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

Final Report

27 October 2023

Published by:

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

ISBN: 978-3-9818913-9-3

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.

Preface

Between 2018 and 2023, the International Nuremberg Principles Academy (Nuremberg Academy) has been exploring the various challenges that arise from the increased usage of digital evidence and sophistication of technology and how these may affect the prosecution of core international crimes. The goal of this exploration has been to see whether the current rules governing the International Criminal Court (ICC) need amending and if so, how and why.

Given the complexity of the subject matter, the project was divided into several clusters, and each cluster's methodology consisted of focused workshops, detailed research and discussions with experts from relevant fields, including practitioners in international criminal law (ICL) and international human rights law (IHRL), experts in digital evidence, digital forensics and open-source investigations as well as experts in the documentation of human rights violations generally.

Our research and analysis focused on the following complex issues:

- The identification of guidelines and manuals that could be potentially relevant to the investigation of core international crimes and which relate to digital evidence;
- The identification of gaps arising from the ongoing work of those involved in documenting and prosecuting human rights violations and core international crimes;
- Any current practices and criteria regarding the admissibility of digital evidence and the weight of digital evidence and challenges to these practices arising from "newer types" of sophisticated technology (such as deepfakes, information generated from artificial intelligence (AI) and deleted accounts);
- Correlations between human rights investigations and international criminal law investigations and digital evidence challenges that arise in respect of each type of investigation; and
- How the identified digital evidence challenges can (and how they cannot) be addressed in light of the ICC's structure, rules and governing practices.

With respect to the last point in particular, our research regarding the current practices at the ICC and how they may need to change or be adapted to deal with the challenges arising from digital evidence, has focused on the following questions: Is the law clear, public and flexible? Is the process fair, accessible and efficient? Is the outcome timely and carried out by competent, independent representatives (with adequate resources)?

Our key takeaways are described in this report and can be briefly summarised as follows:

1. There is no imminent need to amend the governing rules of the ICC. Rather, there needs to be more discussion between relevant ICC stakeholders leading to decisions, where possible, on the following matters:
    a. The Court's limitations (including in respect of its resources and its role) in light of the technological advancements that may affect the evidentiary process;
    b. The standards that should apply to the collection, preservation and verification of digital evidence; and
    c. Whether the current admissibility criteria and practice needs to change in light of the unique challenges that digital evidence brings and the need to safeguard the accused's right to a fair trial.

2. This report is not conclusive, nor does it necessarily cover all possible challenges that arise from the increased usage of digital evidence and the sophistication of technology. Rather, by contextualising the identified challenges to the relevant rules and practices of the ICC[1] and breaking them down into smaller elements, this report serves as a starting point for further research and discussions amongst ICC stakeholders and other actors in the field of international criminal justice.

This report should be read in light of three major and ongoing developments in the field of technology and criminal justice that have affected our ability to carry out a more conclusive investigation and analysis:

- Digital evidence and technology are ever-changing, consistently giving rise to new challenges at various stages of the criminal proceedings, including in regard to both discovery and verification.
- Standard-setting, with regards to the practices affecting digital evidence, is still developing at the international level.
- The ICC (and the field of international criminal justice) is currently in a state of change and adaptation, and we are seeing strong demands for the restructuring of the Court and its practices to ensure the efficiency and effectiveness of proceedings generally.

This report progresses the discussions around the impact of the increased usage of digital evidence and the sophistication of technology on the ICC and its proceedings: (1) it identifies the relevant rules that might be affected by the identified challenges and (2) it breaks down the digital evidence and technology challenges into smaller elements and considers how they interrelate with each other. In this way, it is the hope that the report offers not only a critical perspective on the challenges arising from the increased usage of digital evidence and the sophistication of technology but also serves as a roadmap for to ultimately analysing and addressing some of these challenges within the wider discussions around changes happening at the ICC today.

It is clear from the research findings that any digital information submitted to the Court, which ultimately becomes digital evidence, needs to be of sufficient quality to allow for a proper assessment of its admissibility, thus advancing, rather than hindering or delaying, the proceedings with burdensome re-evaluations of evidence at later stages. Clarity, transparency, efficiency and guiding standards are essential terms when discussing the usefulness of digital evidence in the context of international criminal justice.

The Nuremberg Academy is grateful to the broad range of experts and consultants who have contributed to this project by providing their views and helping to identify the relevant challenges.[2] Moreover, we are grateful to the experts and consultants who helped us bring this, and other reports, together. Special thanks go to Olivia Flasch for combining the research findings into this report.

[1] Our Analytical Roadmap, which forms the basis of this report, sets out and categorises the identified challenges against the relevant rules governing the ICC. A simplified revised version of the Analytical Roadmap is contained in Annex 1.
[2] See Annex 3 below for an overview of the contributing institutions and organisations.

The Nuremberg Academy welcomes any feedback and further engagement in addressing the challenges identified in this research project. We stand ready to further explore the impact that the increased usage of digital evidence and the sophistication of technology has on international criminal proceedings and in particular the ICC. It is our hope that by addressing these challenges and in such way strengthening the judicial proceedings, we are not only able to contribute to the employment of fair processes and increased accountability for the commission of international crimes but also, in the long-term, to the upholding of the rule of law and the achievement of sustainable peace through justice.

October 2023

Jolana Makraiová
Senior Officer for Interdisciplinary Research
International Nuremberg Principles Academy

1 Executive Summary

This report forms part of Cluster E of the International Nuremberg Principles Academy's interdisciplinary project on digital evidence, the purpose of which is to provide a conclusive answer to the project's research question: the potential impact that the increased usage of digital evidence and sophistication of technology might have on the rules and practices of the International Criminal Court (and potentially beyond).[3]

Digital evidence is ever-changing and so is the field of international criminal justice. The purpose of this report is to offer a critical perspective and analysis of the challenges arising from the increased usage of digital evidence and the sophistication of technology, with the aim of kickstarting a discussion on how to strengthen and, if need be, amend judicial procedures so that they may be properly adapted to the changing times.

Evidence adjudicated before all courts, including the ICC, needs to be of sufficient quality to enable it to be properly assessed and to ensure that proceedings are effective with respect for the fair trial rights of the accused. There is therefore a need for the development of standards to guide the collection, preservation and verification of information before it is admitted as evidence. Transparency as to the methodologies adopted in the transition of information to evidence is essential, as is transparency as to the admission criteria and determination of the weight of evidence in light of all the evidence on the case record. Biases connected with or arising in the context of newer, more sophisticated forms of digital evidence ought to be discussed and addressed preventatively. Moreover, ensuring that appropriate safeguards are in place to preserve the fair trial rights of the accused ought to be discussed so that, even in the context of the challenges brought by sophisticated technology, the guarantees provided to the accused conform to the appropriate international human rights law standards.

This report reflects on the articles and rules contained in the Rome Statute (RS) and Rules of Procedure and Evidence (RPE) of the ICC by identifying and expanding on the challenges identified in previous clusters. By compiling the identified challenges pertaining to each article and rule under five specific categories affecting the work of the ICC, the report seeks to contextualise the challenges and summarise the potential impact they have on international criminal proceedings as a whole as well as how they interrelate with one another.

The report discusses the potential impact of the challenges on the legal framework of the ICC by analysing its investigatory and judicial practices. The aim of the analysis has been to ensure that the procedures and practices of the Court, which were established in 1998, are flexible enough to maintain the functionality of the ICC in an era where digital evidence is becoming more and more prolific.

[3] In this report, the terms "digital evidence" and "digital information" are often used to describe the same type of information. The term "digital information" is used to refer to such information prior to its transition into evidence. The term "digital evidence" is used to refer to such information after it has become digital evidence for the purposes of international criminal proceedings. The relevant distinction is thus determined by the stage of the proceedings. Where discussing several stages at once (for instance, the collection, preservation and verification stages) the term "digital evidence" is used to refer to the information across all stages.

At this stage, and considering the project limitations outlined below, the conclusion of the project is that there is no immediate need to amend the RS or the RPE; rather, the rules are sufficiently broad and flexible to allow a balance between sufficient procedural guarantees and judicial discretion to be struck, even in an era of increased usage of digital evidence, and sufficient to provide the parties with the necessary opportunities to challenge the evidence on the record.

There is, however, a pressing need:

1. For discussions to be had regarding the ICC's ability to deal with the increased usage of digital evidence and the sophistication of technology, with an emphasis on the need to formulate realistic limitations for coping with the challenges that arise.
2. To address the possible gaps and lack of uniformity of practical guidelines and standards that have the potential to assist judicial practitioners in collecting, preserving and verifying digital evidence.
3. For more comparative research to be undertaken and further discussions to be had on the current evidentiary rules, practices and evolving standards at the ICC and how they might affect or be affected by the increased usage of digital evidence and sophistication of technology, including any difficulties that the parties have experienced with the current rules, and whether they are adequate to ensure the fairness and expeditiousness of proceedings.
4. For more clarification with respect to any admissibility and weight criteria that are currently being used and how they are to be applied to digital evidence, ensuring that the accused may effectively challenge the evidence against them (and ensuring that victims are given the opportunity to present their evidence and to consent to the use of digital evidence in which they are featured).

This report, albeit detailed, is not short of limitations that are important to bear in mind when reading it and considering its findings. In particular, the research, especially comparative research, was limited in terms of its scope and has not sufficiently considered any in-depth analysis of domestic proceedings and useful practices gained from, for example, universal jurisdiction cases. Moreover, while the challenges identified in this project have been discussed with experts and practitioners to a certain extent, further discussions would be needed to fully understand these challenges in practice.

Finally, it should be noted that this project has been limited in its scope and research to the time and resources available, thus the identified challenges and conclusions in this report would benefit from additional in-depth research and tailored, inclusive discussions to further understand the complexities and implications of the below recommendations and findings.

2 Introduction

2.1 Background

There is no doubt that digital evidence, and in particular open-source digital evidence, is changing international criminal justice: from new means and methods of documenting atrocities to quicker spread and access of digital information, the sophistication of technology is democratising justice in a way never seen before. This is an immense opportunity for ensuring accountability and justice for victims; however, as with most opportunities, it also brings with it an immense number of challenges. If these challenges are not addressed appropriately, and if our accountability frameworks and judicial processes are not updated to reflect the changing environment, digital evidence and the sophistication of technology has the unfortunate potential of creating more problems than it solves.

While often easy to produce and, in some cases, easier to access than physical evidence, digital evidence is nevertheless plagued with complexities—often because of its easy access. Digital evidence can be captured on a personal mobile phone and uploaded to social media in a matter of seconds. It is estimated that "approximately 6000 tweets are created every second and more than 500 hours of video are uploaded to YouTube every minute".[4]

Not only does the sheer volume of digital media cause issues for human rights investigators and, later down the line, prosecutors and judicial staff, but its susceptibility to manipulation, hacking and, more recently, various forms of artificial intelligence interactions means that legal professionals and court staff who are trained in traditional forms of evidence must suddenly retrain their minds to understand the fluid and dynamic environment that is digital information. These individuals are now increasingly being faced with the dilemma that what they see in a video or image or what they hear in a recording may not reflect reality and cannot by definition be relied upon. They must also consider that evidence repositories, that until this date have been considered secure, may not be secure enough to protect from malware, hacking and deletions and that significantly stronger protections may need to be put in place.[5]

If that weren't enough, these same individuals must contemplate whether the victim and witness protective measures that were put in place over the past decade or longer are sufficient to protect both individuals featured in digital open-source information and the long line of sources that may have been involved in providing that information to the Court: the user, the uploader, the person filming, the owner of the electronic device or even the technology company involved in processing the media.[6] The right to privacy and related

---

[4] A. Koenig, "Digital and Open Source Information Can Play a Critical Role in Improving the Overall Efficiency and Efficacy of the International Criminal Court", *ICC Forum* [blog post] (n.d.), https://iccforum.com/cyber-evidence#Koenig, accessed 20 October 2023, citing K. Smith, "60 Incredible and Interesting Twitter Stats and Statistics", *Brandwatch* [blog post] (2 January 2020), https://www.brandwatch.com/blog/twitter-stats-andstatistics/, accessed 20 October 2023; K. Smith, "57 Fascinating and Incredible YouTube Statistics", *Brandwatch* [blog post] (21 February 2020), https://www.brandwatch.com/blog/youtube-stats/, accessed 20 October 2023; A. Frangoul, "With Over 1 Billion Users, Here's How YouTube is Keeping Pace with Change", *CNBC* [blog post] (14 March 2018), https://www.cnbc.com/2018/03/14/with-over-1-billion-users-heres-how-youtube-is-keeping-pace-with-change.html, accessed 20 October 2023.

[5] C. Quilling, "The Future of Digital Evidence Authentication at the International Criminal Court" *Princeton University Journal of Public International Affairs* (20 May 2022), https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court, accessed 20 October 2023.

[6] See e.g., L. Freeman & R. Vazquez Llorente, "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age", *Journal of International Criminal Justice*, 19/1 (2021), 163, 169, https://doi.org/10.1093/jicj/mqab023.

access rights are likely to come into play at an increasing rate when the ICC and other international and internationalised courts and tribunals are having to deal with digital evidence originating from open sources.

It is against this backdrop that the Nuremberg Academy developed its interdisciplinary project that explores challenges relating to the use of digital evidence in international criminal proceedings (the Digital Evidence Project).[7] The main research question of the Digital Evidence Project was as follows:

> *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 project sought to address and consider the potential impact of the challenges raised in this context on the 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 focused on the legal framework of the ICC as the first permanent international criminal court.

The project consisted of five research clusters, where this report forms part of Cluster E:

A. A Repository Mapping the Existing Guidelines on Digital Evidence Practices and Standards

B. Research Gap: A Mapping of Missing Guidelines on Digital Evidence Practices and Standards

C. Jurisprudence Regarding the Substantive and Procedural Rules Governing Admissibility and the Evidentiary Weight of Digital Evidence

D. Human Rights Correlations of Digital Evidence

E. Recommendations or Amendments to the ICC Rules of Procedures

Clusters A and B collected existing (and aimed to identify missing) 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 the application of the ICCs framework regarding the admissibility and inadmissibility of digital evidence at the pre-trial, trial and appeals phases and delivered a report encompassing a legal and, to some extent, comparative assessment of practices and standards at the ICC.[8] Cluster D analysed the correlations between IHRL and ICL investigations as they pertain to the collection, preservation and verification of digital evidence.[9]

The current Cluster E attempts to answer the main research question of the Digital Evidence Project by analysing the identified challenges arising from the collection and use of digital evidence in international criminal proceedings and considering the ability of the legal framework of the ICC to adequately deal with these challenges. The report culminates in a number of recommendations that relate to the ICC rules and practices.

---

[7] 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 20 October 2023.
[8] Cluster C Report.
[9] Cluster D Report.

2.2 Methodology

For Cluster E, the groundwork started with adopting the methodology for combining and building on all the challenges identified through Clusters A–D that needed further exploration. The challenges were combined and structured into our Analytical Roadmap, which contained a list of all provisions of the RS and RPE that could in some way relate to digital evidence. Each identified challenge was then listed next to the potential provision under which it might arise.

After each general digital evidence-related challenge was allocated to one or more provisions from the RS and RPE, further analysis was undertaken to categorise "digital evidence" into three separate types. Type 1 Digital Evidence referred to digital, or digitalised, information that is already being used and considered as evidence in international criminal proceedings on a regular basis, such as non-social media videos, non-social media photographs, aerial and satellite images, audio intercepts, call data records, audio recordings from radio or podcasts or other digitalised documents.[10] Type 2 Digital Evidence referred to digital evidence or digitally derived evidence that is used to some extent in international criminal proceedings but for which no sufficient evidentiary guidelines on its use can be deduced from international cases. This includes digital evidence originating from social media or private users, such as social media posts (videos, photographs and text) and email correspondence.[11] Finally, Type 3 Digital Evidence referred to sophisticated technology permeating both Type 1 and 2 Digital Evidence, which international criminal courts may not be prepared to deal with, such as deepfakes, AI-generated photographs and videos, deleted accounts and sophisticated data breach technologies.[12]

---

[10] See the types of digital evidence covered by the Leiden Guidelines due to sufficient discussion in international criminal cases in Leiden University, "Leiden Guidelines on the Use of Digitally Derived Evidence", *Leiden Guidelines on the Use of Digitally Derived Evidence* (4 April 2022), Introduction, https://leiden-guidelines.com/guidelines/, accessed 20 October 2023. See also Y. McDermott, A. Koenig & D. Murray, "Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations",*Journal of International Criminal Justice*, 19/1 (2021), 85, 86, https://doi.org/10.1093/jicj/mqab006; Berkeley Human Rights Center & UN OHCHR, "Berkeley Protocol on Digital Open Source Investigations", *UN OHCHR* (3 January 2022), 3, https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf, accessed 20 October 2023. See also the definition of "Documents" in: European Union Agency for Criminal Justice Cooperation, "Documenting international crimes and human rights violations for accountability purposes: Guidelines for civil society organisations" [media release] (21 September 2022), 32–33, https://www.eurojust.europa.eu/news/eurojust-and-icc-prosecutor-launch-practical-guidelines-documenting-and-preserving-information, accessed 20 October 2023.

[11] See Leiden University, *Leiden Guidelines*, for the types of digital evidence not covered by Leiden Guidelines due to insufficient discussion in international criminal cases. See also Berkeley Human Rights Center & UN OHCHR, *Berkeley Protocol*, 3; Quilling, *The Future of Digital Evidence*: "[I]n the 2017 case, *Prosecutor v. Mahmoud Mustafa Busyf Al-Werfalli*, the Court relied heavily on several videos posted to Facebook to issue an arrest warrant for a high-ranking Libyan military officer, Major Mahmoud Mustafa Busyf Al-Werfalli, for the murder of 33 people. Al-Werfalli is not presently in ICC custody, so the effect of the introduction of social media evidence remains to be seen. Al-Mahdi and Al-Werfalli demonstrate the Courts' willingness to evaluate digital evidence in substantially new ways. In the case of Al-Werfalli, there would likely not be a case at all without the Facebook videos of these alleged crimes. While digital evidence has not yet played a central role in the final judgment of a case before the ICC, these two cases demonstrate that this change is inevitable."

[12] See A. Koenig, "'Half the Truth is Often a Great Lie: Deep Fakes, Open Source Information, and International Criminal Law", *AJIL Unbound*, 113 (2019), 250, https://doi.org/10.1017/aju.2019.47; Quilling, *The Future of Digital Evidence* .

Once this categorisation of digital evidence was complete, further research was carried out to specify the challenges that may arise in relation to each category of digital evidence and under which provisions of the RS or RPE such specific challenges might arise; the result of which completed our Analytical Roadmap, mentioned above. This roadmap was then transformed into a simplified version, which streamlined the challenges identified and, where more than one challenge per category was identified, emphasised the main such challenge.[13]

The Nuremberg Academy also decided in January 2022 to undertake a three-fold approach towards answering the main research question of Cluster E. First, it created three working groups, with each focusing on one of the three key topics arising from our research at that time: (1) investigative practices and their impact on the procedural rules of the ICC; (2) admissibility assessments and evaluation of evidence; and (3) identification of key rule of law indicators to set the parameters for the usage of digital evidence in international criminal proceedings. The first two working groups explored the questions and challenges relating to investigation practices and admissibility of digital evidence, the conclusions of which are set out more in detail below. The third working group focused on identifying key rule of law indicators[14] which would contribute to the establishment of parameters for the effectiveness, efficiency, integrity and impartiality of the judicial proceedings. These parameters would then be used to identify whether a particular challenge would require a rule or provision to be amended and in what way (for example, if the provision as drafted could no longer uphold the integrity of the proceedings given its allocated digital evidence challenge).

