?		
Has the area been targeted more than once? When?		
What forces were operating in the area?		
Were there any secondary explosions?		
Did more than one munition impact occur?		
Is there any evidence of why the munition was launched at this target?		
PROPERTY APPROPRIATION		
What property was appropriated?	Core conduct for war crimes under the RS including pillaging.	
Who appropriated it?		

What did they do with it?		
CREATION OF CONDITIONS LEADING TO DEATH OR SERIOUS HARM		
What conditions were created?	Core conduct for a range of crimes, including crimes against humanity, genocide and the war crime of starvation.	E.g. the town was cut off from the outside world such that no supplies could enter.
How were the conditions created?		E.g. blockades of all roads leading into the town; shelling of food stores
What was the effect on the civilians?		E.g. Civilians starved
Is there any evidence of a policy in place, either through patterns in behaviour or direct evidence such as leaks or statements?		
USE OF PARTICULAR WEAPONS		
Was an unconventional weapon used? What was the weapon?		Apply this along with all the relevant questions for explosives generally.
Was a cluster munition used? Where was it used?		Apply this along with all the relevant questions for explosives generally.
If there are incidents which appear to have a lot in common or take place on a repeated basis or wider scale: (discuss any such analysis with the legal team)		
Is there any evidence of a policy in place? Are there any public or leaked statements from the party alleged to be responsible?	Pertains to whether the acts are part of a widespread or systematic attack, or whether the conduct was done with the intent of destroying part of a specific group <i>because of their belonging to that group.</i>	

<p>What similar incidents have taken place? What do they have in common, and what is different? How many have there been? If you are focusing on a particular pattern, create 'stub' incidents for all related allegations, even if they remain allegations. This is so you can group them and retain everything relevant. Discuss any patterns you identify with the legal team.</p>	<p>Goes to the widespread and systematic nature of an attack; if a range of attacks display an identical fact pattern, this could be evidence of a system in place.</p>	
<p>Is there evidence of the reason certain acts were conducted from the perspective of the immediate attacker?</p>	<p>Relevance to intent. The perpetrator must know or intend that the act form part of a widespread or systematic attack (CAH) or intend to destroy, in whole or in part, members of a particular group "as such".</p>	<p>E.g. things that were said to victims or on leaked radio conversations about the incidents. This has overlap with the harm types set out above.</p>
<p>Are there incidents of the same party showing restraint in similar circumstances?</p>	<p>This is important to establish whether some instances of harm are being carried out by rogue actors, as opposed to pursuant to a policy.</p>	<p>E.g. some soldiers not executing civilians where others are in the same circumstances.</p>

ANNEX VII: STYLE GUIDE AND NAMING CONVENTIONS

For general style guide formatting, please examine the [BBC Style guide](#). However, don't get too caught up in the specifics of this guide. The most important elements for formatting the incident assessments are listed below.

If in doubt, ask the lead researcher (Nick Waters) about how to format or word something you want to include in your assessment.

Where possible, describe your work in passive language. If you need to refer to yourself, use the terms 'primary investigator' and 'reviewing investigator' as appropriate. Do not identify yourself in the reports.

Neutral Language

When reporting these events, be sure to use neutral language. Report what you can see and assess with factual and neutral descriptions.

For example:

The video appears to depict a munition falling in a populated area. A man can be heard saying "There's been an explosion!" After around ten seconds, a second explosion occurs. The area appears to have shops that sell clothing items and food.

When describing what analysis you performed, do so in the passive tense where possible. For example:

Reverse image search was performed, and it appears that [this content](#) first appeared online at 1242 on 10/05/2022 on Telegram.

Online searches that do not result in usable UGC can also be recorded in your Research Notes document. For example:

Searched for the closest military base, which appears from this website (hyperlinking) to be located at [GPS coordinates]. The airbase shows that X jets were present 30 minutes before the strike occurred and Y jets were present after.

Jets at the closest airbase were identified as [model/make] based on measurements of wingspan and distinct characteristics.

Testimony published by [news source] claimed that civilians were walking around buying bread when the strike hit.





Try to identify the items by their name as it will appear in the database (i.e. their unique value), so that they can be cross-referenced.

Date & Time

Write all dates in the DD/MM/YYYY format. For example, 03/12/2015. When exact time can be referenced, use the 24 hour clock set to Eastern European Standard Time. For example, 1545. When the time of day can not be referenced, use AM/PM or N/A.

