INTERNATIONAL NUREMBERG PRINCIPLES ACADEMY

E-Procedure

The Impact of the Increased Usage of Digital Evidence and Sophistication of Technology on the Rules and Practices of the International Criminal Court

Cluster D

The Correlations between Human Rights and International Criminal Investigations and their Relationship with Digital Evidence: Opportunities and Challenges

Published by:

International Nuremberg Principles Academy
Bärenschanzstraße 72, 90429 Nuremberg, Germany
www.nurembergacademy.org

ISBN: 978-3-9827094-2-0

Cover design by Martin Küchle Kommunikationsdesign
Cover picture: © Vecteezy.com

This publication was financially supported by the Federal Foreign Office of Germany.

Table of Contents

The International Nuremberg Principles Academy and its mandate

The International Nuremberg Principles Academy (Nuremberg Academy) is a non-profit foundation dedicated to the advancement of international criminal law and human rights. It was established by the Federal Republic of Germany, the Free State of Bavaria and the City of Nuremberg in 2014. The Nuremberg Academy is located in Nuremberg, the place of the first international trial before the International Military Tribunal. For the first time in history, an international tribunal was authorised to hold leading representatives of a state personally accountable for crimes under international law.

The foundation carries forward the legacy of the Nuremberg Trials and the “Nuremberg Principles”, which comprise the principles of international law recognised in the Charter of the Nuremberg Tribunal and in the judgment of the Tribunal. They were formulated by the International Law Commission of the United Nations General Assembly in 1950.

Conscious of this historic heritage, the Nuremberg Academy supports the fight against impunity for universally recognised international core crimes: genocide, crimes against humanity, war crimes and the crime of aggression. Its main fields of activity include providing a forum for dialogue by convening international conferences and expert meetings, conducting interdisciplinary and applied research, engaging in specialised capacity building for practitioners of international criminal law and human rights education. Dedicated to supporting the worldwide enforcement of international criminal law, the Nuremberg Academy upholds the Nuremberg Principles and the rule of law with a vision of sustainable peace through justice, furthering knowledge and building capacities of those involved in the judicial process in relation to these crimes.

Project Background

The Nuremberg Academy has developed an interdisciplinary project that explores challenges relating to the use of digital evidence in international criminal proceedings.[1] With the continued advancement of information and communication technologies and the increased usage of digital information in the documentation of human rights (HR) abuses and core international crimes, the operations in judicial and quasi-judicial mechanisms are likely to be impacted.

The project seeks to address and consider the potential impact of the challenges raised in this context on the rules of procedure and evidence (RPE) in international criminal courts and tribunals. Considering the Nuremberg Academy's vision of furthering knowledge and building capacities of those involved in the judicial process in relation to core international crimes, the project focuses on the legal framework of the ICC as the first permanent international criminal court.

The project consists of five clusters that will take place both consequentially and simultaneously, as appropriate, and is estimated to be completed in 2023. Clusters A and B collected manuals and guidelines relating to judicial proceedings and digital evidence, which are now available through an online repository called the "Digital Evidence Database". Cluster C focused on analysing international and internationalised criminal jurisprudence concerning digital evidence and delivered a report encompassing a legal and comparative assessment of practices and standards. The current cluster D analyses the correlations between international HR law and ICL investigations as they pertain to digital evidence. The cluster C and D reports were finalised in 2022, and in 2023, the Nuremberg Academy is focusing on analysing the various challenges identified with respect to the ICCs legal framework.

With respect to cluster D and its methodology, the Nuremberg Academy conducted initial research in 2020 exploring the correlations between IHRL and international criminal investigations, culminating in a report dated February 2021 found in Annex 1 of this document. Building on these findings, experts engaged in a series of workshops that took place in 2021 which focused on understanding the challenges arising from the verification of digital evidence (see Annex 2). Throughout 2021 and 2022, further internal research was carried out to explore and build on some of the challenges identified and the feedback collected, all of which are analysed within this report.

Cluster D has contributed to exploring the various challenges with digital evidence and their scope in relation to investigation practices and subsequent disclosure processes in international criminal proceedings. However, the report has several limitations pertaining primarily to the shortage of resources as compared to the broadness of the field and the following should, in particular, be born in mind:

1. the research has been conducted specifically with newer forms of digital information and evidence in mind (including the proliferation of deepfakes, AI-generated information and deleted accounts);
2. the research has focused on verification processes and the challenges relating to verifying digital information that is later used as evidence at trial; and

[1] More information about the project can be found at International Nuremberg Principles Academy, "Digital Evidence", https://www.nurembergacademy.org/projects/detail/45ed2d129b0e19459764c4684e317a95/digital-evidence-23/, accessed 13 December 2022.

3. the research has aimed to explore newer challenges that might arise due to the advancement of technology rather than re-discussing challenges that actors in the field are already addressing either via the development of manuals and guidelines or by using and sharing best practices.

The Nuremberg Academy is grateful to the broad range of actors operating in the field of digital evidence and to the various HR investigators and international criminal investigators who have been consulted for contributing to the initial conceptualisation and tailoring of the project idea from 2018 to 2020.[2] Moreover, we are grateful to the experts and consultants who helped us bring this report together. Special thanks go to Olivia Flasch for combining the research findings into this report.

This report and the cluster C report constitute internal biproducts; they advance our exploration of the concept and help us build on the analytical work that is ongoing with respect to the main project question:

> *Considering the increased usage of digital evidence (and relevant changes) in the prosecution of core international crimes, should the Rules of Procedure and Evidence of the International Criminal Court be amended? If so, how and why?*

The Nuremberg Academy welcomes feedback on this report and the project in general and looks forward to further engagement with relevant stakeholders in addressing the project question.

December 2022
Jolana Makraiová
Senior Officer for Interdisciplinary Research
International Nuremberg Principles Academy

[2] See Annex 3 below for a list detailing the institutional affiliations and areas of expertise of the contributing experts.

Contents

1 Executive Summary

This report has been largely based on the initial research undertaken by Alisdair Putt and Neha Dubey on digital evidence in ICL and HR investigations in 2020 and supplementary research carried out by the Nuremberg Academy in the context of its digital evidence project. The comments and expertise from engaged experts have been taken into consideration, especially from those who participated actively in workshops on the subject.

The purpose of this report is twofold. Its primary purpose is to summarise the explored correlations between criminal investigations carried out for the purpose of proceedings before international courts and tribunals (ICL investigations) and investigations carried out by HR bodies or civil society organisations for the purpose of documenting HR violations in a given situation (HR investigations) when it comes to the preservation and verification of open-source information that has the potential to become digital evidence in international criminal proceedings. In this sense, the focus is not on investigations and other work in this field being carried out by local actors in a domestic context. The project's secondary purpose is to highlight the general challenges arising from the increased use of digital evidence in international criminal trials and from the sophistication of technology and the specific challenges that arise in relation to the preservation and verification of open-source information, both in the context of HR and ICL investigations.

The focus of this report is on: (1) open-source information that has the potential to become digital evidence; and (2) digital evidence derived from open-source information. While the two concepts are distinguished (that is information ≠ evidence), the terms are often used interchangeably as the substance of the two concepts is the same; the proper terminology rather depends on which stage of the evidentiary process the information is currently in.

It is acknowledged that the term "digital evidence" is far broader and comprises much more than open-source information. In addition, open-source information is not exclusively digital and may comprise non-digital forms of publicly available information. However, given the unique challenges presented specifically by digital evidence deriving from open-source information, the efforts are concentrated on those challenges and this report should be considered with that perspective in mind.

By setting out the differences and similarities between the collection, preservation, verification and disclosure processes of HR and ICL investigations and listing all the possible challenges that digital evidence may give rise to (and when they may arise), these challenges are further considered with respect to the main project question: whether the ICCs RPE need to be amended to take into account these challenges and if so, which specific challenges would such amendments be addressing and how.

The importance of this subject cannot be underestimated. Although the digital evidence project is not yet at its completion stage and more analysis is needed, the conclusions so far highlight that there is a noticeable lack of clarity regarding the usage, application and relevance of existing guidelines, standards and procedures applicable to the collection, preservation, verification and disclosure of digital evidence, both when it comes to HR and ICL investigations. Part of this problem stems from the fact that multiple institutions and organisations have sought to develop "best practices" pertaining to the same subject matter (for example, the verification or preservation of digital information), but it remains unclear which of these standards should be referred to, preferred and/or adopted in the context of international criminal proceedings and why. The absence of clarity around the applicability of the existing standards may have an impact on the procedural guarantees during the criminal proceedings and specifically the rights of victims, witnesses and the accused.

In drafting this report, a comprehensive research on the various existing standards and guidelines has not taken place, especially with respect to those which address some of the identified challenges. Merely, they have been referenced and identified within this report.[3] That is because the focus of this report is to identify the challenges and highlight that there is generally no uniformity in addressing them. Moreover, although certain guidelines may exist, these have not yet been adopted as such by the ICC and so court rules and procedures setting out how to address these particular challenges are still missing.

Additionally, the identified challenges are those which arise from the increased use of digital evidence rather than those facing any specific investigative body. This is done on the understanding that different investigative bodies and agencies may face different obstacles. In addition, it is worth mentioning that some of the challenges raised in this report that relate to digital evidence may also arise in relation to the collection and use of evidence generally.

A lot of progress has been made in the field already in addressing the challenges with digital evidence. This report and the subsequent discussions are intended to contribute to the work that other institutions are doing in this sphere already.

[3] The Nuremberg Academy has released an online repository compiling useful manuals and guidelines relating to digital evidence. It could serve as a starting point for any relevant future research in this field. The Nuremberg Academy welcomes feedback on the database and plans on updating the resource collection in the near future. See Nuremberg Academy (n 1) above.

2 Useful Definitions

Deepfake: an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.[4]

Deleted Accounts: Social media accounts used to disseminate messages and then deleted to protect the identity of the account holder and the traceability of the information published.

E-Discovery: The electronic aspect of identifying, collecting and producing electronically stored information in response to a request for production in a lawsuit or investigation.[5]

Open-Source: Publicly available on the internet; any member of the public can observe, purchase or request it without requiring special legal status or authorised access.[6]

3 Background and Introduction

This report explores the correlations between ICL and HR investigations as they relate to the collection and processing of information and, in particular, information of a digital nature that has the potential to become evidence in international criminal investigations.

These correlations have been highlighted and various challenges have been identified, especially those that arise or are likely to arise as a result of the use and development of technology and the new forms of digital information it has created. A summary of challenges that are ripe for further analysis within the context of our digital evidence project is provided, with the aim of obtaining feedback from consulted experts and other stakeholders in relation to these challenges.

In considering the challenges, the focus is on those pertaining to the "newer" forms of digital evidence, including deepfakes, evidence generated by AI and deleted accounts, which give rise to more novel issues with respect to the verification process.[7]

[4] "Deepfake", *Merriam-Webster Dictionary* (2022), https://www.merriam-webster.com/dictionary/deepfake, accessed 13 December 2022.
[5] CDS Legal, "The Basics: What is e-Discovery? From the CDS Knowledge Base", *CDS Legal* (n.d.), https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/, accessed 13 December 2022.
[6] Annex 1, 22, and references therein.
[7] Ibid.

4 ICL and HR Investigations

4.1 HR Investigations

HR investigations are carried out by a number of different types of investigative bodies, including non-governmental organisations, private actors, international fact-finding missions, commissions of inquiry, other bodies established by the United Nations and national HR commissions.[8] The purpose and working methods are not uniform across each of these bodies, but there are certain common guiding principles to which they all seek to adhere, namely: impartiality, confidentiality, independence, credibility and the principle of "do no harm".[9] However, there is no mechanism by which to ensure compliance with these guiding principles.[10]

HR bodies focus on the search for information, as opposed to evidence.[11] In that sense, they are mostly not looking to establish the commission of crimes or identify individual perpetrators, but rather to draw attention to gaps in accountability, lobby governments for change and/or expose serious HR violations by creating a record of their occurrence. Occasionally, this leads to the identification of key individuals, which may provide leads for future investigations, including ICL investigations.

Since they search for information rather than evidence, the standard of proof applicable to HR investigations is typically lower than that applicable to ICL investigations. Generally, the applicable standard of proof to HR investigations will be the "reasonable grounds to believe" standard;[12] however, the applicable standard of proof in any given case is inherently linked to the purpose or mandate of the investigation and may thus fluctuate.[13]

4.2 ICL Investigations

ICL investigations are carried out by prosecution and defence teams and, in some cases, investigative judges, all of which form part of a court system. In the case of the ICC, the Prosecutor has been granted investigatory powers by the Rome Statute, Articles 54 and 55 of which ensure that the Prosecutor abides by the "do no harm" principle, maintains their independence and confidentiality and collects all relevant evidence, including exculpatory evidence, that is required to "establish the truth".[14]

---

[8] Ibid, 20.
[9] The principle of "do no harm" provides that the investigation should not jeopardize the safety of the source of evidence, the investigators or the information collected. See ibid, 10.
[10] Ibid, 20.
[11] Ibid. See also section 4.3 below.
[12] Some bodies have been inclined to employ a slightly different terminology, including "reasonable suspicion" (see UN Human Rights Council (United Nations), *Report of the independent international commission of inquiry on the Syrian Arab Republic* (2011), UN Doc A/HRC/S-17/2/Add.1, para. 5), "reasonable grounds to conclude" (see UN Human Rights Council (United Nations), *Report of the independent international fact-finding mission on Myanmar*, (2019), UN Doc A/HRC/42/50, para. 19) or "reasonable grounds" (see UN Human Rights Council (United Nations), *Report of the detailed findings of the commission of inquiry on human rights in the Democratic People's Republic of Korea* (2014), UN Doc A/HRC/25/CRP.1, para. 67; UN Human Rights Council (United Nations), *Report of the independent international fact-finding mission on Myanmar* (2018), UN Doc A/HRC/39/64, para. 6).
[13] Annex 1, 8.
[14] Ibid, 14; ICC, *Rome Statute of the International Criminal Court* (2187 UNTS 90), arts. 54 and 55.

The purpose of ICL investigations is to establish criminal accountability for the commission of crimes and to identify individual perpetrators of such crimes. It follows that ICL investigators are specifically looking for information that has the potential to become evidence in a criminal trial.

As mentioned above, an ICL investigation also differs from an HR investigation in respect of the applicable standard of proof. Proceedings at the ICC take place in different stages, and the level of scrutiny and standard of proof becomes more onerous at later stages of the proceedings.

In the preliminary stages, the ICC employs a lower standard of proof, which allows it to rely on findings in HR investigations to consider whether a criminal investigation should take place.[15] In later stages, individual criminal responsibility must be established beyond a reasonable doubt.[16] In the past, the Pre-Trial Chamber of the ICC appears to have accepted evidence derived from open-source information as a sufficient basis for the issuing of arrest warrants and the granting of provisional release but has preferred other, more direct forms of evidence to confirm charges.[17]

4.3 Overlap between ICL and HR Investigations

4.3.1 Information and Evidence

As mentioned above, there is a distinction between the search for information and the search for evidence. However, the two concepts do overlap. First, locating and recording information often serves as a starting point for ICL investigations, as information gathered in HR investigations provide background and context as well as "lead intelligence".[18] The information collected by HR investigators might become evidence itself in a future ICL investigation or, alternatively, such information may serve to corroborate other pieces of evidence uncovered in ICL investigations. The authors of HR investigation reports may also be called as expert witnesses during a trial.[19]

Second, since evidence may lead to a conviction, ICL investigators employ a high threshold when it comes to the reliability and probative value of a piece of evidence.[20] However, even HR investigators may sometimes apply a higher threshold in their search for information than is required of them by way of their mandate. Generally, both ICL and HR investigators will seek to ensure that, more than on a balance of probabilities, a piece of information is reliable.

---

[15] Annex 1, 17, 19, citing C. Stahn & D. Jacobs, "Human Rights Fact-Finding and International Criminal Proceedings: Towards a Polycentric Model of Interaction" *Grotius Centre Working Paper*, 2014/017-ICL (2014) , 16, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2388596, accessed 13 December 2022.
[16] Annex 1, 20-21.
[17] Ibid, 19, citing Stahn & Jacobs, *Human Rights Fact-Finding*, 17-19, in turn, citing *Prosecutor v. Gbagbo*, Third decision on the review of Laurent Gbagbo's detention pursuant to article 60(3) of the Rome Statute (2013) ICC-02/11-01/11-454, para. 42. See also *Prosecutor v. Al-Werfalli*, Warrant of Arrest (2017) ICC-01/11-01/17, para. 3; *Prosecutor v. Al-Werfalli*, Second Warrant of Arrest (2017) ICC-01/11-01/17, para. 19.
[18] Annex 1, 16.
[19] Ibid.
[20] At the ICC, the rules on the evaluation of evidence are as follows: ICC, *Rome Statute*, arts. 64(2), 64(9)(a), 69(3), 69(4) and 74(2); ICC, *Rules of Procedure and Evidence*, (ICC-ASP/1/3 and Corr.1), rule 63(1), 63(2), 63(4) and 64(2).

Though their roles differ from ICL investigators, HR investigators will still have some sort of presumption of innocence checks integrated into their clearance procedures and will have some rules relating to disclosing names in their reports to address this concern. Where individuals are identified in an HR investigatory report, and an ICL investigator wishes to rely on such report in criminal proceedings, the ICL investigator needs to be very cognisant of the mandate of the HR investigatory body. A real discussion should be had about whether the investigative duties and powers of the ICL investigator can cure the potential conflict that may arise in relation to the presumption of innocence.[21]

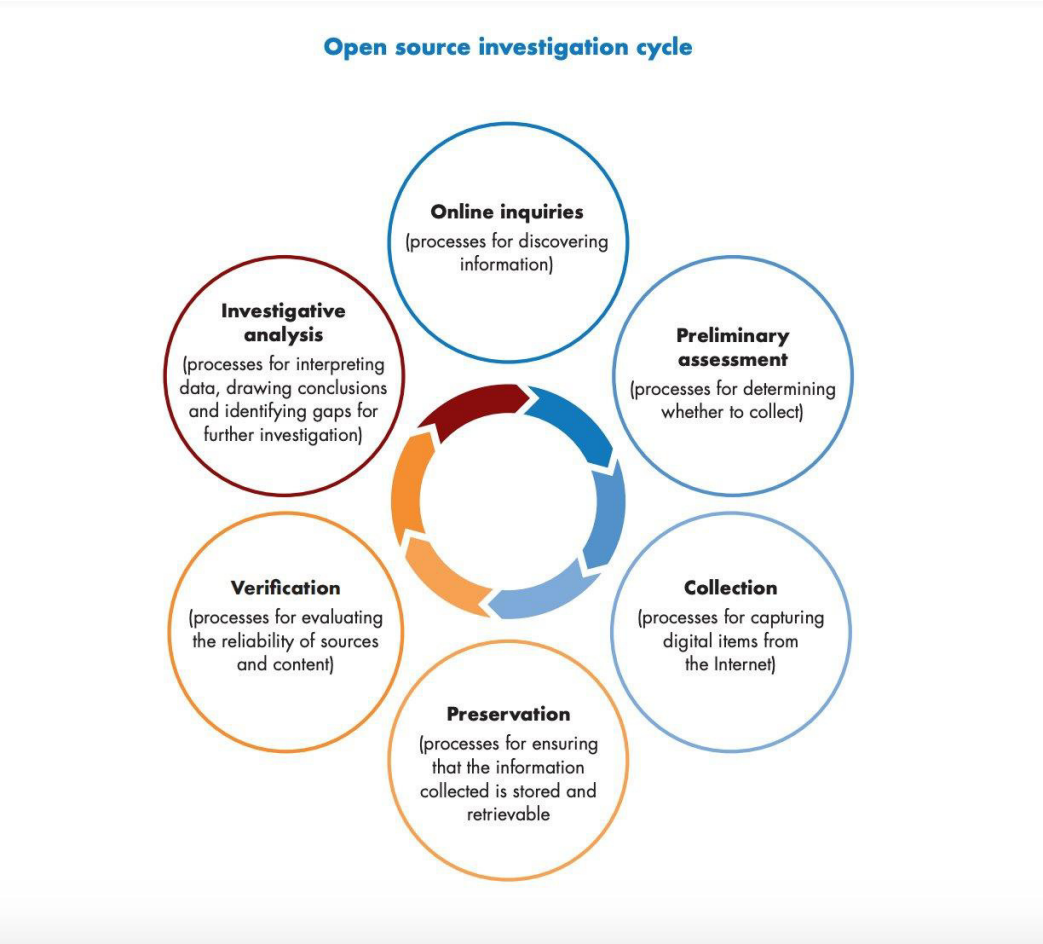
Whether information gathered will be tendered in court as evidence depends on if it has the ability to "prove or disprove a fact material to the allegation, be authentic rather than false, and [be] brought from a reliable and credible source to court along an unbroken chain of custody to avoid contamination, tampering or fabrication".[22]

[21] Annex 2, 20 and expert comments.

[22] Annex 1, 23, citing L. Syunga, "Can International Criminal Investigators and Prosecutors Afford to Ignore Information from United Nations Human Rights Sources?" in M. Bergsmo & C. Stahn, ed., *Quality Control in Fact Finding* (2nd edn, Torkel Opsahl Academic EPublisher, 2020), 382.

Open-Source Investigation Cycle

ICL and HR investigations overlap in the way that digital information, and in particular open-source information, is collected and processed. The Berkeley Protocol on Open Source Investigations (Berkeley Protocol) has identified what it refers to as the open source investigation cycle; a cyclical, non-linear process of investigating open-source information (both in the context of HR and ICL investigations):[23]



The steps in the cycle are typically divided into two broad categories: the **preservation stage** (comprising online inquiries, preliminary assessment,[24] collection and preservation of information) and the **verification stage** (verification and investigative analysis of information). However, due to the cycle's non-linear nature, these steps are often repeated at different stages of the case-building process.[25]

[23] Berkeley Human Rights Center & UN OHCHR, "Berkeley Protocol on Digital Open Source Investigations", *UN OHCHR* (3 January 2022), 55, https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf, accessed 13 December 2022.

[24] It should be noted that the "preliminary assessment" part of the cycle, that is, the use of processes for determining *whether* to collect a certain piece of information, does require some analysis. Thus, while informing the collection of information and thus forming part of the preservation stage, it still overlaps somewhat with the verification stage, which is more analytical. The standards remain unclear given this overlap between preservation and verification.

[25] Annex 1, 23.

There are a number of correlations between ICL and HR investigations when it comes to the steps in the open source investigation cycle. Both types of investigators will make online inquiries to locate and identify information. Moreover, both types of investigators will use available investigatory guidelines (such as the Berkeley Protocol), which explain how to properly collect and preserve digital information. Indeed, the recent ICC/Eurojust Guidelines for Civil Society Organisations on Documenting International Crimes and Human Rights Violations for Accountability Purposes "are intended to further assist [civil society organisations] in [their] efforts to collect and preserve information that may ultimately become admissible evidence in court."[26]

Both types of investigators will seek to ensure that such information is properly stored and retrievable. Both types of investigators will also seek to evaluate the reliability of their sources and content, albeit applying slightly different standards in this process. Finally, when it comes to the investigative analysis, both types of investigators will have in place some processes for interpreting data, drawing conclusions and identifying gaps for further investigation.

This report covers challenges arising from both the preservation and the verification stages in the investigation of digital evidence. The focus is on verification challenges—as this is the stage which might be impacted most by the sophistication of technology;[27] however, due to the overlap in stages as per the open source investigation cycle above, many of the challenges identified will be relevant to preservation as well.

It is argued that the identified challenges may transfer into judicial proceedings in terms of impacting procedural and substantial rights of the accused but also victims, witnesses and the overall fairness of the trial. The following sections set out the process of transforming open-source information into digital evidence and the challenges arising from the preservation and verification of such information.

[26] ICC & Eurojust, "Guidelines for Civil Society Organisations on Documenting International Crimes and Human Rights Violations for Accountability Purposes", *Eurojust* (21 September 2022), 4, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-icc-csos-guidelines.pdf, accessed 13 December 2022.
[27] Annex 1, 22.

5 Transforming Information into Evidence

5.1 Stages of Criminal Proceedings at the ICC

Before setting out the challenges relating to the preservation and verification of digital evidence, it is useful to first explain how information that has been collected is transformed into and used as evidence for the purpose of an international criminal trial. The first stage of this trajectory is the opening of an investigation. Article 15 of the Rome Statute sets out the legal requirements that the Prosecutor is bound by when opening an investigation. It requires the Prosecutor to analyse the seriousness of the information received, allows the Prosecutor to seek additional information from reliable sources and requires the Prosecutor to request authorisation from the Pre-Trial Chamber to open an investigation if there is a reasonable basis for to proceed with such investigation.[28]

Article 53 also provides that the case must meet the jurisdiction, admissibility and "interests of justice" criteria before an investigation can be opened. This is at the stage of the proceedings where information has not yet become evidence and is still being gathered. Once an investigation has been opened, Article 54 provides that the Prosecutor must investigate incriminating and exonerating circumstances equally and respect the interests and personal circumstances of victims and witnesses. Article 55 provides for the right against self-incrimination, the right not to be subjected to coercion or arbitrary detention and the right to translation services.

Both Articles 54 and 55 are based on the presumption of innocence. These provisions set the standards for the collection of evidence. Evidence that does not conform to these standards is at risk of being declared inadmissible in ICL proceedings. It is at this stage that information begins to be converted into evidence, based on its compliance with the relevant provisions. The respective resources of the parties will affect the nature, scope and quality of the investigation and the information gathered.[29]

Once the investigation is complete, Article 63(1) states that trials must take place in the presence of the accused. Articles 66 and 67 relate to the presumption of innocence and the rights of the accused, respectively, and provide, *inter alia*, that the ICC can only convict when the accused's guilt has been established beyond a reasonable doubt and that the evidence, that the Prosecutor intends to rely on, needs to be disclosed to the Defence.[30] Where witness testimony is considered (including the testimony of victims and experts), Articles 64 and 68 provide that the Trial Chamber may put in place protective measures for witnesses and victims where appropriate and that evidence from a witness who cannot attend court, or evidence where the source or author is unknown, will be treated as hearsay and thus be afforded less weight.[31] Finally, pursuant to Article 69(7), evidence obtained in breach of human rights is inadmissible.