After considering the work of the third working group on the key rule of law indicators, the challenges that digital evidence brings into the judicial process, the relevant guidelines or recommendations for effective and efficient judicial proceedings and other procedural standards developed by various relevant bodies working with digital evidence, an initial "checklist" comprising the following parameters for digital evidence use at the ICC was proposed:

1. The criminal *investigation* must be timely and effective, which includes the following:
    a. There is transparency in the standards applied for collecting, preserving and verifying digital evidence, which protect the rights of the accused and the safety of victims and witnesses and which ensure non-discrimination and consider potential biases.
    b. There is a standardised disclosure regime that ensures predictability and expeditiousness of the proceedings and reflects the charges brought before the Court. The regime ensures that disclosure is fully finalised before the trial, that all matters related to disclosure are solved in a timely and effective matter and that disclosure is handled in a way that ensures equality of arms.
2. The criminal *adjudication* must be timely and effective, which includes the following:
    a. There are sufficient guarantees in place to ensure the presumption of innocence.
    b. The legal standards are clear, ensuring both effectiveness of the adjudication and consistency of the law (including standards for the charges brought against the accused and for the evidence).

[13] See Annex 1.

[14] See e.g., "What is the Rule of Law?", *World Justice Project* (n.d.), https://worldjusticeproject.org/about-us/overview/what-rule-law#:~:text=The%20rule%20of%20law%20is%20a%20durable%20system%20of%20laws,are%20accountable%20under%20the%20law, accessed 20 October 2023.

c. There is equality in and before the law, ensuring that all efforts are made to ensure both equitable and impartial adjudication, addressing unknown and unintentional biases.

After carrying out further work on the Analytical Roadmap, which considered in detail the flexibility of the rules to adequately deal with the changing technological environment, the checklist above evolved into a series of simple questions that are considered, in part, in the below sections and which were taken into account in the assessment of the legal framework:

1. Is the law clear, publicised and stable?
2. Is the process fair, accessible and efficient?
3. Is the outcome timely and carried out by competent, ethical and independent representatives (with adequate resources)?

It was concluded that the ability of the RS and RPE to effectively deal with the challenges of digital evidence might be assessed against these questions, that is, if the provisions are considered sufficient to tick off the requirements in the checklist (or to answer in the affirmative the three simple questions above) when faced with the challenges arising from the increased usage of digital evidence and sophistication of technology, amendments to the provisions themselves are unlikely to be needed. While we have not carried out a full assessment or comprehensive consultations on the requirements contained in the checklist due to time limitations, it has prompted and furthered fruitful discussions with the experts of the working groups. The checklist parameters have been taken into account by looking at the specific challenges with digital evidence and the mandate, role and responsibility of the ICC and its legal framework and should be further developed in any follow up work.

Throughout each of the phases in this project, complementing research on different topics was consistently carried out, including regarding how each of the identified challenges may impact the rights of victims, witnesses and the accused, how the weight of evidence is assessed at the ICC and a comparison of the practical utility of existing guidelines and manuals on digital evidence and open-source information. Our research findings were complemented by expert workshops and, where possible, feedback from practitioners and academics.[15]

The deliverables from this entire project are as follows: Digital Evidence Database (Cluster A and B findings),[16] Cluster C Report with its accompanying Annex 2,[17] Cluster D Report with its accompanying Annex 1[18] and this current Cluster E Report.

[15] Cluster E's first workshop discussing and agreeing on the proposed methodology took place in late 2021 and four more workshops took place in 2022 advancing the goals of working groups 1–3. Written feedback was also sought on a draft memorandum on the weight of evidence, which was helpfully annexed to the Cluster C report, shedding more light on the challenges arising from the expert discussions and ongoing research on the admissibility challenges. The Nuremberg Academy has on record, as internal files, the agenda, notes and the list of institutions participating in these workshops.
[16] International Nuremberg Principles Academy, "Digital Evidence Database", https://www.nurembergacademy.org/resources/digital-evidence-database/, accessed 20 October 2023.
[17] Cluster C Report.
[18] Cluster D Report.

2.3 Focus of the Report and Exclusions

Cluster Es aim has been to review the relevant provisions of the RS, the RPE and the current practices through the case law of the ICC to determine whether the legal framework and related practices are flexible enough to deal with the challenges arising from the increased usage of digital evidence and the sophistication of technology. The aim has not been to consider whether and how digital evidence can improve or expedite criminal proceedings. While an assumption of the Digital Evidence Project is that the use of digital evidence may help expedite international criminal proceedings and make them more efficient in the long run, many shortcomings of the current legal framework and court practices would first need to be addressed for that to occur, including for the industry to agree on a set of authoritative and practical guidelines for the collection, preservation and verification of digital evidence.

Cluster E has primarily focused on the current versions of the RS and the RPE. It has not focused on undertaking any comparative analysis with other statutes or court rules and procedures and, due to time limitations, has also not focused to any great extent on the commentaries accompanying the RS or the RPE. Additionally, while the ICC Regulations were reviewed on a superficial level, with one provision (Regulation 44) included in the Analytical Roadmap, the Regulations do not form part of the focus of this research project and any future research on the topic of this project would benefit from a more thorough review of the ICC Regulations and other accompanying texts.

To produce the Analytical Roadmap forming the basis for this report, all provisions of the RS and the RPE were reviewed. A number of provisions were then excluded from the scope of the research, as they were deemed to be insufficiently relevant to the topic of digital evidence in court proceedings. The excluded provisions are articles 21, 55 and 83(2) of the RS and rules 40(1), 67, 69, 72, 111, 112, 124(3), 134 bis, 137 and 149 of the RPE.

Other topics that were excluded from the scope of this research due to time limitations which may benefit from further analysis are as follows: research into how the establishment of the Court and the organisation of the Assembly of States Parties might affect the ICCs approach and future development relating to the use of digital evidence in international criminal proceedings, financing and available resources of the ICC and how the process of search and arrest warrants may need to change with the increased usage of digital evidence and the sophistication of technology.

2.4 Structure

As mentioned above, we have throughout this report worked on the basis of three "Types" of digital evidence with the aim of specifying where and in which context the identified challenges arise. The challenges arising from each of these three categories have been divided into five broad categories as follows and are discussed in the sections below:[19]

> Challenge Category 1: operational limitations affecting judicial functions.
>
> Challenge Category 2: the collection, preservation, storage and verification of digital evidence, including in relation to disclosure processes.
>
> Challenge Category 3: the impact of digital evidence on procedural guarantees.
>
> Challenge Category 4: other specific challenges that impact procedural guarantees, including unexplored biases.
>
> Challenge Category 5: the evaluation of digital evidence in judicial proceedings.

2.5 Definitions

Artificial Intelligence: the capacity of computers or other machines to exhibit or simulate intelligent behaviour; the field of study concerned with this. Abbreviated AI.[20]

Authenticity: genuineness;[21] an item being what it purports to be.[22]

Credibility: reasonably capable of belief or reliance.[23]

Deepfakes: 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.[24]

Digital Evidence: data, information or evidence that is created, manipulated, stored or communicated by any (digital) device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding. This can include information which is created by and originates from digital technology as well as information that is transmitted or stored in a digital format. It can also include digitally derived evidence, namely data, information or evidence which has been converted from its original format to a virtual or digital format for the purpose of storing, archiving, organising or presenting the information.[25]

---

[19] Note that the most appropriate way to categorise the challenges has evolved throughout the drafting of this report and the categorisation in Annex 3 and the Analytical Roadmap may therefore be slightly different as compared to the categorisation of the challenges provided in this report.

[20] "artificial intelligence", Oxford English Dictionary (2023), https://www.oed.com/search/dictionary/?scope=Entries&q=artificial+intelligence, accessed 20 October 2023.

[21] "authenticity", Oxford English Dictionary (2023), https://www.oed.com/search/dictionary/?scope=Entries&q=authenticity, accessed 20 October 2023.

[22] *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé*, Reasons of Judge Geoffrey Henderson (2019) ICC-02/11-01/15-1263-AnxB-Red, paras 32, 37.

[23] Cluster C Report, Annex, 8, and its accompanying footnotes.

[24] "Deepfake", *Merriam-Webster Dictionary* (n.d.), https://www.merriam-webster.com/dictionary/deepfake, accessed 20 October 2023.

[25] Cluster C Report, 13.

Evidence: information that has been submitted to a court, which satisfies the admissibility requirements of the jurisdiction concerned, and is admitted into the record of the case.[26]

Information: any kind of tangible and intangible material which is obtained or inspected during the course of a criminal investigation. Information can be secured from numerous sources, including suspected perpetrating structures, witnesses, victims, governing entities, open sources as well as information generated or inferred by the investigation team. Information can take a wide range of forms including documentary, physical, digital or testimonial materials.[27]

Open-Source Evidence: open-source intelligence (OSINT) collected from publicly available information found on the Internet that is used as evidence in a proceeding. It can consist of other forms of digital evidence, such as photographs, videos, audio clips, satellite images etc.[28]

Preservation: an action to protect an item from damage, decay or destruction.[29]

Probative value: a "fact-specific" inquiry, taking into account countless factors including "the indicia of reliability, trustworthiness, accuracy or voluntariness… as well as the circumstances in which the evidence arose. It may also take into account the extent to which the item has been authenticated".[30]

Relevance: pertaining "to the matters that are properly to be considered by the Chamber in its investigation of the charges against the accused".[31]

Reliability: the quality or fact of being reliable. Ability to be relied on with confidence; trustworthiness, sureness, reliableness.[32]

Verification: establishing the provenance, source, date and location of a piece of content.[33]

---

[26] Ibid.
[27] Cluster C Report, 13.
[28] Ibid., 14.
[29] "preservation", *Oxford English Dictionary*, https://www.oed.com/search/dictionary/?scope=Entries&q=preservation, accessed 20 October 2023; "preserve evidence", *Colins Dictionary*, https://www.collinsdictionary.com/dictionary/english/preserve-evidence, accessed 20 October 2023.
[30] Cluster C Report, Annex, 6 and its accompanying footnotes.
[31] Ibid.
[32] "reliability", *Oxford English Dictionary*, https://www.oed.com/search/dictionary/?scope=Entries&q=reliability, accessed 20 October 2023.
[33] Annex 1 of Cluster D Report, 24.

3 Operational Limitations Affecting Judicial Functions

3.1 Overview of the Main Challenges

The changes to the functioning of the judicial proceedings at the ICC that may need to occur as a result of the increased usage of digital evidence and the sophistication of technology do not exist in a vacuum. The Court's ability to implement substantive changes that fully address the challenges identified must be considered in light of its technological, human and financial resources, the demands placed on the ICC by its various stakeholders, its ability to cooperate with international organisations, States and individuals and the need for judicial proceedings to always remain efficient and effective, notwithstanding the changes that the Court may be experiencing.

When it comes to digital evidence, there are two main challenges that need to be addressed in regard to the Court's operations:

1. The question of what limitations the ICC is likely to face in light of the increased usage of digital evidence and the sophistication of technology (for example, in respect of budget) and what effect these limitations will have on the functioning of the Court and the criminal proceedings;
2. The question of how the ICC will obtain the expertise required to understand and address the challenges arising from the increased usage of digital evidence (especially its newer forms), ensuring that proceedings remain efficient and expeditious.

These two challenges underlie many of the more specific digital evidence challenges that come up during the collection phase, preservation phase, verification phase and throughout the trial proceedings and interact with several provisions of the RS and the RPE, as set out in our Analytical Roadmap.

Additionally, over the years, many demands for change have been placed on the ICC by different stakeholders, calling for it to, *inter alia*:[34]

- Improve its international cooperation with States and organisations;
- Strengthen its investigation practices;
- Strengthen victim participation and improve legal aid;
- Improve protection of witnesses, including human rights defenders and intermediaries; and
- address the financial challenges that arise from an increasing workload without an increasing budget, in an effective way.

The way in which the Court will be able to address the specific challenges arising from the increased usage of digital evidence will therefore likely depend on, or at least be connected to, how it is planning to address the more general demands for improvement that it is facing, and any discussions regarding the two main challenges mentioned above need to take all of this into account.

[34] See e.g., "The Rome Statute at Twenty (1998-2018): 10 Challenges to an Effective and Independent International Criminal Court", *International Federation for Human Rights* (July 2018), https://www.fidh.org/IMG/pdf/report_20_years_icc_rome_statute-2.pdf, accessed 20 October 2023.

The increasing access to electronic devices and the ease and speed at which digital information can be published online[35] means that: (1) there will likely be more evidence submitted into the case record at the ICC in any given case[36] and (2) much of that evidence will be in a different format—or require different technological measures—compared to what the Court and its personnel are used to.[37] These two changes may have a knock-on effect on a wide variety of trial management processes. More evidence means more resources will be needed across all spectrums, including financial, human and technological resources.[38] Will the Court have the capacity to increase its resources, or will this mean that fewer investigations will be initiated and fewer cases will proceed to trial? Similarly, having to deal with the new format of evidence (for example, more social media posts and videos and other open-source digital information) means that the ICC may need to focus more of its financial resources on security considerations.[39] How will the digital evidence be kept safe from manipulation and deletion? What sort of software might be needed? Where will the evidence be stored, and who will have access to it and responsibility for its safekeeping?[40]

Before any more concrete steps or recommendations can be considered, it is essential that the Court carries out a self-evaluation on how it sees itself functioning in this new digital era. How will the ICC ensure that proceedings are carried out efficiently and expeditiously while still guaranteeing fair trial rights for the accused and adequate protective measures for victims and witnesses? How will it ensure equality of arms in the proceedings, and what sort of amendments to the processes and procedures are realistic, given the limitations or restrictions it will inevitably face in terms of budget and personnel? For instance, is it anticipated that judges would play a greater forensic role in evaluating the technical complexities of certain types of sophisticated digital evidence or not? Does the ICC foresee itself being the gatekeeper of an advanced digital repository of user-generated evidence, or will it outsource the responsibility for this type of system? Depending on the answers to questions like these, any professional development that is required may need to be specifically tailored. As a result, the focus of this report is not on recommending specific trainings or development for judges and court staff: rather the focus is on setting out the challenges that will need to be raised in further discussions amongst relevant stakeholders so that a decision can ultimately be made on how the Court will address them, given the limitations it faces.

It is foreseen that the ICC may need to review some of its current practices to address the demands to increase its efficiency in light of the new challenges raised by digital evidence. For example, the ICC may need to consider whether the Victims and Witnesses Unit (VWU) should be working directly with technology companies to facilitate effective digital communications with survivors in situation countries or consider implementing a witness education programme which informs potential witnesses of the privacy protection tools that are available for them to use when documenting attacks.[41] Similarly, the ICC might consider whether its current witness protection protocols are still adequate to protect victims and

[35] See Koenig, *Digital and Open Source Information*.
[36] Ibid.
[37] See e.g., E. Irving, "And So It Begins… Social Media Evidence In An ICC Arrest Warrant", *Opinio Juris* [blog post] (17 August 2017), http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/, accessed 20 October 2023.
[38] See e.g., Koenig, *Digital and Open Source Information*.
[39] See e.g., Quilling, *The Future of Digital Evidence*.
[40] See Comment by Maria Nava on the Cyber Evidence Question in "Digital Evidence Repositories and Vulnerable Populations: How the Accumulation of Digital Evidence May Interact with the Privacy of Sexual Assault Survivors", *ICC Forum* [blog post] (31 May 2020), https://iccforum.com/forum/permalink/122/33559.
[41] Koenig, *Digital and Open Source Information*.

witnesses who might be featured and identifiable in user-generated social media evidence without their knowledge or consent.[42] As explained elsewhere in this report, the RPE and the RS have been drafted in such a way as to be flexible enough to encompass technological changes, such as the increased usage of digital evidence. However, current court processes and policies may not be as flexible.

Additionally, it is clear (and other scholars have recommended[43]) that ICC judges, the Prosecutor and other relevant court organs may need to participate in specific training sessions to increase their awareness of the challenges accompanying the increased usage of digital evidence (including, for example the existence of deepfakes and the necessary steps needed in preserving and verifying digital evidence). For example, judges are required to explain their admissibility rulings but their ability to do so will increasingly depend on their capacity to interrogate technology systems and increase their familiarity and understanding of digital evidence and new sources of information.[44] The extent to which the judges will realistically be able to do that, given the various limitations that they face, needs to be considered. Moreover, the technological complexity of digital information and media means that experts are often required to decipher the technology so that judges are able to assess the reliability and value of the evidence.[45] Indeed, without appropriate training in the technical aspects, judges may find it difficult to comprehend any possible shortcomings—for instance, whether the experts have considered the possibility of the digital evidence having been manipulated at some stage of the process and how this would have been investigated.

It is not only in respect of the judges' expertise where training might be needed. The Office of the Prosecutor (OTP) could also benefit from training on the topics addressed above. The Prosecutor may also require assistance from experts in topics affecting digital evidence, such as archiving and authentication practices. As a result, any OTP Protocols may need to be updated to reflect lessons learned and any new practices employed as a result.[46] Moreover, the Registry has a mandate to operate in accordance with the accused's right to a fair trial.[47] This may require training in the existence of deepfakes and the proper authentication of digital evidence which is particularly relevant to the rights of the accused due to the ability of manipulated evidence to lead to an erroneous charge or finding of guilt.[48]

[42] Nava, *Digital Evidence Repositories*.
[43] See e.g., Koenig, *Digital and Open Source Information*; Freeman & Vazquez Llorente, *Finding the Signal in the Niose*,, 186.
[44] Freeman & Vazquez Llorente, *Finding the Signal in the Noise*, 186.
[45] Problematically, this places the admissibility, relevance and probative value decision-making away from the Court and onto the forensic experts as ICC judges are unlikely to have the required technical expertise to make this analysis themselves. See Freeman & Vazquez Llorente, *Finding the Signal in the Noise*, 186 *et seq*.
[46] D Kayyali, R. Althaibani & Y. Ng , "Digital Video Evidence, When Collected, Verified, Stored, and Deployed Properly, Presents New Opportunities for Justice", *ICC Forum* [blog post] (n.d.), https://iccforum.com/cyber-evidence#Kayyali, accessed 20 October 2023.
[47] ICC, *Rules of Procedure and Evidence* (ICC-ASP/1/3 and Corr.1), rule 20.
[48] See generally, Koenig, *Half the Truth is Often a Great Lie*.

The potential need for professional development is not a new phenomenon, and trainings are already taking place within the ICC to address a myriad of challenges facing the Court. What is important, based on the research findings underlying this report, is that before engaging in any training, the ICC first engages its stakeholders in a comprehensive review of its current management policies and procedures to identify:

- Strategically, the types of procedures that may need to change or be adjusted in light of the increased usage of digital evidence and the sophistication of technology, bearing in mind the benefits and shortcomings of digital evidence in those discussions;
- The changes that may be required to the ICCs practices and protocols in light of the increasing demand for effective yet efficient criminal proceedings and improved trial management; and
- The resources the ICC is likely to have at its disposal to make these necessary changes.

Only after these discussions have taken place can the Court and its stakeholders obtain clarity as to where it is headed and how it will address the challenges arising from digital evidence. This is especially the case in light of its ongoing work to address the challenges and recommendations identified in the Independent Expert Review of 2020.[49]

3.2 Recommendations

As mentioned above, this report emphasises that further clarity is needed in regard to how the ICC sees itself operating in this new, technological environment and what limitations it will face in ensuring effective and efficient trial management and the overall fairness of the proceedings. This includes: (1) formulating its limitations, that is, understanding what (and how) the ICC can realistically do to address the identified digital evidence challenges with the financial, technological and human resources it has at its disposal; and (2) discussing the often-mentioned lack of expertise and deciding on how the gaps will be addressed.

These discussions should culminate in a strategic plan focusing on addressing the digital evidence challenges and a roadmap towards implementing the solutions ultimately agreed on by the parties to these discussions. This strategic plan and roadmap must take into account the various challenges relating to digital evidence and the sophistication of technology, the realistic budgetary restraints and suggestions for collaborative practices and opportunities, including with technology companies.

[49] "Independent Expert Review of the International Criminal Court and the Rome Statute System: Final Report", *International Criminal Court* (30 September 2020), https://asp.icc-cpi.int/iccdocs/asp_docs/ASP19/IER-Final-Report-ENG.pdf, accessed 20 October 2023.

4 The Collection, Preservation and Verification of Digital Evidence

This section evaluates the main challenges arising from the collection, preservation and verification of digital evidence in international criminal proceedings in light of our observations from the Analytical Roadmap and the overall goals and objectives of the ICC, including ensuring that proceedings are effective, efficient and that they safeguard the rights of the accused, victims and witnesses.