Note that different social media will timestamp posts differently. See below for a quick guide:

How social networks display time and date

 3:13 PM - 15 Sep 2015 Time and date shown in the timezone selected in your Twitter settings , not the local time of the user who posted the tweet If you are not logged in, you will see time and date in Pacific Time	 September 15 at 3:13pm Time and date shown in the timezone selected on your computer or device , not the local time of the user who posted the update
 Uploaded on 15 Sep 2015 Date shown in Pacific Time Using Citizen Evidence Lab's YouTube Data Viewer you can see the exact time it was uploaded in UTC (Coordinated Universal Time)	 3d Date shown in Pacific Time View the embed code to see exactly when a photo or video was posted, in Pacific Time

firstdraftnews.com

Note that Telegram posts display the time set to your mobile device or computer.

Coordinates

When entering coordinates, enter them in decimal degree format only.

For example:

*Geolocation determined that the image was captured at the following coordinates:
15.140625, 43.570938.*

Reporting Casualties

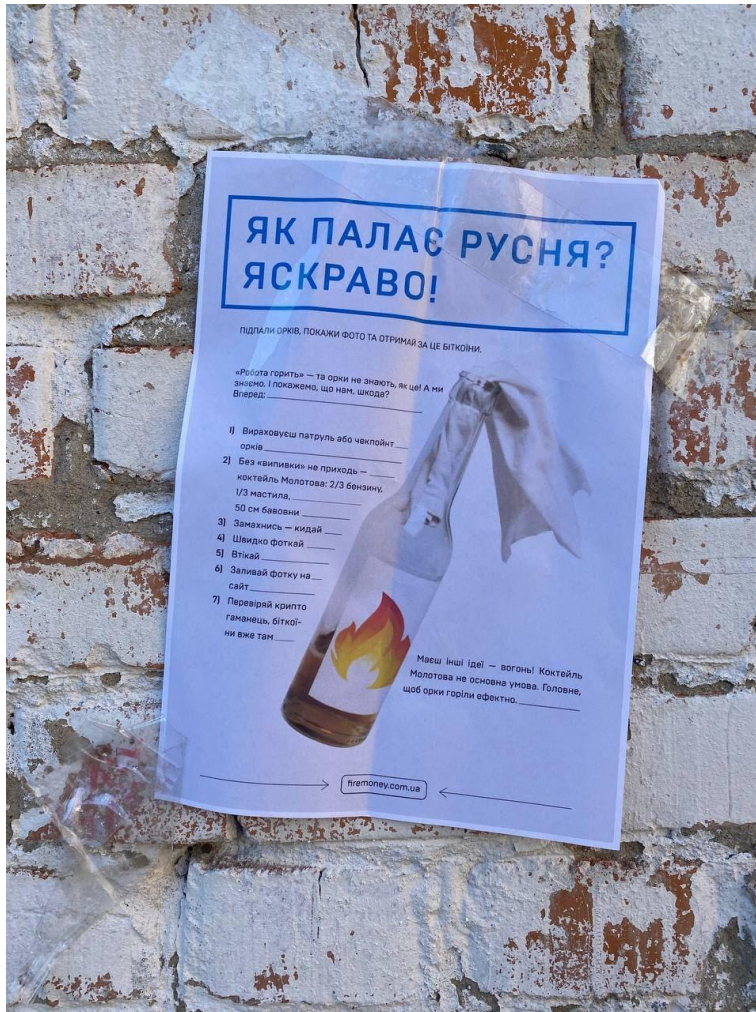
The language around casualties in conflict is very specific. Refer to this guide in order to correctly describe the events you are working on.

- “Fatalities” should be used to describe individuals who have been killed.
- “Wounded” or “injured” should be used to describe individuals who have suffered injuries, but who do not appear to be dead.
- “Casualties” is a broad term that can be used to describe both fatalities and injured. Ideally, use “fatalities” or “wounded” instead of “casualties”.

Images

Include a caption below the image in italics in font size 10 with a brief description and a hyperlink to the source of the image. The image and the caption text should be centered on the page. If used in the report, ensure to upload to the images file in the Ukraine Project GDrive.

For example:



The poster above, allegedly pictured in Kherson, contains instructions on how to make a Molotov Cocktail (Source: [Telegram](#)).

Satellite Imagery

When you use satellite imagery, describe where you got the image, if possible.

For example:

Satellite imagery was downloaded downloaded from Planet Labs and entered into Uwazi [INSERT ENTITY ID]

Include a caption below the satellite imagery in italics in font size 10 with the date the satellite imagery was captured. Ensure that you have the correct time that the image was

captured, as some services, such as Google Earth Pro, will show you the date the image was taken based on your location.