[28] ICC, *Rome Statute*, arts. 15(2) and (3).
[29] Annex 1, 51.
[30] ICC, *Rome Statute*, arts. 66(3) and 67(2).
[31] ICC, *Rome Statute*, arts. 64(2), (6), (7) and 68.

It is during the proceedings that the Trial Chamber (or Pre-Trial Chamber) typically rules on the relevance and admissibility of evidence by considering the probative value and potential prejudice that the evidence may cause to a fair trial. In doing so, the Chamber will undertake its own verification process. In that context, the chain of custody and corroboration will be relevant factors.[32] The process can take place at various stages of the proceedings. If the authenticity of a piece of evidence is questioned early on, it may be verified by the Pre-Trial Chamber.[33] At this stage, information becomes crystallised as evidence unless it is found to be inadmissible.

5.2 Disclosure, Digital Forensics and E-Discovery at the ICC

Article 61(3)(b) of the Rome Statute provides that the accused shall, within a reasonable time before a confirmation of charges hearing, "[b]e informed of the evidence on which the Prosecutor intends to rely at the hearing". Article 67(2) of the Rome Statute provides that the Prosecutor is also required to, as soon as practicable, "disclose to the defence evidence in the Prosecutor's possession or control which he or she believes shows or tends to show the innocence of the accused, or to mitigate the guilt of the accused, or which may affect the credibility of prosecution evidence." In *Lubanga*, the Trial Chamber clarified that the Prosecutor's disclosure duty relates to all information under their possession or control, including exculpatory evidence.[34]

When considering whether and what evidence to collect, the Prosecutor must bear their disclosure obligations in mind.[35] However, overly burdensome obligations and the fear of possibly breaching them has the potential to hamper the investigative process and can create a risk of losing relevant digital material in such process.[36]

The Defence also has disclosure obligations at the ICC. Pursuant to Rule 79 of the RPE, the Defence shall notify the Prosecutor of its intent to raise the existence of an alibi or raise a ground for excluding criminal responsibility, in which case it must notify the Prosecution of the evidence it intends to rely on to establish the alibi or ground.[37]

If the accused intends to present evidence at the confirmation of charges hearing, the Defence must also provide a list of that evidence to the Pre-Trial Chamber no later than 15 days before the date of the hearing. The Pre-Trial Chamber shall transmit the list to the Prosecutor without delay.[38] The Chambers of the ICC also have the right to order disclosure of any other evidence.[39]

---

[32] Annex 1, 52.
[33] See e.g. *Prosecutor v. Lubanga*, Decision on the confirmation of charges (2007) ICC-01/04-01/06, paras. 95 *et seq*.
[34] *Prosecutor v. Lubanga*, Decision on the consequences of non-disclosure of exculpatory materials covered by Article 54(3)(e) agreements and the application to stay the prosecution of the accused, together with certain other issues raised at the Status Conference on 10 June 2008 (2008) ICC-01/04-01/06-1401, paras. 59-61.
[35] L. Freeman & R. Vazquez Llorente, "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age", *Journal on International Criminal Justice*, 19/1, 163, 177, https://doi.org/10.1093/jicj/mqab023.
[36] Ibid, 178.
[37] ICC, *RPE*, rule 79(1)(a) and (b).
[38] ICC, *RPE*, rule 121(6) and ICC, *Rome Statute*, art. 61(6).
[39] ICC, *RPE*, rule 79(4).

According to the consulted experts, the disclosure obligations at the ICC are burdensome and the process was complicated even before the use of digital evidence.[40] However, digital forensics and E-Discovery have been shown to reduce the burden.

Digital forensics is a scientific process that focuses on identifying, acquiring, processing, analysing and reporting on data stored electronically.[41] It involves a three-stage process of (1) seizing the digital information, (2) creating a forensic image of the digital information (also known as "acquiring it") and (3) analysing the forensic image so as to preserve its original digital form.[42]

Considering that social media platforms such as YouTube, Twitter or Facebook are private corporations with control over the content posted on their sites, potential evidence may only be available for a short period of time before it is taken down. Methods of collecting such material before a platform deletes it involves:

1. identifying the location and file structure of the content;
2. downloading the content from the platform; and
3. taking a snapshot of the offline content and recording the metadata.[43]

Given the sophistication of technology, digital forensics is playing an increasingly important role in transforming digital information into evidence.[44] Indeed, as stated by Interpol in its Digital Forensics Guidelines, "[i]f digital equipment is seized and not handled correctly, there will be potential for the data to be lost through deletion by the user, remote wiping or manipulation by a third party."[45]

Once the digital forensics process has taken place, the analysed information is ripe for E-Discovery. E-Discovery, as defined above, involves electronically identifying, collecting and producing digital evidence in the context of legal proceedings. Once all the evidence has been captured and stored on the electronic E-Discovery platform, it allows parties to evaluate how much evidence has been gathered and the resources they have available to process that amount of evidence. They can then make the appropriate decisions, bearing in mind the limitations, the legal requirements that need to be met and the necessary practices, procedures and processes that need to be followed for case-building.

Much of the digital forensics work and subsequent E-Discovery process is done prior to the verification stage, at the preservation stage. The digital forensics processes mainly involve capturing and organising the digital material collected but not necessarily ensuring that the data is not a deepfake or other manipulated piece of information.

---

[40] See *Prosecutor v. Paul Gicheru*, Decision Setting the Regime for Evidence Disclosure and Other Related Matters (2020) ICC-01/09-01/20, for a detailed explanation of the disclosure procedure.
[41] Interpol, "Digital Forensics", *Interpol* (n.d.), https://www.interpol.int/How-we-work/Innovation/Digital-forensics, accessed 13 December 2022.
[42] Annex 1, 26, citing M. Novak, J. Grier & D. Gonzales, "New Approaches to Digital Evidence Acquisition and Analysis", *National Institute of Justice Journal*, 280 (2018), https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis, accessed 13 December 2022.
[43] Annex 1, 28.
[44] Interpol's Guidelines for Digital Forensics First Responders was released in March 2021 and provides a detailed set of best practices for search and seizure of electronic and digital evidence. See Interpol, "Guidelines for Digital Forensics First Responders", *Interpol* (March 2021), https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf, accessed 13 December 2022.
[45] Ibid, 10.

However, digital forensics is also used in the verification stage. For instance, the ability to authenticate digital evidence, particularly deleted accounts and deepfakes, is mostly dictated by the quality and capability of digital forensics tools.[46] The next sections explain the preservation and verification stages in more detail and the challenges that arise in each of these stages.

[46] Annex 1, 56.

6 Preservation and Verification of Evidence

6.1 Preservation

Should all collected information be preserved?

Preservation, in the context of digital evidence, has as its purpose to collect, store and archive information relevant to an investigation. Any challenges relating to what information should be collected and stored, and when, arise in the context of the preservation stage.

As mentioned above, both HR investigations and ICL investigations will follow broadly similar guidelines relating to the preservation of information, but digital information which has the potential to become evidence and, in particular, newer forms of such information (such as AI-generated information) gives rise to additional challenges and complexities.

First, in relation to the collection of information, there are issues with overcollection which can give rise to further concerns, as discussed below[47]. Particularly where whole servers are collected rather than specific documents or folders, material may be duplicated and a significant amount of irrelevant material may be collected inadvertently. Thus, sound document management has been identified as a "must" to avoid overcollection and thus avert a "storage crisis" in the digital database. Applying the appropriate digital forensics tools early on is key.

When seeking to collect potentially relevant information, investigators may also stumble upon access issues. Third party servers and encrypted documents may be difficult to access and there is a general absence of established rules pertaining to access. Readers might be familiar with the difficulties law enforcement agents run into where electronic devices that form part of a criminal investigation are password protected and the private manufacturers of such devices either have no means of unlocking, or no willingness to unlock, such devices.[48] A balance will often need to be struck between privacy concerns and the public interest.

As mentioned above, where information is not preserved properly, there is a real risk of evidence tampering which may lead to inadmissibility or less weight being given to it in subsequent in court proceedings and a real risk of its inadvertent deletion, and thus permanent loss. The current practices of preserving digital evidence suffer from a lack of clarity regarding the usage and applicability of existing standards and/or guidelines, particularly regarding (i) the redaction of potential witness or victim names from open-source information, (ii) the scope of preservation obligations and (iii) the appropriate standard to which information should be preserved. These challenges may impact disclosure obligations and processes in international criminal trials and would therefore benefit greatly from clarity regarding the standards or best practices that exist and could apply to a given situation.

[47] See section 6.2 below.
[48] Annex 2, 13.

6.2 Verification

Should all preserved information be verified?

Verification, in the context of digital evidence, has as its purpose to check whether the collected digital information is reliable. The question at the heart of verification is "how do you know that?".[49] "Verification" is understood in the sense of verifying the information at hand and its origin to be able to assess the reliability of the piece of information later in the process. This applies to both the HR and ICL investigations.

Although there is no established definition of verification, it will involve establishing the provenance of information (that is, its originality), the source of the content, when the content was created and where the content was created.[50] The sophistication of technology and the existence of and reliance on digital information has given rise to a number of challenges.

First, it has caused the number of relevant actors (that is, sources) to increase. The source of a piece of information might now comprise the user who generated the content, the person who uploaded the content to the internet and/or the person who provided the uploaded content to the relevant authorities.[51] The verification process becomes increasingly complex as an investigation proceeds. Due to the difficulties often involved in verifying digital information, there is increased reliance on digital forensics experts to explain the technicalities surrounding the verification process of evidence.[52]

The second challenge relates to over-collection of evidence. As mentioned above, given the vast amounts of digital data that is generated constantly, there is a real risk of over-collection of digital information in an HR or ICL investigation. This is a situation that highlights the importance of evidence triage, that is, prioritising digital evidence collected based on certain criteria.[53]

In this regard, it has been suggested by experts to employ a three-prong, multifunctional approach to data analysis when triaging evidence: source analysis, content analysis and technical analysis.[54] These three forms of analyses allow for multifactor verification, which is considered essential as each of these analyses can reveal whether information is fake or forged.[55]

---

[49] Annex 1, 24, citing C. Silverman, ed., *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage* (European Journalism Centre, 2014), 16, https://verificationhandbook.com/downloads/verification.handbook.pdf, accessed 13 December 2022.
[50] Ibid, 27.
[51] Annex 2, 14.
[52] Ibid, 15.
[53] In the medicinal field, the Golden Hour refers to the time period immediately after an injury where there is a high likelihood that prompt medical treatment will prevent death. With respect to verification of evidence, investigators may find it helpful to adopt this concept to ensure that they verify the source of the digital information as soon as possible to prevent possible deletion or manipulation of data. See M. K. Rogers, "Computer Forensics Field Triage Process Model", *Journal of Digital Forensics, Security and Law*, 1/2 (2006), 19, 26. See also Annex 2,16-17.
[54] Annex 2, 17.
[55] Ibid.

As part of the source analysis, investigators may find it helpful to assess the following issues:

1. **Authenticity of the source**: This mostly arises in relation to online interactions with bots, botnets, trolls and unauthentic behaviours. Identifying whether a source is authentic is usually done by assessing various signs and indicators of authenticity.
2. **Attribution of content to a source**: Traditionally, this is done by connecting the username and/or avatar to an individual. This is relevant particularly in relation to social media evidence.
3. **Originality of the source**: Ensuring that the information captured stems from the original source is particularly important in light of the high amount of circular reporting or online sharing of information.[56]

Standardisation of the collection processes (that is, the establishment of a clear methodology, scope and understanding of the available resources for an investigation) is a useful tool for avoiding over-collection of information. As mentioned above, the ICC/Eurojust Guidelines are helpful in this regard, as they seek to standardise the collection process for investigators gathering digital information.[57]

A final challenge relating to the verification of evidence arises from the existence of deepfakes, deleted accounts and AI-generated information. The development of these technologies has given rise to greater uncertainty regarding the availability and/or correctness of certain types information and the motive behind the creation of certain types of information. This makes authenticating the originality, date, location and even content of a piece of information extremely difficult. Experts are concerned that "perfect deepfakes" might soon exist, which are indistinguishable from an authentic piece of information.[58] Additionally, the existence of deepfakes and the difficulty in distinguishing between fake and real information gives rise to the danger that authentic information could be dismissed as fake in criminal proceedings.

In conclusion, the verification process of digital evidence is currently suffering from the below main issues:

1. No established definitions of "verification" or "source".
2. Source verification requires a very careful assessment of the source of a piece of digital information, including an assessment of the cost of verification (which requires financial, technological and human resources).
3. Reliance on cooperation from third parties (for example, private service providers).
4. Real risk of overcollection, and a less specificity in collection.
5. Deepfakes, deleted accounts and AI-generated information.
6. No existing verification standards or not enough knowledge and understanding about existing verification standards.

The next section sets out the challenges relating to the use of digital evidence in international criminal proceedings.

---

[56] Ibid.

[57] For example, the foreword of the ICC/Eurojust Guidelines explains that they: "provide some key principles which, we believe, may be of assistance in ensuring that documentation efforts are carried out in a way that preserves the integrity of information and evidence and increases the ability of national and international accountability processes to draw on your work". See ICC & Eurojust, *ICC/Eurojust Guidelines*, 4.

[58] Annex 1, 30.

7 Challenges relating to Digital Evidence

7.1 General Challenges relating to the Sophistication of Technology

The increased usage of digital evidence and the sophistication of technology has given rise to a number of new opportunities, but also new challenges, for HR and ICL Investigators. First, it has increased the amount (and type) of information that is available in any given conflict situation or HR violation. Second, it has allowed for the existence of a longer time period of documentation of conflict or HR violation. Third, it has "decentralised" or "democratised" the documentation process, and investigators now more than ever make use of information captured by the general public and uploaded to social media accounts in their investigations.

This democratisation has, as mentioned above,[59] created challenges with identification and verification of the source of a piece of information, not in the least because the verification process is often reliant on cooperation from service providers such as social media providers or mobile phone manufacturers. The investigative mandates and tools available for identifying information have also changed as a result of the sophistication of technology.

These challenges relate specifically to the nature of digital information and how we use it and access it. There are other, logistical, challenges that the sophistication of technology has given rise to as well. For instance, due to the speed at which technology has developed, there is still no uniform set of terminology or definitions used by HR and ICL investigators or any universally accepted standards or guidelines pertaining to digital evidence. Moreover, different bodies at different levels, national, regional and international, are all engaged in the development of standards and guidelines relating to digital evidence, which creates a real risk of a disparity between the approach taken by international as compared with domestic judicial institutions.[60] Although national and regional implementations of the developed guidelines relating to digital evidence are outside the scope of this project, the risk that a two-tier system of best practices may develop remains and is worth recognising.

Another major challenge is the shortage of resources available to those investigators, including information technology resources, digital forensics tools, translation resources and other human resources needed to access and assess information relevant to a given violation. The lack of clarity around applicable procedural rules and standards (for example, in relation to E-Discovery and witness and victim protection in the digital age) and around digital information and its use in criminal proceedings causes confusion.

These are the general challenges that the development of technology has given rise to. But which specific areas of criminal proceedings before international courts and tribunals are particularly problematic and would benefit the most from legal clarity surrounding the applicable rules and standards and the existence of guidelines and best practices? The sections below expand upon the specific challenges relating to the evidentiary process, disclosure, victims and witnesses and the accused.

[59] See section 6.1 above.
[60] See generally Annex 2.

7.2 Evidence-Related Challenges

7.2.1 Collecting Information

While the information collection process is evolving with the sophistication of technology, it is still not generally understood how such process should be carried out to ensure the authenticity of the digital information and to verify its source. The collection process requires a thorough methodology to ensure that the chain of custody is kept intact and that the digital evidence remains untampered with. The lack of knowledge of best practices around this process increases the risk of evidence manipulation and admissibility concerns later in the process.[61] This risk is even greater if the information to be collected pertains to the acts of the accused and the collection and/or preservation is not handled with great care. Indeed, linkage evidence (evidence linking facts to a specific individual) might require more careful preservation and verification than other, more general evidence purely proving the existence of certain facts.

There is also the added challenge, alluded to elsewhere in this report, of accessing information from third parties. This arises, for example, where data has been deleted or not been preserved properly, where platform hosts or device manufacturers refuse to disclose information about their users or where investigative bodies have confidentiality procedures in place that prevent a source from being revealed.[62]

7.2.2 Assessing Evidence

The approach of the ICC, and the concept of free evaluation of evidence, means that practically all evidence is admitted, except if it has the potential to prejudice the proceedings.[63] The preferred approach of most Chambers of the ICC is to defer any admissibility decisions to a later stage in the proceedings and assess admissibility and weight at the same time while undertaking a holistic review of all the evidence.[64]

This approach gives rise to several challenges. First, it is unclear whether evidence that has been admitted will ultimately be declared inadmissible at a later stage. The later review also tends to lead to a conflation of weight and admissibility considerations, giving rise to further uncertainty.

[61] Annex 2, 8.
[62] See above, 11 and 14 and below, 18.
[63] ICC, *RPE*, rule 63(2); ICC, *Rome Statute*, art. 69(4).
[64] See F. Guariglia, “Admission v. Submission of Evidence at the International Criminal Court: Lost in Translation”, *J Int'l Crim Just*, 16 (2018), 315, 316; *The Prosecutor v. Dominic Ongwen*, Trial Judgment (2021) ICC-02/04-01/15-1762-Red, para. 234; *The Prosecutor v Jean-Pierre Bemba Gombo*, Judgment pursuant to Article 74 of the Statute (2016) ICC-01/05-01/08-3343, para. 222.

Second, assessing the nature of digital evidence can be a particularly technically complex affair. This might necessitate that the Chambers are aware of digital manipulation methods, such as deepfakes and AI-generated information, and other evidence-related challenges that exist, including how to properly verify the source and content of a piece of digital evidence.[65] Given the sophistication of technology, over-reliance on social media could be particularly problematic, as social media posts tend to highlight the social media user's individual narrative. Care needs to be taken to avoid promoting that particular narrative over other sources of evidence. There is a risk that judges are not yet fully familiar with the constantly developing technology in this regard, particularly when it comes to assessing open-source information as evidence.[66]

Third, given the proliferation of guidelines and standards that are being and have been developed in the context of preserving and verifying digital evidence across different bodies and levels, there is the added challenge of assessing when and whether a particular set of best practices have in fact been followed. For instance, there may be more than one set of guidelines relating to preserving the chain of custody of digital information that suggest different but equally efficient approaches. As the clarity around the standards that exist and are applicable is missing, there may subsequently be a lack of understanding from judges on how to assess that the applicable standards have been followed.

Finally, the time lag between the conclusion of an investigation (where the collection of evidence takes place) and the proceedings (where the evidence is assessed) is also a challenge to bear in mind in the context of evidence assessment. During this time, the evidence collected is transferred from the investigators to the prosecutors. Since the investigators may be subject to lower evidentiary and investigative obligations and different data protection rules than ICL investigators or the parties to international criminal proceedings, this might cause a real problem for the parties to the proceedings in the authentication and verification process that ensues.[67]

7.2.3 Source Verification

The definition and scope of what is included in a verification process, and in particular the verification of a source, needs clarification. Experts suggest that HR and ICL investigators should put greater emphasis on source verification at the early stages of an investigation, especially when dealing with open-source information.

Thus, when the information gathered is at a stage where it will be used for criminal proceedings, the Prosecution and Defence should be submitting into the case file evidence from well-verified sources. There is a need for clarity in terms of the standard of verification of the evidence that will be admissible and the scope of the information that can be relied on and for what purposes.

[65] This might include having a general understanding of the best or current practices and any guidelines and standards available that address the specific challenges relating to digital evidence.
[66] Annex 1, 49.
[67] Annex 2, 21 and expert comments.

Another challenge relating to source verification arises in relation to the type of information that is gathered during the collection stage. Despite the duty of an international criminal investigator to gather exculpatory evidence, practice suggests that investigative agencies tend to collect relevant incriminating evidence while not devoting significant resources to exculpatory searches or indeed verification processes.[68]

Where the source of a piece of digital evidence is anonymous, the preservation methods used for preserving that evidence will be particularly relevant. Judicial guidance on preservation methods would also be particularly helpful to deal with the challenges arising from unverifiable sources.

7.2.4 Hearsay Digital Evidence

Where a source is unidentifiable, it is likely to be categorised as hearsay digital evidence. The probative value of hearsay digital evidence (for example, content uploaded anonymously and shared multiple times by different users) and how it can be used in international criminal proceedings remains a real challenge in the digital age.

When dealing with hearsay evidence, including hearsay digital evidence, which can oftentimes be unreliable, there is usually a need for some form of corroborative evidence to strengthen its probative value.[69] In this regard, the reliability of hearsay digital evidence might be able to be strengthened with live testimony from, for example,. people involved in gathering that evidence, the methods they used and the chain of custody.[70]

Parties should, however, be careful not to seek to strengthen digital hearsay evidence with other hearsay evidence—as Judge Henderson noted in *Gbagbo and Ble Goudé* that "if two items of evidence assert the same fact based on anonymous hearsay, the combined evidentiary weight remains negligible, even if there are grounds to believe that the respective anonymous sources are independent of each other."[71] As with the other challenges raised in this report, clarity and knowledge of the applicable standards and guidelines on how to approach and utilise hearsay digital evidence would be of great benefit to parties engaged in proceedings at the ICC and other international criminal courts and tribunals.

---

[68] Annex 1, 46.

[69] *Prosecutor v. Laurent Gbagbo and Charles Blé Goudé*, Reasons for oral decision of 15 January 2019 on the Requête de la Défense de Laurent Gbagbo afin qu'un jugement d'acquittement portant sur toutes les charges soit prononcé en faveur de Laurent Gbagbo et que sa mise en liberté immédiate soit ordonnée, Reasons of Judge Geoffrey Henderson (2019) ICC-02/11-01/15-1263, paras. 1114, 1151, 1730.

[70] Annex 1, 40.

[71] Prosecutor v. Laurent Gbagbo and Charles Blé Goudé, Reasons for oral decision of 15 January 2019 on the Requête de la Défense de Laurent Gbagbo afin qu'un jugement d'acquittement portant sur toutes les charges soit prononcé en faveur de Laurent Gbagbo et que sa mise en liberté immédiate soit ordonnée, Reasons of Judge Geoffrey Henderson (2019), ICC-02/11-01/15-1263, 16 July 2019 (Reasons of Judge Henderson), paras. 47-49.

7.2.5 Admissibility and Privacy Concerns

The reliance on open-source information as digital evidence gives rise to a number of privacy-related admissibility concerns. For example, if data is hacked, leaked or published on the internet without permission from the relevant owner or user, to what degree is it, or should it be, inadmissible in international criminal proceedings?[72]

The characteristics of deepfakes, AI-generated digital information and deleted accounts have not yet been explored in international criminal proceedings, but due to their nature, their use has the potential to violate the right to privacy. Article 69(7) of the Rome Statute provides that evidence will not be admissible where it was obtained by means of a violation of international human rights.[73] It is thus unclear to what extent this will create a challenge in future criminal proceedings. It will also be important to consider how the right to privacy interplays with the "do no harm" principle and how it may affect the reliability of the evidence.[74]

To what extent might technology be sufficient to verify the content of digital evidence without disclosing the source? What sort of probative value will digital evidence that has been verified with an unverified source have? How might this affect the rights of the accused to challenge the evidence against them? These are all evidence-related challenges that need to be considered in light of the increased use of digital evidence.

7.3 Disclosure Challenges

As stated above, the disclosure process at the ICC is complicated and burdensome, perhaps particularly for the Prosecution. However, it presents challenges for the Defence as well.

The prosecution team at the ICC has a separate forensics unit to specifically examine digital evidence, whereas defence teams operate on a smaller budget and smaller staff.[75] Given the vast amount of open-source information that has the potential to become digital evidence, the process of reviewing documents disclosed by the Prosecution may be particularly onerous for Defence teams.[76] This might affect the accused's right to a fair trial, the presumption of innocence and having sufficient time to prepare and challenge the evidence against them.

Disclosure is essential for successful criminal proceedings. However, restrictions apply when disclosure may prejudice a further ongoing investigation or create a risk to the safety of witnesses and victims.[77] In this regard, redactions are often put in place as a protective measure. However, any decisions relating to redactions or other restrictions must bear in mind the aim of a speedy trial.[78]

---

[72] Annex 1, 47.
[73] Ibid, 48; ICC, *Rome Statute*, art. 69(7).
[74] Annex 1, 48.
[75] Annex 2, 7.
[76] Annex 1, 45.
[77] ICC, *RPE*, rule 81(2) and 81(3).
[78] Thus, in *Prosecutor v. Gicheru*, the Prosecutor wanted the Chamber to allow the parties to simultaneously disclose their documents with redactions in the first instance to prevent the prolonging the disclosure process. The Chamber could then consider the redactions put in place and either authorise them or lift the redactions in line with practice of other cases or in the event that one of the parties applies to lift any specific redactions. See *Prosecutor v. Paul Gicheru*, Decision Setting the Regime for Evidence Disclosure and Other Related Matters (2020) ICC-01/09-01/20, para. 13.

Although the disclosure process at the ICC is fairly standardised (albeit complicated), there is no such standardised disclosure process across HR investigative bodies. For instance, the extent of redactions of sensitive information about individuals by HR investigators can differ based on the intended use of the information collected. Some investigatory bodies may redact all names and identifying information, including of potential perpetrators, while others may apply more nuanced redaction policies if the aim is to share that material with ICL investigators. This might pose further challenges, such as the need to obtain consent from witnesses.[79] The timing of the disclosure is another aspect that may have an impact on the criminal proceedings and the perceived credibility of an item of evidence.

International organisations and other agencies may also be prevented from disclosing information, including their sources, either due to its classified or sensitive nature or for protective purposes. Obtaining permissions, especially after a certain time has passed, can itself give rise to further challenges.[80]

As stated elsewhere in this report, the fact that there are no uniform practices or universally applicable standards and guidelines when it comes to the disclosure of information gathered by HR investigatory bodies and the uncertainty around the guidelines that do exist poses a challenge to the use of such information in criminal proceedings.