4.1 Overview of the Main Challenges

The increased usage of digital evidence and the sophistication of technology is leading to the democratisation of evidence which makes it easier to create and access but which also gives rise to a number of challenges. The main challenges with the collection, preservation and verification of digital information identified in our research are as follows:

- There is an increased amount of information to be captured which is leading to over-collection, giving rise to the need for ways to prioritise and triage relevant digital information;
- The documentation period is often longer, leading to more information collected and a great need for proper preservation and storage techniques;
- Greater resources are required for, in particular, safe storage;
- There may be various access challenges (paywalls, deleted content, etc); and
- Digital evidence is more susceptible to manipulation and tampering.

There is a great variety of standards and practices that are currently being developed by different non-governmental organizations (NGOs) and stakeholders in order to systematise the collection, preservation and verification standards. Yet, there is a lack of clarity around which of the many recent guidelines and manuals[50] is the most authoritative and most able to be adapted for use in international criminal proceedings. This proliferation and confusion render it difficult to outline any sort of best practices or standards that can be used by the ICC in dealing with digital evidence in the context of criminal proceedings. Moreover, while many of the manuals and guidelines offer useful information regarding digital evidence, most of them have not been drafted with judges or prosecutors in mind and thus do not provide practical steps that should be taken to preserve or verify digital information at the evidentiary stage of international criminal proceedings. As such, they have less practical relevance to judges or other court officers when dealing with digital evidence.[51] Finally, the guidelines containing the most practical instructions are often limited in substance to one type of media or one type of crime. Their usefulness to international criminal proceedings is therefore limited by their scope.[52]

[50] See e.g., Berkeley Human Rights Center & UN OHCHR, *Berkeley Protocol*.
[51] For examples of existing relevant guidelines and manuals and an overview of the issues relating to them, see Annex 3.
[52] See e.g., WITNESS, "Activists' Guide to Archiving Video" (n.d.), https://archiving.witness.org/archive-guide/, accessed 20 October 2023, which contains a very practical and helpful chart comprising different stages of the archiving process and useful instructions on how to proceed—however, it is limited in scope to videos.

The verification of digital information gives rise to additional challenges to international criminal proceedings which include the following:

- There are more actors involved in the creation of digital information which leads to more complex and time-consuming verification processes, including in relation to source verification;
- Deepfakes, artificial intelligence and other, newer forms of sophisticated technology are giving rise to unexplored issues;
- Digital manipulation techniques are making it more difficult to establish the probative value of digital evidence; and
- There are no set standards and criteria for verification, including a lack of defined authenticity criteria.

These verification issues are exacerbated by privacy concerns and considerations as well as by certain general challenges with the disclosure process at the ICC, namely the appropriate amount of evidence that should be disclosed and in what manner. These complexities are discussed below.

4.2 The Need for Unified Practices or Standards

4.2.1 Collection, Preservation and Storage Standards

Existing collection, preservation and storage practices at the ICC may not be adequate to address the many challenges that arise in relation to digital evidence. They may need to be adjusted in light of the ICCs long-term goals and strategies with respect to trial management and ensuring the efficiency and efficacy of proceedings in the digital era, which is further discussed in Section 3 above.

Internal practices and standards may need to be updated and/or clarified, particularly those relating to victims and witnesses. For example,

> "[w]hile the current ICC witness protection protocol is comprehensive and, despite some challenges, generally succeeds in offering protections to the survivor-witnesses it engages with, it might not be enough to uphold the Rome Statute's mandate of 'protecting the safety, physical and psychological well-being, dignity and privacy of victims and witnesses' [when it comes to digital evidence] […]. While the current protection protocol for in-chambers testimony, including voice or face distortion, will probably continue to be effective for those witnesses who are providing live testimony, new policies may have to be implemented with a digital evidence repository. These potential new policies should address issues of identification/anonymization, consent, and storage."[53]

With "viral videos" or other social media posts that are shared multiple times, several individuals might be implicated,[54] and the Prosecutor will need some sort of strategy or process to determine which of these individuals are at greatest risk and whose protection needs to be prioritised. Other internal practices and standards may similarly need updating and/or clarification as well.

[53] Nava, *Digital Evidence Repositories*.
[54] See e.g., Freeman & Vazquez Llorente, *Finding the Signal in the Noise*; Nava, *Digital Evidence Repositories*.

In addition to establishing uniform guidelines for preservation, there are other challenges as well, including in relation to safe storage and data retention. Digital evidence that is not safely stored might lead to the confidentiality of victims or witnesses featured in the evidence being breached. For instance, scholars have expressed concern with the ICCs continued use of the "highly insecure and outdated digital signatures algorithm, MD5".[55] This is also where issues relating to transparency of the storage process comes in:

> "[T]he collection and storage of digital evidence does not come without concerns over individual privacy. It is unclear who would control such a repository: The ICC itself? Civil society groups? International governments? Private companies? The answer to this question would also likely dictate whether and to what extent it would be accessible to the public. Keeping it from the public could prompt criticism of a lack of transparency. On the other hand, opening it up to public viewing would increase concerns around the individual privacy of those whose likenesses or other personal information could be gathered from the media. Even if the repository is intended to be private, the likelihood that it would stay that way is questionable, as centralized storage of this sort of data could garner public attention and run the risk of being vulnerable to hacking and publication. There have already been multiple hacks of government data around the world. Whether the repository is public or private, therefore, it is possible that the identities of victims could eventually be made public."[56]

Discussions will need to be had about striking an appropriate balance between ensuring transparency of the ICCs collection and storage systems and ensuring that digital information, and personal data of victims and witnesses, are properly protected. This may involve amendments to current internal evidence storage processes and procedures. The ICC could look to practices and guidelines from digital forensics practitioners for inspiration as the challenges they raise with respect to collecting digital information and the ways to address them and mitigate errors may be particularly useful for the Prosecutor in the digital era.[57]

Additionally, the ICC may need to increase its cooperation with various organisations who capture digital information on the ground or control digital repositories of information that may be valuable to the Court. This is because the permanence and availability of content posted on social media, and any other user-generated content, is precarious as it may be removed or made private by the person who originally uploaded it.[58] Content takedowns are causing serious problems for online repositories of evidence. The *Al-Werfalli* arrest warrant was based largely on videos uploaded to Facebook and other social media evidence, but three months after they were posted the videos had been deleted from Facebook. The evidence would not exist today if it had not been downloaded and saved.[59]

[55] Quilling, *The Future of Digital Evidence*.
[56] Nava, Digital Evidence Repositories.
[57] See below, section 6.1.1.
[58] Kayyali, Althaibani, Ng, *Digital Video Evidence*.
[59] Ibid.

It is likely that the Prosecutor will need to communicate with the various organisations (and States) holding on to relevant digital information and/or controlling these digital repositories to discuss how data can be structured in a way that increases its overall value for ICC proceedings. Agreeing upon a uniform, international and practical set of standards and procedures for the collection and preservation of digital evidence has the potential to solve many of these problems.Crucially, the Prosecutor and OTP investigators will need to think more about the entire trial process, including witness and victim protection, disclosure obligations and the necessary standard of proof that will need to be met at each stage of the proceedings,[60] already at the stage of collection and preservation of digital evidence.

4.2.2 Verification Processes and Standards

It is likely that much of the digital evidence that the Prosecutor will receive will be submitted via OTPLink—the ICCs new database through which digital evidence can be submitted by individuals, States and organisations.[61] Under Article 15, to initiate an investigation, the Prosecutor shall analyse the seriousness of any information received on crimes within the jurisdiction of the Court.[62] Additionally, according to the OTPLink website, "[a]ll communications, regardless of the source, are subjected to the same assessment by the OTP, the purpose of which is to analyse and verify the seriousness of the information received, filter out information on conduct or crimes that are outside of the Court's jurisdiction and identify those that appear to fall within the jurisdiction of the Court and warrant further action."[63] The current OTPLink website, however, does not provide further information as to what criteria need to be fulfilled to verify the information and confirm that it is authentic and whether this is something that the submitting party needs to bear in mind. The standard or standards against which such criteria will be cross-checked are also not clear. More information will likely need to be provided to ensure an effective and successful verification process, especially in cases of anonymous submissions.

[60] In the preliminary stages, the ICC employs a lower standard of proof which allows it to rely on findings in human rights investigations to consider whether a criminal investigation should take place. In later stages, individual criminal responsibility must be established beyond a reasonable doubt. 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. See Cluster C Report, 16-18.

[61] "*OTP Link – FAQs*", (n.d.), https://otplink.icc-cpi.int/faqs, accessed 20 October 2023; ICC, "*ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink*" (24 May 2023), https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink, accessed 20 October 2023.

[62] ICC, *Rome Statute of the International Criminal Court* (2187 UNTS 90), art. 15(1)-(2).

[63] *OTP Link – FAQs*; ICC, *ICC Prosecutor announces launchOTPLink*.

Moreover, verifying digital information is complex. Given the increasing risks of deepfakes and AI-generated information, it is unclear to what extent the Prosecutor will need to verify the information received. For example, experts have suggested that investigators should focus on source verification at the early stages of an investigation to ensure that the information comes from well-verified sources.[64] However, the definition and scope of what is included in such a verification process needs clarifying. What standard of verification should be used? Who will have the responsibility to verify the source? When is the ideal time to do it? The source that needs verifying can comprise several individuals, including the capturer of the digital information, the creator, the uploader, the social media user or the submitter of the information to the Prosecutor[65]—thus, which source should be verified? Exactly what will need to be verified and how is an aspect that will require further discussions.

4.3 The Need to Explore Additional Challenges and Their Relation to Digital Evidence

4.3.1 Cognitive and Technological Biases

Another challenge arising from the use of digital evidence, which has the potential to impact collection, preservation and verification of digital evidence, is the issue of biases. There are inherent technical and cognitive biases in collecting, preserving and verifying digital evidence, particularly that which is found on social media. [66] As Yvonne McDermott notes:

> "Even the apparently objective act of storing information can reflect the politics, perceptions and biases of the individual investigator, through the filenames, data categories and/or tags they choose in preserving and archiving evidence. For example, a video showing violence against protestors may be stored in an archive of evidence using any of the following terms: 'police brutality'; 'disproportionate force', 'violence against protestors', 'attack', 'police suppress riot' or 'police re-establish control'. Each of those terms has its own weight and meaning and reflect the subjective views of the person storing and indexing the information. On the other hand, a dispassionate and detached description (such as, 'person falls to the ground') can be meaningless and may lead to the evidence being overlooked in later reviews."[67]

Other aspects of digital evidence involve certain biases. For example, one technical bias is the algorithmic bias which is embedded in the design of search algorithms on the Internet. This bias can impact what results users see when they conduct a search and the order in which the results are presented.[68] Cognitive biases that typically arise in the collection and analysis of digital evidence include availability bias: the tendency to base decisions or conclusions on information that can be easily accessed, anchoring: the tendency to rely too much on an initial piece of information which causes an investigator to misinterpret or disregard later conflicting information; and confirmation bias: the tendency to search for or favour information that supports one's favoured hypothesis.[69]

---

[64] Annex 1 of Cluster D Report, (Annex 6), sections 2.1.1 et seq.
[65] Freeman & Vazquez Llorente, *Finding the Signal in the Noise* .
[66] McDermott, Koenig & Murray, *Open Source Information's Blind Spot*, 89.
[67] Ibid.
[68] Ibid.
[69] Ibid.

While it might be impossible to overcome our cognitive biases completely, lack of awareness around them can severely impact the right to a fair trial. For example, humans have a tendency to value and weigh sensory information—like videos and audio—more heavily than abstract information, like numbers or statistics.[70] This bias towards video or audio evidence in Court might mean that legitimate non-video and/or audio evidence is not given as much weight, potentially impacting the accused's right to a fair trial. Indeed, these biases can lead to relevant evidence being disregarded or a certain narrative against the accused being promoted by the Prosecution if not adequately addressed.

4.3.2 Striking a Fair Balance in Disclosure

As discussed above, our research has identified certain general challenges with the disclosure process at the ICC which is likely to be exacerbated by the sheer volume of digital information that is able to be collected and stored as digital evidence. These challenges relate to:

1. *Over-disclosure*, that is, is too much information at risk of being disclosable, disrupting the Defence's ability to effectively prepare for trial and examine all the evidence against them?
2. *Over-redaction*, that is, are the privacy concerns discussed below at risk of causing the over-redaction of disclosed information, impacting the right to a public hearing and the Defence's ability to examine the sources of evidence against them?
3. *Non-disclosure*, that is, due to the possibility of content and accounts containing digital evidence being deleted as well as due to a lack of proper preservation standards, is there a risk of crucial evidence being undisclosed or undisclosable? Furthermore, if the Prosecution relies on third party reports, whose underlying information has been deleted, how can they ensure that that information is properly preserved and disclosed?

The Prosecutor of the ICC has burdensome disclosure obligations—that is something most practitioners and academics agree on. When preparing any evidence for disclosure, it is not clear which process the Prosecutor is obliged to follow. If the Prosecutor is to disclose *all* potentially relevant information, the amounts of digital documents and files that this could comprise is almost incomprehensible. If the answer to the question relates to the fairness of the accused, it is not inconceivable that disclosing vast amounts of data is likely to hamper the Defence's representation efforts rather than contribute to the fairness of the proceedings in any meaningful way. However, if not enough information is disclosed, it will also affect the fair trial rights of the accused.

[70] Ibid., 98.

For instance, if too much information is redacted due to confidentiality and safety concerns of victims and witnesses, this could affect the accused's right to examine the evidence against them and their right to a fair and public trial.[71] Additionally, the inability to disclose certain deleted information that might be relied on by way of hearsay, through a third party report, is also problematic.[72] Even if the report is not given much weight, the fact that it makes its way onto the case record could nevertheless impact the accused negatively.

More discussions are needed regarding how to strike an appropriate balance between disclosing enough but not so much as to overly burden the Defence in an era where the Prosecutor will likely be contending with mass amounts of potentially relevant digital evidence.

4.4 Recommendations

The main recommendation arising from the investigations in digital era is to strengthen the sharing of best practices towards developing clearer guidelines, manuals or standards, depending on the needs identified, to ensure that the trajectory of information into evidence, including its collection, preservation and verification, is managed appropriately and effectively.

To initiate further discussions around the needs of the Court that will assist it in developing these clearer guidelines, the report of the Independent Expert Review offers some recommendations for general improvements that could be put in place to ease the burden of disclosure and expedite the proceedings in light of the increased usage of digital evidence. This includes:

- Improving and advancing cooperation and partnerships in data collection, and ensuring that the standards for collection are unified across these partnerships to avoid a divergence in approaches;
- Thinking long-term regarding data collection and analysis, considering storage limitations, analysis process, the protection of relevant actors etc;
- Developing strategies to ensure an analysis-driven approach to avoid over- and under-collection, supporting an evidence-led rather than target-led investigation;[73]
- Strengthening internal review processes, correlated with the need to discuss what and where the ICC will see its role, in light of its overall budget, goals and mission;[74] and
- Giving priority to the cases with the strongest evidence containing limited, well-grounded and well-supported charges.[75]

[71] These privacy and safety concerns are discussed in further detail in Section 5 below.
[72] See e.g., *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé*, Decision on the submission and admission of evidence (2016) ICC-02/11-01/15, para. 13; *The Prosecutor v. Mathieu Ngudjolo Chui* (2012) ICC-01/04-02/12 (Reasons of Judge Henderson), paras. 285, 909.
[73] *Independent Expert Review*, 255, R299.
[74] Ibid., R305–310.
[75] Ibid., R231–235.

5 Procedural Guarantees: Safeguarding the Rights of Victims, Witnesses and the Accused

In all criminal proceedings, the witnesses, victims and accused need different forms of protection. Victims and witnesses could be vulnerable to threats or harm by the public or associates of the accused and may be in need of protective measures that conceal their identity, while the accused's fair trial rights, such as the presumption of innocence, need to be protected. These are the standard procedural guarantees that domestic and international criminal courts have developed good practices for. Digital evidence however brings new perspectives and also challenges to these safeguards and standards. These are addressed below.

5.1 Overview of the Main Challenges

We have identified a number of challenges that arise with respect to certain procedural guarantees from the increased usage of digital evidence and the sophistication of technology. Our analysis suggests that these main challenges, which are listed below, fall under two distinct categories of procedural guarantees: (1) protective measures for victims, witnesses and the accused and (2) the ability of the accused to understand the case (and evidence) against them.

1. *Protective measures for victims, witnesses and the accused*
    a. Digital evidence, due to the secure storage that is required, is more prone to accidental leaking of information, impacting the safety of victims and witnesses and the presumption of innocence of the accused;
    b. Digital evidence is more susceptible to manipulation. This increases the burden on the Prosecution to test the veracity of the information collected;
    c. The need for censoring, redaction and anonymisation may lead to both over- and under-granting of relevant protective measures which requires further discussions; and
    d. The use of digital evidence may give rise to increased disclosure challenges, negatively impacting the length of proceedings.[76]

2. *The ability of the accused to understand the case (and evidence) against them*
    a. Digital evidence is likely to lead to overcollection and difficulties with examining and understanding evidence;
    b. Digital evidence may suffer from issues like deleted accounts and software which makes examination difficult; and
    c. The technologically complex nature of digital evidence may make it more difficult to examine without the use of software or digital forensic experts as well as the fact that the Defence cannot cross-examine a computer system or software which may be produced as evidence by the Prosecution.

Our analysis under the sub-sections below follows this categorisation.

[76] See disclosure challenges impacting length of proceedings in *Independent Expert Review*, para. 476.

5.2 Protective Measures

5.2.1 Accidental Leaking of Digital Evidence to the Public

Ensuring the safe storage of digital evidence in a way that protects victims and witnesses will become more and more expensive and difficult if the Prosecutor has to deal with massive amounts of media and other data. Digital evidence that is not safely stored might lead to the confidentiality of victims or witnesses featured in the evidence being breached. In this regard:

> "Of great concern is the Court's continued use of the highly insecure and outdated digital signatures algorithm, MD5. The risks of weak cryptography are not well-understood by the Court at present. The consequences of a data breach, destruction, or manipulation of the Court's digital evidence would be severe."[77]

Indeed, although the possibility that victim information could be leaked to the public has always been a concern with any type of evidence, the mass scale of digital evidence and the digital repository that will be required to hold it amplifies the concern. If information were to be leaked, it could spread globally in a manner of minutes and could be seen by anyone at any time.[78] While the leaking of information primarily affects the safety of victims and witnesses, the leaking of incriminating evidence against the accused could also affect the presumption of innocence and thus the fair trial of the accused.

In this regard, the question of who would be in control of any digital repository containing massive amounts of collected, user-generated, digital evidence could impact various rights of privacy. Would the ICC control the data, or would it be some other company or organisation? Should the public have access to the data, or should it be confidential—possibly prompting criticism over a lack of transparency? If the public has access to the data, what does this mean for individuals featured in videos and images contained therein? If the repository is private, it could give rise to public attention make it at risk of hacking and leaking. Thus, regardless of the choice, the identities of victims and witnesses and information possibly affecting the presumption of innocence of the accused could be made public at some point.[79] Further discussions are therefore needed on how the ICC will address this in the future.

5.2.2 Manipulation of Digital Evidence

There is another element to digital evidence that makes it susceptible to violating the fair trial rights, including the presumption of innocence, of the accused and that is the issue of evidence manipulation. As Bobby Chesney and Danielle Citron, whose research has focused extensively on deepfakes, note:

> "Deep fakes are not just a threat to specific individuals or entities. They have the capacity to harm society in a variety of ways. Consider the following:
>
> - Fake videos could feature public officials taking bribes, displaying racism, or engaging in adultery.
> - Politicians and other government officials could appear in locations where they were not, saying or doing things that they did not.
>
> […]

[77] Quilling, *The Future of Digital Evidence*.
[78] Nava, *Digital Evidence Repositories*.
[79] Ibid.

- Soldiers could be shown murdering innocent civilians in a war zone, precipitating waves of violence and even strategic harms to a war effort.
  […]
- Falsified video appearing to show a Muslim man at a local mosque celebrating the Islamic State could stoke distrust of, or even violence against, that community.
- A fake video might portray an Israeli official doing or saying something so inflammatory as to cause riots in neighboring countries, potentially disrupting diplomatic ties or sparking a wave of violence. False audio might convincingly depict U.S. officials privately 'admitting' a plan to commit an outrage overseas, timed to disrupt an important diplomatic initiative.
  […]"[80]

All of these scenarios could shape the narrative of an international criminal investigation which could significantly impact the fair trial of an Accused.