The caption should also credit the provider. For images from Google Earth Pro, please include, at the end of the caption: *(Courtesy of Google/XXXX)*. The XXXX in this case would be replaced by the organization displayed at the bottom center of the screen in Google Earth Pro.

For example: *(Courtesy of Google/DigitalGlobe)*.



A satellite image showing a destroyed building at the site of the airstrike on 04/02/2019 (Courtesy of Google/Digital Globe).

Graphic Imagery

Please only include graphic imagery in your report if the situation demands it. If you must include graphic imagery, censor any dead bodies, blood, and/or gore unless it is relevant to a point under discussion.

You can easily pixelate images using SnagIt by selecting More > Blur in the top menu. The intensity of the pixelation should be such that no discernable detail of the person's identity or the extent of their injuries should remain visible.

Footnotes

All source references should appear as hyperlinks in the text of your report. These should also be footnoted, in case a report is delivered as a printed product.

When including information from a source/link, please hyperlink the source directly.

Citing Offline Content

If you notice that a picture or video that you were going to reference in your report is offline, hyperlink it anyway: this will allow it to be identified in Mnemonic's database.

Discovering Earlier Sources

Your report's details should be comprehensive enough to allow a user to find the earliest instance of an item or source. If you later discover an earlier version of the same item or source, simply edit your report to add the earlier source and make a note of this in your research notes. Try to enter the earliest complete version in Uwazi. If you discover an earlier version after you have entered the item into Uwazi, discuss with the team leader.

Referring to Sources

Please ensure that you refer to sources consistently and with a hyperlink. For example, footage taken by the NEXTA Live Telegram channel may be defined initially as ("**Nexta Video 1**") and referred to as such thereafter. If there is a second Nexta video, refer to it in sequential order, as in "the Nexta Video 2". If you define a video like this, use capital letters, because it helps the reader to remember that it has been defined at the beginning of the document.

ANNEX VIII: INCIDENT ASSESSMENT TEMPLATE

Incident ID	XXXX [include CIVHARM and Uwazi Unique ID so it can be searched]
Location	Village, District, Oblast
Coordinates	xx.xxxxxx, xx.xxxxx (hyperlink to Google maps)
Date (Prima Facie)	DD / MM/ YYYY
Date (Assessed)	
Time (Assessed)	Time in 24 hr clock, Eastern European Time

Key Findings

- Key Findings in 2 - 4 bullet points

I. INTRODUCTION

Background Summary of Significant Descriptive Content

Conduct a media / literature review on the event and put those findings here. This should just be reporting what is in the Civharm spreadsheet.

First, describe your process for finding content: What search terms did you use? What searches were most successful? Then, list the content and sources you found below. If there is no Descriptive Content, move to your analysis of the examinable content.

Media Reports

- Name of the organization with hyperlink

NGO Reports

- Name of the organization with hyperlink

Other

- Name of the organization with hyperlink

Describe your searches.

II. Analysis of examinable content

Describe the items of examinable content you have found which you consider relevant. Describe your verification work here. This will form the main body of your Incident Assessment.

When describing social media posts, include:

- Date and Time of the post in EEST -- small description with hyperlink to the post
- Example:

Within your examination of the examinable content, include:

- Timeline of the Incident

Using open sources, describe the timeline of what happened. Don't fill in gaps if you are unsure, simply report and cite the events that happened in the order that the evidence indicates they happened in.

- Describe the events

Using open sources, now describe the events that took place in detail. You can pull on all other sections of your incident assessment in order to inform this section. Cite your open sources and your evidence in your description. If you cannot explain something that happened, it is just as important to note it anyway and describe why you cannot explain it.

III. Questions to address in your write-up

The questions to be addressed will differ depending on the type of incident. The Table of Factual Inquiries sets out some generic questions which will be common to most incidents, along with some harm-specific questions depending on the kind of event being analysed. This can be read with your Legal Briefing so that the relevance of these lines of inquiry is clear - but please discuss with one of the legal team if you have any questions. Please note that this is a guide to what is relevant. You do not need to go through all of these questions serially - use your own judgement.

IV. Statements from parties of the conflict

Ukraine

Include any statement made by the Ukrainian government about this incident.

Russia

Include any statement made by Russia about this incident.

V. Conclusion

A short and factual conclusion to summarize your assessment.

Further Action

Include here any further action that you think needs to be taken. This could include a follow-up investigation, a forensic analysis of some of the images, a data analysis of some data you noticed or collected, etc. It should also note if there are likely linked incidents.