7.4 Challenges relating to Victims and Witnesses

The challenges relating to victims and witnesses have been alluded to in the sections above and pertain specifically to protecting witnesses and victims featured in open-source information or other digital evidence. Ensuring that the appropriate protective measures are put in place before digital evidence is disclosed to the Defence is a key interest for the Prosecution in international criminal proceedings and may involve the need for significant human resources and time to apply the appropriate redactions and gain witness consent.

There appears to be no uniformity in the practice of international courts and tribunals in this regard, and decisions appear to be made on a case-by-case basis. Given that disclosure is an ongoing process at the ICC, the timing of when a sensitive witness's identity should be disclosed, if at all, is a key consideration to bear in mind, particularly in relation to who should preserve the identity of that witness until such disclosure takes place.[81]

[79] Annex 2, 8 and expert comments.

[80] In this regard, the approach taken by the UNOHCHR concerning disclosure is that information gathered in the course of an investigation must be kept confidential, and disclosure can only be made pursuant to relevant UN protocols relating to sensitive and classified information. See UNOHCHR (United Nations), *Who's Responsible? Attributing Individual Responsibility for Violations of International Human Rights and Humanitarian Law in United Nations Commissions of Inquiry, Fact-Finding Missions and Other Investigations* (2018), UN Doc HR/PUB/18/3, 72. Several HR bodies have taken explicit stances against disclosing sources or information to the ICC or other courts and tribunals in the event that the information is used in criminal proceedings. The International Criminal Tribunal for the Former Yugoslavia (ICTY) has recognised the right to non-disclosure of International Committee of the Red Cross (ICRC) information and Rule 82(1) of the ICC RPE requires "prior consent" of the information provider before introducing information into evidence. See ICTY, *Prosecutor v. Simic et al.*, '*Ex Parte* Confidential Decision on the Prosecution motion under Rule 73 for a ruling concerning the testimony of a witness' (1999) IT-95-9-PT, paras. 73, 76; ICC, *RPE*, rule 82(1).

[81] Annex 1, 44.

7.5 Challenges relating to the Accused

Due to the general availability of open-source information and its sheer amount, it will often be easier for the Prosecution to gather digital evidence to use in building its case.[82] As mentioned above, the Prosecution will have more resources available to preserve and verify the open-source information, whereas the Defence may struggle to do the same. As a result, the right to equality of arms may be at risk.

As admissibility of evidence is often considered at the end of the criminal proceedings rather than at the beginning,[83] this often disadvantages the Defence, who might not be given an opportunity to comment on the evidence at an earlier stage if the Chamber has not yet addressed it. Moreover, given that digital evidence is often pre-recorded or the fact that the source might be unidentified, there may be challenges that arise in relation to the accused's right to cross-examine the evidence against them. Indeed, this will be difficult where the source is anonymous, redacted or unverifiable. The fact that the Prosecution may make use of open-source information gathered by HR investigators with varying mandates or agendas and the absence of standardised processes involved has the potential to impact the fair trial rights of the accused and the presumption of innocence.

[82] Ibid, 41.
[83] See section 7.2.2 above on assessing evidence.

8 Annexes

Annex 1: A. Putt & N. Dubey, “From Investigation to Accountability: Digital Evidence in International Criminal and Human Rights Investigations” (February 2021, International Nuremberg Principles Academy) *[internal work product].*

Annex 2: International Nuremberg Principles Academy, ‘E-Procedure: Evidence in Time of Increased Use of Technology and Digitalisation: Cluster D: Preliminary summary of the main challenges discussed during the expert workshops June–July 2021’ (August 2021).

Annex 3: List of Institutions

E-Procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Cluster D - Annex 1

From investigation to accountability:
Digital evidence in international criminal and human rights investigations

Alisdair Putt & Neha Dubey

1 February 2021

The E-Procedure Project:

Evidence in Time of Increased Use of Technology and Digitalization

Cluster D

International Nuremberg Principles Academy

FROM INVESTIGATION TO ACCOUNTABILITY:

DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL AND HUMAN RIGHTS INVESTIGATIONS

Alisdair Putt & Neha Dubey

1 February 2021

Contents

Abbreviations

Amnesty	Amnesty International
Berkeley Protocol	Berkeley Protocol on Digital Open Source Investigations, 2020
HRW	Human Rights Watch
ICC	International Criminal Court
ICL	International Criminal law
IICI	International Institute Criminal Investigations
IIMM	Independent International Fact-Finding Mission on Myanmar
OHCHR	Office of the United Nations High Commissioner for Human Rights
Open source	Information that is freely available and publicly accessible
OTP	Office of the Prosecution, International Criminal Court
Rome Statute	Rome Statute of the International Criminal Court
RPE	ICC Rules of Procedure and Evidence
UGC	User-generated content
UN	United Nations

INTRODUCTION

> ***When the fundamental principles of human rights are not protected, the centre of our institution no longer holds. It is they that promote development that is sustainable; peace that is secure; and lives of dignity.***
>
> Former UN High Commissioner for Human Rights, Zeid Ra'ad Al Hussein

The investigation of human rights violations has traditionally been the responsibility of States, international organisations, non-government organisations and civil society. These are the bodies that we have elected or entrusted with the role of providing accountability for the monitoring, investigation and enforcement of human rights, as the case may be.

However, with the rapid pace of technological development, smartphones being almost universally available and the proliferation of numerous forms of digital evidence, the landscape has changed significantly. The ability to conduct a human rights investigation is no longer confined to the traditional actors, but is in fact open to everybody no matter who they are, where they live or when they capture relevant information. This means that such investigations are no longer limited to human rights and legal practitioners, but have become an interdisciplinary activity that extends into journalism, civil society and even an individual person's ability to collect and analyse information on various platforms, that can, in turn, raise questions on an individual's right to privacy or right to access information. The focus of this study is not these rights per se, but rather, how the methods of collecting digital evidence in an investigation may impact upon those rights.

Yet, this does not necessarily translate into increased accountability for the perpetrators of human rights violations, which occurs within the framework of international criminal law. This context gives rise to the overarching question of this research project, namely, what are the existing and developing correlations between human rights investigations and criminal accountability? To what extent can the increased volume, types and methods of collecting digital evidence impact the judicial process for criminal responsibility, as a system and as against an accused person? How will future developments in digital evidence affect this overlap, and are human rights investigations as they are currently conducted able to adapt to the evolution of technology? These questions will be considered in detail in this project, and in answering them, the study seeks to map out correlated human rights issues that are arise in light of or due to the increased usage and sophistication of digital evidence.

Cluster D

The research methodology of the study is based on a positivist, comparative and evidence-based approach of considering the actual investigative frameworks and practices employed by practitioners in current situations of human rights violations. The study will also use the authors' experience to consider how human rights investigations must adapt or develop when faced with new or unknown forms of digital evidence, and how that evidence could be used in an international criminal prosecution. To the extent that any references are not provided, the statements and opinions in this study are based on the authors' experience.

This study relies on open source materials only as it focuses on the practice and efficiency of investigations rather than an analysis of legal standards, which would require greater academic research. The authors relied heavily on their consultation with an investigator who is working on many of the examples and case studies cited throughout the report, as he was able to provide technical expertise in relation to the technologies discussed and has worked on both international human rights and criminal law investigations. With the benefit of more time, further interviews could have been conducted with investigators with different qualifications, which could be used for distinguishing the human rights and criminal law approaches to investigations and their correlations.

The authors would like to thank Mark Watson for sharing his insight and experience, and his patience in explaining the technicalities of digital evidence. We are also grateful to Peter Nicholson for his insightful review and to Jolana Makraiova for the constant support provided throughout the writing process.

1. HUMAN RIGHTS INVESTIGATIONS

From the outset, human rights investigations must be distinguished from ICL investigations. As will be demonstrated in this chapter, both have a different purpose and scope, are conducted by different actors and have different frameworks. This chapter will set out the correlations between the different approaches to investigation and how this affects the type and quality of evidence collected. It will also explore the overlap where human rights investigations are advocating for international criminal accountability, which is set out in a comparative table at the end of the chapter.

1.1. HUMAN RIGHTS INVESTIGATIONS

1.1.1. What is a human rights investigation?

There is no universal approach or consistent definition of a human rights investigation. The Mission Statement for Human Rights Watch (**HRW**) provides that HRW is an independent, international organisation, guided by international human rights and humanitarian law, and that they "*scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice.*"[1] Amnesty International (**Amnesty**) states that they "*investigate and expose the facts, whenever and wherever abuses happen. We lobby governments, and other powerful groups such as companies. Making sure they keep their promises and respect international law. By telling the powerful stories of the people we work with, we mobilize millions of supporters around the world to campaign for change…*"[2] These are incredibly broad statements that, while easily understood, do not suggest a fixed outcome. At the same time, this is consistent with the fact that there can never be a 'one size fits all' approach to human rights investigations. Human rights investigations can in fact serve a multiplicity of purposes, as recognized by Navanethem Pillay, former United Nations High Commissioner for Human Rights, when she said that

> *[t]hey help identify perpetrators and protect victims, or contribute to establish both a chain of accountability and vehicles to deliver justice and redress to the victims. They aim at influencing positive change in laws and practice. They draw attention to serious violations and accountability gaps, and help mobilize action nationally and internationally to grant justice to victims. The ultimate goal of this and other human rights work is preventing abuses or, at a minimum, mitigating and stopping*

[1] Human Rights Watch, 'About Us' <https://www.hrw.org/about/about-us/about-our-research> (accessed 21 October 2020).
[2] Amnesty International, 'What does Amnesty Do?' <https://www.amnesty.org/en/who-we-are/> (accessed 21 October 2020).

> *violations when they do occur. This ambitious "manifesto" has not always been matched by adequate means and know-how.*[3]

In general, human rights investigations are conducted for purposes such as:

(i) public dissemination, raising awareness of human rights issues and abuse in the general population, and increased transparency on human rights issues;

(ii) advocating for change through educating people about their rights, being part of conversations for cultural change and shifting attitudes; and

(iii) lobbying actors with the power to stop human rights abuses, improve education and create or enforce accountability for human rights violations.

Other than NGOs, these investigations can be undertaken by various different mechanisms, such as international fact-finding missions, commissions of inquiry, other bodies established by the UN or national human rights commissions. An examination of the differences between these structures is beyond the scope of this study, which is focused on the methodology of evidence collection and how that may be informed by the mandate of the investigative body. The mandate should include, as a minimum, the investigative body's purpose, working method, the geographic scope and time span of the fact finding, the applicable law, and the scope of the commission's conclusions (i.e. fact finding or legal findings).[4]

1.1.2. <u>What are human rights investigators looking for?</u>

The framework of the investigation is set by the body that is conducting the investigation and any safeguards in the investigation depend entirely upon the standards applied by that body. In the authors' experience, there is no universal approach to the investigation format, and there is similarly no universal methodology of collecting information. Rather, this has to be adopted according to the experience, skills and qualifications of the investigators, by reference to the overall goal or purpose of the investigation, and is driven by the agenda of the organisation conducting the investigation.

In general terms, human rights investigations are looking for *information*, and often will only exercise limited scrutiny as to its source and reliability, other than the pragmatic need for that organisation to maintain a reputation for accurate reporting. The information collected is *not* evidence, as it is

---

[3] N Pillay, 'Lecture on Human Rights Investigations and their Methodology', 24 February 2010, <https://unispal.un.org/UNISPAL.NSF/0/C9222F058467E6F6852576D500574710> (accessed 21 October 2020).

[4] F Yuwen, 'Quality Control and the Mandate of International Fact-Finding' in *Quality Control in Fact Finding* (2nd ed, Torkel Opsahl Academic EPublisher) 2020, pp 163-164.

generally not subjected to the scrutiny that would arise in ICL investigations regarding questions such as relevance (to the issue of a person's guilt under certain charges) as well as authenticity. This allows human rights investigations the flexibility to conceal the origins of their information as coming from a confidential source or an unnamed analyst engaged by the investigative body.

The information that investigators are looking for will depend on the ultimate use of that product. For example, an investigation that seeks to shed light or increase media attention on a particular situation will seek to gather large quantities of credible information on multiple aspects of that situation, and this will provide the basis for more targeted future investigations. In contrast, an investigation that is specifically targeted at gathering sufficient evidence that could be used in the prosecution of an individual perpetrator will need to distinguish between different types of evidence (such as crime base or linkage) and pay closer attention to the source of that evidence (this is discussed further in the next section on ICL investigations). The standard of proof that the investigative body applies to its findings is also inherently linked to the purpose of the investigation. With regard to witness testimony, the investigator considers who to interview, and in what language, who will translate, where the interview should be held in order to protect the security of the witness, how the interview should be recorded so as to protect the security of the information, what the interviewer needs to know before the interview, and how to deal with cultural differences which inhibit communication.[5] On the other hand, the collection of digital evidence depends in large part on the research and extraction skills of the investigator, with completely different security concerns depending on the type and source of the evidence. In both cases, the evaluation and analysis of the evidence is an iterative process that generally develops simultaneously as the evidence is being collected.

A number of standards, handbooks and tools have developed to assist investigators and to ensure a basic amount of information about each item of evidence is collected. In the authors' opinion and experience, the following sources are reliable and relevant guidelines on investigative techniques and the evidence that should be collected in a thorough human rights investigation:

(i) Commissions of Inquiry and Fact-finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice.[6] This OHCHR manual provides an overview of the investigation process, the nine core principles that must be followed in the conduct of investigations, and how different types of evidence should be assessed.

[5] Above n 3.

[6] OHCHR, *Commissions of Inquiry and Fact-finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, 2015, <https://www.ohchr.org/documents/publications/coi_guidance_and_practice.pdf> (accessed 24 October 2020).

(ii) The Verification Handbook, developed by the European Journalism Centre, provides step-by-step guidelines for using user-generated content and prescribes best practice advice on how to verify and use this information.[7]

(iii) The Bellagio Report contains recommendations from a workshop held by the Human Rights Center of UC Berkeley on how online open source investigations can be strengthened to improve investigations and prosecutions.[8] In December 2020, the Human Rights Center has published the Berkeley Protocol on Digital Open Source Investigations, which is a comprehensive guide to "the professional standards that should be applied in the identification, collection, preservation, analysis and presentation of digital open source information and its use in international criminal and human rights investigations".[9] It further states that it is aimed at a diverse group of investigators working in different contexts, and is "designed to standardize procedures and provide methodological guidance across disparate investigations, institutions and jurisdictions to assist open source investigators".[10]

(iv) The PILPG Handbook for Civil Society provides guidelines and best practices for the collection and management of information on serious human rights situations and has been developed for those who are not professionally trained in such documentation practices.[11]

(v) The International Protocol on the Documentation and Investigation of Sexual Violence in Conflict is designed to help strengthen the evidence base for bringing perpetrators of sexual violence in conflict to justice.[12] The Institute for International Criminal Investigations has developed guidelines specific to particular conflicts (Sri Lanka, Myanmar, Iraq, etc.) to supplement the International Protocol.[13]

---

[7] C Silverman (ed), *Verification Handbook*, European Journalism Centre, 2014, <https://verificationhandbook.com/downloads/verification.handbook.pdf> (accessed 24 October 2020).

[8] UC Berkeley Human Rights Center, *The New Forensics: Using Open Source Information to Investigate Grave Crimes*, 2017, <https://www.law.berkeley.edu/wp-content/uploads/2018/02/Bellagio_report_2018_9.pdf> (accessed 24 October 2020).

[9] 'Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law', Human Rights Center, UC Berkeley School of Law and OHCHR, 1 December 2020, p 3. Available at: <https://www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news> (accessed 21 December 2020).

[10] Ibid, p 4.

[11] F D'Alessandra et al (eds), *Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices*, Public International Law & Policy Group, 2016, <https://static1.squarespace.com/static/5900b58e1b631bffa367167e/t/59dfab4480bd5ef9add73271/1507830600233/Handbook-on-Civil-Society-Documentation-of-Serious-Human-Rights-Violations_c.pdf> (accessed 24 October 2020).

[12] UK Foreign and Commonwealth Office, *International Protocol on the Documentation and Investigation of Sexual Violence in Conflict* (2nd ed), March 2017, <https://www.gov.uk/government/publications/international-protocol-on-the-documentation-and-investigation-of-sexual-violence-in-conflict> (accessed 24 October 2020).

[13] IICI Publications, <https://iici.global/publications/> (accessed 24 October 2020).

However, it should be noted that there is no mechanism that ensures that an investigation has complied with these protocols. This allows an organisation the flexibility to adapt the investigation according to its mandate and the situation on the ground, but again opens the investigation up to greater scrutiny where a transparent and detailed methodology has not been followed.

Where an investigation is conducted to establish violations of international human rights law, the investigative body must be satisfied to the applicable standard of proof that the violation occurred under the substantive human rights law (e.g. prohibition against torture); and that the violation, through an act or omission, was committed by the State or other party.[14]

The OHCHR Manual[15] and PILPG Handbook[16] set out several key principles that have to be kept in mind in the overall collection of evidence that overlap in both international human rights law and ICL investigations. These include:

(i) Do no harm: The investigation should not jeopardize the safety of the source of evidence, the investigators, or the information collected. This includes doing no harm to any person involved in the collection or provision of the information, i.e. obtaining informed consent. It also means preserving the evidence (chain of custody) and protecting it from tampering or unauthorised access.

(ii) Independence, impartiality and objectivity: Investigators should act independently of any third parties and must investigate all allegations to take account of inculpatory and exculpatory evidence so that objective conclusions can be drawn from the information gathered.

(iii) Credibility and consistency: Investigators should comprehensively examine and analyse all evidence received in order to ensure that the most complete understanding of a situation is achieved, thereby gaining the trust and cooperation of victims, witnesses and others.

(iv) Confidentiality: The investigation must always respect the confidentiality of its sources.

The Berkeley Protocol appears to group guiding principles by referencing what it considers to be the core duties of an open source investigator. The three groups – professional, methodological and ethical – reflect that the scope of an open source investigator's role has evolved due to the

[14] OHCHR, *Who's responsible? Attributing individual responsibility for violations of international human rights and humanitarian law in United Nations commissions of inquiry, fact-finding missions and other investigations*, pp 29-30, <https://www.ohchr.org/Documents/Publications/AttributingIndividualResponsibility.pdf> (accessed 24 October 2020).

[15] Above n 6, pp 33-35.

[16] Above n 11, pp 21-38.

increased use and sophistication of digital evidence, as well as the technical understanding required to conduct high quality, reliable investigations.[17] The principles are:

Professional principles	Methodological principles	Ethical principles
Accountability	Accuracy	Dignity
Competency	Data minimization	Humility
Objectivity	Preservation	Inclusivity
Legality	Security by design	Independence
Security awareness		Transparency

These principles generally have the same meaning or intention across different publications. In the authors' opinion, the Berkeley Protocol represents the most detailed and considered multi-disciplinary standard for open source digital investigations currently available to practitioners. Its intended audience extends beyond investigators to "lawyers, archivists and analysts who work for international, regional and hybrid criminal tribunals; national war crimes units; commissions of inquiry; fact finding missions; independent investigative mechanisms; international organizations; transitional justice mechanisms; and nongovernmental organizations (NGOs)."[18] This also reflects the reality that professionals with different backgrounds and qualifications work together on investigations, and that the evidence they collect may be submitted in multiple legal jurisdictions.

Nonetheless, and as noted from the outset, these are all guidelines that have been developed through practice and lessons learned in human rights investigations. Adherence to these standards improves the legitimacy and credibility of the investigation findings. But they do not provide hard and fast rules about how investigations should be conducted and what outcome they should achieve – this will always be driven by the entity conducting the investigation and how it chooses to use its findings. It is perhaps for this reason that the credibility, objectivity and accuracy of human rights reporting is often subject to enhanced scrutiny, even though there is no agreed or standardised method of investigations.[19]

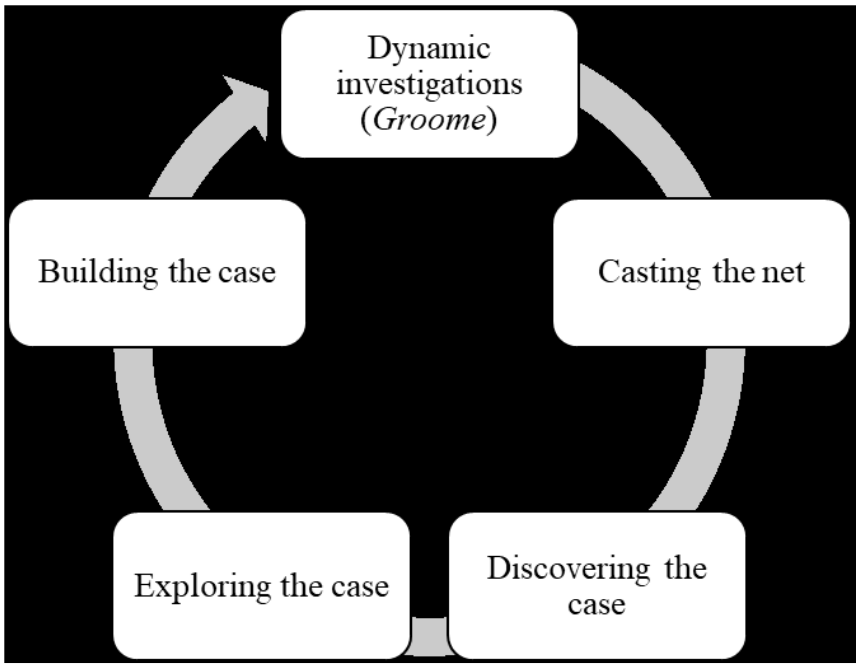
[17] Above n 9, pp 11-16.
[18] Above n 9, p 5.
[19] M Aksenova et al, 'Non-Criminal Justice Fact-Work in the Age of Accountability', in above n 4, p 30.

1.2. INTERNATIONAL CRIMINAL INVESTIGATIONS

1.2.1 What is an ICL investigation?

ICL investigations are the means by which the international community pursues individual criminal responsibility, prevents impunity against the commission of international crimes (such as genocide, war crimes and crimes against humanity) and provides reparations to victims. Unlike the variety and breadth in the mandate of human rights investigations, ICL investigations have an explicit legal framework as there are different stages in the investigation process to prosecution. They are usually focused on the collection of evidence against the specific elements of a crime(s).

At the ICC, the OTP first conducts a preliminary examination to determine whether there is a sufficient basis to open a full investigation. This stage is described as consisting of four phases and requires legal direction throughout to ensure that the evidence collected could be used at trial:[20]



(i) **casting the net** to establish what actually happened;

(ii) **discovering the case** by analysing the evidence available to develop theories and identify suspects;

(iii) **exploring the case** by pursuing concrete investigative leads and eliminating doubts; and

(iv) **building the case** to identify the crime base, modes of liability and remedying any evidentiary gaps.

[20] C Stahn, 'From Preliminary Examination to Investigation: Rethinking the Connection' in X Agirre et al (eds), *Quality Control in Criminal Investigation*, (Torkel Opsahl Academic EPublisher), 2020, pp 59-60.

Cluster D

Under Articles 53(1)(a)-(c) of the Rome Statute, preliminary examinations require the OTP to consider jurisdiction (temporal, material, and either territorial or personal jurisdiction), admissibility (complementarity and gravity) and the interests of justice. The OTP provides reasoned decisions on whether or not to proceed with investigations and issues regular reports on its activities in order to promote transparency.[21] Whereas preliminary examinations largely rely on open source material as the OTP cannot deploy significant investigative resources at this stage, the opening of an investigation entails a more formal process with the specific purpose of deciding whether there is a sufficient basis for prosecution, identifying individual perpetrators and reducing uncertainties.[22]

ICL investigations are usually conducted by the prosecution team and require collection of both inculpatory and exculpatory *evidence*, not just information. The safeguards or checks on the quality and reliability of the evidence exist in the rules of evidence and the onus of proof: the purpose of the investigation is to collate sufficient material for the prosecution team to persuade the court or tribunal beyond a reasonable doubt that the accused committed the crimes. The rules on admissibility, relevance and credibility allow the court or tribunal to make an assessment as to whether the evidence meets the standard of proof. Unlike the information collected in human rights investigations, ICL investigations will ultimately have to disclose their sources, which can provide additional challenges in relation to such things as witness security, witness tampering and delegation of investigations to biased intermediaries in hostile environments.

In practical terms, bodies conducting ICL investigations require investigative staff to have significant skills and experience, usually obtained in a national jurisdiction. However, the most significant difference to human rights investigations is the prosecution's disclosure obligations in ICL proceedings. At the ICC, for example, the Prosecution must disclose to the defence exculpatory material[23] and the "names of witnesses whom the Prosecutor intends to call to testify and copies of any prior statements made by those witnesses".[24] It must also "permit the defence to inspect any books, documents, photographs and other tangible objects in the possession or control of the Prosecutor, which are material to the preparation of the defence or are intended for use by the Prosecutor as evidence for the purposes of the confirmation hearing or at trial, as the case may be, or were obtained from or belonged to the person".[25]

---

[21] OTP, *Policy Paper on Preliminary Examinations*, November 2013, [15]. Available at: <www.legal-tools.org/doc/acb906/> (accessed 20 December 2020).
[22] Above n 19, pp 40-42.
[23] Rome Statute of the International Criminal Court (**Rome Statute**), Article 67(2).
[24] Rule 76, Rules of Procedure and Evidence of the ICC (**RPE**).
[25] Rule 77, RPE.

ICL investigations have traditionally relied upon State cooperation to facilitate physical access, whereas human rights investigations have been more flexible in this regard. However, digital evidence provides an opportunity for the ICC and other bodies to access challenging hostile operating environments, particularly where State parties are not cooperating with the investigation.

1.2.2 What are ICL investigators looking for?

ICL investigators will be guided by the same principles as human rights investigators in their methodology of collecting evidence. However, unlike human rights investigations, the evidence they are looking for is necessarily guided by the legal elements of the crime and the legal requirements for that evidence to be admissible and reliable in court or tribunal proceedings. The investigators do not have the same flexibility in their conduct of the investigation, as their findings must always comply with the legal rules in order to achieve the requirements to fairly present the evidence. Ultimately such investigators may be required to give evidence, and be available for cross examination, on the means and methods of the collection of the evidence, and its source.