Due to the increasing sophistication of artificial intelligence and the technology around deepfakes, there is a discussion to be had around who has the responsibility, and to what extent, to test the veracity of the information collected from open sources. This issue has come up before. In *Al-Mahdi*, "[w]hile the Prosecution made an effort to geolocate some of the opensource videos and photographs, limited forensic analysis was admitted alongside […] the Prosecution focused on ascertaining the date, time and location, but did not show concern that the images and videos may be doctored or staged. In sticking with the standard from the ICTY, without any indication of fraud, the Prosecution need not take extra steps to verify that an image has not been falsified."[81] The question is, whether the authentication methods required under the current rules of the ICC are sufficient to deal with sophisticated technology, like deepfakes? Internal procedures and standards may need to be updated to match the sophistication of manipulation technologies and deepfakes, and the burden on the Prosecutor to verify the digital information collected may need to become higher.

[80] B. Chesney & D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", *California Law Review*, 107 (December 2019), 1753, 1766, https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security.

[81] L. Freeman, "Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials",*Fordham International Law Journal*, 41/2 (2018), 283, 318, https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1/.

5.2.3 Anonymisation and Censoring of Victims and Witnesses in Digital Evidence

While witnesses have in the past expressed fears that they could be identified through court transcripts, with digital evidence that fear has extended to someone viewing a video or photograph of a victim's attack and identifying them through that.[82] The fact that victims and witnesses featured in videos and images circulating online that may ultimately end up in the court room has led to discussions around the need for anonymisation of such individuals as well as the need for court protocols currently in use at the ICC and other international criminal courts and tribunals to extent their protection to such individuals even if they are not considered "witnesses" in the strict sense of the word.[83]

The ICC may need to look at the protection of witnesses as something to be done during the collection of evidence.[84] When dealing with digital evidence, a "witness" may never engage directly with the Court. Thus, witnesses may no longer need to first be identified and then require protections from the Court—the protections may need to be in place from the start. The ICC will need to consider "how it will effectively and adequately protect an exponentially larger number of witnesses than it has ever had before and do so while possibly never being able to identify the individuals in the manner required by the current protection protocol."[85]

5.2.4 Disclosure Challenges Impacting the Length of Proceedings

As mentioned above, the sheer amount of digital evidence has the potential to significantly lengthen international criminal proceedings, especially from the disclosure stage onwards. Defence teams often struggle to review the plethora of documents disclosed. Indeed, one of the main aspects that determine the length of proceedings at the ICC is the disclosure process. The disclosure process is particularly burdensome at the ICC and is often described as a major problem. As noted by the Independent Expert Review, "dealing with disclosure has become increasingly difficult with the proliferation of material relating to events that are the subject of the Court's trials. On the other hand, the very features of our digital age which cause the proliferation of available material should be capable of being harnessed to aid the identification of what matters and what does not."[86]

---

[82] Nava, *Digital Evidence Repositories*.

[83] Ibid: "In 2017, the Office of the Prosecutor issued an arrest warrant for Libyan military commander Mahmoud Mustafa Busayf Al-Werfalli which heavily relied on open source information, specifically media that depicted several victims being shot and killed. When describing the videos in the warrant, the victims are generally referred to as 'unidentified men', while others are described as hooded or otherwise not identifiable. This is a notable weakness in the ICC's victim protection protocol going forward. An inability to identify survivors does not mean the presentation of their data in Court shields them from privacy risks. By its nature, digital evidence will mean that it should be easier to provide evidence for crimes in the Court; victims will no longer have to be individually identified and the Prosecutor will have to expend less resources, both in money and time, to gather evidence. However, the fact that the survivors are unidentified to the Court does not mean they are unidentifiable."

[84] Ibid.

[85] Ibid.

[86] *Independent Expert Review*, para. 479.

The Experts note that disclosure requires special attention and needs to be made the subject of urgent review due to it being the most significant factor in causing a delay in international criminal proceedings.[87] Indeed, "[t]he amount of witnesses and hours of testimony required to authenticate and understand the relevance and probative value of the [digital] evidence is significant, because it refutes the notion that using this type of technologically derived evidence would be more efficient than eyewitnesses."[88] Discussions will need to be had about striking the right balance between verifying information to a sufficient extent while keeping the proceedings expeditious.

5.3 Understanding the Case: The Accused's Right to Examine the Evidence

5.3.1 Overcollection of Digital Evidence

Given the vast amounts of digital data that is generated constantly on the Internet, there is a real risk of over-collection of digital information in a prosecutorial investigation.[89] Without the ability to collect just the right media from the start, investigators often collect as much media as possible in the short term, focusing on the cleaning up and tagging of any relevant documents later.[90] Volume can create a real burden for the Prosecutor and the analysts and lawyers working in the OTP, particularly in relation to their disclosure obligations. While tools currently exist that would allow the Prosecutor to collect evidence more efficiently even when confronted with large data sets, some experts suggest that they are currently not being used in the most effective ways.[91]

For example, lawyers in domestic systems have implemented various e-discovery techniques, such as metadata searches or technology-assisted review, which help identify relevant documents for disclosure.[92] However, successful use of these types of tools at the ICC will "require changes in the structure and function of the Court and the OTP beyond just the adoption of new technologies". As mentioned above, this may be prevented by a lack of resources.[93] Thus, to avoid over-collection and the consequences of it, the Prosecutor and its investigators may instead decide to exclude information. This risks the loss of important digital evidence.[94] While the ICCs new platform, OTPLink, symbolises a starting point for the adoption of new technologies to help with the collection of digital evidence, it is not yet clear whether this will solve the problems of, *inter alia,* overcollection,[95] and further discussions are needed.

---

[87] Ibid., para. 481.
[88] See Freeman, *Digital Evidence and War Crimes Prosecutions*, 313.
[89] See e.g. J. D. Aronson & E. Piracés, "The OTP and ICC Can Take Advantage of Open Source Evidence and Digital Evidence Repositories, Core Elements of Almost All Grave Crimes Investigations, if They Undertake Cultural, Procedural, and Bureaucratic Changes to Create a More Agile and Open Institutional Environment", *ICC Forum* [blog post] (n.d.), https://iccforum.com/cyber-evidence, accessed 20 October 2023.
[90] Ibid.
[91] Ibid.
[92] Freeman & Vazquez Llorente, *Finding the Signal in the Noise*,, 178.
[93] Aronson & Piracés, *The OTP and ICC*.
[94] Ibid.
[95] "Welcome to OTPLink", *International Criminal Court*, https://otplink.icc-cpi.int/, accessed 20 October 2023.

5.3.2 Deleted Accounts and Content

All digital evidence suffers from the potential of deletion, if not properly downloaded, archived and stored. For example, in a 2020 audit Human Rights Watch found that 11% of the digital content it had cited in its reports since 2007 had been deleted.[96] Digital evidence disclosed in proceedings before the ICC could be subject to the same fate, if not preserved properly.

Of course, anything which has been deleted will be very difficult to examine. While deleted evidence should not make its way into the case file, the question remains whether current safeguards are sufficient to prevent this from happening (for example in cases where the evidence the Prosecutor is relying upon is a secondary source of evidence, like a report by Human Rights Watch, and the underlying evidence has been deleted).

5.3.3 Technological Complexity of Digital Evidence

Under international human rights law, the Defence must have a "genuine opportunity to challenge evidence presented against them and to present their own evidence."[97] However, due to its technological nature, and depending on the type, some digital evidence may be too complex to understand without accompanying expert evidence, such as, for example, telecommunications experts, which have been used in the past to explain how cellular signal and cell tower sites are used to geolocate the cell phone user.[98]

The technological complexity of digital evidence means that experts are often required to decipher the technology so that judges are able to decide whether it should be admitted. It is argued by some scholars that this practice might impact fair trial rights if the judges are not equipped with understanding the various technical complexities, effectively leaving it up to the experts to guide the evidence assessment process.[99] This practice could also potentially lead to delay of proceedings in two ways: first, the complex nature of the evidence might make it more difficult for the Defence to challenge and may delay proceedings by requiring digital forensic experts to analyse the data. Second, a lack of understanding around which types of digital evidence require an expert and which can be assessed by anyone also has the potential to delay the proceedings. These are issues that need to be discussed and addressed.

---

[96] See G. Fiorella, C. Godart & N. Waters, "Digital Integrity: Exploring Digital Evidence Vulnerabilities and Mitigation Strategies for Open Source Researchers", *Journal of International Criminal Justice*, 19/1 (2021), 147, 150, https://doi.org/10.1093/jicj/mqab022.

[97] "Policy Brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters", *Fair Trials* (October 2018), 9, https://www.fairtrials.org/app/uploads/2022/02/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf, accessed 20 October 2023, ECtHR, *Barberà, Messegué and Jabardo v. Spain* (1988) Series A no. 146, para 78.

[98] See Freeman, Digital Evidence and War Crimes Prosecutions, 313.

[99] L. Freeman & R. Vazquez Llorente, "How to Prepare the International Criminal Court for our Digital Future", *Opinio Juris* [blog post] (12 October 2021), http://opiniojuris.org/2021/10/12/how-to-prepare-the-international-criminal-court-for-our-digital-future/, accessed 20 October 2023.

6 Specific Challenges that Further Impact Procedural Guarantees

6.1 Avoiding or Minimising the Effect of Unexplored Biases on Judicial Proceedings

Section 4 above discusses the existence of various unexplored cognitive and technological biases that may arise in the context of digital evidence in various stages of the judicial proceedings. The purpose of this section is to highlight the need to consider other disciplines, such as digital forensic science, to discuss and address these "unexplored" biases, to avoid or minimise errors, inconsistencies or wrong interpretations in the context of the judicial proceedings.

As mentioned elsewhere in this report, digital evidence, due to its technological and often complex nature, tends to require some form of analysis by digital forensics experts. These persons are susceptible to the same technological and cognitive biases as discussed above. Digital forensics experts may be biased by contextual information and produce inconsistent results.[100] This may therefore impact the judicial proceedings in a number of ways. This is important to discuss because it correlates strongly with the question of when and how authentication and verification of a piece of evidence should take place to ensure that a charge is accurate and that the underlying evidence is reliable. There is a need to understand the end goal in order to discuss how procedures will need to be amended and adapted: to what extent and how should digital evidence be authenticated and verified and when should this take place? Any digital forensics experts working with the Court will need clear instructions on what is required of them, and of the criminal adjudication process, with regard to verification and authentication of the digital evidence. For instance, digital forensics examiners may need to be told to provide their methodologies on how they have verified that a piece of evidence has not been manipulated rather than simply stating that it is authentic.

It is also important to discuss these digital forensic biases to better understand the role of the Prosecution, Defence and the judges when it comes to understanding the uncertainties in forensic analysis clearly, including biases. The ICC will need to discuss how to strike a balance between the organs of the Court having sufficient awareness of these types of biases while ensuring that the Court operates within its means and mandate.[101]

[100] N. Sunde, "Unpacking the Evidence Elasticity of Digital Traces", *Cogent Social Sciences* 8/1 (2022), 1.

[101] See e.g., the opinion of Aronson & Piracés, *The OTP and ICC*: "The Court and the OTP cannot be expected to become a scientific institution or employ experts in all relevant emerging technologies. The Court could learn from the experience of other communities of practice where practitioners often find solutions by relying on trusted networks with specialized organizations. The Court should, as much as possible, distribute these connections and knowledge widely across the institution so that no one unit becomes the gatekeeper to accessing technology."

6.1.1 Digital Forensic Strategies for Safeguarding Examiner Objectivity

Nina Sunde has analysed digital forensics strategies for verifying digital evidence and safeguarding examiner (reviewer) objectivity which may arise in the collection process of digital evidence and may be considered by the ICC Prosecutor when analysing evidence submitted by way of Article 15 communications. Her findings indicate that digital evidence is prone to both technical and non-technical errors. Technical errors include system or processing errors and programming flaws. Non-technical errors include the existence of irrelevant, contextual information accompanying the relevant digital evidence which may give rise to biased observations when analysing the evidence.[102] These errors are a natural and unavoidable part of any process involving human decision-making, but error mitigation is key to prevent miscarriages of justice.[103] Sunde recommends that anyone dealing with digital evidence should implement effective investigative strategies to manage contextual information, maintain examiner objectivity and control evidence credibility.[104]

Regarding the management of contextual information, it is often impossible to keep this type of information away from the person examining the evidence. In the context of the ICC it may form part of the Article 15 communications submitted to the OTP, or it may be intertwined with the relevant evidence in a user-generated social media post. Where an electronic device is being reviewed for digital evidence, there might be a vast amount of irrelevant information, such as web search history and images, which may bias the examiner's observations.[105] The first step is thus identifying what is relevant and what is irrelevant.[106] To maintain examiner objectivity once the information is being reviewed, some digital forensics practitioners have implemented strategies to focus only on the facts by collating and reviewing the necessary artefacts in isolation from the case background and any other information and actively avoiding looking for guilt. Although there are many ways examiner objectivity could be safeguarded, for instance through different internal processes that filter out irrelevant contextual information before it is provided to the individuals in charge of examining and making decisions regarding the evidence, it is clear that the discussion needs to be had at the ICC and a choice made.

Regarding verifying the evidence to ensure its reliability, the most frequently used tool for digital forensics practitioners has been dual tool verification: using two different tools to examine the data and checking for variations in the tools' interpretations. Where the conclusions by the tools are the same, the evidence is likely to be valid and reliable. This technique is recommended by many guidelines and standards, including Interpol.[107]

---

[102] N. Sunde, "Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations", *Forensic Science International: Digital Investigation*, 40 (2022), 1, https://doi.org/10.1016/j.fsidi.2021.301317.
[103] Ibid.
[104] Ibid., 2.
[105] Ibid., 3.
[106] Ibid., 2–3.
[107] Ibid., 6 and accompanying footnotes. Note, however, in ibid, that "[u]sing two tools that share libraries, engines or methods may, in the worst-case, result in a similar but flawed interpretation of the same data and create an illusion of valid results. These limitations imply that although using 'dual tool' verification may seem straightforward, knowing which tools to use and evaluating the strength of the result requires more advanced knowledge and skills. Accurate documentation of which tools were used to verify results is thus crucial for the transparency and evaluation of the result's credibility."

6.1.2 Implication of Unexplored Biases on Judicial Proceedings

While there is considerable scholarship on the danger of cognitive and technological biases in collecting and preserving digital information, as well as on the reliance on such information, what is lacking is more in-depth understanding of the biases that are particularly at risk of arising in the judicial proceedings in the context of digital evidence, especially with regard to newer forms of sophisticated technology (such as deepfakes).

In this regard, it is clear from the sections above that cognitive and technological biases arise in the investigation phase, both in the collection and preservation of digital evidence by the Prosecutor and verifying and authenticating it through digital forensics experts. This may impact the judicial proceedings and court practices in a plethora of ways. For example, who should carry out the verification and authentication of the evidence? Is the burden on the Prosecutor to do so, and to what standard should it be carried out? What methodologies should the digital forensics experts use, and can these be questioned? How can judges know that a piece of evidence has been adequately verified by an expert?

For instance, "In the legal domain several issues with unreliable forensic evidence are reported and discussed at length. Several reports have concluded that false confessions and unreliable forensic science evidence are factors in wrongful convictions."[108] Moreover, judges are consistently provided insufficient guidance on how they should determine evidence reliability, which is why digital forensics investigations have been considered as a threat to the presumption of innocence, with a risk that they rather function based on a data-driven presumption of guilt.[109] To avoid these biases there is a need for quality management, which may again require resources that the Court does not have.

The findings above necessitate further discussion around how court practices and procedures should be amended. Addressing the possible errors arising from the biases requires a multi-faceted approach, involving awareness, education, standardisation and quality management, and interaction between these processes is important.[110] Therefore, specific discussions need to be had around:

- The implications that these biases will have on court practices and how standardisation and other quality management systems could assist with filtering out task-irrelevant contextual information in the review of digital evidence;
- How we can ensure that the methodology for verification applied by digital forensics experts is clear to the judges, within their competence, allowing for judicially sound decision-making; and
- The vitality of implementing systems or measures for error mitigation. There needs to be an increasing look at digital forensic-related writing on how a system of control or peer review could look like at the ICC.

[108] R. Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence", *Computer Law & Security Review*, 42 (2021), 1, 10, https://doi.org/10.1016/j.clsr.2021.105575.
[109] Ibid., 9.
[110] See generally, Sunde, *Strategies for safeguarding examiner objectivity*.

7 Evaluating Digital Evidence

Our findings on the challenges arising from the admissibility and the determination of weight of digital evidence are comprehensively set out in our Cluster C Report and its accompanying Annex 2, both of which are contained in Annex 5 of this report. The below section will evaluate some of these challenges in light of our observations from the Analytical Roadmap and the overall goals and objectives of the ICC, bearing in mind the need to ensure that proceedings are effective, efficient and safeguard the rights of the accused, victims and witnesses.

7.1 Overview of the Main Challenges

The main concerns that arise from the evaluation of evidence at the ICC and which are likely to become more challenging with the increased usage of digital evidence and the sophistication of technology can be summarised as follows:

- Need for greater transparency or clarity around what is required for an item to be considered sufficiently relevant and of sufficient probative value;
- Need for earlier establishment of authenticity of an item of evidence, both as an elimination tool before the trial to filter out weak evidence and to ensure application of the "best evidence" rule;
- Need for clearer verification standards, especially with regard to who bears the burden and responsibility of authenticating evidence, which methodologies are most appropriate to use and how verification should be used to mitigate potential biases; and
- Need for greater clarity around the convoluted terminology or mixed application of the factors used by judges in assessing and evaluating evidence.

These challenges affect the following fair trial rights that need to be taken into account in any discussions and future potential solutions, and they are addressed in more detail below. There needs to be:

1. Adequate opportunity to challenge evidence, including transparency in the disclosure process and access to information;
2. Time and facilities to prepare the Defence and ensuring equality of arms;
3. The provision of a reasoned judgment with transparent admissibility and weight criteria;
4. Precise and accurate investigation techniques, including applicability of the "best evidence" rule and a high standard of authentication of any submitted evidence; and
5. Protection against a reversal of the burden of proof.

7.2 Admissibility and Weight

7.2.1 The Role of the Pre-Trial Chamber

The role of the Pre-Trial Chamber in assessing the admissibility of evidence is closely linked to the standard of proof applied at the various stages of the proceedings that fall under the responsibility of the Pre-Trial Chamber. The Pre-Trial Chamber is required to determine whether there is a "reasonable basis" to proceed with an investigation and whether a case falls within the jurisdiction of the Court.[111] The Pre-Trial Chamber shall then issue a warrant of arrest if it is satisfied that there are "reasonable grounds" to believe that the person has committed a crime within the jurisdiction of the Court. To so determine, the Chamber must examine the Prosecutor's application and the evidence or other information submitted.[112]

Articles 61(5)-(6) of the RS provide that, at the confirmation of charges hearing, the Prosecutor shall support each charge with "sufficient evidence" to establish "substantial grounds to believe" that the charged person committed the crime, and the charged person may object to those charges or challenge the evidence presented by the Prosecutor.[113] Article 61(7) then provides that the Pre-Trial Chambe shall, on the basis of the hearing, determine whether there is sufficient evidence to establish the substantial grounds to believe that the person committed each of the crimes, confirm those charges and commit the person to the Trial Chamber for trial.[114]

While not expressly provided in Article 61(7), this determination of the Pre-Trial Chamber necessitates some level of assessment of the evidence presented by the Prosecutor. However, as confirmed by the Pre-Trial Chamber in its decision on the confirmation of the charges in *Mbarushimana*:

> "The Chamber will refrain from entering into an assessment pursuant to article 69(4) of the Statute as to the admissibility of each item of evidence submitted for the purposes of the confirmation hearing, in the absence of a challenge in this regard from either of the parties. This approach is consistent with the evidentiary rules applicable to and the scope of the evidentiary analysis undertaken at the pre-trial stage of proceedings."[115]

The Pre-Trial Chamber noted that this approach is justified by the "limited object and purpose" of the confirmation hearing, which is to separate those cases which should go to trial from those which should not. The purpose is not to determine the guilt or innocence of the suspect and undertaking a "wholesale assessment" of the admissibility of each item of evidence at that stage would unduly delay the proceedings, which would be incompatible with the fair trail rights of the suspect.[116] Nevertheless, the Pre-Trial Chamber underlined that this did not mean that all evidence that is not "incredible on its face" would be accepted or that the Defence would not have a chance to challenge the evidence brought by the Prosecutor.[117]

---

[111] Cluster C Report, 16.
[112] Ibid., 17.
[113] ICC, *Rome Statute*, article 61(5)-(6).
[114] ICC, *Rome Statute*, article 61(7)(a)-(b).
[115] *The Prosecutor v. Callixte Mbarushimana*, Decision on the confirmation of the charges (2011) ICC-01/04-01/10-465-Red, para. 43.
[116] Ibid., para. 44.
[117] Ibid., paras. 45–46.