ANNEX IX - UWAZI FIELDS

Provisional - under regular review - shared to encourage collaboration

Field	Instruction	Sample
INCIDENT		
Title	CIVHARM ID, OBLAST IN BLOCK CAPITALS, short description to help describe which incident this is	CIV0463, KHARKIV, Cargo warhead impacted into road outside what may be a healthcare facility.
CIVHARM ID		
Date	PRIMA FACIE - either claimed date, or date of first posting of the content.	
Assessed date or date	Only populate if you have assessed based on information other than descriptive claims.	
Reported civilian deaths	This can be loosely estimated based on credible reporting - it's for identifying the general seriousness of an incident - Bellingcat is not claiming to have verified these figures.	
Reported civilian injuries	This can be loosely estimated based on credible reporting - it's for identifying the general seriousness of an incident - Bellingcat is not claiming to have verified these figures.	
Description	This should give the reviewer a very short overview of what they'll find if they read the full report.	A cargo section of what appears to be a 9M55K rocket motor is seen embedded in a road on Novhorods'ka St, 4, Kharkiv, Kharkivs'ka oblast, Ukraine. The impact location is in a residential area, meters from a red cross location and across the road from a location registered on Google Maps as a school. The exact area of

		launch was not identified, however it was possible to identify the general direction of origin.
Level of investigation	Detailed or stub. Stub incidents are incidents which are backed up by either a credible third party claim or a piece of Examinable Content.	
Incident Assessment	Link to Google Doc	
Geolocation	Must be decimal	
OBLAST		
Type of object affected	From drop-down. Select all that apply.	
Military presence	Colocated, direct vicinity or broad area (within 1 KM). Threshold is 'yes or maybe', and 'maybe' will be satisfied if there is a claim that is credible. Spurious claims which cannot be backed up will be reported in the incident assessment but will not be logged through this filter. We have had to take a common-sense approach since distances become arbitrary depending on weapon type, density of building, and many other factors. Therefore, we have 'colocated' (e.g. a school being in use as a base), direct vicinity (e.g. so close that the actual affected object could feasibly have been hit by mistake, either because the weapon went off course or because the intel was a bit off), or 'general area'. There is no way to turn this into an exact science - it's just for filtering purposes.	
Cautions	To be selected if an item has been shown to be bogus, for example. You would also want to include a high profile incident even if it was staged or unsubstantiated so that you can show that you have looked into it.	
Research Notes	Insert Research Notes Google doc link under 'Label'.	
Type of attack	For filtering - can be populated if we're unsure. Includes explosives attacks and other killing and injury.	
Investigator Responsible	The first assigned investigator who writes the research report.	

Incident Assessment	[Duplicate]	
Implicated Unit	Only if concrete link and ensure link is explained in your Incident Report or in the Incident description. No automated linking. Consider the role of Incident Groups for linking units.	
Perpetrator	Leave blank unless further discussions take place	
Victim	Leave blank unless further discussions take place	
Investigated by	Select other NGOs or prosecutors if they have looked into this incident. Add as an actor if they are not already in the database.	
Ukraine Witness ID	If you know which item in the UW database the content relates to, enter it. It is helpful if you can take a minute to find it in their dataset (e.g. by searching the original links), but it is not necessary to trawl through and find it. Sometimes the J&A Tool auto populates these - they need to be checked.	
Red Flags	See SGBV and CAAC annexes	
Reason for Red Flag	Only complete if not obvious	
Generated ID	Automated - paste into Incident Assessment during Legal Review	
Incident Group	Attach to the relevant incident group, if there is one.	
Stage of investigation		
CONTENT		
Title	Name for reviewer to understand what the video shows - does NOT need to have the incident code, since it will be linked to the incident. Include what kind of content it is.	“Video of smoke column filmed from a distance” OR “Video of multiple small munition detonations” OR “Photograph of rocket motor lodged in path”
UW_CATEGORY	Ignore	
Original title on social media	Cut and paste the text associated with the content in the post	ПЗДЦ. Гаражи на Бучмы! Салтовка