The Rome Statute gives the International Criminal Court (**ICC**) jurisdiction over four crimes and provides the definition of what is encapsulated by each of those crimes in Articles 6 (genocide), 7 (crimes against humanity), 8 (war crimes) and 8*bis* (crime of aggression). Further, Article 9 provides that the interpretation and application of these articles should be guided by the Elements of Crimes. That document sets out each of the elements of the crimes that must be proven by the prosecution in order to establish the crime itself.

Articles 54 and 55 of the Rome Statute define the Prosecutor's mandate in carrying out investigations as well as the rights of the accused person during an investigation. Similar to the standards and principles identified for human rights investigations, these articles confirm that the Prosecutor is required to abide by the do no harm principle, maintain their independence and confidentiality, and collect all relevant evidence required to "establish the truth".

> **Article 54. Duties and powers of the Prosecutor with respect to investigations**
> 1. The Prosecutor shall:
> (a) In order to establish the truth, extend the investigation to cover all facts and evidence relevant to an assessment of whether there is criminal responsibility under this Statute, and, in doing so, investigate incriminating and exonerating circumstances equally;
> (b) Take appropriate measures to ensure the effective investigation and prosecution of crimes within the jurisdiction of the Court, and in doing so, respect the interests and personal circumstances of victims and witnesses, including age, gender as defined in article 7, paragraph 3, and health, and take into account the nature of the crime, in

particular where it involves sexual violence, gender violence or violence against children; and

(c) Fully respect the rights of persons arising under this Statute.

2. The Prosecutor may conduct investigations on the territory of a State:

(a) In accordance with the provisions of Part 9; or

(b) As authorized by the Pre-Trial Chamber under article 57, paragraph 3 (d).

3. The Prosecutor may:

(a) Collect and examine evidence;

(b) Request the presence of and question persons being investigated, victims and witnesses;

(c) Seek the cooperation of any State or intergovernmental organization or arrangement in accordance with its respective competence and/or mandate;

(d) Enter into such arrangements or agreements, not inconsistent with this Statute, as may be necessary to facilitate the cooperation of a State, intergovernmental organization or person;

(e) Agree not to disclose, at any stage of the proceedings, documents or information that the Prosecutor obtains on the condition of confidentiality and solely for the purpose of generating new evidence, unless the provider of the information consents; and

(f) Take necessary measures, or request that necessary measures be taken, to ensure the confidentiality of information, the protection of any person or the preservation of evidence.

Article 55. Rights of persons during an investigation

1. In respect of an investigation under this Statute, a person:

(a) Shall not be compelled to incriminate himself or herself or to confess guilt;

(b) Shall not be subjected to any form of coercion, duress or threat, to torture or to any other form of cruel, inhuman or degrading treatment or punishment;

(c) Shall, if questioned in a language other than a language the person fully understands and speaks, have, free of any cost, the assistance of a competent interpreter and such translations as are necessary to meet the requirements of fairness; and

(d) Shall not be subjected to arbitrary arrest or detention, and shall not be deprived of his or her liberty except on such grounds and in accordance with such procedures as are established in this Statute.

2. Where there are grounds to believe that a person has committed a crime within the jurisdiction of the Court and that person is about to be questioned either by the Prosecutor, or by national authorities pursuant to a request made under Part 9, that person shall also have the following rights of which he or she shall be informed prior to being questioned:

(a) To be informed, prior to being questioned, that there are grounds to believe that he or she has committed a crime within the jurisdiction of the Court;

(b) To remain silent, without such silence being a consideration in the determination of guilt or innocence;

(c) To have legal assistance of the person's choosing, or, if the person does not have legal assistance, to have legal assistance assigned to him or her, in any case where the interests of justice so require, and without payment by the person in any such case if the person does not have sufficient means to pay for it; and

(d) To be questioned in the presence of counsel unless the person has voluntarily waived his or her right to counsel.

The Prosecutor is also bound by due process – evidence that is collected in a manner contrary to Articles 54-55 is unlikely to be admissible in any court or tribunal proceedings. In general, there are only two circumstances where an item of evidence will not be admissible: where it was obtained by means of a violation of internationally recognized human rights, such as by torture, duress or coercion; or if it would breach the accused's right to a fair trial.[26] Once admitted, it will then be for the Court to determine the weight to be given to each item of evidence in establishing the facts.

1.3. THE OVERLAP BETWEEN HUMAN RIGHTS AND ICL INVESTIGATIONS

Human rights investigations have been crucial contributors to judicial procedures and transitional justice mechanisms. They are equal contributors to the ultimate cause of accountability and creating a historical record for both individual criminal responsibility as well as mass atrocity events, singular or multiple, that occur over a longer period of time. In light of the principle of complementarity in international criminal law, 'no stone should be left unturned' in trying to strengthen the ability and political will of national investigations and prosecutions into human rights violations and criminal responsibility.[27]

Considering the overlap between the two types of investigations requires an examination of how the findings of human rights investigations can be used at different stages of ICL proceedings. The information gathered in human rights investigations will be relevant for analysis and examination of a situation before ICL proceedings are instituted, as open source materials and reports by human rights bodies generally provide background and context, as well as 'lead intelligence'. Prosecutors can review such documentary materials before considering whether to commence a criminal investigation and what its mandate should be, and definitely before any victims or witnesses are contacted for interviews. Documentary evidence can also be used for context, as corroboration evidence, and in some cases, the authors of human rights investigation reports may be called as expert witnesses during trial. In the ICC context, there will be a lower level of scrutiny applied to human rights reports and fact-finding by the Court. Stahn and Jacobs observe that the evidentiary basis for cases referred to the Court by the Security Council are not reviewed at all, and where the Prosecutor seeks to open a case through the exercise of his or her *proprio motu* powers,

[26] See Rome Statute Article 69(7); ICTY RPE Rules 89(B) and (D); ICTR RPE Rule 89(B); SCSL RPE Rule 89(B); STL RPE Rules 149(B) and (D); ECCC Internal Rule 87(3)(d). The authors are not aware that this provision has been tested in any international criminal proceedings.
[27] Above n 19, p 12.

> *all supporting documentation brought forward by the OTP for opening an investigation, whether in relation to the general context, or the commission of particular crimes comes from third party sources (NGOs, United Nations, press) and receives near to no level of scrutiny from the Pre-Trial Chamber.*[28]

Once the ICC has opened an investigation, there is a significant overlap with the findings in a human rights investigation, especially in relation to contextual and crime base evidence. Human rights investigations can provide leads for ICL investigators to interview witnesses or reveal gaps that need to be filled as the ICL investigator is concerned with an individual case rather than an overall situation. But by the same token, the ICL investigator has to take more care in gathering evidence specific to a case, ensuring that witnesses that are interviewed multiple times are not re-traumatized or do not provide inconsistent evidence, that chain of custody is maintained and that the evidence is relevant and reliable. They also need to keep their legal team updated of their progress and ensure that only the investigator or the lawyer is contacting witnesses. In particular, investigators need to be aware that poor coordination and multiple interviews of the same witness can lead to that individual's re-traumatization, as well as fatigue in a community being overwhelmed by inquiries and then perceiving others as potentially betraying or accusing them, or in the case of sexual or gender-based violence victims, attaching a negative stigma to them. This will affect both investigative leads and the quality of witness testimony.[29] As Abbott has observed,

> *The greater the number of statements a victim or witness gives, the more likely that there will be inconsistencies between their different accounts, especially if those statements are taken by different actors. Such inconsistencies may be used to undermine their credibility at any trial, and may even lead to the person not being called as a witness at all.*[30]

Case study: Helping or hindering prosecution? Release of confession videos in Myanmar

The serious human rights violations in Myanmar, as well as how this may translate to crimes under international law, has been documented by a number of journalists, NGOs, UN bodies and the opening of an investigation by the OTP of the ICC (in addition to legal action by State parties in the International Court of Justice). The *New York Times* recently reported on two low level Myanmar Army soldiers who fled from Myanmar to Bangladesh and gave video testimony that they had carried out the orders of their commanding officers

[28] C Stahn and D Jacobs, 'Human Rights Fact-Finding and International Criminal Proceedings: Towards a Polycentric Model of Interaction', *Grotius Centre Working Paper 2014/017-ICL*, 31 January 2014, p 16. Available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2388596> (accessed 24 October 2020).

[29] K Abbott, 'Myanmar: documentation practices may raise challenges for accountability', Opinio Juris, 24 January 2019. Available at: <http://opiniojuris.org/2019/01/24/myanmar-documentation-practices-may-raise-challenges-for-accountability/> (accessed 28 November 2020).

[30] Ibid.

to kill Rohingya civilians in Rakhine State, Myanmar in August 2017.[31] The videos were produced by the Arakan Army (**AA**), an armed opposition group, who also made them available to some media outlets. The soldiers have since been reportedly transferred to the Hague, after interviews by ICC personnel.

Fortify Rights, an NGO that investigates human rights violations, obtained and analysed these videos against existing documentation and assessed the confessions to be credible. They were able to corroborate the soldiers' accounts of mass graves with other witness testimony, satellite imagery of the particular villages and their previous reports documenting killings, violence and the systematic destruction of Rohingya villages.[32]

Although Fortify Rights and the *New York Times* have claimed that these videos and taking the soldiers into custody are a "monumental moment for Rohingya and the people of Myanmar in their ongoing struggle for justice", others consider that this publicity potentially endangers the safety of the two soldiers, their family members, and close friends and associates still in Myanmar to reprisals.[33] As a result, this could deter other potential witnesses to atrocities from coming forward.[34] Mathieson considers that this raises three questions which could seriously affect the use of this information in any future prosecution:[35]

- it is not clear how Fortify Rights had access to the footage, which was produced by the AA and whether it was in any way repackaged;
- which parties (the Arakan Army, the Bangladeshi government or ICC officials) allowed the release of the video and determined how it was published?; and
- now that the videos have been made public, is there any reason they would not be admissible and/or should a court accord them less weight?

The publicity garnered by this story has most likely made it more difficult for other actors who are trying to conduct investigations into alleged war crimes within Myanmar. This case also shows how the AA are posting various testimonies by deserters/prisoners of war online, and how human rights organisations seek to exploit such materials, which may tend to 'feed the beast' and encourage the contravention of the requirement for the dignified treatment of such detainees/prisoners and their right to privacy.

[31] H Beech, S Nang and M Simons, "'Kill all you see": In a first, Myanmar soldiers tell of Rohingya slaughter', *New York Times*, 8 September 2020. Available at: https://www.nytimes.com/2020/09/08/world/asia/myanmar-rohingya-genocide.html (accessed 28 November 2020).

[32] 'International Criminal Court: Prosecute and Offer Witness Protection to Myanmar Army Deserters', Fortify Rights, 8 September 2020. Available at: <https://www.fortifyrights.org/mya-inv-2020-09-08/> (accessed 28 November 2020).

[33] Based on the authors' discussions with practitioners for the purpose of this study, similar concerns have also arisen in the Syrian context where witnesses provided testimony at one point in time. They withdrew their testimony months later because there had been a regime change in the territory where they lived, and they no longer felt safe in being on the record.

[34] DS Mathieson, 'Commodifying prisoners of war in Myanmar', Asia Times, 25 September 2020. Available at: <https://asiatimes.com/2020/09/commodifying-prisoners-of-war-in-myanmar/> (accessed 28 November 2020).

[35] Ibid.

Coming back to the ICC, much greater scrutiny is applied to the findings of human rights investigations at later stages of judicial proceedings and as the standard of proof becomes more onerous. The Pre-Trial Chamber appears to have accepted open source evidence to provide a sufficient basis for the issuing of arrest warrants and granting provisional release, but prefers direct evidence in order to confirm charges.[36] This suggests a stricter application of legal criteria to evidence from human rights investigations which would have been collected for a broader or different purpose.

The table on the following page compares and summarises the scope and purpose of human rights and ICL investigations. The fact that different frameworks apply to the collation and use of the findings in different types of investigation does not detract from their value in any way. Rather, the overlap between the two types of investigation must bear in mind that human rights investigations will be important sources for credible evidence of human rights violations. Whether that evidence can be used to establish individual criminal responsibility is an entirely separate question, and will remain for the adversaries to argue and judges to determine.

[36] Ibid, pp 17-19.

Cluster D

Features of investigation	Human rights	Correlation or Overlap	ICL
Body conducting investigation	NGOs, private actors, international fact-finding missions, commissions of inquiry, other bodies established by the UN or national human rights commissions		Prosecution and defence teams Civil law countries – the investigating judge
Purpose	Looking for *information* Draw attention to gaps in accountability Basis for lobbying government for change Increase public awareness Protect victims	Provide leads for other investigations. Expose serious violations, create a record.	Looking for *evidence* Prevent impunity Establish the commission of crimes Identify individual perpetrators of crimes Provide reparations to victims
Working method	Not uniform, various guidelines available. Most recent publication on open source digital evidence is the Berkeley Protocol, which is trying to introduce harmonised standard. Common guiding principles: independence, impartiality, confidentiality, credibility, do no harm. No compliance mechanism for adhering to these guidelines.	Methodology should be consistent with due process. Crime base and corroborative evidence from human rights investigations can be used in ICL investigations. Human rights investigators can be called as witnesses in ICL proceedings. Investigation planning and coordination is crucial to the quality of evidence obtained.	Rely on ICC policy papers and practices developed by OTP investigations and forensics teams. Evidence should not jeopardize the safety of the source of evidence, the investigators, or the information collected. Also, have to preserve the evidence (chain of custody) and protecting it from tampering. Poor quality working methods will make evidence inadmissible in court or reduce weight and probative value of evidence. Consider inculpatory and exculpatory evidence, disclosure requirements during proceedings

Cluster D

Standard of proof	Collecting information, not evidence. Any standard of proof will be defined by the mandate of the investigation.	Evidence collected needs to be authentic, credible and reliable. It should be more than the balance of probabilities (50%).	Individual criminal responsibility must be established beyond a reasonable doubt.
Geographic scope	Depends on the purpose of the investigation		Requirements provided in Rome Statue regarding jurisdiction over particular crimes, committed in the territory of member states by member states.
Time span	Depends on the purpose of the investigation		As provided in the charges in the indictment.
Applicable law	International human rights law and any domestic implementing legislation (protection of civil rights) Procedural law of national courts or human rights body		International criminal law Procedural law of the court/tribunal
Conclusions	This links back to the *purpose* of the investigation – generally fact finding and conclusions are drawn from those facts.	Human rights investigation can conclude that there is a sufficient basis to further investigate prosecution of identified individuals	Legal findings that are admissible and meet the standard of proof.
Stage of investigation	Preliminary assessment, collection, verification and preservation, analysis for leads, gaps or handing over to litigation.	Complementarity – human rights investigation findings can be relied upon in preliminary examination	ICC has two stages: (1) preliminary examinations; which can progress to (2) investigation.

2. DIGITAL EVIDENCE

An examination of digital evidence in the context of international investigations requires an understanding of what that evidence actually is and how it was created. In broad terms, digital evidence can be defined as the storage, receipt or transmission of evidence by electronic means.[37] Digital open source evidence can be defined as information on the internet that any member of the public can observe, purchase or request without requiring special legal status or unauthorised access.[38] Consequently, the focus of the inquiry into the use of digital evidence in international human rights and criminal law investigations will be on how it was obtained and whether it is reliable, rather than concepts of ownership of the evidence.

This chapter first provides the preliminary issues that investigators have to consider when collecting digital evidence, namely, how to access the evidence, the checks on the quality of that evidence and how open source materials become 'evidence' that becomes the property of the investigation.

The chapter examines three technologies or phenomena that the authors consider to be of key importance based on their experience of ongoing investigations, and that have potential to develop rapidly in the near future: deleted accounts, deepfakes and artificial intelligence. These examples have also been selected on the basis that they already exist on multiple existing open source platforms and are not confined to one particular form of publication. For instance, although the technical features of a deleted account on Facebook and YouTube may be different, the evidentiary issues that arise from the changes to that account from an investigations and legal perspective are the same.

In the authors' experience, these technologies raise novel *verification* issues. Deleted accounts are arguably analogous to disappearing messages or emails, deepfakes modify images and videos, and artificial intelligence is used to generate data that we are already familiar with. However, they require investigators to focus on the quality and format of evidence generated – the evidence itself is not new.[39] Nonetheless, they raise additional practical challenges in the investigations context.

[37] L Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', 41(2) *Fordham International Law Journal* 283 (2018), p 297. Available here: <https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1/> (accessed 5 December 2020).
[38] Above n 9, p 6.
[39] Other technologies that were considered but not included for this study include messaging on different applications (such as Signal, WhatsApp, etc.), Tweets, satellite imagery, blockchain technology and cyber security or data breaches.

2.1 GATHERING OPEN SOURCE DIGITAL EVIDENCE

As a preliminary point, this study focuses on open source evidence that can be collected by anyone with access to the internet. Whether this evidence could eventually be tendered in court would require it to "prove or disprove a fact material to the allegation, be authentic rather than false, and brought from a reliable and credible source to court along an unbroken chain of custody to avoid contamination, tampering or fabrication."[40] These features are not necessary from a human rights perspective, but would improve the credibility and reliability of any conclusions drawn in a human rights investigation from such evidence.

The Berkeley Protocol describes the open source investigation cycle – for both human rights and ICL investigations – as rarely being linear, often requiring repetition during case-building, and comprising the following tasks:[41]

[40] L Syunga, 'Can International Criminal Investigators and Prosecutors Afford to Ignore Information from United Nations Human Rights Sources?' in *Quality Control in Fact Finding* (2nd ed, Torkel Opsahl Academic EPublisher) 2020, p 382.
[41] Above n 9, p 55.

2.1.1 Verification and corroboration

From the outset, it should be remembered that all evidence must be verified and corroborated. The question at the heart of verification is: "how do you know that?"[42] This requires establishing four elements:

(1) provenance – is this the original piece of content?;

(2) source – who uploaded the content?;

(3) date – when the content was created; and

(4) location – where the content was created.[43]

Confirmation of these elements allows the investigator to have a strong measure of confidence in the evidence in its own right and its ultimate use after the investigation. There are several open source materials that explain how to verify images and video in layman terms, and provide general guidelines on the investigation of human rights violations.[44] Verification can be made more difficult where the same evidence is repeatedly published on different platforms or used by different organisations. The Content Authenticity Initiative provides a workflow for human rights activists to capture secure and provable details of an asset without unnecessary exposure of privacy details,[45] and Witness has a number of guides for activists on how to archive video and which tools allow the collection of evidence in a secure format, all the time protecting the privacy of the activist.[46]

Whereas rules of evidence are designed to provide guidance regarding the admissibility and weight to be assigned the particular piece or item of information in criminal investigations, as explained in the previous chapter, human rights investigations have different mandates and are not bound by these standards. Nonetheless, investigators still have to overcome a number of practical challenges when collating and compiling digital evidence to ensure that it meets the standards of accuracy and reliability set by the mandate of their investigation, as the key risk to a human rights organisation

---

[42] Above n 7, p 16.
[43] Above n 7, p 27.
[44] See for example:

- Verifying images, Data Journalism: https://datajournalism.com/read/handbook/verification-1/verifying-images/4-verifying-images
- Witness – video as evidence field guide: https://vae.witness.org/video-as-evidence-field-guide/
- Exposing the invisible: The Kit https://kit.exposingtheinvisible.org/en/how/visual-evidence.html#managing-visual-evidence
- How to investigate human rights violations:
- https://www.humanrightscareers.com/magazine/beginners-guide-how-to-investigate-human-rights-violations/

[45] Rosenthol et al, "The Content Authenticity Initiative: Setting the Standard for Digital Content Attribution", August 2020. Available at: https://documentcloud.adobe.com/link/track?uri=urn%3Aaaid%3Ascds%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19#pageNum=1> (accessed 27 January 2021).
[46] Witness Library. Available at: <https://www.witness.org/resources/> (accessed 27 January 2021).

in publishing its findings is the possible reputational damage if the evidence is proved to be demonstrably wrong.

Case study: An interactive digital platform for presenting evidence on Mali

SITU is an "unconventional architecture practice" that collaborated with the ICC's Office of the Prosecutor to develop an interactive digital platform in the Al-Mahdi case concerning the destruction of cultural property. This platform combines geospatial information, historic satellite imagery, photographs, open source videos, and other forms of site documentation to effectively recreate the sites before, during and after their destruction.[47] This is the first and only digital tool of its kind where the Court was provided a visual *and* spatial evidential tool to examine heritage sites from the comfort of the courtroom. On the one hand, separate forms of corroborative evidence have been combined into one interactive item of evidence that effectively places judges in the investigator's shoes and gives them a unique perspective. It would undoubtedly incline the judges towards considering the platform reliable and of considerable weight in the prosecution's argument. On the other hand, this kind of project may only be suitable for this particular crime and may create inequality of arms for the defence. For example, it would be difficult to rebut individual items of evidence that contributed to the interactive platform and this may disproportionately prejudice the defendant's case. At the same time, this evidence is contextual and will not be determinative of other elements of a crime. Issues with equality of arms could also be overcome if defence investigators are included in the process of compiling evidence that will be fed into the interactive platform, although this may not be consistent with the adversarial approach.

Case study: The open source investigation on chemical weapon attacks in Syria that resulted in criminal prosecution in Germany

Following a two-year-long investigation, on 5 October 2020, the Open Society Justice Initiative, the Syrian Center for Media and Freedom of Expression, and the Syrian Archive together submitted a dossier to the German federal prosecutor on behalf of victims of sarin gas attacks in Syria in 2013.[48] There were three investigation objectives:[49]

[47] ICC Digital Platform: Timbuktu, Mali, 2016. Available at: https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali (accessed 28 November 2020).

[48] B McKernan, 'Criminal complaint submitted to German court over sarin gas attacks in Syria', The Guardian, 6 October 2020. Available at: <https://www.theguardian.com/world/2020/oct/06/criminal-complaint-submitted-to-german-court-over-sarin-gas-attacks-in-syria> (accessed 28 November 2020). See also <https://www.justiceinitiative.org/litigation/chemical-weapons-attacks-in-syria> and <https://www.aljazeera.com/news/2020/10/7/syria-leader-named-in-criminal-complaint-against-chemical-attacks>.

[49] 'Chemical Weapons Attack in Eastern Ghouta, Syria: A Visual Summary of an Open Source Investigation', Human Rights Center, UC Berkeley, 8 October 2020. Available at: https://storymaps.arcgis.com/stories/56c19f1dbcbb4054b524cacc5f6a9fa5 (accessed 28 November 2020). See also <https://storymaps.arcgis.com/stories/f353d0a2893e4396b9d82b9ba5458d69>.

(1) Verify and map the geographic locations of all impact sites. This was done by compiling images and videos of the sites after the attack and matching them with satellite imagery.
(2) Identify, collect and verify all available online information, including from open source reports published by other NGOs, on the munitions and delivery system used in the attacks. This was incorporated into the maps.
(3) Identify public statements made by the Russian and Syrian government officials or their surrogates in press releases, media interviews and social media posts. This was done to consider the extent to which public officials had knowledge of the attacks, and to identify disinformation or counter-narratives.

This project shows the power of open source investigations that are conducted systematically and with a well-defined purpose, perhaps made easier in this case as the focus was on the Syrian government's responsibility for the attacks, and this did not rely on witness testimony. The project highlights the detailed, manual labour required to work through vast volumes of evidence to ensure quality, but which is increasingly done using artificial intelligence and automated searching techniques. It followed existing protocols for the verification of evidence and identified responsible individuals, which makes the prosecutor's job easier in terms of establishing the elements of crime and also the reliability of the evidence.

2.1.2 Source of the evidence

Digital forensics can be considered a three stage process of seizing the evidence, acquiring it (creating a forensic image of the media), and analysing it (analysis is conducted on the forensic image so as to preserve the original media form).[50] For seizure, the data that constitutes digital evidence generally originates from a device, not a device or a service provider. Evidence from a device refers to physically stored data on a device, such as a phone, laptop, camera, disks, flash drives and memory cards. Evidence extracted from a physical device generally has the data on when and where it was created (the metadata), and the chain of custody of the evidence remains intact as it is based on how the device was seized. Many investigative agencies have protocols that ensure that any digital item obtained is first captured in an unalterable form, such as by encrypting it, and making a working copy at the same time for investigative/review purposes.

Evidence that is not from a device refers to open source data that is available on web pages and any other media that is not on a physical device. Establishing how that data was created and the chain of custody will depend on the extent to which that data is published and the forensic tools

[50] M Novak et al, *New Approaches to Digital Evidence Acquisition and Analysis*, National Institute of Justice, 7 October 2018. Available at: <https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis> (accessed 22 November 2020).

available to the investigator. The analysis and methodology applied to open source evidence will also have to contend with data availability, the risk of incomplete data sets, and false information.

Evidence from a service provider refers to data that is stored in the cloud or any other virtual storage system – although it may still exist in a storage mechanism that saves the data from the virtual location at a particular point in time. Cloud data raises a number of concerns for investigators. There can be issues with restricted access to the cloud due to lack of cooperation of the service provider, and the general limitations of controlling the acquisition or recovery of the data depending on the forensic tools available to the investigator.[51] Data might be stored in multiple physical locations and jurisdictions, and the volume and complexity of the data might be so vast that it would be impractical for the investigator to extract all of the evidence.[52] For example, cloud services like Office365 provide easy security operations to capture data from an email inbox, but the data might reside in one jurisdiction and be backed up to another jurisdiction.

2.2 DELETED ACCOUNTS

It is common practice for individuals to set up accounts on social media, use the account to disseminate messages and then delete the account once it is no longer required as a means to protect their identity and the traceability of the information published on that account. Flipping this on its head, it is also possible that after an individual posts disturbing content on a host platform such as YouTube (which could be vital evidence in an international human rights or criminal investigation), content moderators will delete that content for being inappropriate or extremist. The question therefore arises whether deleting an account or content in fact totally removes the information that was formerly published from the internet? For example, Facebook has two types of databases: one for user-generated content (such as status updates and photos) and one for log data (when the user logs in, what they click on and where they comment).[53] While the user-generated content is deleted with the account, the log data, including data that other Facebook users have shared about you, is not deleted and Facebook can use or sell this data at its discretion.