Rather,

> "[…] the introduction of conflicting evidence by the Defence necessarily engages the Chamber in an assessment of the credibility and weight of this evidence in light of the whole of the evidence submitted for the purposes of the confirmation hearing […] Accordingly, and consistent with the approach adopted in other cases, the Chamber will assess the intrinsic coherence of each item of evidence in light of the whole of the evidence submitted for the purposes of the confirmation hearing."[118]

Thus, rather than assessing the admissibility of each item of evidence at the confirmation of charges hearing, the Pre-Trial Chamber's role is to assess the "intrinsic coherence" of each such item *in light of the whole of the evidence submitted* for the purposes of the hearing.

According to the report of the Independent Expert Review, the confirmation of charges hearing should serve as a filter for inadequately supported charges to safeguard the fair trial rights of the accused.[119] However, given the lower standard of proof applied at the confirmation of charges stage, and the limited role of the Pre-Trial Chamber in assessing evidence at that stage, evidence that has not been sufficiently verified and authenticated may nevertheless make its way onto the case record through its admission by the Pre-Trial Chamber. This is particularly concerning as at least one Trial Chamber of the ICC has held that the Trial Chamber will only depart from a ruling of the Pre-Trial Chamber if there are compelling reasons to do so.[120] Discussions need to be had about how best to preserve the function of the Pre-Trial Chamber as a gatekeeper of evidence in light of the verification challenges that arise with digital evidence and whether the current approach to evidence assessment at the Pre-Trial stage may need to change.

7.2.2 Approaches of the Trial Chamber

As noted in our Cluster C Report and its accompanying Annex 2, there is not much guidance provided to the judges on how specifically to approach the evaluation of evidence at the ICC (including the admissibility of evidence), and the discretion afforded to judges in this regard is significant. While the discretion afforded to judges at the ICC is similar to that afforded to judges at other international and internationalised tribunals,[121] the judicial discretion at the ICC has led to a divergence of approaches, now commonly known as the "submission" and the "admission" approaches.

In the admission approach, the Trial Chamber assesses the relevance, probative value and prejudice that the admission of a piece of evidence may cause to the fairness of the proceedings or the rights of the accused on a *prima facie* basis.[122] Once the relevance and probative value has been confirmed to outweigh any potential prejudice, and following the review of any admissibility challenges by the parties, the item of evidence is admitted onto the

---

[118] Ibid., paras. 46–47.
[119] *Independent Expert Review*, R191.
[120] See *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui*, Order concerning the presentation of incriminating evidence and the E-Court Protocol (2009) ICC-01/04-01/07, para. 34: "[T]he Chamber cannot simply ignore the decisions by the Pre-Trial Chamber, considering that the latter is bound to apply the same criteria as the Chamber in evaluating the relevance and admissibility of evidence. Accordingly, even though the Chamber is not bound by any evidentiary rulings made by the Pre-Trial Chamber, the Chamber will only depart from a previous ruling on a challenge to the admissibility of a particular item of evidence where there are compelling reasons to do so."
[121] See e.g., ICTY, *The Prosecutor v. Popovic et al*, Appeals Judgment (2015) IT-05-88-A, para. 131; ICTR, *Prosecutor v Ndahimana*, Appeal Judgment (2013) ICTR-01-68-A, para. 45.
[122] See Cluster C Report, Annex, 5–6.

case record (unless deemed inadmissible).[123] The relevance and probative value of each piece of evidence is then assessed by the Trial Chamber in light of the totality of the evidence, on the record at the end of the proceedings, when the Trial Chamber is deciding what weight to afford each item.

While the admission approach involves an assessment of the relevance and probative value of evidence at the time of admission, this admissibility assessment is on a *prima facie* basis, meaning that the threshold for its admissibility is lower compared to the assessment taking place at the end of the trial. During the *prima facie* review, each item of evidence that a party is seeking to admit is considered independently from the rest of the evidence submitted. The totality of the evidence is subsequently evaluated in the final stage of the trial, when the Chamber decides which facts or allegations are supported by the evidence on the record, what weight it should ascribe to each piece of evidence and whether it will rely on that piece of evidence for the purpose of its final determination of the guilt or innocence of the accused.[124]

In the submission approach, which now seems to be the preferred approach adopted by the judges,[125] the Trial Chamber formally acknowledges the submission of an item of evidence without ruling on its relevance, probative value or potential prejudice. When each of the parties to the trial proceedings make their case, they will seek to prove that the evidence they submitted to the case record is relevant and of sufficient probative value to be relied on by the Chamber. These criteria are then evaluated by the Trial Chamber at the end of the trial, when the Chamber is deciding what weight should be afforded to each piece of evidence in light of all the other evidence on the record, to establish the guilt or innocence of the accused.[126] As such, the admissibility and weight assessment takes place at the same time.[127]

[123] Ibid.

[124] Ibid., 7–8. During the admissibility assessment, an item's relevance and probative value is considered on a preliminary basis and then assessed "more accurately" in light of the entirety of the evidence submitted. See *The Prosecutor v. Dominic Ongwen*, Trial Judgment (2021) ICC-02/04-01/15, para. 239, 244. See also Bemba Gombo Decision on Admissibility, para. 18: "[A]ny factual analysis undertaken […] is preliminary in nature and has been performed for the limited purpose for the Chamber's admissibility determination. It does not in any way predetermine the eventual assessment of the evidence or the weight to be afforded to it."

[125] In November 2021, the ICC judges agreed to use the submission approach for all documentary, digital and physical evidence to "facilitate consistency and predictability amongst the various trial chambers in terms of the actual proceedings". The decision was a response to the recommendations contained in the final report of the Independent Expert Review of the ICC and Rome Statute System, in which the experts commented that the "inconsistent approaches adopted by different Chambers were said to be causing confusion and uncertainty among counsel". See "ICC judges agree on reforms in response to Independent Expert Review at annual retreat", *ICC* (22 November 2021), https://www.icc-cpi.int/news/icc-judges-agree-reforms-response-independent-expert-review-annual-retreat, accessed 20 October 2023; *Independent Expert Review*.

[126] Cluster C Report, Annex, 5, *The Prosecutor v. Bemba et al*., Trial Judgment (2016) ICC-01/05-01/13, para. 192. See also *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé*, Decision on the submission and admission of evidence (2016) ICC-02/11-01/15, para. 13; *The Prosecutor v. Dominic Ongwen*, Trial Judgment (2021) ICC-02/04-01/15, para. 234.

[127] Cluster C Report, Annex, 5.

Regardless of which approach is used, there are a number of specific concerns with regard to fair trial rights, clarity and transparency of procedures. First, there is a lack of clarity and transparency around the criteria used to assess the admissibility and weight of evidence at the ICC, including as to whether there is any difference in the applicable criteria between the two assessments. Where the submission approach is used, case law suggests an insufficient discussion regarding the relevance and probative value of each individual piece of evidence,[128] as the evidence is rather evaluated as a whole at the end of proceedings.

7.2.3 Terminology Challenges

As mentioned above and in our Cluster C Report and its Annex 2, one of the main challenges with understanding the criteria and factors used by the judges in determining admissibility and weight is the confusion, or convolution, of the relevant terminology.

For instance, the terms “reliability” and “credibility” are often referred to as the main factors for assessing the probative value of witness testimony, while “reliability” and “authenticity” are often used to assess the probative value of documentary evidence. However, these terms do get confused and are used interchangeably.[129] While efforts have been made by some judges to explain the meaning behind each of these terms, these explanations also differ from judge to judge[130] and despite these explanations, the words are applied differently in different contexts.

Even if they are not used interchangeably, the terms are closely linked. For a piece of evidence to be reliable, it must be authentic. Authenticity is therefore sometimes viewed as a factor for determining the reliability of an item of evidence.[131]

Additionally, the term “reliability” appears to have two meanings, depending on in which context it is used. When considered in the context of assessing probative value, it is often convoluted with the terms “credibility” or “authenticity” of a piece of evidence. However, the Chamber also uses the term differently in the determination of weight, when concluding whether the piece of evidence is of sufficient weight that it can be “relied” on. In that context, reliability of a piece of evidence means that it is strong enough and has sufficient weight to prove the innocence or guilt of the accused.[132]

This confusion around terminology does not assist with safeguarding the rights of the Defence to adequately challenge the evidence against them as it will be difficult to understand what the criteria are for determining that a piece of evidence is “reliable” in each of the different contexts.

---

[128] Cluster C Report, 4 and accompanying footnotes.
[129] See e.g., Cluster C Report, Annex, 7, 10. See also e.g., *The Prosecutor v. Bosco Ntaganda*, Trial Judgment (2019) ICC-01/04-02/06, para. 50; *The Prosecutor v. Thomas Lubanga Dyilo*, Trial Judgment (2012) ICC-01/04-01/06, para. 94; *The Prosecutor v. Mathieu Ngudjolo Chui*, Trial Judgment (2012) ICC-01/04-02/12, paras. 45–46; *The Prosecutor v. Jean-Pierre Bemba Gombo*, Trial Judgment (2016) ICC-01/05-01/08, para. 225; *The Prosecutor v. Germain Katanga*, Trial Judgment (2014) ICC-01/04-01/07, paras. 79–80.
[130] See cases cited in Cluster C Report, Annex, sections 6.2–6.4.
[131] See e.g. *The Prosecutor v. Bemba et al*., Trial Judgment (2016) ICC-01/05-01/13, para. 208; *The Prosecutor v. Jean-Pierre Bemba Gombo*, Trial Judgment (2016) ICC-01/05-01/08, para. 237; *The Prosecutor v. Germain Katanga*, Trial Judgment (2014) ICC-01/04-01/07, para. 91, describing authenticity factors as “indicia of reliability”.
[132] See e.g., *The Prosecutor v. Jean-Pierre Bemba Gombo*, Trial Judgment (2016) ICC-01/05-01/08, paras. 301, 355-356.

7.2.4 Understanding the Scope of Potential Biases

As mentioned in Section 6 above, there are a wide range of potential technological and cognitive biases that may affect the judicial process in different ways, including in the verification techniques applied by digital forensics experts. While the above section explains the various mitigation measures that should be undertaken to limit the effect these biases can have on the proceedings, judges need to be aware of the strengths and weaknesses of digital evidence and the specific biases that arise in relation to that type of evidence, in both the collection and analysis phase. This is particularly so with evidence that relates directly to the acts and conduct of the accused.

An early, robust verification of the authenticity of evidence at the Pre-Trial Stage may help prevent the occurrence of some of the potential biases and other challenges that can arise later down the line. During such an early assessment, it is envisaged that the party tendering the evidence would be required to substantiate the specific techniques used by any digital forensics experts to verify the evidence they are seeking to tender, including through the use of dual verification tools as discussed above. However, discussions need to be had about how this assessment would be carried out while still honouring the role of the Pre-Trial Chamber and ensuring that proceedings remain efficient and expeditious.

7.2.5 Burden of Proof Challenges

Under article 69(4) of the RS, the Trial Chamber has the freedom to rule on the relevance or admissibility of any evidence, taking into account the probative value of the evidence and any prejudice that it may cause to a fair trial.[133] There is a general requirement during trial proceedings at the ICC that the submitting party bears the burden of proof to ensure that authenticating data is submitted, which can verify documentary evidence.[134] When it comes to videos, photos and other similar digital evidence, the current rules on verification require that the submitting party include information on source, originality and integrity, date, location and that the entire evidence, rather than excerpts of the evidence, is submitted.[135] However, "without any indication of fraud, the Prosecution need not take extra steps to verify that an image has not been falsified."[136] Trial judges in the *Al Hassan* case confirmed that in the context of a determination on the admissibility under article 69(4) of the RS, "*if a challenge* is made to the admissibility of the evidence, the burden [to prove that the evidence is admissible] rests with the party seeking to introduce the evidence."[137] This suggests that if a challenge is not made, the evidence is assumed admissible. This corresponds with the finding of the Trial Chamber in *Katanga and Ngudjolo Chui*, where the Chamber confirmed that unless an item of evidence was "self-authenticating" or the parties "agree that it is authentic", the party

[133] ICC, *Rome Statute*, article 69(4).
[134] Cluster C Report, 28, *The Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, Decision on the Prosecutor's Bar Table Motions (2010) ICC-01/04-01/07-2635.
[135] Cluster C Report, 28, *The Prosecutor v. Jean-Pierre Bemba Gombo*, Public Redacted Version of "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" of 6 September 2012 (2012) ICC-01/05-01/08-2299-Red, paras 83, 120, 122; *Prosecutor v. Dominic Ongwen*, Trial Judgment (2021) ICC-02/04-01/15-1762-Red, fn. 4440 and fn. 4622; *Prosecutor v. Bosco Ntaganda*, Trial Judgment (2019) ICC-01/04-02/06-2359, paras 281–282.
[136] Freeman, Digital Evidence and War Crimes Prosecutions, 318.
[137] *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohammed Ag Mahmoud*, Decision on requests related to the Submission into Evidence of Mr. Al Hassan's Statements (2021) ICC-01/12-01/18-1475, para. 36.

tendering the item had the burden of demonstrating the item's authenticity.[138] However, given the sophistication of technology and the high susceptibility to manipulation of digital evidence today, it is difficult to see how digital evidence can ever be "self-authenticating" or how the parties can agree to an item's authenticity without the Prosecution having verified its evidence and thus fulfilled the burden of proving that the evidence is authentic.

The Defence may thus be required to show that there is an indication of fraud to a particular piece of evidence for it to be sufficiently verified. This may become increasingly problematic when it comes to digital evidence and sophisticated technology because its high susceptibility to manipulation through AI and deepfakes may mean that manipulated evidence becomes admitted onto the case record without having been properly verified. For instance, in *Al Mahdi*:

> "While the Prosecution made an effort to geolocate some of the open source videos and photographs, limited forensic analysis was admitted alongside […] the Prosecution focused on ascertaining the date, time and location, but did not show concern that the images and videos may be doctored or staged [...]"[139]

In the second *Al-Werfalli* arrest warrant, the Prosecution submitted an expert report concluding that a video had "no traces of forgery or manipulation", which the Pre-Trial Chamber considered sufficient to conclude that the video was authentic.[140] This raises questions as to what extent judges need to question the authentication methods of forensic experts.[141]

---

[138] *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, Decision on the Prosecutor's Bar Table Motions (2010) ICC-01/04-01/07-2635, paras. 22–23.

[139] Freeman, Digital Evidence and War Crimes Prosecutions, 318.

[140] *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Second Warrant of Arrest (2018) ICC-01/11-01/17-13, para. 18.

[141] In this regard, the "Daubert Standard", originating from domestic U.S. Supreme Court practice, which allows a court to act as a "gatekeeper" of any forensic expert report accompanying scientific evidence may be of relevance to the ICC and how it decides to verify digital evidence in the future. The Daubert Standard allows a court to scrutinise a scientific expert's methodology and the underlying scientific principles on which the expert has relied. It requires the Court to consider the following factors: (1) Whether the technique or theory in question can be and has been tested; (2) Whether it has been subjected to publication and peer review; (3) Its known or potential error rate; (4) The existence and maintenance of standards controlling its operation; and (5) Whether it has attracted widespread acceptance within a relevant scientific community. The Daubert Standard is just one example of approaches the ICC could adopt for stricter verification. There may be more options to gather from domestic jurisprudence and practice. See "Daubert Standard", *Cornell Law School Wex* (n.d.), https://www.law.cornell.edu/wex/daubert_standard, accessed 20 October 2023. See also Quilling, *The Future of Digital Evidence*: "[Caroline Foster] argues that judges should engage with scientific concepts, embrace scientific uncertainty, and adjust the way they apply the rules of burden of proof beyond a reasonable doubt to accommodate inherently uncertain scientific issues. This approach has a clear advantage of increasing the literacy of judges in basic aspects of science or technology […] Applying Foster's logic to digital evidence authenticity, Lindsey Freeman points out that 'the ability of the Judges to exercise their adjudication power will increasingly depend on their capacity to interrogate technology systems, enhance their familiarity with digital evidence, and increase their understanding of new sources of information'. Increasing judges' capacity to understand and interrogate digital evidence would require some form of continuing judicial education, something that has not gained widespread support among ICC judges […] Caroline Foster's approach would require judges to modify their standard for burden of proof and accept a level of technological uncertainty. Such an accommodation of doubt also has its dangers. ICC judges would benefit from an increased understanding of the basic concepts of the technologies or scientific processes they are charged with evaluating. However, altering the standard of proof raises questions of how much uncertainty is acceptable, and whether this uncertainty still complies with Article 66(3) of the Rome Statute that requires guilt beyond a reasonable doubt."

The question remains whether the authentication methods required of the Prosecutor, and indeed of the judges, under the current rules of the ICC are sufficient to deal with sophisticated technology that is increasingly susceptible to manipulation. Simply submitting screenshots from social media into the case record may not be enough for the Prosecution to prove their authenticity. On collecting the evidence, the Prosecutor may need to consider how the data should be captured and preserved in terms of its technical, intellectual, structural or aesthetic characteristics to ensure its accessibility, usability, interpretability and authenticity for the Court.[142]

In circumstances where digital evidence is in effect presumed authentic unless objected to, this may place an undue burden on the Defence to prove that images or videos submitted have not been manipulated which will take time, resources and indeed technological resources that the Defence may not have access to adequate time and facilities to examine the disclosed evidence and prepare for trial, thus possibly conflicting with the rights of the accused under articles 64 and 67.[143]

7.2.6 The Development of Exclusionary Rules

Under the relevant rules, evidence can be excluded or found inadmissible where the Chambers have determined that one of two conditions have been met: (i) a human rights violation casts substantial doubt on the reliability of the evidence, or (ii) the integrity of the proceedings would be seriously damaged.[144] If those conditions are not met, exclusions can be made following the application of a party, on the Chamber's motion or as part of the general admissibility determinations made by the Chambers, but the rules do not contain any further specific criteria for such exclusions.

The findings above, which derive from our Cluster C Report, indicate that there might be a greater need for the development of more exclusionary rules that are clear and transparent. While the practice of evaluating evidence, assessing its admissibility and determining its weight is clearly within the discretion of the Chamber judges, the process should be clearly set out to conform to the requirement of a "reasoned" judgment[145] so that the parties are able to adequately follow that reasoning. Additionally, clearer standards and procedures need to be developed when it comes to verifying evidence and how this is approached. Similar concerns have been expressed in relation to other international tribunals that can be applied to the ICC as well.

[142] Kayyali, Althaibani, Ng, *Digital Video Evidence*.
[143] ICC, *Rome Statute*, article 64(3)(c), 67(1)(b), 67(1)(e).
[144] ICC, *Rome Statute*, article 69(7). See also Cluster C Report, 45 *et seq*.
[145] ICC, *Rome Statute*, article 74(5).

As noted by Joelle Vuille et al. in the context of the European Court of Human Rights:

> "[T]he limited rules [for examining evidence] are insufficient to guarantee that scientific evidence that is unreliable, misleading or whose probative value has been exaggerated can be challenged effectively by the defence if they wish to do so. Indeed, even if the domestic proceedings are structured in a way that ensures equality of arms, if the defence has a right to participate in the examination of the expert, if all favourable evidence has been disclosed to the defence and if the defence has the legal opportunity to challenge experts and call experts of their own, there is still a nonnegligible risk that the scientific evidence brought against the accused will not be critically evaluated in the context of the case."[146]

The scholars contend that the main reason for this is variations in forensic expert techniques and methods that are inadequately reported and often difficult for attorneys and judges to understand.[147] The ICC and its stakeholders need to consider how evidence, particularly in this digital era, will be deemed inadmissible and excluded from the case record and how its weight will be determined. There needs to be adequate consideration for the protection of the presumption of innocence and the protection against cognitive and technical biases that arise in the collection and analysis process.