Generated ID	Automated - insert into written report for each item.	
Incident	Link to the incident it refers to. If it refers to multiple incidents (e.g. is a composite showing the incidents in question), link to all the incidents. If it is a general piece of content that you can't link to a specific incident (e.g. denial of any Russian involvement in cluster munition attacks in February/March), then do not link here, link to the Incident Group.	
SITE_SIGNIFICANCE	This filter is going to be used to map military bases/activity and significant protected objects. It is only to be selected if the site would have significance for other incidents - e.g. if you discover that there is a military base or a hospital at the exact location. If in doubt, please consult with wider team as this filter's usefulness might only become apparent a little later and it needs to be used correctly.	
UW_ID	As with Incident - if you know the UW ID of the item, include it.	
Online link	Type 'Link' into the left field and include the live link.	
Archived_Link	This should be populated already but if the autoarchiver hasn't worked, it will need to be done manually (see Workflow).	
Graphic Content Warning		
POSTED_DATE		
POSTED_TIME	24 hour clock, local time	
FILMED_DATE	If you have this information, include it. It should be easier for things like satellite imagery. This will often be left blank	
Description	This is important to complete in Uwazi because otherwise someone looking at the database without the incident assessment open doesn't understand what the video shows. Especially important if the item doesn't clearly show the incident taking place or the aftermath.	
Geolocation	Insert location of event taking place and	

	point of filming if significantly different (e.g sometimes it can be hundreds of metres away). Tens of metres unlikely to be significant but include if the info is there.	
Content_type	This should be self-explanatory.	
People visible	Self-explanatory - should not be over-thought, since this is just for filtering purposes.	
Red Flags	See SGBV and CCACAnnexes	
Reason for flagging	Only complete if not obvious	
Images and video fields		
DEATH_DATE	Ignore - will be used if importing dataset on soldier fatalities	
SOLDIER_CAPTURE_DATE	As above	
Country	Populate - will make sense if we import the UW data where some is in Russia	
OBLAST [fix the thesaurus]		
Entered by	Initial person to enter the entity	
BULK_SOURCE	Deselect	
Source	Online source. Create actor if not present	
Linked Group of Incidents		
Open query?		
Query for		
Query		
ACTORS		
Name	Name as displayed on social media profile - copy paste	Война Украина Россия Труха ⚡ Украина
Image	Screenshot the person's social media profile or other image that can identify them visually, and upload from your desktop. This is not evidence and can be	

	deleted from your computer afterwards. It is just to aid recognition of sources.	
Description	[Describe source, including any comments about affiliations, credibility and length of presence online]	
Social media profile (1)		
Social media profile (2)	If you know the same source's other profiles, insert them here. Do not create a new actor for different accounts if you think they're the same person/entity.	
Profile/Home Page Screenshot	[if different from image]	
Type of Actor		
Status		
Entered by		

ANNEX X: ACKNOWLEDGMENTS

The methodology was kindly reviewed in-depth by an Independent External Advisory Panel, who gave oral and written feedback. Amendments have been made since their review, and all errors remain our own. The panel consisted of:

Dato' Shyamala Alagendra (International Criminal Lawyer: Prosecution/Defence/Investigations), Essa Faal (International Criminal Lawyer: Defence - Senior Partner, Faal & Co.), Dr Alexa Koenig (Co-Executive Director and Adjunct Professor, UC Berkeley School of Law), Professor Alex Whiting (Professor, Harvard Law School).

On data protection and privacy, we are grateful to Monika Sobiecki (Barrister, Bindmans LLP), Ben Silverstone and Alex Bailin QC (Barristers, Matrix Chambers)

Countless colleagues - too many to mention individually - have provided input on our work since 2018. We would like to particularly thank the following individuals and organisations, who have advanced this methodology in invaluable ways, both directly and indirectly:

Shina Animashaun; Darius Bazargan; Roksolana Burianenko; Brian Castner, Andrew Cayley KC; the Centre for Information Resilience; Paul Clark; Iona Craig; Jeff Deutch; Sam Dubberley; Jude Dugan; Global Rights Compliance; Hunch.ly; HURIDOCS; Dr Emma Irving; Dr Philip James, Joshua Kern; Azmat Khan, Hadi al-Khatib, Her Honour Judge Joanna Korner CMG KC, Helen Malcolm KC; Kelly Matheson; Libby McAvoy; Mnemonic; Shabnam Mojtahedi, Catriona Murdoch; Daragh Murray; Fabio Natali, Yvonne Ng; Dr Liam O'Reilly, Enrique Piraces; Emilie Pottle; Adam Rawnsley; Dan Robinson; Justin Seitz; Matel Sow; SJAC, Benjamin Strick; Friedhelm Weinberg; WITNESS; Nancy Yu; Wim Zwijnenberg, A Digital investigator, International Crimes Unit - Dutch Police.

Special thanks to Raja Althaibani; Rawan Shaif; Tara Vassefi.

We are extremely grateful to all of our generous funders. In particular, we would like to thank **Avaaz** and its supporters, whose generous contribution has enabled our work.