[51] I Ahmed and V Roussev, 'Analysis of Cloud Digital Evidence', *Security, Privacy, and Digital Forensics in the Cloud*, 2019, p 4. Available at <https://www.researchgate.net/publication/330976466_Analysis_of_Cloud_Digital_Evidence> (accessed 22 November 2020).
[52] J Koppen et al, 'Identifying Remnants of Evidence in the Cloud', *Digital Forensics and Cyber Crime*, 2013, p 43. Available at: <https://link.springer.com/chapter/10.1007/978-3-642-39891-9_3> (accessed 22 November 2020).
[53] A Picchi, 'OK, you've deleted Facebook, but is your data still out there?', CBS News, 23 March 2018. Available at: <https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/> (accessed 28 November 2020).

This is a recognized problem and individuals rely on techniques such as using private mode when browsing and disabling or deleting application, system and security logs to reduce their traces.[54] Although investigators have developed various means to recover data from a deleted account, they are dependent on the quality of the forensic tools available to conduct digital investigations and the time available. In the authors' experience, one method that can be employed *during* an investigation to identify, capture and preserve content before a platform deletes it, is to take the following measures:

(i) identify the location and file structure of the content;

(ii) download the content from the platform;

(iii) take a snapshot of the offline content and recording its metadata.

These steps allow for evidence to be preserved before it is deleted from the source, without compromising the authenticity or integrity of the evidence and maintaining a transparent chain of custody.

Coming back to the YouTube example for a different hypothetical, what steps can an investigator take if YouTube has mistakenly or wrongfully deleted crucial, relevant evidence – YouTube may have algorithms for detecting and automatically deleting certain content, it operates in multiple jurisdictions and the servers on which the content is stored might be in another jurisdiction to the one in which copies of the content are requested to be produced by investigators.[55] Similarly, Facebook has been under scrutiny for the mass suspension, deactivation or removal of accounts of journalists and human rights activists without explanation in Syria, Tunisia and Palestine, to name a few.[56] These accounts appear to have been miscategorized as having links to terrorism, which would appear to interfere with those individuals' freedom of expression, especially in countries that rely on Facebook as the platform of advocacy and debate. These all present obstacles to the recovery of the evidence.

[54] MI Al-Saleh, 'Forensic artefacts associated with intentionally deleted user accounts', International Journal of Electronic Security and Digital Forensics 9(2):167, January 2017. Available at: https://www.researchgate.net/publication/316615418_Forensic_artefacts_associated_with_intentionally_deleted_user_accounts (accessed 28 November 2020).

[55] R Costello, 'Crucial video evidence of war crimes is being deleted. How can it be saved?', The World, 30 September 2018. Available at: <https://www.pri.org/stories/2018-09-25/crucial-video-evidence-war-crimes-being-deleted-how-can-it-be-saved> (accessed 28 November 2020).

[56] O Solon, "'Facebook doesn't care": Activists say accounts removed despite Zuckerberg's free-speech stance', NBC News, 16 June 2020. Available at: <https://www.nbcnews.com/tech/tech-news/facebook-doesn-t-care-activists-say-accounts-removed-despite-zuckerberg-n1231110> (accessed 28 November 2020).

It should be noted that these issues appear to have been contemplated in the *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda* (the **Joint Declaration**), which provides a general principle that:

> 4a. Where intermediaries intend to take action to restrict third party content (such as deletion or moderation) which goes beyond legal requirements, they should adopt clear, pre-determined policies governing those actions. Those policies should be based on objectively justifiable criteria rather than ideological or political goals and should, where possible, be adopted after consultation with their users. [57]

However, as social media platforms are not signatories to the Joint Declaration, they are not bound to follow this principle. Their accountability is limited to their internal policies and the extent to which those policies correspond to domestic or international legislation.

2.3 DEEPFAKES

The increasing use of open source evidence has undoubtedly expanded the practice of international human rights and ICL investigations. But with the preponderance of evidence comes increased risks in identifying the best evidence, especially where open source and user-generated content becomes more mainstream. One such risk is that of a "deepfake", which can be used to spread disinformation and misinformation and present an alternative but false version of events.

Koenig defines this "acute threat" as follows:

> *The term "deep fake" refers to manufactured imagery that is developed via generative adversarial networks, a process that pits two neural networks against each other. The first network, known as the "generator," produces a sample output (such as an image) based on an underlying dataset of images, which is then evaluated by the "discriminator," which provides critical feedback about the generator's success in replicating the characteristics of the underlying data. The two iterate to generate increasingly realistic "fakes" that come closer and closer to the images in the original dataset and thus to seeming as if a false event actually occurred…* [58]

The generator and discriminator networks continually compete – often for thousands or millions of iterations – until the generator improves its performance such that the discriminator can no longer distinguish between real and fake data.

---

[57] Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda, signed by OHCHR, OAS, OSCE and ACHPR, 3 March 2017.

[58] A Koenig, "'Half the truth is often a great lie": Deep fakes, open source information, and international criminal law', Symposium on non-state actors and new technologies in atrocity prevention, 2019. Available at: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/FB05229E78A65BEE8D7126766DA8F2D4/S2398772319000473a.pdf/half_the_truth_is_often_a_great_lie_deep_fakes_open_source_information_and_international_criminal_law.pdf> (accessed 28 November 2020).

Cluster D

Another less common method of deepfake creation is variational autoencoders which similarly rely on two different networks working together:

> *The encoder network produces a smaller, dense representation of the input data and the decoder takes this output and attempts to reproduce the original data. These networks are trained as a whole on a single dataset, for example, hundreds of images of a celebrity, until the input and output roughly match. The decoder can then be adjusted to create the desired effect, such as adding glasses to a specific target from the original [audio visual] media.*[59]

Deepfakes should be distinguished from other forms of manipulated audio and visual evidence. This includes cheap fakes or shallow fakes, which are created with cheaper, more accessible software (or none at all), do not rely on machine learning and can be rendered through Photoshop, lookalikes, re-contextualizing footage, speeding, or slowing.[60] It is clear that the quality of the fake depends on the sophistication of the technology available, and it is even possible that "perfect deepfakes" will soon exist: evidence that makes copycats indistinguishable from reality.[61] This evidence would be void of any defects and indistinguishable from real footage by any expert or algorithm, but since there is no way to verify that a perfect deepfake has actually been created, we would be dependent on the trustworthiness and transparency of the developer admitting to their invention.[62]

The range of deepfakes in terms of how they are created and how they can be applied is best described on Paris and Donovan's spectrum[63] on the next page.

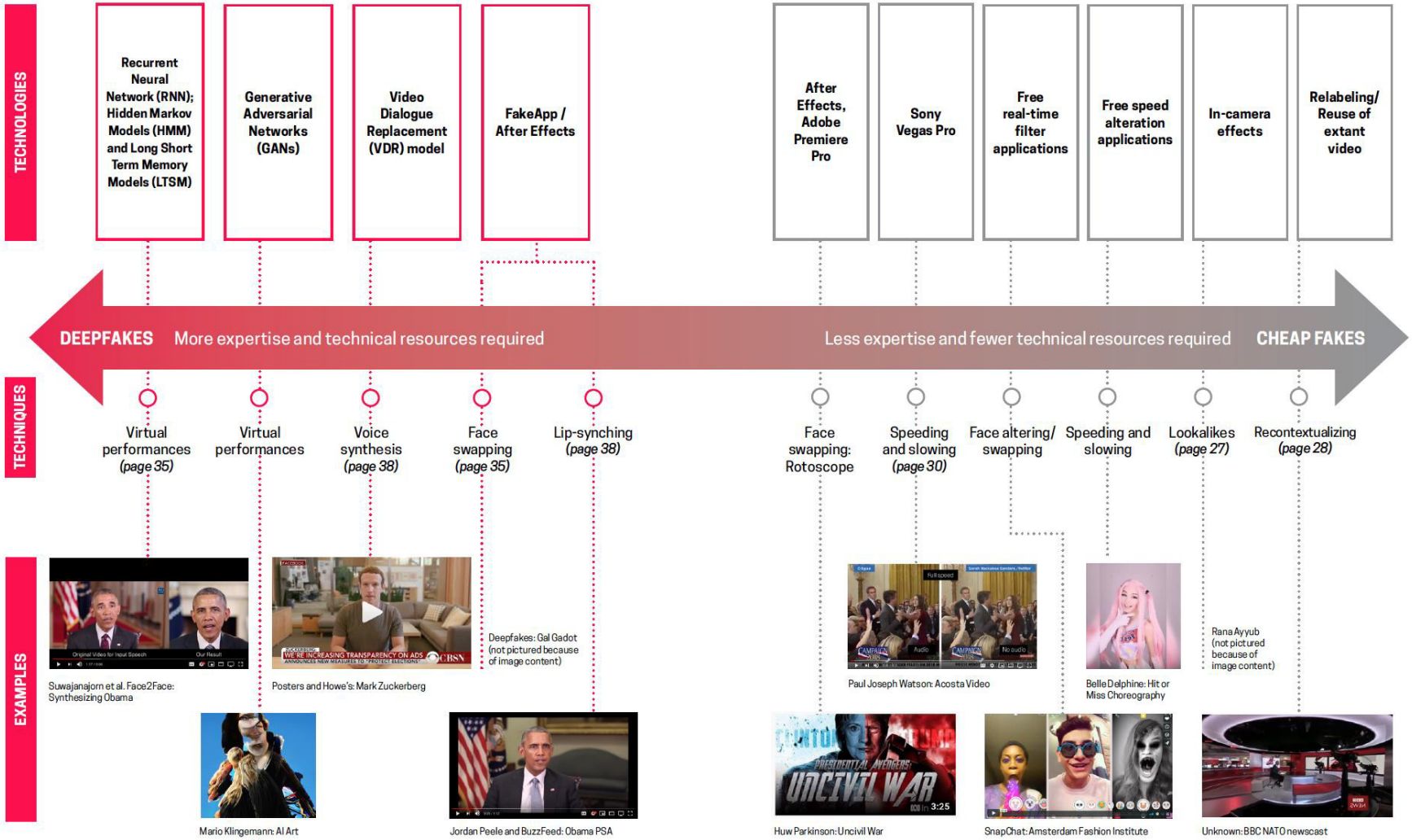
[59] B Paris and J Donovan, 'Deepfakes and Cheapfakes: The manipulation of audio and visual evidence', Data & Society Research Institute, 18 September 2019. Available at: <https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf > (accessed 28 November 2020).
[60] A Carter and L Manley, 'Deepfakes', Harvard Kennedy School Belfer Center, Spring 2020, p 2. Available at: <https://www.belfercenter.org/sites/default/files/2020-10/tappfactsheets/Deepfakes.pdf> (accessed 28 November 2020).
[61] T Mosley, 'Perfect Deepfake Tech Could Arrive Sooner Than Expected', WBUR, 2 October 2019. Available at: <https://www.wbur.org/hereandnow/2019/10/02/deepfake-technology> (accessed 28 November 2020).
[62] Above n 60, p 3.
[63] Above n 59, p 11.

Cluster D

THE DEEPFAKES/ CHEAP FAKES SPECTRUM

This spectrum charts specific examples of audiovisual (AV) manipulation that illustrate how deepfakes and cheap fakes differ in technical sophistication, barriers to entry, and techniques. From left to right, the technical sophistication of the production of fakes decreases, and the wider public's ability to produce fakes increases. Deepfakes—which rely on experimental machine learning—are at one end of this spectrum.

The deepfake process is both the most computationally reliant and also the least publicly accessible means of manipulating media. Other forms of AV manipulation rely on different software, some of which is cheap to run, free to download, and easy to use. Still other techniques rely on far simpler methods, like mislabeling footage or using lookalike stand-ins.



Cluster D

Though media manipulation is not a new phenomenon, deepfakes are causing concern because the results are increasingly realistic, rapidly created, and cheaply made with freely available software and the ability to rent processing power through cloud computing. This necessarily makes them extremely difficult to investigate. Thus, even unskilled operators can download the requisite software tools and, using publicly available data, create increasingly convincing fake content. For example, Generated Photos provides a collection of 100,000 images of faces generated by an artificial intelligence algorithm (artificial intelligence is discussed in the next section). These deepfake images are free to download and the website states that "[a]ll images can be used for any purpose without worrying about copyrights, distribution rights, infringement claims, or royalties."[64] Although the company behind Generated Photos may profess that its aim is to "solve diversity issues in stock imagery",[65] the lack of any regulation or oversight equally means that these deepfake images can easily be used to set up fake accounts on social media, which can then be deployed for various other purposes. In the authors' opinion, social media platforms do not necessarily have the mechanisms in place to detect the difference.

Deepfake content could be used by parties sending videos and photographs directly to human rights organizations and courts, and to compile information that has been posted to social media sites like YouTube, Twitter, and Facebook, with the goal of seeing that data used in court. Even though deepfakes may be exposed by cross-source fact-checking, and thus less likely to create long-lasting effects, they are nonetheless capable of causing short-term chaos and could be used in an extensive disinformation campaign, or deployed at a particular time (such as within a few hours of voting in an election) to have specific impact.[66]

Of particular concern is the use of deep fakes in propaganda and misinformation in regions with fragile governance and underlying ethnic tensions. Misleading content spread via social media, such as decontextualised photos and false claims, has fuelled ethnic violence and killings in countries including India, Myanmar and Sri Lanka.[67] Misattributed images are already used as an effective tool for information warfare. This highly divisive content spreads quickly because it appeals to

[64] See <https://generated.photos/> (accessed 30 January 2021).
[65] S Cole, 'This Company Thinks It Can Solve Diversity With 100,000 Fake AI Faces', *Vice*, 21 September 2019. Available at: <https://www.vice.com/en/article/mbm3kb/generated-photos-thinks-it-can-solve-diversity-with-100000-fake-ai-faces?fbclid=IwAR1eUYCPu8hQ7A_sAgz_EOFFw4kAMFjguiRxtHPYHWeUpgcHw2iMoSAs9AU> (accessed 30 January 2021).
[66] S Lyu, 'Deepfakes and the New AI-Generated Fake Media Creation-Detection Arms Race', Scientific America, 20 July 2020. Available at: <https://www.scientificamerican.com/article/detecting-deepfakes1/> (accessed 5 December 2020).
[67] 'Deepfake videos could "spark" violent social unrest', BBC News, 13 June 2019. Available at: <https://www.bbc.com/news/technology-48621452> (accessed 28 November 2020).

emotions. In addition, there are innumerable platforms facilitate global connectivity. Generally speaking, the networked environment blends the few-to-many and many-to-many models of content distribution, democratizing access to communication to an unprecedented degree. This reduces the overall amount of gatekeeping, though control still remains with the companies responsible for our digital infrastructure.

Case study: Online influence and disinformation about West Papua

The Bellingcat Project published its findings on an online campaign by a Jakarta-based communications company, InsightID, which aimed to influence international opinion about the increasingly violent situation in West Papua, where Indonesian security forces are cracking down on the local pro-independence movement.[68] This investigation was based entirely on open source information: Twitter activity over a five day period was captured based on the hashtags #WestPapua and #FreeWestPapua, which was then used to identify a network of accounts. Most of the accounts were found to be automated and often linked to, or amplified content from, related Facebook pages. The Bellingcat team was able to test the veracity of the information and campaign using open source digital forensics. Importantly, this investigation identified the extent to which fake news and fake accounts were used to spread propaganda. Domain names for websites were registered using fake names, InsightID repurposed its stable spam accounts to spread fake news, and one of the persons under investigation also appeared to publish completely fabricated "UN statements". Facebook independently verified the findings of this report and removed 69 Facebook accounts, 42 Pages and 34 Instagram accounts (some of which had hundreds of thousands of followers), noting that it had received the equivalent of around $300,000 in advertising.[69]

Chesney and Citron note that deepfakes will make it easier for liars to deny the truth: a person accused of having said or done something might create doubt about the accusation by using altered video or audio evidence that appears to contradict the claim, or try to escape accountability by denouncing authentic video and audio as deep fakes.[70] A recent illustration of this is Brigadier General Ahmed Taiwo, who heads the Nigerian army's 81st Division in Lagos, claiming at a judicial hearing in November 2020 that many videos showing soldiers shooting civilian protesters in

[68] B Strick and E Thomas, 'Investigating Information Operations in West Papua: A Digital Forensic Case Study of Cross-Platform Network Analysis', The Bellingcat Project, 11 October 2019. Available at: <https://www.bellingcat.com/news/rest-of-world/2019/10/11/investigating-information-operations-in-west-papua-a-digital-forensic-case-study-of-cross-platform-network-analysis/> (accessed 22 December 2020).
[69] Ibid, pp 1 and 7.
[70] R Chesney and D Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', 107 *California Law Review* 1753 (2019), pp 1785-1786. Available at: <https://ssrn.com/abstract=3213954> (accessed 28 November 2020).

Nigeria had been manipulated.[71] Unfortunately, such a stance necessarily enhances the 'liar's dividend' – perpetuating a lie by dismissing reality as being fake. This is a high-risk strategy in terms of reputation, but depends on factors such as the level of media involvement, whether there is technical capacity to expose the liar, and the level of public education on deepfakes: a sceptical public will be primed to doubt the authenticity of evidence, which can be invoked just as well against authentic as against adulterated content.[72]

Specific to international human rights and criminal investigations, deepfakes pose a threat due to their capacity to spread misinformation, alter the course of parliamentary, legal or military processes, and generally erode trust in public institutions.[73] The potential intersection with the right to privacy and international criminal law is considered further Section 3.2.5 below, but deepfakes also raise questions of freedom of information and who, if anyone, bears the obligation to ensure that information in the public domain is accurate and true.

The international community has expressed its concern over the prevalence of 'fake news' fuelled by State and non-State actors alike in the Joint Declaration, which introduces a number of general principles that attempt to protect the freedom of expression. In particular, it places the onus on States to control the quality and accuracy of information disseminated by public organs:[74]

> 2. Standards on Disinformation and Propaganda:
> c. State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).

This does not place any obligation on non-state actors (such as social media companies), who may instead be regulated by domestic legislation or not be regulated at all. To the extent that these companies 'fact-check' their content, this appears to be motivated by public pressure and marketing rather than a consideration of any potential human rights violations.

Despite being alert to the dangers, the ability to counteract deepfakes will depend on developing forensic tools and technologies that can automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity

[71] A Akwagyiram, 'Nigerian general dismisses bloody Lagos protest videos as fake', Swiss Info, 21 November 2020. Available at: <https://www.swissinfo.ch/eng/nigerian-general-dismisses-bloody-lagos-protest-videos-as-fake/46176810> (accessed at 28 November 2020).
[72] Above n 70.
[73] H Smith and K Mansted, 'Weaponised deep fakes: National security and democracy', Australian Strategic Policy Institute, 29 April 2020, pp 11-14. Available at: <https://www.aspi.org.au/report/weaponised-deep-fakes> (accessed 28 November 2020).
[74] Above n 57.

of visual media.[75] A manual review and contextualising the deepfake would likely expose it, although this would be a long and laborious task.

For example, the US Defense Advanced Research Projects Agency has developed a Media Forensics program that can catch deepfake videos by looking for physiological cues such as eyes not blinking, odd eye colour or strange head movements.[76] Another forensic tool that is currently being used is Griffeye Analysis, which has facial detection and facial recognition capacity, and allows the analyst to break down or slice videos and run several checks across the data in quick time.[77] However, based on the authors' discussions with investigators, the functionality of Griffeye is best with high-quality videos rather than, for example, shaky camera phone footage.

Facebook has even held the Deepfake Detection Challenge, "an open, collaborative initiative to spur creation of innovative new technologies to detect deepfakes and manipulated media" which drew more than 2,000 participants in 2020.[78]

Such developments are part of what many have dubbed the 'arms race' between advancements in machine-learning versus deepfake solutions, between video forgers and investigators. The practical challenge will always be that the technology to create deepfakes moves faster than the technology to detect it.[79]

2.4 ARTIFICIAL INTELLIGENCE

The consideration of deepfakes naturally leads to larger questions on big data and artificial intelligence (**AI**) in international human rights and criminal investigations. AI can be described as the 'constellation' of processes and technologies that enables computers to complement or replace tasks performed by humans with automated decision-making.[80]

---

[75] KM Sayler, 'Artificial Intelligence and National Security', Congressional Service Report, 10 November 2020, p 12. Available at: <https://fas.org/sgp/crs/natsec/R45178.pdf> (accessed 28 November 2020).
[76] W Knight, 'The Defense Department has produced the first tools for catching deepfakes', MIT Technology Review, 7 August 2018. Available at: <https://www.technologyreview.com/2018/08/07/66640/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes/> (accessed 5 December 2020).
[77] See https://www.griffeye.com/ (accessed 30 January 2021).
[78] 'Deepfake Detection Challenge Results: An open initiative to advance AI', Facebook AI, 12 June 2020. Available at: <https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/> (accessed 5 December 2020).
[79] For more information on new technologies developing to authenticate digitally obtained evidence, watch 'Term Member Discussion on Provenance Media: The Future of What We See and Hear Online', *Council on Foreign Relations*, 11 December 2020. Available at: <https://www.cfr.org/event/term-member-discussion-provenance-media-future-what-we-see-and-hear-online> (accessed on 27 January 2021).
[80] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), Report, UN Doc. A/73/348, 29 August 2018, p 3.

There are three specific characteristics of AI that touch upon human rights investigations:[81]

- **Automation** removes human interaction from decision-making and allows for the processing of vast quantities of data in a short period of time, and at a massive scale. Yet, automation can only be as good as the dataset that it relies upon and the design and implementation of the algorithms that are rapidly processing the data. This makes it naturally susceptible to bias or discriminatory effects. For example, a State border may have a system to flag individuals based on criminal history, visa status or religious beliefs. If investigators are looking for persons with particular characteristics fleeing from a conflict zone into another country, it is easily foreseeable that the system might many more people than could reasonably match the profile of the individuals sought.
- **Data analysis** or the dataset that forms the basis of any AI system could include a combination of personal, anonymized or open source information. This raises serious concerns about the origins, accuracy and individual rights over the information, as well as the human methodology used to input the data into the AI system. It follows that the integrity of the outcomes generated by the AI system may be questionable.
- AI systems are **adaptable** – the Council of Europe has recognized that "algorithms model problems based on data sets and produce new solutions that may be impossible for a human being to grasp. Essentially through constant trial and error techniques, algorithms detect patterns in existing data, identify similar patterns in future data and make data driven predictions."[82]

In addition, there is a general difficulty with the transparency of AI systems, the actors sponsoring them and whether an individual can scrutinize the technical underpinnings of those systems. As a result of these features of AI, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has recognised that

> *[u]sers also lack access to the rules of the game when it comes to AI-driven platforms and websites. A lack of clarity about the extent and scope of AI and algorithmic applications online prevent individuals from understanding when and according to what metric information is disseminated, restricted or targeted.*[83]

[81] Ibid, pp 5-6.
[82] Council of Europe, 'Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications', Study No. DGI (2017) 12, 2018, pp 5-6. Available at <https://www.coe.int/en/web/freedom-expression/-/algorithms-and-human-rights-a-new-study-has-been-published> (accessed 28 November 2020).
[83] Above n 8080, p 12.

Cluster D

These complexities of AI affect a number of human rights and how they can be investigated:

- the right to freedom of opinion – who or what has generated an opinion and who is the holder of that opinion?;
- the right to freedom of expression – AI cannot detect the cultural context, irony, extremist content and what would be considered hate speech, which means that AI-generated content will necessarily affect certain individuals' the freedom of expression, but there will be limited or no means to investigate why, how or on what basis;[84]
- the right to privacy – as mentioned above, AI systems depend on the source of the dataset and generally exploit existing datasets, such that it would be difficult for an individual who publishes information in one place to control how that information is used anywhere else;
- the design and datasets of AI systems also have the potential to contravene the obligation of non-discrimination.

As with deepfakes, an investigator's capacity to counter the effects of AI systems to obtain the best evidence will depend on the quality of forensic tools available to them. As Leins recognises, we need to proactively contemplate the possible misuse, dual-use and unintended consequences of new technologies because the same cyber tools that can improve the efficiency of critical infrastructure, can also be used to maliciously to shut down that same infrastructure.[85] This remains a largely unregulated field, and the authors are not aware of any AI systems that are currently being used in human rights investigations. It will not only be difficult for States or international bodies to develop standards, it will be equally challenging to monitor and enforce any such standards.

This backdrop heightens the need for investigators to follow clear principles, such as the protocols and guidelines in the previous chapter, and arguably the challenges posed by these new types of evidence are mitigated by the systematic use of verification and corroboration.[86]

[84] Above n 80, p 13.
[85] K Leins, 'Disarmament: What is it good for?', *Pursuit*, University of Melbourne, 22 March 2020. Available at: <https://pursuit.unimelb.edu.au/articles/disarmament-what-is-it-good-for> (accessed 13 January 2021).
[86] Above n 58.

Case study: Analysis of hate speech in Myanmar

C4ADS, an American NGO that conducts data-driven analysis of international conflict and security issues, published a report in 2016 on hate speech in Myanmar. C4ADS conducted its research by identifying and manually monitoring[87] the public content of 100 Facebook accounts.[88] This sample consisted of monks on the Ma Ba Tha Central Committee, government officials and politicians who were identified as being key disseminators. C4ADS also conducted quantitative social network analysis using automated programs to map the connection between the 100 accounts and their public friends list, and used a sample 18 accounts to map which messages were being actively disseminated from those 18 accounts outwards. C4ADS was able to use this analysis to identify discourse trends and whether there was a consistent narrative, and concluded that, "*[w]hile it is very difficult to prove a direct causal link between hate speech and physical violence, it is clear that an ongoing and intensifying campaign of dehumanization has placed many Muslim populations around Myanmar, especially the Rohingya, at heightened risk of persecution and violence.*"[89]

This investigation appears to provide a reliable methodology for the type of analysis that could be conduct by automated algorithms, but also reinforces the importance of having human input to properly analyse what constitutes hate speech and whether any links can be drawn between online content and physical attacks that occurred in Myanmar.

Hate speech and incitement has also been investigated by the IIMM's monitoring of social media (and particularly Facebook) accounts. Irving notes that the common thread between the accounts was that they were influential, but because they were the account of both private individuals as well as organised groups, it was not clear how the evidenced gathered corresponded to primary or corroborating sources of information.[90] Compared to the C4ADS study, this lack of clarity makes it harder to understand, verify and asses the reliability of the IIMM's approach to social media content.