Stronger exclusionary rules, and clearer criteria for exclusion, are one way to ensure the fairness of the proceedings, in particular to ensure that the burden does not lie solely on the Defence to raise objections as to the verification process and factual accuracy of the evidence gathered by the Prosecutor. This burden should rest on the Prosecutor from the beginning, which may require stricter verification methods and clearer proof of verification submitted together with any digital evidence. Future discussions should be focused on ensuring how the burden of proof can remain with the submitting party, including discussions around whether an item of digital evidence can ever be "self-authenticating", and the extent to which forensic expert reports guaranteeing an item's authenticity can be accepted without further investigation into the methods of the experts. More specificity around the admissibility (vs the weight) criteria is likely to be required in the digital era.

[146] J. Vuille, L. Lupària & F. Taroni , "Scientific evidence and the right to a fair trial under Article 6 ECHR", *Law, Probability and Risk*, 16/1 (2017), 55, 57, https://doi.org/10.1093/lpr/mgx001. See also discussion around developing forensic standards in Sections 4 and 5 above.
[147] Vuille, Lupària & Taroni, *Scientific evidence*.

7.3 Challenges Arising from Unverifiable Sources

The challenges arising from unverifiable sources and how they affect current corroboration practices of the ICC (including how these practices may need to be addressed or discussed in light of the increased usage of digital evidence) are also important to raise.

Pursuant to Rule 63(4), there is no strict requirement that a piece of evidence has to be corroborated by other evidence for the Court to be able to rely on it and establish a specific fact. Corroboration tends to be used where there are issues with the reliability or especially credibility of a witness or piece of evidence.[148] Statements constituting anonymous hearsay can be also relied on by the Chambers, although the weight afforded to this type of evidence seems to be determined on a case by case basis, with factors such as the consistency of the information, the reliability of the source and the opportunity for the Defence to challenge the source taken into account.[149]

For instance, in the case of *Gbagbo and Blé Goudé*, Judge Henderson stated 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."[150] Thus in this case, it was stated that two weak pieces of evidence cannot corroborate each other to increase the strength of their combined evidence.[151] Considering the novel challenges that digital evidence brings, the question remains whether statements or evidence from unverifiable sources, which constitute anonymous hearsay, could qualify for direct exclusion of evidence from the trial proceedings. If not, it needs to be considered whether appropriate safeguards are in place to ensure that such statements or evidence do not prejudice the trial proceedings.

There may also be instances where other types of evidence, like United Nations (UN) and NGO reports, rely on unverified sources from social media, and there is a question around to what extent these reports can be relied on. In the past, they have not been considered strong enough on their own to prove a certain fact or allegation but have been used to corroborate other stronger evidence, like witness testimony.[152] But even using reports like these for corroboration can be problematic in an era of sophisticated technology. For instance, where a third-party report from an NGO is based on deleted accounts, as discussed above,[153] or where such a report has inadvertently relied on deepfakes or other manipulated open-source evidence, the question arises when and whether judges of the ICC should need to review the underlying information relied on in the third-party report before it can even be used as corroborating evidence.

[148] *The Prosecutor v. Bemba et al*., Trial Judgment (2016) ICC-01/05-01/13, para. 204.
[149] *The Prosecutor v. Callixte Mbarushimana*, Decision on the confirmation of the charges (2011) ICC-01/04-01/10-465-Red, para. 49; *The Prosecutor v, Germain Katanga*, Decision on the Confirmation of Charges (2008) ICC-01/04-01/07, para. 141.
[150] *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé*, Reasons of Judge Geoffrey Henderson (2019) ICC-02/11-01/15, paras. 47–49.
[151] Ibid., paras. 47–49.
[152] *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé*, Dissenting Opinion of Judge Herrera Carbuccia (2019) ICC-02/11-01/15, para. 31.
[153] See Fiorella, Godart & Waters, *Digital Integrity*, 150.

In situations where there is no corroborating evidence or where the judges decide no corroborating evidence is required due to the perceived strength of the evidence, the Trial Chamber will need to be particularly mindful of the existence of deepfakes and other sophisticated technology, as well as any relevant cognitive biases that may arise in the judicial proceedings. For instance, it will need to be mindful of the conclusions it draws from digital evidence such as videos, given the human tendency to attach more weight to evidence involving sound and images.[154]

7.4 Recommendations

The RS and RPE provide for sufficient leeway for the judges to use their discretion when evaluating evidence, ensuring a fair trial overall. Digital evidence, however, does bring in new peculiarities which benefit from further evaluation and discussion, including:

- Engagement with experts to ensure that the submission approach is still the most suitable approach to the evaluation of evidence, in light of the increasing usage of digital evidence and sophistication of technology, and the need to ensure that any evidence on the case record is reliable and authentic; and
- Further research into how known and unknown biases (cognitive and technical) can influence judicial decision-making (and case-building) and the mitigation measures and practices that may need to be adopted to ensure fairness of the proceedings.

In addition, the judges, who drive and manage the proceedings, will need to ensure that the following is adequately considered:

- Ensuring consistency in the terminology and language used in their decisions and judgments, avoiding the convolution of terms such as authenticity or credibility and reliability;
- Ensuring that only authentic (and authenticated) material enters the case record and makes into the trial proceedings;
- Ensuring transparency and clarity in their reasoning, especially when it comes to the overall evaluation of evidence and the assessment of the guilt or innocence of the accused; and
- Ensuring that the adopted procedures and practices do not disadvantage the Defence and that the burden of proof always remains with the party seeking to tender evidence onto the case record.

[154] McDermott, Koenig & Murray, *Open Source Information's Blind Spot*, 98.

8 Project Limitations and Overall Conclusions

The goal of this research project was to determine whether there is a need to amend any of the rules governing the ICC as a result of the increased usage of digital evidence and the sophistication of technology and if so, what the reasons are for such a proposed amendment. Due to the complexity of the research question and the fact that it interrelates strongly not only with the current operational challenges and demands of the ICC but also the many unexplored challenges connected with digital evidence, like the ways in which the documentation of human rights violations is changing, means that it is not possible at this stage to recommend the amendment of any particular rule.

The work underlying this report has however, advanced our goal of seeing how we can strengthen the judicial proceedings in light of the challenges identified and arising from the increased usage of digital evidence and sophistication of technology. We have created an analytical roadmap that can be built upon, which analyses the identified challenges in the context of the current legal framework in place at the ICC. We have started creating a potential checklist of issues and challenges against which any proposed amendment should be assessed before taking a definitive stand. We have also begun categorising the digital evidence challenges based on how they interrelate not only with different types of digital evidence but with other general challenges and issues relating to procedural guarantees. As a result, the purpose of this report is to raise awareness of the challenges we have identified and to serve as a basis for other researchers and experts operating in the field of digital evidence and international criminal justice to undertake further, more tailored research into these specific challenges. It should also serve as a starting point for discussions amongst relevant ICC stakeholders looking to make lasting changes in the efficiency and effectiveness of the Court and its judicial investigations and proceedings in the future.

The limitations of this project must be considered. While we consulted many experts, the number of those actively participating in the project was limited. Moreover, our research approach continued to develop as we advanced the work in each of our clusters, and in many regards, our expert consultations were limited and tailored to specific issues arising at the time rather than discussing the wider scope of the project. The scope of the research and time constraints were also limiting factors that one must bear in mind when reading the report and recommendations. For instance, while we shared and obtained feedback on some of our research findings that underlie this report with our experts, we have not shared the draft report itself with the experts due to time constraints.

All findings and recommendations should be read with our general findings in mind: The current lack of clarity around applicable standards and practices means that more work needs to be put into clarifying these matters first before considering any possible solutions.

We remain committed to advancing the discussions around strengthening the judicial proceedings as we believe that only fair, effective and efficient judicial proceedings can ensure accountability for perpetrators of (core international) crimes.

9 Annexes

The following documents are annexed to this report:

Annex 1: Simplified analytical roadmap containing a categorisation of the identified challenges and the governing rules to which they relate;

Annex 2: List of current guidelines and manuals relating to digital evidence and an analysis of their relevance and added value to ICC judicial proceedings;

Annex 3: List of institutions

E-Procedure: Simplified analytical roadmap containing a categorisation of the identified challenges and the governing rules to which they relate

Final Report - Annex 1

27 October 2023

Annex 1

Simplified Analytical Roadmap:

Categorisation of Identified Challenges

This document serves to categorise and simplify each of the category 1, 2 and 3 challenges identified in relation to provisions of the RS and the RPE in the Analytical Roadmap. The challenges identified have been collected from our analysis of the relevant rules, expert reports and feedback and academic writing.

The document presents the challenge categories, lists the provisions that relate to each category, summarises the specific challenges relating to each type of digital evidence (category 1, 2 and 3) and ultimately summarises the main impact on the accused, the victims and the witnesses that arise in relation to each challenge.

This document serves as a starting point for further discussions and should be read together with the Analytical Roadmap.

Table of Contents

1 Challenge 1: Lack of training in digital evidence and technology

1.1 Judges' lack of training: articles 36, 39; regulation 44

1.1.1 Challenges

- Ability to explain admissibility rulings will increasingly depend on judges' capacity to interrogate technology systems and increase their familiarity and understanding of digital evidence and new sources of information (category 1–2 challenge).

- Satellite and aerial images may need to be submitted together with expert reports summarising the forensic evidence to contextualise the images. Technical flaws with satellite imagery or lack of information regarding their creation can be cured with expert evidence. With adequate expert corroboration, aerial and satellite images can be considered authentic and reliable, even if they have technical errors, markings, removal of certain data such as coordinates or lack certain information. Moreover, expert testimony is often technologically complex, so a rigorous technical process is often required to assess the reliability and value of the expert evidence, and a judge or the Defence may find it difficult to comprehend the shortcomings of the expert evidence, given its technical nature. Another challenge is the lack of clarity or understanding around what types of digital evidence require an expert to decipher it and which types can be spoken to by anyone (category 1–2 challenge).

- Forensic experts are often needed to assess the authenticity and reliability of digital evidence, ensuring that the evidentiary material that reaches the Court is of significant probative value and has not been manipulated. The problem is that this places the admissibility, relevance and probative value decision-making away from the court, such as the ICC, and onto the forensic experts—as the ICC judges will not have the required technical expertise to make this analysis themselves (category 1–2 challenge).

- Assessment of probative value and prejudicial effect of evidence will become more complex when it comes to "newer types" of digital evidence, for example, AI-generated data. Judges may need specialised training in certain software (category 3 challenge).

  As social media and other forms of open-source evidence becomes more proliferated in international criminal proceedings and technology becomes more sophisticated, the gap of technological expertise of the judges becomes bigger. This gives rise to challenges with understanding and interpreting the technological shortcomings of the open-source information presented as evidence. Using experts and expert reports to assist only helps insofar as the expert explains whether the technology is sound—but the judges must still understand the technology to be able to assess the expert report (category 3 challenge).

1.1.2 Impact on accused and witnesses and victims

- **Impact on accused:** Unexplained admissibility rulings may lead to the accused not being able to question why evidence has been admitted or omitted. Judges untrained in, for example, AI-generated data might lead to false evidence being admitted or real evidence being omitted.
- **Impact on witnesses and victims:** Lack of training in new tech systems and newer forms of digital evidence could lead to accidental leaking of information on witnesses and victims featuring in digital evidence. The need for technical experts to decipher digital evidence might delay or complicate the proceedings and thus justice for the victims.

1.2 Prosecutors' lack of training: article 42

1.2.1 Challenges

- Prosecutor needs assistance from experts in archiving and authentication or OTP staff needs to be trained on this. OTP protocols must be updated accordingly (category 1 challenge).
- Prosecutor should be open to specialised training that gives them the foundation needed to investigate crimes involving technology. Assembly of States Parties must understand the importance of investing in training (category 2 challenge).
- The OTP and ICC cannot be expected to become scientific institutions or employ experts in all relevant emerging technologies. ICC not designed for innovation. Should learn from other communities, where practitioners often find solutions by relying on trusted networks with specialized organizations. ICC should distribute these connections and knowledge widely across the institution so all units can access relevant technology (category 3 challenge).

1.2.2 Impact on accused and witnesses and victims

- **Impact on accused:** Lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to Prosecution relying on digital information that has been manipulated.
- **Impact on witnesses and victims:** Lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to Prosecution not preserving digital evidence properly, which results in victim and witness data being leaked.

1.3 VWU lack of training: article 43; rules 18, 19

1.3.1 Challenges

- VWU lacks specialised expertise in digital evidence and open-source investigations, both of which might affect their work with witnesses and victims. The VWU should work directly with technology companies to facilitate effective digital communication with survivors in situation countries and receive ongoing training on open-source investigations. In order to successfully protect survivors, the Court should consider implementing a witness education program, which informs the public of privacy protection tools when documenting attacks, as well as consider setting a time limit for data retention (category 1 challenge).
- VWU should be open to specialised training that gives them the foundation needed to investigate crimes involving technology. Assembly of States Parties must understand importance of investing in training. The Court also should consider its current witness protection protocols which, although shown to be successful in offering protection to past witnesses, might not be enough as a result of new issues of identification, consent and storage length (category 2 challenge).
- ICC must invest in new technologies, additional staff and ongoing training regarding rapid changes in the digital information ecosystem. Should collaborate with states, companies and civil society organisations for digital archives and preserve content at risk of removal (category 3 challenge).

1.3.2 Impact on accused and witnesses and victims

- **Impact on accused:** Lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to stringent protective measures being put in place unnecessarily, which can impact the accused's right to cross-examine evidence against them.
- **Impact on witnesses and victims:** Lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to VWU not adequately protecting victims and witnesses featuring in digital evidence. Could also lead to VWU failing to identify major witnesses and victims.

1.4 Registry lack of training: rule 20

1.4.1 Challenges

- Registry has a mandate to operate in accordance with accused's right to a fair trial. It would benefit from receiving ongoing training on open-source investigations and digital evidence to be able to achieve its mandate. This will necessitate training in deepfakes and proper authentication of digital evidence. It will also play an important role in making sure the roster of experts can help judges comprehend intricacies of highly technical evidence (category 1–2 challenge).

- ICC should invest in new technologies, additional staff and ongoing training regarding rapid changes in digital information ecosystem. Should collaborate with states, companies and civil society organisations for digital archives and preserve content at risk of removal. To be able to support professional investigators, specific Registry training in digital evidence is needed (category 3 challenge).

1.4.2 Impact on accused, witnesses and victims

- **Impact on accused:** Lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to Registry not fulfilling its mandate to act in accordance with fair trial rights of the accused.
- **Impact on witnesses and victims:** Given the Registry's focus on the fair trial of the accused, lack of training and/or funding for training and specialised staff in digital evidence and new technologies could lead to inadequate resources spent on considering also the need to protect victims and witnesses.

2 Challenge 2: Collecting digital evidence

2.1 How much evidence to collect (overcollection risks): articles 15, 61(5), 61(7)-(8), 64

2.1.1 Challenges

- It is unclear how much information needs to be collected to reach the threshold to initiate an investigation in Article 15, and this might give rise to overcollection when it comes to digital evidence (category 1 challenge).
- "Sufficiency" is not defined under Article 61 nor is "substantial grounds to believe". Satellite imagery, for example, is rarely sufficient in and of itself and will, due to its technical nature, often require expert or witness testimony to contextualise. Corroborating evidence, the use of probabilistic methods and other social science research tools can lessen the need for expert or witness testimony. However, this need "reflects the worrisome reality that witnesses are the soft underbelly of any criminal prosecution". (category 1 challenge).

- Tools currently exist for OTP to collect evidence efficiently, but they are not being used in the most effective ways. OTP should make use of machine learning and AI to look for patterns in large data sets, such as social media digital evidence (category 2 challenge).
- Because of fear of content deletion, often too much information is preserved, leading to overcollection. With the proliferation of social media evidence and the sheer amounts that will be collected, it will become increasingly difficult for the Prosecutor to adhere to her or his disclosure obligations, and judges may thus struggle to ensure the fairness of the trial (category 3 challenge).
- Since "sufficiency" in Article 61 is not defined, it may come down to a question of volume and probative value of relevant evidence. If the OTP and investigators are not familiar with issues pertaining to deepfakes and deleted accounts, they might either have manipulated evidence at their disposal, there is the risk of "real evidence" being disregarded for being fake or the evidence they do have, if not stored properly, might be deleted and hamper future proceedings (category 3 challenge).

2.1.2 Impact on accused and witnesses and victims

- **Impact on accused:** Overcollection may lead to errors in disclosure processes or overwhelming the Defence with "evidence dumps". That makes it very difficult for Defence teams to protect fair trial rights by examining all evidence. The need for technology, software and expert reports to contextualise and understand certain types of digital evidence can increase the burden on the Defence.
- **Impact on witnesses and victims:** The desire to obtain "sufficient evidence" might lead to overcollection. Overcollection may lead to errors in protecting victims and witnesses due to an overwhelming amount of digital evidence to review. Confidentiality protocols may inadvertently be breached.

2.2 What type of evidence to collect: article 58, rule 79

2.2.1 Challenges

- Linkage evidence is the key to establishing individual responsibility. Key linkage evidence like the order of battles and objectives of military operations, the functioning of military structures, communication patterns, etc, may be less susceptible to open-source research. Linkage evidence is often the most difficult evidence to find and can be drowned out by other open-source evidence showing the general situation on the ground but not necessarily linking human rights violations or crimes to any particular person or persons. Prioritising open-source evidence (like electronic intercepts, satellite imagery, etc) that links to particular perpetrators is key (category 1–3 challenge).

- The development of deepfakes and sophisticated technology may make it difficult for the Defence to raise an alibi and/or exclude criminal responsibility where they are depicted in a video that they claim to be fake. However, satellite and aerial images can be used to place people at a specific time and place. Investigators and the Prosecutor may need to rely more on traditional category 1 evidence as deepfakes and sophisticated technology become more prevalent (category 1–3 challenge).
- The use of triangulated social media content can help counter deepfakes, where there is enough corroborating evidence from different sources. User-generated evidence is rarely introduced or processed on its own but once corroborated by other types of evidence, it gains significant probative value in court. Open-source evidence may need to be introduced in conjunction with files found on electronic devices and flash drives (category 2 challenge).
- Deepfakes are not just a threat to specific individuals or entities but also to society. Fake videos could feature public officials taking bribes, displaying racism or engaging in adultery. Soldiers could be shown murdering innocent civilians in a war zone, precipitating waves of violence and even strategic harms to a war effort. All of these issues may become relevant where a ”witness“ is featured in a piece of digital evidence which is in reality a deepfake (category 3 challenge).

2.2.2 Impact on accused, witnesses and victims

- **Impact on accused:** The development of deepfakes and sophisticated technology may make it difficult for the Defence to raise an alibi and/or exclude criminal responsibility where the accused are depicted in a video that they claim to be fake.
- **Impact on witnesses and victims:** Lack of linkage evidence could lead to a prosecution not proceeding—this could harm victims and witnesses. The existence of deepfakes might cause real evidence to be dismissed as fake, harming victims and witnesses in the process.

2.3 Lack of uniform standards: articles 44, 53, 64(9), 70, 87(6); rules 48, 73, 104, 165

2.3.1 Challenges

- Given the obstacles the ICC faces in collecting traditional evidence such as documents due to its lack of enforcement powers and its dependency on voluntary cooperation, the “best evidence” rule is far more likely to involve digital evidence, particularly evidence generated online and available through open-source investigations. The ICC is therefore most likely to be the first major global jurisdiction to focus predominantly on the newest emerging forms of evidence in cooperation with NGOs and other investigators. The lack of uniform standards gives rise to increasing challenges with collecting and preserving digital evidence (category 1–3 challenge).