[87] Monitoring can be assisted by setting up Google alerts based on keywords, or TweetDeck, the Twitter service that allows you to have multiple accounts, follow from them and tweet simultaneously across them. Similarly, Google Earth can be used to plot events and movements and saved as an electronic file.

[88] 'Sticks and Stones: Hate speech narratives and facilitators in Myanmar', C4ADS, 5 February 2016, pp 13-15. Available at: <https://c4ads.org/reports> (accessed 28 November 2020).

[89] Ibid.

[90] E Irving, 'Finding facts on Facebook: Social media in the work of human rights fact-finding bodies', above n 4, p 526.

3. CORRELATIONS BETWEEN INTERNATIONAL HUMAN RIGHTS AND CRIMINAL INVESTIGATIONS

This chapter will consider the correlations between the technical advancements to digital evidence identified in Chapter 2 and ICL investigations. In particular, it will explore how those advancements would be treated if the same evidence was used in an ICL investigation for the purpose of court or tribunal proceedings and any fair trial rights that may be affected by the use of that evidence. The chapter will also consider areas for further research that are relevant to mapping the correlations between international human rights and criminal law investigations.

3.1 ADMISSIBILITY AND EVALUATION OF EVIDENCE

There are two questions faced by international criminal courts in the assessment of each item of evidence presented: is the item admissible, in the sense that it is relevant to the matters at issue and has *prima facie* probative value; and what weight should be given to it, in the sense of whether it is a source that is reliable, credible and authentic enough in light of the evidence as a whole so as to serve as the basis for a finding of fact.

While some domestic legal systems have various exclusionary rules of evidence (for example, the rule against hearsay in common law countries),[91] international criminal courts and tribunals have taken a more liberal approach which reflects the civil law principle of 'free evaluation of evidence': the rules of procedure and evidence generally provide judges with unfettered discretion to admit all material.[92] Therefore, admissibility is unlikely to be an issue *per se*, with courts instead focusing on the weight to be given to each item of evidence in establishing the facts.

When a court is evaluating digital evidence from any investigation to determine whether the standard of proof has been met, the weight assigned to each item of evidence will always be a fact-sensitive decision.[93] There is no finite list of possible criteria that can be applied to determine probative value, nor should there be any automatic reason for admitting or excluding a piece of evidence, and any 'indicia of reliability' that have been suggested in case law should not impose artificial limits on a court's ability to consider evidence freely.[94] The credibility and reliability of any

[91] ICTY, *Annual Report of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia Since 1991 (A/49/342; S/1994/1007, 29 August 1994)* [72].
[92] *Prosecutor v Delalić et al*, Decision on the Prosecution's Motion for the Redaction of the Public Record (IT-96-21-T, TC II, 5 June 1997) [59].
[93] *Prosecutor v Lubanga*, *Situation in the Democratic Republic of Congo*, Decision on the Admissibility of Four Documents (ICC-01/04-01/06-1399, TC I, 13 June 2008) [32].
[94] Ibid [29].

item will equally depend on its contents, the surrounding context and the purpose for which it is being adduced. Where evidence is demonstrably lacking in reliability, the court must carefully consider whether to exclude it at the outset or whether to leave that decision until the end of the case.[95]

In light of this framework, there are four key considerations that are specific to digital evidence:[96]

(i) international criminal courts place a high priority on live witness testimony that can corroborate the **authenticity** of digital evidence, although the need to establish authenticity has to be balanced against the need to protect the witness' identity;

(ii) the probative value, reliability and credibility of **hearsay** digital evidence can be strengthened by providing live testimony from the people who were involved in gathering that evidence, the methods they used and the chain of custody;

(iii) establishing the **authorship** of the digital evidence is crucial to assigning weight to that evidence; and

(iv) there has been little judicial guidance on the best means of **preserving** digital evidence, and the methods used will be particularly relevant for evidence obtained from unverifiable sources or unknown authors.

3.2 FAIR TRIAL RIGHTS

As set out in Chapter 1, one of the critical distinguishing features between international human rights and criminal law investigations is the purpose of the investigation. Human rights investigations are not bound by the criminal standard of proof, the principles of equality of arms or individual criminal responsibility. Instead, their mandate can simply be to gather as much evidence as possible on a particular incident or from a particular location. Consequently, the adherence to procedural fairness (or a lack thereof) in human rights investigations will be critical to whether the evidence gathered can or should be used in any later criminal proceedings.[97]

[95] Ibid [30].
[96] A Ashouri et al, 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts', *Digital Evidence and Electronic Signature Law Review*, 11 (2014), pp 125-126. Available at: <https://journals.sas.ac.uk/deeslr/article/view/2130/2060> (accessed 21 December 2020).
[97] Above n 19, p 27.

3.2.1 The use and presentation of digital evidence in international courts

The value of digital evidence has never been in issue, but it is worth noting that this kind of evidence tends to favour the prosecution perspective. This is because the prosecution has the initial task of inquiring into allegations and is required to establish the essential elements of an offence beyond reasonable doubt to secure a conviction.[98] This is not to say that the defence would not be able to access the same evidence, but rather to recognize that the defence is only put on the same footing after the indictment has been confirmed and as the party responding to the prosecution case, may take a different approach to investigations.[99] However, any such disadvantage is clearly outweighed by the potential benefits of more investigations being conducted today than ever before, and their ability to convert into prosecutions.

Case study: Russian airstrikes on civilian hospitals in Syria

In October 2019, the New York Times analysed evidence into the Russian Air Force's bombing of Syrian hospitals from four sources: logs of Russian overflights over Syria by 'plane spotters'; Russian language transmissions between Russian fighter aircraft overflying Syria and ground stations; videos of bombings of Syrian underground hospitals; and social media posts, and interviews with hospital staff.[100] The reporting was based on the analysis of this data, which showed that Russian fighter aircraft were deliberately targeting Syrian civilian hospitals in May 2019, in contravention of humanitarian law and international criminal law. As a result, the UN launched an internal board of inquiry which would not produce a public report or identify legal responsibility, but would ascertain the facts of the incidents and report back to the Secretary-General.[101] This step provides, at the very least, confirmation that the UN takes the attacks seriously and is conducting investigations, especially where Russia and China have vetoed any UN Security Council resolutions that would have referred the indiscriminate bombing of civilian facilities to the ICC.

[98] ICTY, *Annual Report of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia Since 1991 (A/49/342; S/1994/1007, 29 August 1994)* [72]. See also Rome Statute Articles 66(2) and (3): 'the onus is on the Prosecutor to prove the guilt of the accused' and 'in order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt.'

[99] Ibid.

[100] E Hill and C Triebert, '12 Hours. 4 Syrian hospitals bombed. One culprit: Russia', *New York Times*, 13 October 2019. Available at: <https://www.nytimes.com/2019/10/13/world/middleeast/russia-bombing-syrian-hospitals.html (accessed 5 December 2020). See also the Visual Investigations team of the *New York Times* which "combines traditional reporting with digital sleuthing and the forensic analysis of visual evidence to find truth, hold the powerful to account and deconstruct important news events": <https://www.nytimes.com/spotlight/visual-investigations>.

[101] 'Secretary-General Establishes Board to Investigate Events in North-West Syria since Signing of Russian Federation-Turkey Memorandum on Idlib', United Nations Press Release SG/SM/19685, 1 August 2019. Available at: <https://www.un.org/press/en/2019/sgsm19685.doc.htm> (accessed 5 December 2020).

3.2.2 Evidence from an unidentified source or from a source that cannot attend trial

For an item to be admitted into evidence it must meet three criteria:

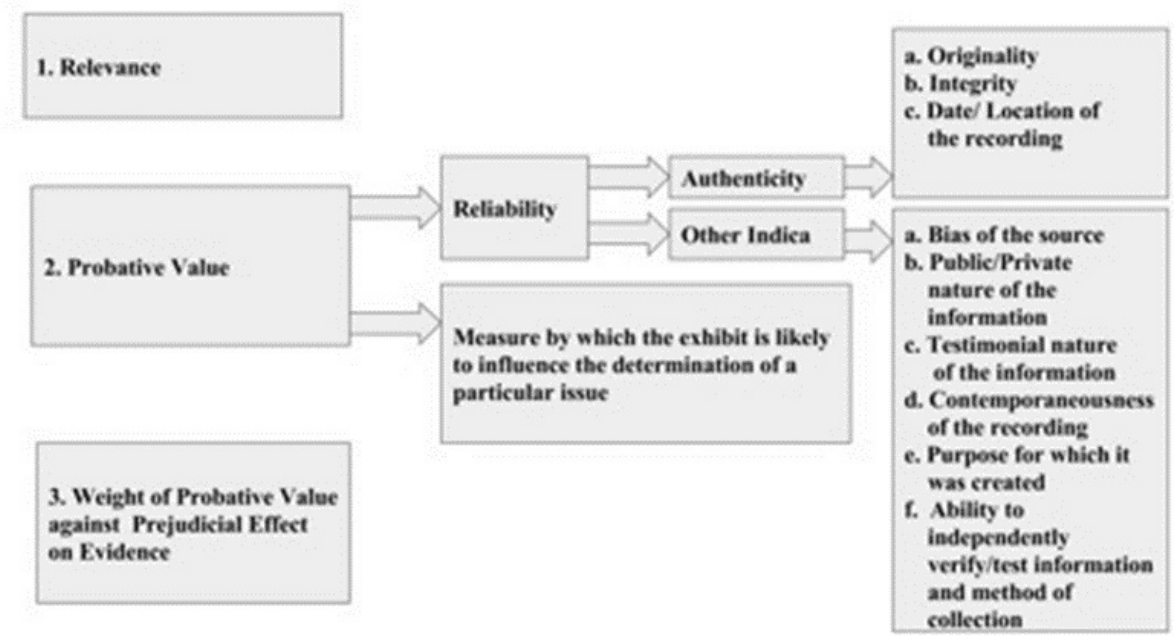
(i) relevance;

(ii) probative value; and

(iii) absence of prejudicial effect.[102]

Article 69(4) of the Rome Statute further outlines that the Court may rule on the "***relevance*** *or admissibility of any evidence, taking into account, inter alia, the* ***probative value*** *of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness, in accordance with the Rules of Procedure and Evidence.*" (emphasis added).

The ICC defines relevance as making the "*existence of a fact at issue more or less probable*", and probative value is comprised of two parts: the reliability of the exhibit; and the extent to which the exhibit is likely to influence the determination of a particular issue.[103] Reliability can be established in two ways: by authentication, the preferred method, or 'other indicia', as outlined in the chart below.[104]



Evidence from an unidentified source or evidence that originates from a source that cannot attend trial, even by video link, can be problematic because of the inability to test the evidence by cross-examination, and for the judges to judge its admissibility and weight. An unidentified source could

[102] *Prosecutor v Bemba*, ICC-01/05-01/08, Decision on the admission into evidence of items deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute", ¶ 9 (27 June 2013).
[103] N Mehandru and A Koenig, 'Open source evidence and the International Criminal Court', *Harvard Human Rights Journal*, 15 April 2019. Available at: <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/#_ftn19> (accessed 7 December 2020).
[104] Ibid.

be a witness who wishes to remain anonymous or unnamed in any legal proceedings. This arguably reduces evidence from such sources to mere hearsay. Although there is no general prohibition to the admission of hearsay, without the opportunity to (cross-)examine the author of the evidence, a court may not be able to contextualise it or draw conclusions about its authenticity, nor can it make use of it in a meaningful way in its overall deliberations in the case, thereby reducing the probative value or weight that should be placed on that evidence (if any at all).[105] This is perhaps why the ICC has held that as a general rule, it would only rely on anonymous hearsay evidence (evidence from an unidentified source) to corroborate other evidence.[106]

However, consider the hypothetical scenario where investigators have been able to authenticate the source, location and chain of custody of certain evidence, but the author of that evidence wishes to remain anonymous due to security or privacy concerns. The technologies available to investigators allow them to verify the content of the evidence without compromising the privacy of the human involved in capturing the evidence. In these circumstances, does a court *need* to know the author of that evidence or does it necessarily have to be treated as hearsay? The authors are not aware of any legal precedent or authority on this issue, but consider it is more likely a question that turns on the verification of the evidence, and the inferences that can reasonably be drawn if that evidence is considered relevant and reliable, rather than a fair trial issue.

Evidence may also be anonymous because it has been difficult for the investigative agency to trace the original author of the evidence, particularly in relation to social media that may enable the content to be quickly circulated amongst a very wide audience before it is collected by the investigators. Alternatively, digital evidence may be anonymous because the author of the content has security concerns that exposure of their identity linked to the evidence may result in adverse ramifications for them.

Some have suggested that security concerns in relation to digital evidence, like other physical evidence, may be resolved by offering anonymity to the source. This protective measure may not violate the accused's right to a fair trial provided that:

(i) the judges can observe the demeanour of the witness to assess the reliability of the testimony;

(ii) the judges are aware of the identity of the witness;

[105] *Prosecutor v Karadžić*, Decision on Guidelines for the Admission of Evidence Through a Witness (IT-95-5/18-T, TC I, 19 May 2010) [10]-[11].

[106] *Prosecutor v Lubanga*, Decision on the Confirmation of Charges (ICC-01/04-01/06, PTC I, 29 January 2007) [106].

(iii) the defence is given ample opportunity to question the anonymous witness on issues unrelated to their identity or whereabouts; and

(iv) the identity of the witness can be released once their security is no longer at risk.[107]

However, judges may not make sufficient inquiries about prosecution witnesses afforded anonymity to ensure that the accused has a fair trial. An example was the very first prosecution by the OTP of the International Criminal Tribunal for the former Yugoslavia (ICTY) in the *Tadic* case. One prosecution witness, Witness L, had been afforded protective measures by the Court, however, his identity was still disclosed to defence counsel. Matters then emerged as a result of defence inquiries relating to Witness L's credibility such that the OTP elected not to continue to present him as a witness of truth and requested that the protective measures be withdrawn. Given the very long delays frequently encountered between the commission of international crimes, investigation and related prosecutions, it is usually the case that there will not be the need to disclose a sensitive witness' identity for many years until disclosure obligations are triggered by an imminent prosecution.

It is unclear how protective measures would be adopted to digital evidence that meets the requisite criteria above, especially if it could obviate the need for witnesses. Instead, witness testimony may have the greatest impact where it is accompanied by playback of a video in the courtroom. But it is worth contemplating whether there could ever exist circumstances in which a video, a combination of photos or an audio recording of an event, together with documentary and other forms of corroborating evidence, could replace the need for witness testimony altogether. It will be up to the party relying on the video to put it in context and explain what inferences it asks the court to draw from the video, as well as any undue prejudice that would be suffered by the other party if the court were to rely on that video. It is a well-established principle in international human rights law that where an item of evidence constitutes the main, decisive or sole basis for a conviction, the right to a fair trial dictates that the accused be able to examine and thereby test that evidence.[108] If evidence from an anonymous or unidentified witness was adduced to establish a fact that was material to determining the guilt of the accused, and that for any reason precluded the right of examination, it could not be relied upon as the sole or decisive basis for conviction.

---

[107] *Prosecutor v Tadić*, Decision on the Prosecutor's Motion Requesting Protective Measures for Victims and Witnesses (IT-94-1-T, TC II, 10 August 1995) [67]-[75].

[108] The accused's right to examination as a minimum guarantee is enshrined in ICTY Statute Article 21(4)(e), ICTR Statute Article 20(4)(e), SCSL Statute Article 17(4)(e) and STL Statute Article 16(4)(e). ECCC Statute Article 33 broadly provides for trials to be conducted 'with full respect for the rights of the accused' and 'in accordance with international standards of justice, fairness and due process of law, as set out in Articles 14 and 15 of the 1966 International Covenant on Civil and Political Rights'. Rome Statute Article 69(2) requires any measures imposed by the Court on witness testimony to not be prejudicial to or inconsistent with the rights of the accused'.

3.2.3 Equality of arms

As stated by the ICTY, equality of arms goes to the very heart of the fair trial guarantee and requires a judicial body to answer:

(i) whether the defence was put at a disadvantage *vis-à-vis* the prosecution; and

(ii) whether the accused was permitted a fair opportunity to present his or her case.[109]

These concerns are especially apparent during the investigations stage and once the trial has commenced. Before trial, the most obvious concern is of course the means available to the defence as equality of arms does not require parties to have material equality in financial, personal or technical resources.[110] The ICC OTP has a separate forensics unit to specifically examine digital evidence, whereas defence teams operate on a smaller budget and with less staff. On the one hand, open source evidence is available to the world at large and the parties have equal access. On the other hand, the review of digital evidence may become increasingly onerous as there may be a large volume of evidence.[111] The defence may not have the same software analysis tools and may not be able to hire private investigators to acquire the same evidence or more importantly, exculpatory evidence. Added to this is the lack of enforcement powers of international courts and tribunals to compel the production of evidence or a police force to conduct investigations, and even the possible non-cooperation of a state – all of which contribute to the defence being on the back foot from the instigation of proceedings. For example, user-generated content is more likely to be gather by users documenting incriminatory rather than exculpatory evidence, which further exacerbates the inequality between the parties.[112]

These issues may be overcome to some extent by the prosecution's disclosure requirements,[113] but again, given the prolific nature of digital evidence that would have to be discovered and reviewed in international criminal proceedings, the rationale of equality underlying such disclosure and the responsibility this places on the parties may not translate from theory into practice. The defence may therefore rely upon the inequality of arms to request that the court take a more restrictive approach to the admission of digital evidence. However, in doing so, the defence must also accept that digital evidence is only one of many avenues of evidence collection, and that over-reliance on any one form of evidence can lead to problems.

---

[109] *Prosecutor v Stakić*, Judgment (IT-97-24-A, AC, 22 March 2006) [149].
[110] Ibid.
[111] Having too much evidence and voluminous disclosure have been described as "investigative bottlenecks" in core international crime cases: X Agirre and M Bergsmo, 'Investigative Bottlenecks and the Mindset of Quality Control' in X Agirre et al (eds), *Quality Control in Criminal Investigation*, (Torkel Opsahl Academic EPublisher), 2020, pp 5 and 9.
[112] R Hamilton, 'User-Generated Evidence', *Columbia Journal of Transitional Law*, 57:1 (2018), p 40.
[113] At the ICC, Article 67(2) requires the prosecution to disclose any exculpatory or mitigating evidence to the defence, and proper disclosure is also inherent in the rights of the accused in the *ad hoc* tribunals' statutes.

3.2.4 The presumption of innocence

Another residual issue is the presumption of innocence of the accused, a principle enshrined in a number of human rights instruments and a fundamental tenet of the right of fair trial.[114] The burden of proof on a prosecutor is a direct consequence of this principle. The advantage to the defence arising from these strict procedural requirements is that the prosecution must establish its case beyond reasonable doubt and cannot discharge this burden by using 'weaknesses' in the defence case.[115] Rather, the defence can prove weaknesses in the authenticity and credibility of digital evidence on the balance of probabilities to effectively challenge the case against it and preserve the presumption of innocence.

In practical terms and based on the authors' experience, despite the duty of the international criminal investigator to gather exculpatory evidence, investigative agencies tend to add what they see as relevant incriminating evidence and are unlikely to actively devote significant resources to also conducting either exculpatory searches, or even in some instances investigations to verify the authenticity of the material obtained. These concerns are of course alleviated when the open source material is just used for lead intelligence services, for example to identify a potential witness in relation to an investigation, from whom corroborating evidence will be sought.

There is also a reputational aspect in protecting the defendant's image and personal dignity by treating them as innocent throughout all stages of the proceedings, which may prove increasingly difficult in the current landscape of digital evidence, particularly social media posts and deepfakes. Regardless of the authenticity or potential bias of the creator of the item, the ability to provide a picture of an event naturally creates an impression on the decision-maker which may be more difficult to rebut than the inferences to be drawn from a document.

For example, the IIMM used social media content for a variety of reasons, including to build a picture of the identity of the perpetrators of the crimes and their chain of command. It used Facebook posts to establish which military units visited specific villages, whether that timing matched the alleged commission of crimes and which soldiers were pictured at those sites.[116] Irving observes that the IIMM Report was "carefully phrased" and did not in fact draw conclusions based

[114] Article 14(2) *International Covenant on Civil and Political Rights*, Article 11(1) *Universal Declaration of Human Rights*, Article 6(2) *European Convention on Human Rights*, Article 8(2) *American Convention on Human Rights* and Article 7(1)(b) *African Charter on Human and Peoples' Rights*.
[115] *Prosecutor v Hadžihasanović and Kubura*, Judgment (IT-01-47-T, TC II, 15 March 2006) [240].
[116] Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar, A/HRC/39/CRP.2, 17 September 2018, [1254].

on this evidence alone, which demonstrates that it was neither elevated to a special status nor unduly downplayed,[117] making it all the harder to rebut from a defence perspective.

Another relevant example is the second ICC arrest warrant issued for Mahmoud Al-Werfalli for an additional count of murder, where the Pre-Trial Chamber (**PTC**) relied upon a video where Mr Al-Werfalli shoots and kills ten kneeling men. Although the PTC noted that Mr Al-Werfalli is mainly seen from behind in the video and is not identifiable based on his facial features, they considered that there was sufficient corroborating evidence to finds reasonable grounds to believe that he was indeed the person appearing in the video.[118] Further,

> *The Chamber is satisfied that the above mentioned video has sufficient indicia of authenticity in order to be relied upon at this stage of the proceedings. The Chamber notes, in particular, that the Prosecutor has submitted an expert report on the authentication of the video, prepared by a renowned, independent institute. Having analysed the video and its key frames, the report concluded that there were no traces of forgery or manipulation in relation to locations, weapons or persons shown in the video. The location has also been confirmed by a witness, who stated that the video was shot "[i]n front of the mosque at Al-Salmani" where "[a] day before […] there was a bombing".*[119]

The combination of the video's authenticity and corroborating evidence give the impression of conclusive evidence against Mr Al-Werfalli before he is even arrested. These examples demonstrate the power of such evidence to digs the presumption of innocence into an even deeper "buried treasure" rather than promoting it as the primary position of the accused.

3.2.5 The right to privacy

The right to privacy enshrined in human rights law (Article 17 of the International Covenant of Civil and Political Rights and Article 12 of Universal Declaration of Human Rights) is an important consideration in open source digital investigations and gives rise to a number of practical questions. For example, to what degree do individuals of a repressive state have a right to privacy? If people post videos of a senior military officer attending a village and being apparently briefed before the commencement of a major military operation that targets the civilian population, has that officer forfeited the right to privacy? The overlap with criminal law surfaces in relation to admissibility – if data is hacked, leaked or otherwise published on the internet, to what degree is it inadmissible in subsequent criminal proceedings? Will deepfakes necessarily breach the right to privacy? The

[117] Above n 90, p 521.
[118] *The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Pre-Trial Chamber I, Second Arrest Warrant, ICC-01/11-01/17, 4 July 2018, fn 33.
[119] Ibid, [18].

unique features of deleted accounts and deepfakes digital evidence have not yet been tested in an international court. This could fall within Article 69(7) of the Rome Statute (evidence will not be admissible where it was obtained by means of a violation of international human rights), although in some national jurisdictions, even illegally obtained material can be admissible if the probative effect outweighs the prejudicial effect of being seen to encourage illicit behaviour.

While this may not necessarily be a fair trial consideration, it is relevant to examine how the right to privacy interplays with the obligations on investigators to do no harm, and whether that can, in turn, affect the credibility and reliability of witness testimony.

3.2.6 An over-reliance on digital evidence?

Just as technology has been praised for expanding and enhancing ICL research, investigations and legal proceedings, others are now questioning whether the pendulum has swung in the opposite direction, to an over-reliance on technology and digital investigations. Alrwishdi has recently highlighted these concerns in the context of investigating atrocity crimes, and makes an indirect case for increased expenditure on tried and true investigative methods based on the following reasoning:[120]

(i) That it is questionable whether tech-based connection tools (like Zoom and WhatsApp calls) can facilitate meaningful communication on the sensitive topics implicated by international criminal justice proceedings with affected groups, particularly because in-person interactions are essential to build trust and credibility.

The authors agree that while remote communications make it difficult to establish an initial rapport and trust, in the long term, they are an excellent means of maintaining rapport and lines of communication, and after initial meetings, technology can be used to reduce the need for further physical meetings that might put the witness at risk.

(ii) That there are serious concerns as to whether virtual hearings can offer due process protections for litigants and serve the needs of justice.

The authors consider this concern is exaggerated. At least based on domestic Australian experience, lawyers have been taking evidence by video link within Australia and overseas for years, well before the pandemic, and it is now well accepted that it can be adequate for the purposes of observing witness demeanour with only occasional technical inconvenience.

[120] D Alrwishi, 'Reconsidering the Digitalization of International Criminal Justice', *Just Security*, 19 January 2021. Available at: <https://www.justsecurity.org/74166/reconsidering-the-digitalization-of-international-criminal-justice/> (accessed 27 January 2021).

(iii) Overuse of technology has the potential to further marginalize certain communities, creating a victimhood hierarchy that prioritizes the perspectives of victims with access to advanced technology. For instance, in conflict zones such as Yemen and Syria, where more than two-thirds of the population do not have internet access, relying on the internet to document crimes can therefore be expected to reproduce patterns of privilege and inequity in these communities, rather than advancing neutral justice.

The authors consider this may be partly true if you are putting "all your eggs in one basket', however, it is usually possible to collect crime base evidence from a sampling of populations. It is not necessary to obtain a large number of witness statements for this purpose, and remote access could instead facilitate better sampling.

The extent to which a party, whether it be an international human rights investigator or an ICL prosecution investigator, relies on digital evidence should be dictated by the specific purpose and context of the proceedings. It should not necessarily be given more weight than evidence that is gathered by other investigative methods. Rather, investigators need to recognize the value in having a multi-disciplinary and multi-pronged approach to collecting evidence, within the constraints of their mandate or the charges that are the subject of legal proceedings.

3.2.7 Assessing the evidence

As the saying goes, "a picture is worth a thousand words" – another key concern that emerges in relation to a court's evaluation of digital evidence is the unavoidable subjectivity of the task. For example, an over-reliance on social media would risks obscuring certain violations and prioritising others, or giving greater visibility to a particular community and inadvertently promoting their narrative.[121] This links back to the danger of not having a developed set of rules on both the gathering of evidence, as well as how courts should evaluate it, as there is no yardstick by which to measure the true worth of new types of evidence. Something as simple as one judge being technology-savvy and another being uncomfortable with the origin of the item could affect their "gut" feeling towards it and its importance compared to other evidence. Courts and tribunals need to acknowledge the influence of these factors in their evaluation process. Particularly for digital evidence, more caution is required where the individual items are being relied upon as direct rather than circumstantial evidence, if they contain hearsay and how they corroborate allegations. The reliability of the evidence must be tested by the defence in order to ensure the fairness and integrity of the proceedings.

[121] Ibid, p 539.

Cluster D

The table on the following page compares and summarises fair trial right considerations, their equivalent, if any, in human rights investigations, and the correlations in how evidence from both international human rights and criminal law investigations is assess.

Cluster D

Stage of ICL proceeding	ICL requirements (Rome Statute and fair trial rights)	Human rights investigation issues	Correlation or overlap
Opening an investigation	Rome Statute Article 15 Prosecutor has to analyse the seriousness of the information, can seek further information from reliable sources and must proceed if there is a reasonable basis for investigation. Rome Statute Article 53 In order for the Prosecutor to open an investigation, the case must meet the jurisdiction, admissibility and 'interests of justice' requirements.	The decision to investigate and the scope of the investigation is determined by the body conducting the investigation. There are no restrictions based on jurisdiction or admissibility.	The Prosecutor is subject to the Rome Statute requirements and is accountable to the Court's States Parties and the UN Security Council. Human rights investigators are accountable to the stakeholders of the body that has mandated the investigation. Jurisdictional issues can arise in relation to digital evidence where material is stored or published in multiple locations, e.g. the storage of active and deleted social media accounts.
Conduct of investigation	Article 54 Prosecutor must investigate incriminating and exonerating circumstances equally. Prosecutor must respect interests and personal circumstances of victims and witnesses. Article 55 Rights of persons during investigation to not incriminate themselves, not be subject to coercion or arbitrary detention, and have access to translation services as required. Both these provisions are based on presumption of innocence of the accused person.	Human rights investigators have to act according to the principles of doing no harm, impartiality, independence, confidentiality, credibility and consistency.	Effectively, these requirements mean that both human rights and ICL investigators are required to collect evidence of the same standard. The difference arises in the inferences that can be drawn from evidence that does not meet these standards: it reduces the credibility of human rights investigation findings; it becomes inadmissible in ICL proceedings. Equality of arms – parties' resources will affect the nature, scope and quality of investigation and information/evidence gathered, e.g. ability to detect deepfakes or AI algorithms. Consider the Al-Werfalli example in Section 3.2.4.

Stage of ICL proceeding	ICL requirements (Rome Statute and fair trial rights)	Human rights investigation issues	Correlation or overlap
Trial	Trial must be in the presence of the accused (Article 63). Presumption of innocence and rights of the accused (Articles 66-67): Court can only convict when convinced of the accused's guilt beyond a reasonable doubt. Prosecution has disclosure requirements.	Purpose of investigation may not be to identify alleged perpetrators of human rights violations. No requirement to prove or disprove an element of crime – human rights investigations gather information. Accordingly, no requirement regarding disclosure of material. No standard of proof applies.	Human rights investigations seek to identify "accountable" individuals but do not have the machinery to hold them to account. ICL investigations seek accountability by identifying the individual with greatest criminal responsibility.
	Trial Chamber shall rule on the relevance and admissibility or evidence (Article 64). The Court may rule on the relevance or admissibility of any evidence by taking into account the probative value of the evidence and any prejudice that such evidence may cause to a fair trial (Article 69). Verification, chain of custody and corroboration are essential considerations when assessing evidence.	Verification of information is crucial to the credibility of investigation findings. No exclusionary rules (such as hearsay) apply to the information collected. Prejudicial information can be included in findings.	Assessment of information/evidence is always based on the facts of the particular case. Need to know the source/author and the provenance of the information/evidence. Importance of corroboration evidence. Does information/evidence generated by new technologies have more or less weight than other types of information/evidence? The relevance and reliability of the material will be more important than its form. Consider various protocols in Section 1.1.2, the Berkeley Protocol's investigation cycle in Section 2.1.

Cluster D

Stage of ICL proceeding	ICL requirements (Rome Statute and fair trial rights)	Human rights investigation issues	Correlation or overlap
Witnesses (including victims and experts)	Trial Chamber can make orders regarding confidentiality and protection of witnesses (Article 64). Court shall take appropriate measures to protect witnesses and facilitate victim participation in the proceedings (Article 68). Evidence from a witness that cannot attend court or evidence where the source/author is unknown will be treated as hearsay and of less weight. Evidence obtained in breach of human rights is inadmissible (Article 69(7)).	Witnesses not required for all aspects of human rights violations or other conduct sought to be established. Potentially, video or audio recordings could substitute for physical attendance or confirming identity. Information from sources who wish to remain unidentified may have reduced credibility but this may not change the relevance and reliability of their information. Investigator has duty to do no harm and protect witnesses.	Hypothetical scenario where evidence witness who wants to remain anonymous due to security or privacy concerns but all other aspects of their evidence can be authenticated – this would be considered sufficiently reliable for a human rights investigation but may still only be hearsay in an ICL investigation/court proceeding. Right to privacy could be waived or compromised by publication of open source evidence.

3.3 AREAS FOR FUTURE RESEARCH

This study presents a variety of practical issues that must be considered by all investigators, whether conducting a human rights investigation or an ICL one, in the collation of evidence and its ultimate use. The research into the correlations between the two investigations has also revealed the various gaps and the need for further research into both theoretical and practical issues which impact upon the effectiveness of investigations. This includes:

- **A harmonised approach to the collection and indicative features of digital evidence**: As noted throughout this study, none of the bodies conducting fact-findings missions or investigations follow a consistent or uniform approach, which means that the quality of the work produced also varies. For the reasons set out in Chapter 1, the authors consider that the Berkeley Protocol provides the most comprehensive and recent guideline to conducting investigations. However, it will take some time and examples of its actual application to consider its adaptability to new technologies and whether the information collected under it will be useful for justice and accountability purposes.
- **The correlations between evidence collected in human rights and ICL investigations:** Where there is an overlap, can the gaps in an ICL investigation be retroactively filled with the evidence in a human rights investigation, or vice versa? For example, in developing a uniform approach, should investigators always err on the side of collecting more evidence so that the option of converting it to evidence that can be used in a prosecution exists? Alternatively, since human rights and ICL investigations have distinguishable mandates, is there much utility in increased collaboration between the two?
- **Preferred types of digital evidence:** In light of the different types of technology identified in Chapter 2 and the case studies, do investigators have a preference for particular types of evidence for different investigations? If yes, why? Is the more realistic approach that all evidence is good evidence and that the true test of its value will come at the time a prosecution case is being built? Based on the authors' experience, this has to be assessed on a case-by-case basis. In a human rights investigation which is collecting information, preferences may be possible, but in an ICL investigation, the best evidence will be that which is authentic, relevant and credible.
- **Key concerns:** Whether there are any "red flags" or problematic trends in the current use and application of digital evidence, or any specific technologies, beyond those identified in Chapter 2.
- **Financial incentives:** For the purpose of this study, we have not considered the scenario of buying data or evidence on the internet and the moral principles that may arise from, for example, a NGO purchasing location information that shows that a prominent military

or civilian visited a physical location where a massacre took place days earlier, and then using that information to establish that person's likely knowledge of, and failure to prevent, the massacre. However, this practice is becoming more prevalent and should therefore be discussed in more detail by human rights practitioners.[122] Specifically, can paying for information compromise the integrity of the investigation or is this irrelevant to the admissibility, provenance and reliability of the evidence? How does this affect the overall fairness and due process of the investigation?

- **Money, people and the institution:** Wiley observes that "donor fatigue cannot be measured quantitatively until funding to a given institution is cut"[123] – although criticism of particular States reducing funding to institutions may be valid, financial restrictions also force us to give more thought to the role of investigators and prosecutors and apply creative thinking. The leadership of an organisation, and the training and development opportunities available to investigators, will be critical to the growth and quality of investigations. The financial impact of digital evidence on the scope of an investigation and the requisite qualifications of the investigators, and how this affects the overall efficiency of the investigation, should be considered.
- **The future of digital evidence:** The types of digital evidence, new technologies and forensic tools that investigators consider will be of prime importance in the near future and how they fit within our current understanding. The question will be whether, as the authors consider, we have to react to new technologies based on our current understanding of verification methods and legal procedures for the admission of evidence in court; or whether a new framework is required depending on the type of technology deployed.

[122] For example, the Bellingcat Project openly states that they paid a "fairly modest fee" to acquire telephone records with geolocation data, passenger manifests, residential data and other personal information when investigating the poisoning of Russian opposition figure Alexey Navalny: A Toler, 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers', Bellingcat Project, 14 December 2020. Available at: <https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology> (accessed 21 December 2020).

[123] WH Wiley, 'International(ised) Criminal Justice at a Crossroads: The Role of Civil Society in the Investigation of Core International Crimes and the 'CIJA Model', in above n 4, p 563.

CONCLUSION

The law is always criticised for being behind technology, but by the same token, when cars were first introduced onto roads, there was no term for jaywalking.[124] International human rights and criminal law investigations have developed much in the same way, constantly being criticized for their failings and yet always adapting to the advent of new technologies and tools to help them achieve their ultimate aim: capturing information and using evidence in a court room.

This study has sought to review the differences and correlations between international human rights and criminal law investigations by first setting out the theoretical basis on which they are conducted: their mandates, the organisations that run them, and how the information or evidence gathered is put to use. Through this exercise, it became clear that both types of investigations overlap in their (1) purpose: exposing serious violations of human rights or criminal law; and (2) action required: creating investigative leads. These are the two most significant correlations between international human rights and criminal law investigations. From there, both types of investigations require planning, coordination and a consistent methodology. The key distinguishing factors remain the standard of proof applicable in each type of investigation, the scope, and the agenda of the body conducting the investigation.

The examination of deleted accounts, deepfakes and artificial intelligence provided practical examples of both the overlap and the challenges of open source digital evidence. Regardless of whether that evidence is relied upon in a human rights or criminal law investigation, it must be verified and corroborated so that it is credible and has weight. The ability to authenticate digital evidence, particularly deleted accounts and deepfakes, is mostly dictated by the quality and capability of digital forensic tools. However, the unifying feature of these three types of evidence is the lack of regulation, at a national and international level, when it comes to related concerns of ownership of information, privacy, freedom of information and freedom of speech. While these do not impact the use of the evidence as such, they raise novel concerns regarding the reliability of the information in a human rights setting, and the extent to which it can be corroborated and be admissible in a criminal law setting.

[124] K Leins, 'AI: It's time for the law to respond', *Pursuit*, University of Melbourne, 17 February 2020. Available at: <https://pursuit.unimelb.edu.au/articles/ai-it-s-time-for-the-law-to-respond?utm_source=GENERAL+LIST+EXTRAS&utm_campaign=536ccf7f7e-Experts+Alert_COPY_01&utm_medium=email&utm_term=0_085c968cd3-536ccf7f7e-160120449&ct=t(Y_COPY_01)> (accessed 13 January 2021).

Cluster D

Finally, from a legal perspective, the evidence collected must first be verified to be admissible in the proceedings. The weight or probative value assigned to that evidence, whether by the judge or the parties relying on it, will always be assessed on a case-by-case basis. The fair trial rights that are engaged by the use of digital evidence include the presumption of innocence, challenges where the source of the evidence cannot or does not want to be identified, and equality of arms. Ultimately, a judge will want to review the *totality* of the evidence. A party cannot, and should not, rely on digital evidence alone, but instead use it to build a detailed picture in support of that party's narrative.

The correlations between digital evidence collected in international human rights and ICL investigations are likely to grow as the scope and purpose of human rights investigations expands and becomes more sophisticated. This prediction is based on the fact that there appear to be more investigations on foot than trials, that there may be no accountability mechanism for the human rights violations and crimes committed in certain conflict zones, and that there may be no political will for accountability through existing international courts or tribunals. Our understanding of how new and emerging digital technologies fit within our existing frameworks will be crucial to encourage the expansion of human rights and ICL investigations, the time and resources that are invested in them, and ultimately, documentation, awareness and access to justice for victims.

E-Procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Cluster D - Annex 2

Preliminary summary of the main challenges discussed during the expert workshops
Internal work product

June-July 2021

August 2021

Table of contents

1. Background

1.1. E-procedure: Evidence in Time of Increased Use of Technology and Digitalisation

With the continued advancement of information and new technologies, the increased usage and sophistication of digital evidence in the documentation of human rights abuses and core international crimes, the operations of judicial and quasi-judicial mechanisms will likely be impacted. The International Nuremberg Principles Academy ('Nuremberg Academy') has developed an interdisciplinary project to explore the impacts and challenges related to the usage of digital evidence in international criminal law proceedings. The project seeks to address and to consider the potential impact that the increased usage of digital evidence and sophistication of technology might have on the rules of procedure and evidence at the international level. Considering the Nuremberg Academy's mandate regarding core international crimes, the project focuses on the Rules of Procedure and Evidence of the International Criminal Court ('ICC') as the first permanent international criminal tribunal.

The project consists of five clusters that take place both consecutively and simultaneously. As part of cluster A, a repository has been developed comprising relevant guidelines on practices and standards concerning digital evidence, both at the investigation stage and in judicial proceedings. Cluster B focuses on further identifying and mapping out missing elements and guidelines that can be relevant, especially concerning standards on digital evidence. For the time being, the Nuremberg Academy, through the mentioned repository above, has created a research gap platform that aims to advance the debates and discussion in the field, with the practical focus on addressing or creating the relevant guidelines. The third cluster, cluster C, analyses international and internationalised criminal jurisprudence and standards concerning digital evidence. It aims to deliver a report encompassing a legal and comparative assessment of these practices and standards. The final cluster's (cluster E) objective is to provide a conclusive answer to the project's research question:

Considering the increased usage of digital evidence (and relevant changes) in the prosecution of core international crimes, should the Rules of Procedure and Evidence of the International Criminal Court be amended? If so, how and why?

Relevant to this document and for the purposes of the expert workshops, cluster D analyses the correlations between human rights and digital evidence, exploring their impact on investigative practices and procedural guarantees in international criminal proceedings. It aims to explore (increase and changes of) human rights safeguards in international criminal investigations in light of the novelties of digital evidence. Cluster D examines these issues from a forward-looking perspective, assessing the challenges posed *inter alia* by social media, the responsibility of social media providers, deep fakes and artificial intelligence.

1.2. Cluster D: 2021 expert workshops and methodology

In June and July 2021, the Nuremberg Academy held three expert workshops as part of its ongoing work on cluster D within its interdisciplinary project on digital evidence. The three expert workshops focused on addressing the challenges regarding the verification of information and evidence in the context of correlations between human rights and digital evidence. Verification of information and evidence has been identified as an area of investigative practices that might be most-impacted by the increased usage of digital evidence and the sophistication of technology. The workshops explored potential future challenges arising from the above-mentioned correlations and their impact on the investigation practices.

The workshops addressed the disclosure obligations, the concept of anonymity and investigative techniques directly impacting fair trial rights (for example, the right to remain silent). The workshops further addressed the potential future challenges regarding the evidentiary rules and standards in light of the increased usage of digital evidence during fact-finding missions, human rights investigations, and international criminal proceedings. This preliminary summary report compiles the challenges and practices identified and discussed among the experts. The report has been drafted by the Nuremberg Academy and intends to generate feedback from the expert participants on the mentioned challenges as well as additional remarks or comments. The Nuremberg Academy aspires to incorporate the received feedback before proceeding to further stages of the project. Once the report is finalised, it will be part of the project deliverables and will be made available on its project site.

2. First expert workshop: digital evidence, data protection, right to privacy and confidential 'formal' agreements

The first workshop was held on 16 June 2021 and addressed the interaction of digital evidence, data protection, the right to privacy and confidential 'formal' agreements. The workshop started with a brief introduction to the Nuremberg Academy and its e-procedure project, followed by expert presentations on challenges at the domestic, regional and international levels.

Furthermore, the workshop sought to foster a discussion on the following questions:

1. Are there any developments within the increased usage of digital evidence and sophistication of technology that have indicated a practice limiting disclosure?

   a. What conditions are normally followed (MoU, confidentiality, formal agreements)?
   b. What challenges related to evidence verification have been raised?
   c. What safeguards are put in place to maintain proper investigative files (for future disclosure)?

2. Would you agree that the disclosure rules set in the practice of the international tribunals are to safeguard the protection of the fair trial, and the defence rights in particular?

   a. Have you observed any changes in the practice? New developments?

3. With regard to the right to privacy, would the legitimate and proportionate need for an investigation overrule the privacy concerns?

The main challenges were clustered according to the following categories:

a. Lack of specific rules
b. Fair trial guarantees
c. Data security and evidence integrity
d. Witness security and protection
e. Right to privacy vs. the legitimate need for an investigation
f. Additional and administrative challenges

2.1. Summary of challenges raised and discussed

a. Lack of specific rules

- Lack of specific procedural rules and standards

Procedural rules do not always cover all forms of non-physical evidence. This lack of specific rules or standards concerning the disclosure of digital evidence implies that general disclosure provisions must be applied to digital evidence, e.g. those relevant for physical evidence.

- Analogy in civil law jurisdictions

Due to the lack of specific legislation, judicial operators in civil law are compelled to apply analogy between rules relevant for other evidence typologies to digital evidence, e.g. between postal communication and e-mail communication. However, analogy in *criminal* law often presents a challenge concerning its implementation, the potential infringement upon human rights and tension with the principle of legality.

- Potential lack of legal certainty

Another result of the lack of specific legislation is the potential legal uncertainty in civil law jurisdictions, since the interpretation of available procedural rules on disclosure for their application to digital evidence would then be left to judicial interpretation and potentially could also result in inconsistent jurisprudence.

- Cooperation between police and judicial authorities and service providers

While applicable multilateral frameworks, such as that of the European Union, encompass cooperation between police and judicial authorities of Member States for the transfer of digital evidence, these frameworks often do not cover the required cooperation with service providers. The issue resides in the applicable law for these cooperation requests, since service providers are often based in third-party States, such as the United States. This legal vacuum extends to the required cooperation between the police and judicial authorities of a particular Member State and an international organisation or tribunal.

b. Fair trial guarantees

- Fair trial guarantees and the principle of equality of arms

- In common law jurisdictions, and due to their adversarial nature, disclosure obligations are not simply procedural duties but are also considered essential to fair trial rights, and form a requirement for the equality of arms principle. For this reason, compliance with disclosure obligations, and certainty regarding their scope, is essential for the integrity of proceedings. The anonymity of the source

The anonymity of the source implies an additional challenge for upholding fair trial guarantees as part of the disclosure, as it clashes with the accused's right to cross-examine witnesses. For the prosecution, this translates into the challenge of providing a witness for the defence to cross-examine.

- Prosecutorial obligation to investigate incriminating and exculpatory evidence

Under Article 54(1)(a) of the Rome Statute, the Office of the Prosecutor of the ICC ('ICC-OTP') is mandated to investigate incriminating and exculpatory evidence equally. This translates into the ICC-OTP collecting a wide range of material that must be processed before being disclosed to the defence in the form that is most useful. Even though this is a general evidentiary challenge, it would be intensified in light of digital evidence.

- Defence's duty and right to investigate on their own

Similarly to the challenges faced by the prosecution, the defence faces obstacles concerning the investigation, collection, preservation and analysis of digital evidence. These challenges are further exacerbated by the high number of digital evidence materials that need to be handled and by the lack of funds, access to experts, or success regarding cooperation requests.

- Timeliness of disclosure

The timeliness of disclosure and its potential delays remain a challenge for both the ICC-OTP and the defence.

c. Data security and evidence integrity

- Lack of clear standards concerning the seizure, preservation and storage of digital evidence

Ahead of its disclosure, digital evidence must be seized, preserved and stored in a forensic manner. On the one hand, the lack of established standards for the seizure, preservation and storage of digital evidence implies a challenge for legal practitioners as to the required and consistent standards ahead of disclosure. On the other hand, the preservation of digital evidence, which has already been submitted as part of trial proceedings and that is in possession of one of the parties or the court, needs to be properly upheld. This may lead to challenges concerning fair trial guarantees.

- Risk of evidence tampering

This challenge manifests particularly in relation to open-source evidence and the timing obligations for disclosure, in some common law jurisdictions arising immediately after charging. This disclosure to the defence might increase the risk of open-source evidence being tampered with, considering that the investigation is still ongoing at this stage. This is a risk and a challenge that remains unaddressed by several domestic jurisdictions.

- Potential 'storage crisis'

Due to its nature, digital evidence may amount to a very high number of materials. The high number of materials may pose a challenge as to the standards required for its storage, including guaranteeing its integrity.

- Potential creation of a ‘digital vault’

The ICC-OTP has worked on the creation of a ‘digital vault’ that might facilitate disclosure to the defence. Such a ‘digital vault’ might store original material that would then be available for both the prosecution and the defence for inspection in their original form. Additional challenges such as customising the access to this material remain yet to be seen as these tools are still being developed.

- Third-party servers

Data transfers between investigative institutions and investigative and judicial mechanisms might be hampered by the use of third-party servers which do not comply with privacy or encryption standards, thus potentially hampering the evidence’s integrity.

- Data authentication

Digital evidence poses a challenge for its authentication, which might impact its admissibility. It is therefore paramount to ensure that the chain of custody is being guaranteed. In this regard, additional tools such as Blockchain can be useful.

d. Witness security and protection

- Security of witnesses featuring in open-source material

While developed rules concerning witnesses’ security during the judicial proceedings (or investigation stage) are clear, rules (or practice) concerning individual/s whose image or personal information feature in open-source material regarding their security (or disclosure obligations, including scope) are unclear. Measures concerning these individuals’ security are required to guarantee that disclosure obligations do not infringe on victims’ or witnesses’ rights.

- Redaction of material and witness consent

The scope and practice of redactions of witness information, including sensitive information, is not unified. This lack of standardisation implies several challenges in processes such as data transfer between institutions. While applying the General Data Protection Rules might offer some guidance, its standards only apply to Europe-based investigative institutions.

Some private investigative mechanisms further adopted a policy of redacting all witness material. This practice implies further challenges with regard to seeking consent forms, additional consent forms, and the need to clarify or reclarify consent forms in place for the given information. Challenges arising from these practices are, *inter alia,* related to the protection of the witness, duty of disclosure and effective and efficient transfer of information.

Redactions intended to guarantee witnesses’ protection can also become burdensome for the ICC -OTP, particularly when they extend to video and audio material.

e. Right to privacy vs. the legitimate need for an investigation

- Private interest vs. public interest

Balancing the private interest of the right to privacy and the public interest, characterised in the legitimate need of an investigation, requires a case-by-case basis assessment. Moreover, this balancing must be carefully assessed, considering whose privacy is affected by the analysis.

The challenge is particularly relevant for a collection of evidence, for which no jurisdiction is established; hence, there is no clear judicial guidance.

- Data retention

The balancing between the right to privacy and the legitimate need for an investigation has an impact on data retention, particularly concerning data collected by service providers for which consent has been given only in a limited fashion.

f. Additional/administrative challenges

- Available resources

In addition to the high number of material to be processed, the ICC-OTP faces a challenge concerning the lack of available resources (IT and human resources) to assess the evidence for the purposes of disclosure.

- Language difficulties

Processing digital evidence in languages like Arabic can be challenging, particularly in light of the prosecutorial obligation to investigate incriminating and exculpatory evidence and to process it for the purpose of the disclosure.

3. Second expert workshop: digital evidence, anonymity, hearsay, and data analysis

The second workshop was held on 30 June 2021. The workshop analysed standards and practices concerning the anonymity of the source in relation to digital evidence, as well as the current framework on anonymous sources and hearsay evidence, and the impact on data analysis. Similarly, the workshop started with a brief introduction to the Nuremberg Academy and its e-procedure project, followed by presentations by experts and subsequent discussions on the challenges pertaining to the verification and corroboration of sources in processes related to fact-finding and international criminal investigations.

On the substance, the workshop sought to foster a discussion on the following questions:

1. What are the challenges pertaining to the anonymity of the source (and hearsay evidence)?

   a. How are they being overcome or could be overcome in the future (considering the future of digital evidence)?

2. What is the prevailing practice concerning anonymous and hearsay evidence?

    a. Human rights fact-finding
    b. Criminal investigations
    c. Other procedural challenges (and future)

3. Where does the burden lie in terms of verifying the sources?

    a. What is the scope and applicable standard?
    b. What are the challenges?

The participants started to discuss the corroboration practices; however, due to time constraints, the topic was addressed as part of the third workshop.

The discussion allowed for the identification of relevant challenges. In order to facilitate their analysis, the present report first seeks to summarise the general challenges discussed and then to summarise the practices adopted to address some of the challenges. The Nuremberg Academy has approached this summary from the following perspectives:

a. General challenges and practices
b. Independent investigative mechanisms (and related actors)
c. International Criminal Court
d. Stakeholders supporting investigations and prosecution of core international crimes

3.1. Summary of challenges raised and discussed

a. General challenges

- Lack of uniform definitions and terminology

The definition of concepts such as ‘source’ remains a challenge for source verification. While relevant tools such as the Berkeley Protocol[1] are useful for this purpose, such definitions imply that each of the investigative and judicial institutions requires a standardisation process to guarantee that their staff are working under the same understanding.

- Anonymity of the source vs. anonymity of the investigator

When assessing anonymous sources, the issue of anonymity of the investigator should also be considered. Anonymity in open-source investigations relates to security and risk avoidance considerations. However, this might also imply a challenge concerning the anonymity of the source and its upholding at later procedural stages.

[1] UC Berkeley School of Law Human Rights Center and UN Office of the High Commissioner for Human Rights, *Berkeley Protocol on Digital Open Source Investigations*, 2020, available at https://www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf (last accessed on 31 August 2021).