- Source verification appears to be less stringent for intercepted audio communications than video or images. For instance, in Ongwen, the ICC found that intercepted radio communications were reliable even though they had been recorded over 10 years ago with rudimentary equipment and other shortcomings relating to their creation. The less stringent approach here could have potential consequences if the approach of the Prosecution in acquiring the information does not properly verify and/or preserve the evidence or take into account potential manipulation techniques (category 1 challenge).

- The discovery, collection and analysis of digital open-source evidence is seldom carried out by legal professionals but rather by independent researchers and citizen journalists applying varied standards or sometimes often without formal and/or relevant training before it is ultimately supplied to the Court. A wide range of actors are collecting and preserving digital evidence, leading to a growing ecosystem of digital repositories around the world. This offers a tremendous opportunity for the ICC because it enables court investigators to gather relevant information at a distance, cutting costs and reducing the need to put individuals in danger, but it also requires learning new skills and taking an adaptive and agile approach, which could be problematic in ICCs institutional bureaucracy and professional hierarchy (category 2 challenge).

- Another major challenge is the lack of resources available to human rights investigators, including IT resources, digital forensics tools, translation resources and other human resources needed to access and assess information relevant to a given violation. 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, as 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 (category 1–2 challenge).

- The author or creator of the material may be different from the source providing the information to the investigator or the custodian from which it is obtained—possibly resulting in variances in the format and in the accompanying information or metadata. The array of collection methods and sources may call for different requirements for authentication at trial, such as through an expert witness, lay witness or with corroborating evidence (category 2 challenge).

- OTP needs to communicate with assisting NGOs to discuss how data can be structured in a way that increases its overall value for court processes—because NGOs and other organisations may have different collection, preservation and/or verification standards (category 1–3 challenge).

- OTP needs to broaden its understanding of what technologies are being used in different locations by increasing cooperation with local organisations in different situation countries (for example, Facebook in Myanmar vs Weibo in China). This is key to understanding newer forms of technology, how they develop, where and why (category 2–3 challenge).

- Civil society organisations are experiencing that content from Muslim and/or Arabic-speaking countries is more likely to be removed from social media platforms. ICC must ensure that the organisations it works with are given the necessary support and funding to preserve relevant evidence where this is likely to be removed (category 3 challenge).
- The ICRC could also come across deepfakes and other forms of sophisticated technology and use that in their reports. If their reports are subsequently relied on, and are assumed privileged, this might cause fair trial concerns because the Defence may not be able to question the information provided, despite it being fake (category 3 challenge).
- The ICC and other international courts frequently place reliance on reports from NGOs. However, a lot of the digital information relied on by NGOs could be deleted. In a 2020 audit, Human Rights Watch found that 11% of the digital content it had cited in its reports since 2007 had been deleted (category 3 challenge).

2.3.2 Impact on accused, witnesses and victims

- **Impact on accused:** Lack of knowledge of which standards of collection, preservation and/or verification are being used makes it more difficult for accused to challenge the authenticity of digital evidence. Lack of collection and preservation standards could lead to evidence being subject to manipulation or key evidence being deleted. This could prevent the accused from being able to examine the case against them and to find evidence to exonerate themself. The fact that each piece of digital information may have many “sources” means that the accused may never be able to question all the relevant individuals, which can compromise their ability to defend themself.
- **Impact on witnesses and victims:** Lack of uniform preservation standards might lead to evidence not being properly preserved, leading to a leak in data or information about witnesses and victims. Lack of uniform collection and preservation standards might compromise the confidentiality of victims and witnesses because their images might be circulated without their consent if not stored correctly.

2.4 Accessing digital information: article 56, 57(3)(d), 72, 73, 93(2)-(6), 99; rules 47, 73, 115, 116, 167, 194

2.4.1 Challenges

- Occasionally, prosecutors may get their hands on government-generated category 1 type information (for example, photographs taken by military photographers etc) that is provided by whistleblowers or in other ways smuggled out of the country. The potential violation of privacy and re-traumatization of using such information is something that the ICC OTP needs to consider (category 1 challenge).
- The ICC might need to consider a solution to the fact that ICRC documents are presumed privileged. If these documents contain open-source information, the judges must be able to ensure themselves that it has been collected and preserved properly. A solution might be proper storage and anonymization techniques as opposed to privilege (category 1 challenge).

- Prosecutor may not always be granted right of access to countries. Digital evidence may be stored in multiple locations—but its collection may not require physical access to the territory of a state. During the investigation phase, Article 56 could be applied to preserve digital information in countries where the Prosecutor is not allowed to enter the physical territory. There is no reason why this provision should be limited to testimonial evidence and can be extended to digital evidence. Where states are refusing to cooperate, the ICC should focus on strengthening relationships with social media companies and other technology companies to facilitate effective investigations (category 1–3 challenge).
- Valuable digital information in early stages of conflict could be lost if the Prosecutor cannot intervene to preserve it. Even during preliminary investigations, the Prosecutor should be able to use cooperation frameworks to make requests from telecommunications and internet service providers to preserve user data (category 1–3 challenge).
- As technology develops, the ICC needs to be mindful of state and/or governmental incentives to provide skewed information to the Court, particularly where the accused is still part of the governmental machinery. Many actors, including states, will have an interest to exploit the capacity of deepfakes to manipulate beliefs. The Court should invest in new technologies, additional personnel and ongoing training to stay abreast of rapid changes in the digital information ecosystem (category 3 challenge).
- The ICRC could also come across deepfakes and other forms of sophisticated technology and use that in their reports. If their reports are subsequently relied on, and are assumed privileged, this might cause fair trial concerns because the Defence may not be able to question the information provided, despite it being fake (category 3 challenge).

2.4.2 Impact on accused, witnesses and victims

- **Impact on accused:** There might be digital information that exonerates the accused. If the ICC (Prosecution or Defence) cannot access the digital evidence, the accused may not be able to prove their innocence. If states or companies refuse to cooperate with the ICC, or if they have an incentive to skew information, this could prejudice the accused and their right to a fair trial. The ICRC could also come across deepfakes and other forms of sophisticated technology and use that in their reports. If their reports are subsequently relied on, and are assumed privileged, this might cause fair trial concerns because the Defence may not be able to question the information provided, despite it being fake.
- **Impact on witnesses and victims:** If the ICC is unable to access digital evidence, it may not be able to identify the commission of crimes or who their victims are. Non-cooperation by states, technology companies or the ICRC could prevent valuable evidence from being captured or relied on, which could negatively affect victims.

3 Challenge 3: Preservation and storage of digital evidence

3.1 Safe storage and preservation of evidence: articles 18, 19, 54, 56, 57(3)(b)-(c), 58, 64(2)-(3), 64(7), 64(8)(b), 68, 87(4), 93(1); rules 10, 15, 46, 47, 49, 59, 86, 87, 107, 138

3.1.1 Challenges

- Preserving the availability, identity, persistence, renderability, understandability and authenticity of a digital object requires much more than just saving its content. Significant costs and resources are involved in collecting, preserving, verifying and analysing open-source information. The OTPs preservation strategies should be customized to its circumstances, the nature of its collections and the needs of its intended use (category 1 challenge).

- The Prosecutor's obligation to protect the confidentiality of information and testimony extends to protecting the confidentiality of the senders of the information as well as the information itself. Videos have multiple stakeholders including the people who created them, the people who may be depicted, the people creating repositories and the communities that the repositories are aimed at protecting. New policies might have to be implemented for adequate protection of digital evidence, and these policies should consider anonymisation, identification, consent and proper storage of digital information (category 1–2 challenge)

- There are inherent biases in storing social media evidence—may reflect politics, perceptions and biases of the investigator through filenames, data categories and tags they choose in preserving the evidence (category 2 challenge).

- Screenshots from social media are not enough for Prosecution to prove their authenticity. The OTP must determine in advance how objects should be captured and preserved in terms of their technical, intellectual, structural or aesthetic characteristics to ensure the object's accessibility, usability, interpretability and authenticity for the Court (category 2 challenge).

- A major concern in open-source investigations is security—of both the people in the region under investigation and of the investigators themselves. Investigators, adhering to the "do no harm" principle, must be careful about using or sharing videos or photographs posted online on the basis that this may make those who created, uploaded or were featured in them vulnerable to reprisals. This is something the OTP will need to consider as it makes more use of digital open-source evidence like social media evidence (category 2 challenge)

- Deleted accounts are a particular challenge in Prosecutor's ability to preserve evidence. E-Court Protocol should be updated regularly for solutions on how to adapt to newer challenges (category 3 challenge).

- The OTP should assess how it intends to maintain authenticity of its stored objects in the face of technological change. Transformations like reformatting or media migration can be necessary for preservation or for rendering or playback and can sometimes involve changing the digital object. The IT infrastructure, including hardware and software, used for the processing, storage and management of digital evidence must be robust, up to date and available to all parties who need it, including the Defence and the legal representatives of the victims. This might require a significant financial commitment (category 1–3 challenge).
- When requesting evidence from States Parties, the Court will have to rely on the preservation techniques employed by those States (category 1–3 challenge).
- The protections offered by the ICC ultimately come to an end where a witness is no longer participating in a trial. The question is when the individual is no longer at risk with a digital repository—prolonged storage of digital evidence could expand the time during which an individual could be considered a witness or engaged with the Court. Might be susceptible to data hacking or other sophisticated technological weapons (category 3 challenge).
- Of concern is the Court's continued use of the highly insecure and outdated digital signatures algorithm, MD5. The risks of weak cryptography are not well-understood by the Court at present. The consequences of a data breach, destruction or manipulation of the Court's digital evidence would be severe (category 3 challenge).

3.1.2 Impact on accused, witnesses and victims

- **Impact on accused:** Cognitive biases in collecting and preserving digital open-source information (for example, which tags are used in preservation process) can lead to relevant evidence being disregarded or a certain narrative against the accused being promoted by the Prosecution. Evidence that is not properly preserved is subject to manipulation and hacking. This could affect the accused's right to a fair trial or prejudice the accused in other ways.
- **Impact on witnesses and victims:** Deleted accounts or information may lead to difficulties in identifying relevant victims and witnesses and their experiences. Protective measures may not be adequate to protect confidentiality and privacy of victims and witnesses featured in digital evidence. There are concerns over privacy when it comes to the storage of digital evidence, as it is not clear who is best placed to control the repository of digital information. Ensuring the safe storage of digital evidence in a way that protects victims and witnesses will become more and more expensive and difficult if the Prosecutor has to deal with massive amounts of media and other data. This might lead to confidentiality of victims and witnesses being breached.

4 Challenge 4: Digital Evidence in Court

4.1 Disclosing digital evidence: articles 61(3)(b), 67(2); rules 76, 77, 78, 82, 84, 121

4.1.1 Challenges

- Overcollection can create a real burden for the OTPs disclosure obligations. Although there are new e-discovery techniques that can use AI to identify items for disclosure, certain types of digital evidence, such as videos, images, audio files and documents in certain languages, cannot be easily addressed with these tools. E-discovery software is also very expensive and will require long-term budgeting (category 1–2 challenge).

- Deleted content and deleted accounts are a real problem for the parties' disclosure obligations and in particular to disclose of exculpatory information to the Defence. If the OTP ingests large quantities of information without the personnel and equipment to adequately comb and index that information and preserve it so that it is not deleted, they won't know what they have (or what they have lost) and yet could be held responsible for any nondisclosure. The OTP should make targeted requests of external repositories, limiting the risk of over-ingestion (category 3 challenge).

4.1.2 Impact on accused, witnesses and victims

- **Impact on accused:** Overcollection could lead to mass amounts of disclosed documents. "Document dumping" on the Defence might make it difficult for the accused to challenge and examine the evidence against them. Moreover, 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.

- **Impact on witnesses and victims:** Over-ingestion of documents might compromise the security and confidentiality of each individual piece of information if the OTP does not even know what it is holding. This could affect the safety of victims and witnesses featuring in the digital evidence.

4.2 Examining digital evidence: articles 61(6), 64(7), 67(1), 68, 69; rules 16, 17, 46, 68, 81, 86, 87, 140

4.2.1 Challenges

- Videos have multiple stakeholders, including the people who created them, the people who may be depicted, the people creating repositories and the communities the repository is ultimately aimed at supporting. Therefore, in digital evidence, there might be several key individuals who could be described as "witnesses" at trial. Given these many options, and the fact that not all of them might be called, this might make it complicated for the Defence to properly cross-examine evidence against them (category 1–2 challenge).

- Audio interceptions and videos of, for example, the accused taken without their consent has the potential to violate various rights. The Court has to distinguish between minor infringements of procedural safeguards and more serious violations. Whereas violations of human rights law may be a ground for excluding evidence, a violation of national laws does not seem to require exclusion as long as it is not a violation of internationally recognised human rights (category 1–3 challenge).

- Prior recorded testimony is essentially an audio recording, but it is subject to more stringent safeguards than other audio recordings. Although there are procedural safeguards in Rule 68(2) for admitting prior recorded testimony in a way that does not prejudice the accused, these are sometimes disregarded as is shown by a number of cases in which Chambers have, for example, admitted prior recorded testimony directly incriminating the accused, relying on Rule 68(2)(b) (category 1 challenge).

- The accused must have "a genuine opportunity to challenge evidence presented against them and to present their own evidence". Thus, one would need to ensure that the accused knows what digital evidence the Prosecutor is relying on and be able to challenge such evidence and that the accused knows how the digital evidence has been obtained. The OTP needs to carry out its work with respect to category 2 forms of digital evidence in a way that anticipates future admissibility challenges (including on privacy grounds) (category 1–3 challenge).

- Open-source information, such as social media videos, has yet to be intensely challenged as evidence in an international courtroom. In one case, for the YouTube videos and publicly available digital images found on the internet, the Prosecution used internal investigators to verify the authenticity of the images by geolocating the landmarks in the images. While the Prosecution made an effort to geolocate some of the open-source videos and photographs, limited forensic analysis was admitted alongside (category 2 challenge).

- Deepfakes will make it easier for liars to deny the truth in distinct ways. 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. Liars aiming to dodge responsibility for their real words and actions will become more credible as the public becomes more educated about the threats posed by deepfakes (category 3 challenge).

4.2.2 Impact on accused, witnesses and victims

- **Impact on accused:** The fact that victims and witnesses featured in digital evidence might never be present in court might prevent the accused from being able to question them and examine the evidence against them. The use of digital evidence in lieu of witness testimony in such circumstances could give rise to contraventions of rights of the accused. Some software, for example, digital explosion reconstruction science and scientific expert reports, are very difficult for the Defence to challenge. The Defence cannot cross-examine a computer program and will need specialised knowledge to understand the evidence. The cost to even be able to challenge it can be incredibly high and the process complicated. The fact that the safeguards for admitting prior recorded testimony are often disregarded means that the Defence's rights might be prejudiced as they may not be able to examine the evidence against them.
- **Impact on witnesses and victims:** Dissemination of images and videos of victims and witnesses featuring in digital evidence could compromise their safety and confidentiality. Recorded testimony being streamed on social media by activists may render it unusable for trial. This could traumatise victims and witnesses and may prevent the proceedings from continuing.

4.3 Verifying digital evidence: articles 64(2)-(3), 64(9), 69, 70, 74, 84; rules 63, 64, 68

4.3.1 Challenges

- Where a forensic report confirms that, for example, an audio intercept has not been tampered with, the Court might accept it even if authenticity cannot be confirmed with certainty. Sophisticated technology can make it more difficult for forensic staff to know whether digital evidence has been tampered with. Manipulated evidence might be inadvertently introduced (category 1 challenge).
- Videos are often not transmitted in full but in excerpts. This may prevent the Court from being able to contextualise the situation portrayed in the video if additional information is not provided by the party tendering the video (category 1 challenge).
- Pursuant to Rule 63(4), there is no strict legal requirement that the video has to be corroborated by other evidence for the Court to be able to rely on it and establish a specific fact. Where there is no corroborating evidence, the Trial Chamber will need to be particularly mindful of cognitive biases and the conclusions it draws from videos. However, video evidence can be more complete than photographs or witness accounts and thus its role should not be delegated to a purely secondary one of corroborating other evidence or providing leads (category 1–2 challenge).
- Manipulation and distortion of aerial and satellite images have been shown not to necessarily affect their admissibility but rather their weight in international criminal trials. This means that manipulated evidence is at risk of being admitted in the case record (category 1 challenge).

- Since humans have a tendency to value and weigh sensory information (such as videos and audio) more heavily than abstract information (such as numbers or statistics), the Chambers might place greater weight on a video or audio intercept as compared to competing evidence that is not in video form. This can encourage biased decision-making (category 1–2 challenge).
- The relevance of a video or photograph depends on its date, time and the location of its recording. It can be hard to concretely establish the time, date and location of the evidence and prove it hasn't been tampered with. If this is not stated clearly in the video, by way of proper verification techniques, the Defence will not be able to fully understand the content of the video (category 1–2 challenge).
- The current E-Court Protocol is largely limited to harmonising the format, means of storage and presentation of evidence. Does not address authentication other than specifying that metadata should be attached and that the cryptographic hashing standard to be adopted is MD5. This is insufficient to address digital evidence (category 2 challenge).
- Widely circulated pieces of information on social media have been found to shape witnesses' accounts and impressions of what they saw, what they thought was important and what they thought investigators wanted to hear. For example, if there was a particularly controversial video, it would be circulated amongst civilians displaced in camps very quickly and would inform their testimony to investigators on the ground. This is a key challenge when considering whether to accept prior recorded testimony (category 2 challenge).
- Evidence originating from social media posts (such as videos documenting a crime scene in a conflict zone) may not adequately protect the privacy of victims and witnesses who may be the source or who may be featured in the video. If the source is anonymous, care must be taken to ensure that the social media evidence containing the undisclosed source is not the only evidence of that particular event (category 2 challenge).
- Disinformation is not always created by the perpetrators of mass atrocities—victims' interest groups, perhaps in the interest of strengthening their case for justice and accountability, presented evidence of atrocities from other countries or contexts claiming it as their own. This may not be deliberate, as the videos or images may be mislabelled on social media and citizens may share it with UN investigators genuinely believing in its relevance. This highlights the importance of reverse image searching to check when a piece of content first appeared online (category 2 challenge).
- Open-source digital evidence is susceptible to problems of verifiability, which may affect its reliability in court. Court should ensure that it does not overly rely on social media evidence which might promote a certain narrative. Cognitive and technical biases also emerge during the analysis, including in the assessment of a piece of information's meaning, reliability and probative value, as well as linking the information to potential crimes within the jurisdiction of the ICC (category 2 challenge).
- There are significant challenges involved in identifying deepfakes. ICC should enter into industry partnerships with open-source platforms (for example, Google, Twitter, Facebook) to obtain greater resources to successfully detect deepfakes and evolve its authentication methodologies (category 3 challenge).

- The ICC and other international courts frequently place reliance on reports from NGOs. However, a lot of the digital information relied on by NGOs could be deleted. In a 2020 audit, Human Rights Watch found that 11% of the digital content it had cited in its reports since 2007 had been deleted (category 3 challenge).

- As technology develops and lots of digital evidence enters the case file, judges should exercise their discretion under Article 69(4) to issue early admissibility decisions and exclude anything that shouldn't be there to avoid cluttering the evidentiary record, including with, for example, manipulated evidence like deepfakes. The challenges of detecting deepfakes are significant. Authentication tools should evolve alongside deepfake technologies themselves (category 3 challenge).

- While the Rome Statute covers false or forged evidence deliberately tendered into the case record by providing criminal liability for those purposes, there is no way of dealing with the production and dissemination of deepfakes which well-meaning researchers, lawyers and even the ICC Prosecutor might provide to the Chamber without realising they are fake (category 3 challenge).

- International crimes are often documented by multiple individuals. Investigators might scan social media for tweets or posts from similar locations to seek to verify the information. However, the long-term risk is that groups which appear to be unconnected, but are actually coordinating with each other, might plant doctored, corroborating information on social media—which investigators, and therefore the ICC, might not pick up on (category 3 challenge).