- Diverse institutional mandates and different stages of proceedings

Independent investigative mechanisms are involved at the beginning of investigative processes without reaching a trial stage, as would be the case of judicial institutions such as the ICC. Consequently, investigation processes carried out by independent investigative mechanisms depend on their mandate and often lack the prerogatives that a prosecutor could have, including subpoena, search and seizure warrants or charging powers. Accordingly, their prerogatives concerning the collection and verification of evidence are connected to specific mandates, roles, and responsibilities.

- Inconsistencies in the law and practice

Experts highlighted the inconsistencies in the existing applicable legal evidentiary framework in the Rome Statute. This variation translates into broad discretion provided to the Chambers, whose determinations and evidentiary assessment may vary from Chamber to Chamber.

This issue is seen as more vital regarding the admissibility of evidence, for example, Article 69(4) of the Rome Statute, which provides that "[T]he Court *may* rule on the relevance or admissibility of any evidence […]". In recent years, the Chambers have interpreted this provision as facultative concerning the timing of such admissibility ruling. Consequently, they have decided not to exclude the evidence submitted and incorporate it in the record without ruling on its admissibility, which ruling is deferred to a later stage of the proceedings.

Moreover, while often consistent practices on assessing the relevance and probative value in connection to authenticity and reliability are required and demanded, this is often not the case in practice. These inconsistencies may lead to an approach at the investigative stage towards discarding evidence due to its potential inadmissibility before the court.

- Civil law vs. common law: exclusion of evidence and judicial expertise

The issue of evidence and source verification poses challenges concerning the judicial expertise required to assess the evidence in different legal systems properly. On the one hand, common law systems incorporate exclusionary provisions in order to shield non-professional jurors from the evidence that may not be trustworthy, reliable or credible, or whose probative value might be questioned. On the other hand, in jurisdictions where the judges are professional judges, such as civil law jurisdictions, exclusionary measures are often not required. In these cases, when the judge allocates zero evidentiary weight to a certain piece of evidence, the consequence would be very similar to that of an exclusion of the evidence, although applying a legal avenue. Arguably, applying civil law practice is often more appropriate concerning evidentiary frameworks of international criminal tribunals in which professional judges are common.

However, even though the evidentiary framework of international criminal tribunals is characterised by features of civil law systems, some of the legal and jurisprudential criteria for assessing weight are very similar to those stemming from common law systems. Moreover, even when presenting evidence before professional judges, a human component exists that cannot be discarded, in addition to constant technological developments such as Artificial Intelligence, facial manipulation, innovative software editing, among others, on which professional judges are not necessarily trained well enough.

- Obstacles concerning fair trial guarantees
    - Defence rights and equality of arms

The challenges related to inconsistent legal frameworks, practices, and judicial discretion, as well as the submission vs. admission of evidence approaches, imply an additional challenge to the defence from a fairness perspective. These challenges are exacerbated by the high amount of evidence that needs to be processed and analysed, and the lack of equality concerning the resources allocated for the defence, as well as its potential limited expertise and resources concerning collecting and analysing digital evidence.

    - Digital evidence, anonymity and the defence right to cross-examine witnesses

The issue of digital evidence, anonymity and defence rights concerning cross-examination of witnesses is a particular challenge in common law jurisdictions prosecuting international crimes, since the anonymity of the source poses a challenge for the defence regarding a proper confrontation of witnesses at trial. While this might be solved through proper judicial instruction from the judge towards the layman juror, it may be a more controversial issue in international jurisdictions integrating elements from civil and common law systems.

- Assessment of cost-effectiveness

The reality of international crimes investigation and prosecution implies an assessment of cost-efficiency, including a balancing of available resources considering the high volume of material collected and its critical analysis.

With the advancement and increased usage of electronic information, the discipline of e-discovery (electronic discovery) has emerged in some jurisdictions. This discipline seeks to evaluate the evidence collected, the resources at hand and the legal requirements to be met, as well as the necessary practices, procedures and processes for case-building.

b. Independent investigative mechanisms (and related actors)

- Source verification requires a cost-effectiveness assessment

In addition to considerations on the mandate of independent investigative mechanisms, an economic assessment is also required when it concerns source verification since a detailed analysis of the evidence requires financial, technological, time, and human resources.

In light of this challenge, and considering the high volume of materials that independent investigative mechanisms collect, a cost-effectiveness assessment is being implemented. This implies an initial determination of the relevance of the evidence collected. Subsequently, more expensive and detailed analytical methods are implemented on the relevant materials, including source verification.

Challenges concerning source verification are reinforced by the COVID pandemic situation, which caused limitations concerning field missions and following evidence collection and preservation.

c. International Criminal Court

- Definition of the source remains contested and subjected to a case-by-case analysis for linkage purposes

In order to carry out the process of the verification of the source, the definition of what is the source is relevant. For example, when a phone is an evidentiary item, it cannot be solely attributed to its owner. An additional exercise needs to be performed to determine who used it and how a person can be linked to it, meaning that additional steps are required for the verification of evidence.

- Verification of the source, linkage analysis and requests to third parties

Verification of the source regarding online information poses a significant challenge for the ICC, mostly due to the emphasis on the linkage between the actual crime and the alleged perpetrator which is required for the successful prosecution of core international crimes. Often, additional steps are required to acquire this information, such as requests concerning IP addresses and additional information from third-party service providers to assist in the corroboration process and for the purposes of linkage analysis. Considering that such requests can only be obtained through a legal process, an additional challenge arises when there is no access to this legal venue.

- Risk of over-collection

Over-collection of evidence items remains a challenge at the ICC. Avoidance and prevention of over-collection are very important at the ICC to avert being overwhelmed at the end of the investigative process. For this purpose, a triage is very important to focus the evidence collection processes on what is required. This relates, for example, in the digital forensic practice to avoid how the seizure of a whole server but to only seizing the relevant material, e.g. e-mails, specific files, etc.

d. Stakeholders supporting the investigation and prosecution of core international crimes

- Triage of sources

Implementing a triage of sources facilitates handling the workload while avoiding bottlenecks at later stages, particularly the disclosure stage. Applying triage of sources from the beginning as a matter of practice was identified as a challenge.

- Varied evidentiary standards

Stronger and mandatory evidentiary standards are required from the beginning of the investigation.

3.2. Summary of practices concerning the anonymity of the source (and hearsay evidence) and verification

a. General practices discussed

- Verification of sources vs. verification of information

A line must be drawn between the verification of information and the verification of sources, for which, concerning the former one, a stronger focus would be placed on the authenticity or on the relevance.

- The burden of the verification of the source is on the party making the submission

Assessing who has the burden of the verification of the source requires defining the notion of 'source'. Moreover, the question on the burden may depend on additional origination processes, e.g. if the evidence was computer-generated or followed a specific process. In any case, the general rule appears to be that the procedural party making the submission is the one tasked with source verification.

- Relevance of purpose of the evidence

Before engaging in any kind of analytical process of the evidence as part of the documentation process, the investigative team must assess the objective of the piece of evidence. This assessment will assist in determining the type of verification and analysis required.

- Digital evidence and expert witnesses

Considering the challenges related to inconsistent legal frameworks and judicial discretion, in addition to judges potentially being barely equipped to operate with digital evidence, a Chamber-appointed digital evidence expert witness (like in the cases of the Special Tribunal for Lebanon or the European Court of Justice) may contribute to the fairness of the proceedings. Moreover, experts who authored or collected the evidence may assist in assessing the evidence completely, fairly and neutrally. In addition, bearing in mind the advantages provided by collegiality, a group of experts might be desired.

b. Independent investigative mechanisms (and related actors)

- The source is considered to be the person who provided the information

Independent investigative mechanisms collect information from different sources, not always from original sources, but from persons who may have created the information, received it, or taken it away from another source. In these cases, independent investigative mechanisms such as the Independent Investigative Mechanism for Myanmar ('IIMM'), consider the source being the person who has provided the information to the mechanism. While steps are taken to verify that the person giving the material is who they say they are, this is not given particular relevance due to the institutions' mandate.

- Source verification as part of collection, preservation, analysis and transfer of evidence, not as an independent step

Due to the mandate and the emphasis on the collection, preservation, analysis and transfer of evidence of the independent investigative mechanisms, source verification is not an independent step but is assessed throughout these processes. Consequently, challenges arise and have to be mastered as new means become available as part of the investigative process.

- Regarding general investigation techniques, the lack of authenticity of the source and the information does not override its corroborative value

The (potential) lack of authenticity of the source or the information does not override its corroborative value. Even if a piece of evidence is clearly false, its value and usage are yet to be determined, for example, concerning its corroborative value of other evidentiary material.

- Source verification is not the most salient question at the investigation stage

Verifying the source is not the most salient question during the early stages of the spectrum of the investigation. The emphasis is placed at this time not on authenticity but on the overall confidence that a piece of evidence can provide to the prosecutorial and investigative team as to the facts that it proves. Investigators cannot provide an 'authentication stamp' on the evidence at this stage but rather assess the characteristics and deficiencies of the evidence.

- Source verification and evidence preservation

Once the collection of the material has taken place, the next step concerns its preservation, which is always the case as long as it is not entirely out of bounds and does not require additional source verification.

- Complex verification analysis increases as the investigation proceeds

At the early stages of the investigation, no complex verification analysis takes place. The need to apply rigorous probing processes to verify the source only emerges when there is an outline of the case, charges, suspects, accused, witnesses, etc. This implies that, at the stage of collection and preservation of evidence, the question of the verification of the source is left for a later stage. However, some broad analysis is already performed to assess, e.g. whether the information has been received before, whether a certain piece of evidence was seen already, whether it had been received from someone else, or whether the information relates to another context or period beyond the mechanism's mandate, among others.

Once the collection and preservation stage is completed and more analytical activities begin, a much narrower set of information is hopefully dealt with. At this stage, the level and type of analysis are dependent on the type of crime or element of the crime that the information relates to. For example, a set of photos that relate to an alleged case of torture might require a deep analysis to be performed, but when the analysis concerns the widespread or systematic element of the crime, the deep analysis of a single piece of information is not required but that of hundreds or thousands. Determining the level of analysis to be performed falls within the assessment of cost-effectiveness explained above.

- Verification as an extremely contextual issue

The issue of verification is extremely contextual. Accordingly, evidence should not be excluded at the early investigative stages under potential admissibility concerns at a later stage. Verification needs to be carried out based on the case at court and the evidence's corroborative weight, as well as its probative value of other crime elements or facts.

- Source verification is related to source management

For independent investigative mechanisms such as the IIIM, verifying the source is an activity related to source management, including cooperation with civil society, States, individuals, victims, survivors, and even perpetrators.

c. International Criminal Court

- Triage of evidence

The e-discovery model has been relevant and useful in allowing for the triage of evidence. This assists investigators in understanding the objective or scope of the evidence, considering that they usually have a huge amount of data, particularly in the case of digital evidence. Categorising data facilitates searching in the pool of information and/or corroborating the collected evidence, which may also assist the verification process.

- Source verification is part of the investigation

At the ICC, the source verification process is part of the investigation, as it seeks to link the evidentiary material with a person of interest.

- Standardisation of the collection process

The standardisation of practices relevant for evidence collection, not limited to purely digital evidence, is important. As such, the ICC-OTP has worked on its Manual on Online Investigations, which was created after a consultative process within the office. The manual (which is an internal work process document and not publicly available) is also helpful for staff to understand their role in the organisation, what they do, how they do it, how to best approach this new type of digital evidence, etc., particularly in cases of online evidence collection.

d. Stakeholders supporting the investigation and prosecution of core international crimes

- Verification of the source as soon as possible

Verifying the source as soon as possible is a good practice because with online information, as soon as something is posted, it enters the "golden hour" of criminal investigations in which the chances are high to connecting the evidence with the original source. As time goes on, the information gets disconnected from the original source and the possibilities of getting to the original source decrease, as do the chances that the source can be reached again at a later stage. Moreover, the voluminous number of social media posts and its continued increase may imply additional challenges regarding the collection and verification.

- The three-prong and multifunctional approach

A three-prong and multifactor approach to data analysis and verification is characterised by:

  - Source analysis
  - Content analysis
  - Technical analysis

The three types of analysis are relevant as they allow for multifactor verification, which is essential, considering that it cannot be foreseen which element will provide verification of whether the evidence is fake or forged.

As part of the source analysis, it is relevant to assess the following issues:

1. Authenticity of the source: Concerning online evidence, this mostly concerns dealing with bots, botnets, trolls and unauthentic behaviours. Identifying this is usually done very quickly by assessing signs and indicators.
2. Attribution: The traditional idea is to connect the username/online personality to the person. In US case law, this is a relevant issue, particularly relating to social media evidence.
3. Original source online: This is extremely important in light of the high amount of circular reporting.

- Relevance of the context and collector information

When the evidence is anonymous, the context and collector information is relevant, for which verification of the source must be carried out efficiently. This also relates to the need for transparency and the practice of disclosing additional information around the collection of the information, such as describing the circumstances in which the information has been collected or received, how its preservation took place, how it is analysed, etc. This information is particularly relevant concerning open-source evidence, where the moment of original posting and that of evidence collection or acquisition may be quite disconnected.

3.3. Remaining question

Remaining questions from the workshop and challenges to explore further:

With the increased usage of digital evidence, should a more in-depth verification of the source be adopted for the investigative practices?

Should it follow higher evidentiary standards (in the context of core international crimes)?

The current approach is to focus on solidifying methodologies. Some investigative institutions work with different jurisdictions, including national, regional and international jurisdictions, and, consequently, must deal with different rules of procedure and evidence. As such, solid methodologies are paramount to properly collect and preserve the evidence. In addition, documenting the methodologies is highly relevant.

4. Third expert workshop: (human rights) investigative techniques directly impacting fair trial rights

The third workshop was held on 14 July 2021. It addressed the challenges related to the verification of information/evidence as part of the human rights fact-finding/investigative practices and their possible impact on the procedural guarantees in international criminal proceedings. The workshop started with a brief introduction on the Nuremberg Academy and its e-procedure project, followed by brief expert presentations addressing the below points:

1. Is digital evidence often used as a corroborative technique and corroborative evidence?

   a. How is the 'search' (discovering the information) methodologically documented throughout the investigative process? What practices are implemented to avoid bias?
   b. In terms of ICL practice (digital evidence being used as corroborative evidence), how does this practice impact the weight of evidence: is the focus on verification of the fact or the authenticity of the source?

2. Fact-finding often includes accountability assessment to a great extent. How is this practice compatible with the presumption of innocence and other fair trial guarantees?

   a. What is the applicable standard, as part of the investigative techniques, concerning the alleged individuals involved in various human rights violations?

3. What is the nature of the content documented, archived and preserved (and verified) to strengthen the accountability efforts, especially concerning serious international crimes?

   a. What are useful guidelines in this regard?

The report summarises the challenges raised and practices discussed, clustered in the following manner:

a. Corroborative techniques and human rights fact-finding / investigative mechanisms
b. Corroborative techniques and international criminal investigations
c. Potential tensions between fact-finding/human rights investigative mechanisms and international criminal investigations
d. Nature of the content documented, preserved and archived

4.1 Summary of challenges raised and practices discussed

a. Corroborative techniques and human rights fact-finding / investigative mechanisms

- Relevance of data and information management systems and evolving practices

Institutions such as the United Nations Office of the High Commissioner for Human Rights are continuously improving their documentation tools. As such, experts referred to a new data and information management database that is being applied in different contexts and includes mandatory fields that trigger staff members to document how they came across a piece of information. It is important, however, to remember that different tools are used, as they are available and relevant in specific contexts depending on the country or region in question.

Moreover, consideration must be given to the complexity provided when a particular mechanism and/or institution inherits evidence and sources from another investigative or quasi-investigative body. Challenges arise regarding the subsequent data and information management processes that must be put in place to guarantee and ensure proper storage and preservation of evidence and information.

- Relevance of an assessment of the feasibility and potential outsourcing/cooperation

An assessment concerning the feasibility of completing the documentation in light of the deadlines to be met is required to properly assess the scope of the investigation carried out. In this line, one practice discussed dealt with the potential outsourcing of collection processes concerning mostly open-source evidence, considering the increasing relevance of social media evidence. As part of this, fact-finding and human rights mechanisms may engage in cooperation with local actors such as universities and human rights clinics who may assist in the collection process, as was the case in relation to the Commission of Inquiry on Gaza and the Democratic Republic of the Congo ('DRC') mapping report.

- Relevance to record documentation methodology and 'tracking' devices

An important part of the documentation process relates to capturing and recording the scope of the documentation process, which includes tracking every step of the fact-finding process. In this line, and in order to document and record the working methodology, tools such as 'Hunchly'[2] might be useful in documenting open-source searches from the beginning to the end. Challenges raised in this regard included the scope of the tracking, a consistent standard and practice, as well as the availability of the tools.

- Open-source is used to identify potential biases and red flags

Experts highlighted the potential bias that may arise in user-generated evidence, as well as the use and analysis of open-source evidence to identify it. The consistent bias in user-generated evidence has proven to be an issue in contexts in which only one party to the conflict cooperates with the human rights investigative processes, e.g. the situation in Gaza. This leads to additional challenges concerning corroboration.

Potential bias might be identified in two main elements: in cases where only the civilian population's perspective is portrayed (e.g. protesters' perspective in the case of demonstrations), and where no female victims are depicted in the material. These elements could imply that the incidents documented are often restricted to incidents committed in 'public' and may portray cultural bias against women, therefore lacking proper documentation of sexual and gender-based crimes.

Bearing in mind these challenges, experts discussed the need of setting up mechanisms to identify bias early on in the documentation processes, particularly concerning user-generated evidence, as well as the relevance of open-source evidence as part of verification processes.

[2] *Hunchly*, The Web Capture Tool Designed For Online Investigations, available at https://www.hunch.ly/ (last accessed on 31 August 2021).

b. *Corroborative techniques and international criminal investigations*

- Traditional evidence types versus digital evidence

The experts noted that it might remain difficult to assess evidence sources during the criminal investigation as long as the parties do not have access to the relevant documentation. Consequently, even in light of the increased usage of digital evidence, the use of 'traditional' forms of evidence such as witness and documentary evidence remains relevant for corroborative processes.

- Time-lag between investigation and criminal prosecution

There is a developing practice and awareness regarding the inability to share the source of evidence. As a result, practices are being strengthened, coinciding with a request to consent to disclosure at an earlier stage. This also poses a challenge concerning the lack of consistency in the methodology which is transferred from the investigative processes to the submission of the evidence in the courtroom. It also relates to the need to understand that different processes refer to different investigative stages, and therefore, the methodologies need to be documented accordingly.

- Documentation in a transparent and traceable manner

Documentation of any type of evidence should be done in a manner that fulfils the investigative and evidentiary standards. Lack of consistency in documenting the methodology is a challenge.

c. Potential tensions between fact-finding/human rights investigative mechanisms and international criminal investigations

- Diversity of mandates

The different mandates of fact-finding/human rights investigative mechanisms and those of international criminal justice institutions create a challenge for the transfer of information and evidence between these entities. These challenges concern mostly the fact that fact-finding/human rights investigative mechanisms do not necessarily pursue accountability, however, they often transfer and share information with institutions investigating and prosecuting core international crimes without necessarily following the same standards.

- Presumption of innocence

- While fact-finding/human rights investigative mechanisms often refer to due process and fair trial guarantees, experts discussed that these standards do not necessarily apply to them. As such, human rights investigative mechanisms are not obliged to uphold the presumption of innocence while carrying out investigations, which may pose challenges and tensions for the transfer and the subsequent use of data in international criminal jurisdictions. Transfer of the responsibility concerning source verification

In addition to the challenges concerning the upholding of fair trial principles such as the presumption of evidence, experts highlighted that due to the time lag between investigations and criminal prosecutions, the burden and obligations concerning the evidence collected are

inadequately transferred from the investigators to the prosecutors, since evidentiary and investigative standards do not apply equally to fact-finding/human rights investigative mechanisms. While fact-finding/human rights investigations may collect evidence and information relevant for international criminal proceedings, prosecutors and parties to these proceedings are the ones faced with the challenges concerning verification and authentication of the source. This constitutes a serious problem as it transfers the responsibility of dealing with this material from investigators to prosecutors.

- Relevance of sound data and information management to ensure proper evidence and information preservation and storage

Considering the tensions, the establishment of proper evidence preservation and storage tools is paramount. Accordingly, information governance and management are key issues for the preservation of the digital file for the transfer and sharing of information between fact-finding/human rights investigative mechanisms and international criminal jurisdictions. Sound data and information management was raised as essential in any documentation process to avoid duplication and overcollection of evidentiary material.

d. Nature of the content documented, preserved and archived

The experts were asked whether defining the nature of the content documented, preserved and archived would be helpful in advancing the accountability efforts. The experts were unsure whether this would add value to their work.

However, experts raised the question of duplication of material and evidence as being a challenge. Sound document management has been identified as a ‘must’ in any documentation process to avoid overcollection.

5. About the International Nuremberg Principles Academy

The International Nuremberg Principles Academy is a non-profit foundation dedicated to the promotion and advancement of international criminal law and human rights. Located in Nuremberg, the birthplace of modern international criminal law (ICL), the Nuremberg Academy was established by the Federal Republic of Germany, the Free State of Bavaria, and the City of Nuremberg in 2014. Dedicated to supporting the worldwide enforcement of international criminal law, the Nuremberg Academy promotes the Nuremberg Principles and the rule of law with a vision of sustainable peace through justice, furthering knowledge, and capacity building of those involved in the judicial process in relation to these crimes.

6. Contact

Should you have any questions or feedback, please do not hesitate to contact Ms Jolana Makraiová, Senior Officer in charge of this project under:

Jolana.Makraiova@nurembergacademy.org

7. Annex 1

E-procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Expert workshops, cluster D

List of invited and participating institutions

	Name of Institution
1.	International Criminal Court
2.	Zentralstelle Cybercrime Bayern
3.	Eurojust
4.	Amnesty International
5.	Commission for International Justice and Accountability
6.	OSR4Rights / Swansea University
7.	International Federation for Human Rights (FIDH)
8.	Berkeley Centre for Human Rights
9.	Open Society Justice Initiative
10.	William and Mary Law School
11.	University of Bologna
12.	American Bar Association
13.	International, Impartial and Independent Mechanism to assist in the investigation and prosecution of persons responsible for the most serious crimes under International Law committed in the Syrian Arab Republic since March 2011 (IIIM)
14.	Independent Investigative Mechanism for Myanmar (IIMM)
15.	Carnegie Mellon University (Center for Human Rights Science)
16.	Stanford Law School
17.	International Bar Association
18.	Strathmore University
19.	Witness
20.	Office of the High Commissioner for Human Rights

8. Annex 2

E-procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Expert workshop, cluster D

Wednesday, 16 June 2021

Zoom meeting

Agenda

16:00-16:10	Welcome and introduction to the Academy, project, and workshops' objectives
16:10-16:20	Introductions: Participants to the Expert Workshop
16:20-16:45	Brief presentation by the experts on the main question addressing the following areas: • Challenges at the domestic level: common law vs. civil law • Challenges at the ICC • Challenges arising from the investigative mechanisms • EU standards and relevant practices
16:45-17:15	Roundtable discussion
17:15-17:30	Summary and conclusion of the workshop

9. Annex 3

E-procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Expert workshop, cluster D

Wednesday, 30 June 2021

Zoom meeting

Agenda

16:00-16:10	Welcome and introduction to the Academy, project, and workshops' objectives
16:10-16:20	Introductions: Participants to the Expert Workshop
16:20-16:45	Brief presentation by the experts on the question of anonymity, hearsay and data analysis, addressing the following areas in particular: • Challenges with verification of source • Prevailing and adopted practices • The question of the burden: anonymous and hearsay evidence in the investigation of grave human rights violations and core international crimes • Corroboration of digital evidence and standards
16:45-17:30	Roundtable discussion
17:30-17:40	Summary and conclusion of the workshop

9. Annex 4

E-procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Expert workshop, cluster D

Wednesday, 14 July 2021

Zoom meeting

Agenda

16:00-16:10	Welcome and introduction to the Academy, project, and workshops' objectives
16:10-16:20	Introductions: Participants to the Expert Workshop
16:20-17:30	Roundtable discussion: • Corroborative techniques and evidence • Accountability assessment and presumption of innocence • Nature of the content documented, archived and preserved
17:30-17:45	Q&A Session
17:45-18:00	Summary and conclusion of the workshop

E-Procedure: Evidence in Time of Increased Use of Technology and Digitalisation

Cluster D - Annex 3

List of Insitutions

Digital Evidence Project – Cluster D Final Report	
Institutional Affiliation	*Area of Expertise*
American Bar Association	International criminal law and evidentiary standards
Amnesty International	Digital data-streams, modern fact-finding, best practices conducting investigation of human rights violations
Berkeley Centre for Human Rights	Human rights, science, and technological innovation
Carnegie Mellon University	Human rights, science, and technological innovation
Central Office for Cybercrime Bavaria (ZCB)	Cybercrime, investigations
Commission for International Justice and Accountability	Criminal justice, (criminal) investigations, gathering evidence, preservation, and analysis of evidence
Eurojust	Cross-border crime, judicial cooperation
EyeWitness to Atrocities	Technology, evidentiary standards, documentation of mass atrocities
FIDH (International Federation for Human Rights)	International Criminal Court, digital evidence, criminal trials
Independent Investigative Mechanism for Myammar	Collection, consolidation, preservation and analysis of evidence, international standards, criminal proceedings
International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011	Criminal investigation, prosecutions, collection of evidence, storage of information, sharing material and international criminal law standards
International Criminal Court	International criminal law
International Bar Association	International criminal law and evidentiary standards
Leiden University	International criminal law
Open Society Foundations	Human rights, technology
Strathmore Law School – Strathmore University	Digital evidence, criminal law

Swansea University	International criminal law, evidence and proof, human rights, fair trial
University of Amsterdam	International criminal law, evidence and proof
Universita di Bologna	International criminal law, comparative law
William & Mary Law School	International criminal law, evidentiary standards
Witness	Human rights, video, technology, documentation standards

International Nuremberg Principles Academy
Bärenschanzstraße 72
90429 Nuremberg, Germany
Tel +49 (0)911 148977-0
info@nurembergacademy.org
www.nurembergacademy.org

www.nurembergacademy.org