4.3.2 Impact on accused, witnesses and victims

- **Impact on accused:** Inadequate authentication methodologies may lead to false or forged evidence being admitted in detriment to the accused. Where the source is protected and undisclosed to the Defence, this might violate the accused's fair trial rights as the accused cannot question the source. Cognitive biases to prefer video or audio evidence might mean that legitimate non-video or non-audio evidence is not given as much weight, potentially impacting the accused's right to a fair trial. As of November 2021, the "submission approach" is the preferred unanimous approach of the Chambers, which means that admissibility and relevance of evidence is not considered by the Chamber when it is submitted, but in the final deliberations of the innocence or guilt of the accused. This might make it more difficult for Defence teams to raise potential issues relating to relevance or admissibility, because lots of documentary, video or audio evidence might be submitted by the Prosecution at the same time and accepted onto the case record without being considered individually by the Chambers.

- **Impact on witnesses and victims:** Victims and witnesses might be more difficult to identify and their experiences more difficult to verify if digital information has been manipulated. Overreliance on corroborating evidence might mean that legitimate evidence is discarded due to lack of corroboration, which might prevent victims from obtaining justice.

4.4 Standard of proof of digital evidence: articles 53, 58, 61(5), 61(7)-(8), 66; rule 48

4.4.1 Challenges

- There exist valid grounds upon which to challenge the admission of certain category 1 evidence, such as Google Earth images which were not made for the courtroom. In one case, these were submitted by the Prosecution in the format of a screenshot. The Prosecution was not required to take the additional step of seeking out the raw images from Google, question employees of Google Earth about their process or verify on the ground the accuracy of the satellites used by Google Earth in that location and time. This is problematic because Google Earth positional accuracy is not fixed but varies from one time to another. The Court must be critical of this type of evidence and consider whether it reaches the threshold of "beyond reasonable doubt" (category 1 challenge).

- Although user-generated social media evidence is very useful, it has the problem of often not being sufficient on its own. For instance, in domestic trials, investigators must triangulate the available user-generated evidence with the available expert reports and open-source evidence available on social media (category 2 challenge).

- ICCs approach to open-source social media evidence might need to change depending on the stage of proceedings as the standard of proof increases. For example, less weight might be afforded to social media evidence in confirmation of charges stage than in the issuance of a warrant of arrest or initiation of an investigation, which bears a lower standard of proof. New technologies might require judges to modify the standard of proof required. Taking a reasonably subjective, flexible approach to standard of proof would allow judges the freedom to determine the standard based on the type of evidence or the facts involved. This approach also aligns well with the Court's general affinity toward flexibility. More efficient authentication and verification mechanisms are needed, and as technology develops, it is possible that the uncertainty in relation to the standard of proof required, and when it has been sufficiently met, will become more difficult (category 2–3 challenge).

4.4.2 Impact on accused, witnesses and victims

- **Impact on accused:** Not employing the appropriate standard of proof for digital evidence depending on the stage of the proceedings might lead to unverified evidence being admitted on the case record.

- **Impact on witnesses and victims:** Employing a too high standard of proof might mean that the Prosecutor's role of authenticating evidence becomes too difficult and victims and witnesses are ignored. If judges are uncertain when the appropriate standard of proof has been sufficiently met, victims and witnesses may suffer from not having the proceedings continue.

4.5 Technical challenges of presenting digital evidence: article 65

4.5.1 Challenges

- Witness testimony is still required to understand and verify a lot of digital information, in particular category 1 digital evidence, such as call data records. If the Court requires more evidence, such as witness testimony, to produce a more accurate picture of the facts, this might take a lot of time and not be very efficient (category 1 challenge).
- In the Al Mahdi case, the Prosecution used specialised technology to create an interactive platform to present their digital evidence to the Court. However, intentional or inadvertent bias in the presentation of these type of demonstrative visual representations raise significant fair trial issues as does the exorbitant cost of creating such intricate presentation tools (category 2 challenge).
- Deleted accounts will pose a particular challenge if the judge requests the Prosecution to present additional evidence and such additional evidence may have been deleted (category 3 challenge).

4.5.2 Impact on accused, witnesses and victims

- **Impact on accused:** Lack of understanding of the limitations of technology in court could negatively impact the accused's right to a fair trial, because of biases or lack of context around digital evidence.
- **Impact on witnesses and victims:** Since witness testimony is still required to decipher a lot of digital evidence, considerations of privacy and protection arise and must be taken into account before the Prosecution decides to present digital evidence that will require witness testimony to understand.

4.6 Witness cooperation and consent: articles 64(6), 72, 87(4), 93(1), 93(7)-(10); rules 65, 74, 87, 88

4.6.1 Challenges

- Article 64(6)(b) creates an obligation of persons to appear and testify before the Court, but States are under no duty to enforce that obligation. Every witness that has provided testimony or otherwise engaged with the Court has ostensibly done so willingly. This may or may not be the case when using digital evidence where witnesses and victims are featured without providing their consent (category 1–2 challenge).
- There is no practical way to ensure informed, explicit consent universally. For example, a third-party may document someone's attack and provide that evidence to the Court without the survivor's knowledge. The person depicted in the evidence cannot give explicit consent, so ensuring maximum anonymization is the next best solution to both the consent and anonymization issues faced by the Court. Censoring evidence to anonymize the identities of those in the video or image should be part of the Court's evidence collection process (category 1–3 challenge).

- The Court should consider issues of consent, which likely have not previously been primary concerns when engaging with witnesses. Article 64(6)(b) creates an obligation of persons to appear and testify before the Court, but States are under no duty to enforce that obligation. Every witness that has provided testimony or otherwise engaged with the Court has ostensibly done so willingly. This may or may not be the case when using digital evidence (category 1–3 challenge).

4.6.2 Impact on accused, witnesses and victims

- **Impact on accused:** The censoring and anonymisation of the identities of those depicted in a video or image might make it difficult for the Defence to challenge the evidence against them.
- **Impact on witnesses and victims:** Individual victims usually have the option to testify or cooperate with an investigation or trial. Using media in which they are featured, which may or may not have been collected with their consent, strips this level of voluntariness from the ICC-victim/survivor relationship.

4.7 Witness protection measures: article 68; rules 16, 17, 43, 86, 87

4.7.1 Challenges

- The resources of the Court are limited and providing protection to witnesses during the pre-testimony, testimony and post-testimony stages of witness cooperation will become exponentially more expensive and difficult if the Court has to contend with massive amounts of media and other data. While the current protection protocol for in-chambers testimony, including voice or face distortion, will probably continue to be effective for the witnesses who are providing live testimony, new policies may have to be implemented when considering how to protect the large number of individuals featuring in digital evidence kept by the Court in any digital evidence repository (category 1–2 challenge).
- The ICC will have to look at the protection of witness privacy as something to be done on the back end of evidence collection. Witnesses will likely no longer first be identified and then require protections from the Court. In fact, when dealing with digital evidence, it is possible that a witness may never directly engage with the Court. Therefore, the Court has to consider how it will effectively and adequately protect an exponentially larger number of witnesses than it has ever had before and do so while possibly never being able to identify the individuals in the manner required by the current protection protocol (category 2 challenge).
- Circulation of an individual's image without their consent could violate their privacy. The Prosecutor needs to take special care to protect the confidentiality of individuals featuring in, for example, social media images or videos. They should not be unnecessarily linked to the Court (category 2 challenge).
- The Al-Werfalli case heavily relied on open-source information, specifically media that depicted several victims being shot and killed. When describing the videos in the warrant, the victims are generally referred to as "unidentified men", while others are described as hooded or otherwise not identifiable. This is a notable weakness in the

ICCs victim protection protocol going forward. An inability to identify survivors does not mean the presentation of their data in court shields them from privacy risks (category 2 challenge).

- It may be more difficult for the VWU to successfully keep survivors from being identified when the evidence comes from digital media sources, which may or may not be traceable and which may have been manipulated or is subsequently deleted. There is little that can be done to offer any of the pre-trial protections currently in place at the ICC when the "witness" in question is not really a witness at all but rather an unidentified individual in a given conflict zone (category 2–3 challenge).
- The protections offered by the ICC ultimately come to an end where a witness is no longer participating in a trial. The question is when the individual is no longer at risk with a digital repository—prolonged storage of digital evidence could expand the time during which an individual could be considered a witness or engaged with the Court. Might be susceptible to data hacking or other sophisticated technological weapons (category 3 challenge).

4.7.2 Impact on accused, witnesses and victims

- **Impact on accused:** Witness protection measures can affect the right of the accused to challenge the evidence against them. The fact that victims and witnesses featured in digital evidence might never be present in court might prevent the accused from being able to question them and examine the evidence against them. The use of digital evidence in lieu of witness testimony in such circumstances could give rise to contraventions of rights of the accused.
- **Impact on witnesses and victims:** Dissemination of images and videos of victims and witnesses featuring in digital evidence could compromise their safety and confidentiality. Some witnesses have expressed fears that someone could read court transcripts and find out who they are. This fear would go from a concern that someone could find a transcript to a fear that someone could find the identifiable video or photograph of their attack. This identification has the potential to irrevocably alter an individual survivor's life.

E-Procedure: List of current guidelines and manuals relating to digital evidence and an analysis of their relevance and added value to ICC judicial proceedings

Final Report - Annex 2

27 October 2023

Annex 2

This Annex constitutes a work-in-progress document intended to become part of the Research Gap Analysis available through our Digital Evidence Database. It lists recent manuals and guidelines (2016-2023) that have been developed by various governmental departments, NGOs and international organisations to address varying aspects of the collection, preservation, verification and analysis of digital evidence. The intention of the Annex is to provide a brief analysis of the challenges covered by the manuals and their limitations. The guidelines and manuals contained in this document have informed and contributed to various stages of this research project.

	Manual	**Year**	**Organisation**	**Digital Evidence Challenges addressed**	**Purpose, Target Audience and Limitations**
1.	Investigating Perpetrators: A guide to mapping parties in relation to international humanitarian law and human rights violations	2023	Public Interest Advocacy Centre and the Human Rights Center at the UC Berkeley	Verifiability of sources Unexplored biases Avoiding overcollection	Offers information and advice for OSINT researchers and international criminal law investigators on the process for collecting, organising and analysing open-source information to map parties and their alleged involvement in incidents that may constitute IHL and/or IHRL violations. Provides an overview of best practices for how to collect, research, analyse and document the relevant information used in mapping work, which consists of six phases: a) digital landscape assessment; b) scoping incidents and parties; c) systematic review of sources; d) review, revise, research; e) perpetrator analysis; and f) final review. Given its focus on mapping perpetrators, it is a practical and helpful resource for prosecutors and international criminal courts.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
2.	Berkeley Protocol on Digital Open Source Investigations	2022	Human Rights Center at the UC Berkeley School of Law under the auspices of the Office of the United Nations High commissioner for Human Rights	Uniformity of collection and preservation standards Preventing overcollection Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Sets out minimum standards for the collection, preservation, verification and analysis of digital open-source information for human rights, ICL and humanitarian investigators. The guide covers many elements relating to digital evidence, including privacy and security concerns, issues and principles relating to the collection of digital evidence and the importance of proper preservation, verification and analysis. It does not, however, set out precise steps or protocols for how to carry out these processes and may not be as practical for judges or prosecutors in international criminal proceedings.
3.	Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals	2022	Kalshoven-Gieskes Forum (KGF)	Evaluation of digital evidence	Offers an analysis of international case law regarding the admissibility of digital evidence within the criminal proceedings. It focuses on the essential elements which should be considered before submitting digitally derived evidence to an international criminal court or tribunal. The scope is limited to the current case law and practices and thus does not cover to any great extent the newer types of digital evidence.
4.	Handbook on Civil Society Documentation of Serious Human Rights Violations	2016	Public International Law and Policy Group	Uniformity of collection and preservation standards	Sets out guidelines and best practices for the collection and management of information on serious human rights violations for laypersons. Constitutes a compilation of best practices for collection and preservation, which makes it useful for international criminal investigators. It is not, however, specific to the collection of digital information.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
5.	NIST Interagency Report: NIST IR 8387 on Digital Evidence Preservation	2022	U.S. Department of Commerce National Institute of Standards and Technology	Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Offers information and addresses challenges relating to the preservation of digital evidence, aimed at evidence management professionals. It raises challenges with the secure storage of digital objects, images and files and different elements that should be borne in mind by digital forensics and related practitioners. While not specifically aimed at ICL investigators, it is likely to be a useful guide of best practices for prosecutors and defence teams working with digital forensics experts in the handling of evidence.
6.	Conference of International Investigators General Principles for Digital Evidence	2021	Conference of International Investigators	Safe and appropriate storage of digital evidence Authentication and verification of digital evidence Evaluation of digital evidence	Combines recommendations and best practices for the proper handling of digital evidence by investigators to ensure their reliability. The manual focuses on the integrity, confidentiality and authenticity of digital evidence. Although not being specifically targeted at international criminal investigators or prosecutors, the general principles in the guide contain helpful practical steps persons handling digital evidence can take to ensure its integrity. This can therefore be useful to both judges and prosecutors in considering whether digital evidence has been properly handled and is therefore reliable.
7.	Tackling deepfakes in European policy	2021	European Parliament	Deepfakes and manipulation of digital evidence Authentication and verification of digital evidence	Offers advice to policymakers on the five dimensions of the deepfake lifecycle that should be taken into account to prevent and address the adverse impacts of deepfakes on society. The guidelines are not specific to criminal investigations or proceedings but do contain certain recommendations on how to mitigate the risks posed by deepfakes, which may still be useful to international criminal investigators.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
8.	SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics	2019	Scientific Working Group on Digital Evidence	Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Provides information to vendors and practitioners on various digital verification tools and their utility. Sets out the limitations of digital integrity and digital signature algorithms, including MD5, which is used by the ICC. The manual is informative rather than practical in the sense that it does not provide recommendations or standards for use but explains the setbacks for each algorithm. It may be a useful informative resource for ICC stakeholders but not a particularly useful guide for prosecutors or ICL practitioners.
9.	SWGDE Best Practices for Mobile Device Evidence Collection and Preservation, Handling, and Acquisition	2020	Scientific Working Group on Digital Evidence	Safe and appropriate storage of digital evidence	Offers best practices for the collection, preservation and extraction of evidence from mobile devices for digital forensics practitioners. The document contains practical steps that can be taken in the extraction of digital evidence from mobile devices but is limited to that source of digital evidence. It does not cover open-source digital evidence. The document also refers generally to other organisational guidelines and procedures. Its usefulness may be particularly relevant for digital forensics experts due to its technical nature.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
10.	Interpol Guidelines for Digital Forensics First Responders	2021	Interpol	Uniformity of collection and preservation standards Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Offers practical information and advice to law enforcement professionals on the collection and handling of digital evidence, as well as various digital forensics techniques to do so safely and securely. However, it does not provide recommendations or instructions in respect of any legal requirements for the collection, preservation, verification and analysis of digital evidence, which it notes differ widely across different jurisdictions. The guide is tailored to domestic law enforcement professionals, for use within national jurisdictions.
11.	International Protocol on the Documentation and Investigation of Sexual Violence in Conflict	2017	UK Foreign and Commonwealth Office	Uniformity of collection and preservation standards Preventing overcollection Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Offers advice to practitioners (including NGOs) on the collection, preservation and verification of digital evidence relating specifically to sexual violence, which is often more difficult to document. Does not include any particular standards to be followed but refers practitioners to existing domestic standards and legal requirements which need to be considered.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
12.	Eurojust/ICC Guidelines for civil society organisations	2022	Eurojust, the EU Network for investigation and prosecution of genocide, crimes against humanity and war crimes (Genocide Network) and the Office of the Prosecutor at the ICC	Safe and appropriate storage of digital evidence	Offers support to civil society organisations in their independent efforts to preserve and collect information on the commission of international crimes and human rights violations for accountability purposes. Provides an overview of basic standards that such organisations should seek to follow when preserving information for accountability purposes. However, the guide does not specify which specific steps should be taken for collection and preservation of digital evidence but rather refers broadly to best practices, applicable regulations and the taking of necessary measures. Its practical utility for international criminal proceedings may therefore be limited.
13.	Istanbul Protocol: Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment	2022 (revised edition)	UN Office of the High Commissioner for Human Rights	Preventing overcollection Safe and appropriate storage of digital evidence Authentication and verification of digital evidence	Offers information and advice on the collection, preservation and verification of digital evidence of torture with reference to the Berkeley Protocol. It discusses the need to collect and preserve such digital evidence in accordance with “recognised techniques of digital forensics” and other best practices but does not set out what those techniques are, thus decreasing its practical usefulness to judges and prosecutors in international criminal proceedings. Its scope is also limited to the specific crime of torture.

	Manual	Year	Organisation	Digital Evidence Challenges addressed	Purpose, Target Audience and Limitations
14.	Video as Evidence Field Guide (Download)	2016	WITNESS	Uniformity of collection and preservation standards Authentication and verification of digital evidence	Offers advice to human rights investigators, activists, citizen journalists and community reporters on how to capture video for the purpose of using it as evidence. However, it focuses on videos only (and not other forms of open-source digital information) and given that it is tailored to human rights investigators, it may have limited utility for international criminal proceedings.
15.	Guide for Journalists on How to Document International Crimes	2022	Centre for Law and Democracy in partnership with News Media Europe	Safe and appropriate storage of digital evidence Authentication and verification of digital evidence Protecting privacy of the source	Provides advice to journalists and editors on the capturing of evidence of the commission of international crimes. The guide is not specific to digital evidence but contains basic recommendations on collecting and preserving digital evidence, capturing relevant metadata, anonymising sources and archiving evidence securely. The guide does not contain specific technical measures that should be taken to carry this out and provides recommendations rather than specific standards. As it is aimed at journalists, it may be less useful to international criminal proceedings.

E-Procedure: List of institutions

Final Report - Annex 3

27 October 2023

Annex 3

Digital Evidence Project –Final Report *Please note that some institutions were involved in more than one cluster and more experts from one institution might have been contacted and consulted for the project.*	
Institutional Affiliation	*Area of Expertise*
1. American Bar Association	International criminal law and evidentiary standards
2. American University	International law
3. Amnesty International	Digital data-streams, modern fact-finding, best practices conducting investigation of human rights violations
4. Association for the Study of War Crimes	International criminal law
5. Bellingcat	Investigative journalism
6. Berkeley Centre for Human Rights	Human rights, science and technological innovation
7. Carnegie Mellon University	Human rights, science and technological innovation
8. Central Office for Cybercrime Bavaria (ZCB)	Cybercrime, investigations
9. Centre for International Law and Policy	International law
10. Commission for International Justice and Accountability	Criminal justice, (criminal) investigations, gathering evidence, preservation and analysis of evidence
11. Crown Court	Criminal law, evidentiary standards, procedures
12. Eurojust	Cross-border crime, judicial cooperation
13. Europol	Investigation, standard setting
14. EyeWitness to Atrocities	Technology, evidentiary standards, documentation of mass atrocities
15. FIDH (International Federation for Human Rights)	International Criminal Court, digital evidence, criminal trials
16. Friedrich-Alexander Universität Erlangen-Nuremberg	Computer security, informatics
17. Goethe University Frankfurt am Main	International criminal law

18. Independent Investigative Mechanism for Myammar	Collection, consolidation, preservation and analysis of evidence, international standards, criminal proceedings
19. International Bar Association	International criminal law and evidentiary standards
20. 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
21. International Criminal Court	International criminal law
22. International Development Law Organisation (IDLO)	International criminal law
23. Jurmatix Legal Intelligence	Legal technology, data protection
24. Leiden University	International criminal law
25. Open Society Foundations	Human rights, technology
26. Oxford Institute for Ethics, Law and Armed Conflict	
27. Radboud University	Criminal law, criminal procedures, criminology
28. Special Tribunal for Lebanon	International criminal law
29. Strathmore Law School – Strathmore University	Digital evidence, criminal law
30. Stockholm University	Evidence and procedures, international criminal law
31. Swansea University	International criminal law, evidence and proof, human rights, fair trial
32. Trial International	Fair trial rights
33. University of Copenhagen	Evidence, jurisprudence, forensic science
34. University of Illinois Chicago	International law, international criminal law
35. Universita di Bologna	International criminal law, comparative law
36. Univesity of Washington	Human rights, qualitative approaches to law and social science research methods and designs

37. University of Technology Sydney	Evidence, criminology, history
38. United Nations International Residual Mechanism for Criminal Tribunals	International criminal law, investigation, and litigation
39. William & Mary Law School	International criminal law, evidentiary standards
40. 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