New Technologies and the Investigation of International Crimes

An Introduction

Alexa Koenig,* Emma Irving,**
Yvonne McDermott,*** Daragh Murray****

1. Introduction

Between April 2012 and January 2013, the historic city of Timbuktu, Mali was ravaged in a series of widespread and systematic attacks, some of which have been characterized as potential crimes against humanity, others as possible war crimes. Many of the victims were civilians. Those believed responsible were members of Ansar Dine and Al Qaeda in the Islamic Maghreb, who were alleged to have committed crimes as disparate as torture, outrages upon personal dignity, rape, forced marriage, sexual slavery, denial of a fair trial, persecution, other inhumane acts, and destruction of historic property.[1] As of the time of writing, two warrants of arrest have been issued by the International Criminal Court (ICC) for individuals believed to be connected to these crimes.

The first accused, Ahmad Al Faqi Al Mahdi, was transferred to ICC custody on 26 September 2015. Al Mahdi's case quickly became notable for the significant quantities of digital information that investigators had collected as evidence of Al Mahdi's possible crimes. This information included photographs and videos that depicted culturally significant buildings before, during, and after their destruction, and satellite images, which helped place the photos and videos in geographic space, including their relative locations. Several of these images were used to compose a 'geolocation report' — a report

* Executive Director and Lecturer-in-Residence, Human Rights Center, University of California, Berkeley, USA. [kalexakm@berkeley.edu]
** Public International Law and International Criminal Justice and Technology consultant. [e.emmairving@gmail.com]
*** Professor of Law, Swansea University, UK. [Yvonne.McDermottRees@swansea.ac.uk]
**** Senior Lecturer, Human Rights Centre and School of Law, University of Essex, Colchester, UK. [d.murray@essex.ac.uk]

1 *Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (ICC-01/12-01/18), available online at https://www.icc-cpi.int/mali/al-hassan (visited 21 April 2021).

Journal of International Criminal Justice **19** (2021), 1–7
doi:10.1093/jicj/mqab040
Advance Access publication 5 July 2021

identifying the geographic coordinates where each of the photographs and videos were taken — which ran to hundreds of pages and was used to corroborate the location of each alleged event. Also notable was a detailed digital platform compiled by the New York-based organization SITU Research,[2] which used an array of research methods — including architectural methods — to help the prosecution, defence, judges, survivors, and the general public better understand how each piece of visual evidence fit into geographic space.[3] The introduction of the geolocation report as evidence and the use of SITU's platform to help make sense of the disparate visual material is especially noteworthy because of the reliance on a considerable amount of digital open-source information, including photographs, videos, and other information pulled from online public spaces.[4]

In September 2016, following a guilty plea, Al Mahdi was found guilty of intentionally directing the destruction of cultural heritage property as a co-perpetrator. Many feel that his guilty plea was the result, at least in part, of the abundant digital evidence in the Court's possession, including videos that showed Al Mahdi helping to destroy the culturally significant property. While the conviction was perceived as a win for the Court, international criminal investigators around the world were disappointed that the defence never had a chance to cross-examine the digital open-source information, the geolocation report, and the report's creators, thereby testing their veracity and underlying methodologies for court purposes.

But then a second accused, Mr Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mamhoud, was surrendered to the court on 31 March 2018, just 4 days after the issuance of a warrant for his arrest. A Malian national, alleged member of Ansar Dine, and de facto chief of the group's Islamic police, Al Hassan is currently on trial. The charges against him include the crimes against humanity of torture, rape, and sexual slavery, as well as other inhumane acts comprised of forced marriage and persecution. He is also on trial for war crimes, including torture, cruel treatment, outrages upon personal dignity, intentionally directing attacks against religious buildings and historic monuments, and rape and sexual slavery, among others.[5]

The trial opened in July 2020 with a statement from the Prosecutor. In September 2020, the case resumed, with the prosecution calling its first witnesses and presenting its initial evidence[6] — including the geolocation report that had been introduced in the *Al Mahdi* case. Al Hassan's trial promises to give those watching the satisfaction that Al Mahdi's did not — the chance to see how the ICC has matured in its ability

2 See SITU Research, *Timbuktu, Mali Platform*, available online at http://icc-mali.situplatform.com/ (visited 26 March 2021). For more about the platform, see SITU Research, *ICC Digital Platform: Timbuktu, Mali*, available online at https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali (visited 21 April 2021).

3 See SITU Research, *supra* note 2.

4 See A. Koenig, 'Open Source Evidence and Human Rights Cases: A Modern Social History', in S. Dubberley, A. Koenig and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability* (Oxford University Press, 2020) 32–47.

5 *Al Hassan*, *supra* note 1.

6 *Ibid.*

to handle closed and open-source digital materials, and to assess the potential utility of such information for international criminal justice.

Most importantly, from our perspective, Al Hassan's case will spotlight how digital technologies may be increasingly deployed to help satisfy the elements of international crimes. For example, spotlighting just one allegation — the crime against humanity of sexual slavery — investigators and prosecutors may use a range of digital technologies and methodologies to prove the necessary underlying facts. Satellite imagery that reveals the scope, scale, dates, and pattern of attacks may help confirm that the underlying acts were systematic and widespread — a key contextual element of crimes against humanity — before tackling the base crime of sexual slavery. Artificial intelligence (AI), including machine learning, may be used to identify videos that feature the accused, any co-perpetrators, witnesses and/or victims from among enormous datasets of videos available online — completing in hours what it might take humans months or even years to systematically comb. Records found in the deep or dark web (the non-indexed portions of the internet that are inaccessible via search engines) may include slave logs, which could help to establish the sale of victims of trafficking, and videos, which may document the sale or transfer of prisoners. Videos and photographs posted to social media by co-perpetrators, victims, or bystanders may help tie the accused to the underlying acts, or serve as leads to witnesses who may eventually testify in court.

New technologies stand to support a new era in the prosecution of international crimes. However, while digital methods — pulling videos from Facebook, creating timelines from tweets, aggregating disparate online information to help tell the who, what, when, where, and why underlying egregious events — hold tremendous promise, there are also noteworthy pitfalls. For example, digital information is notoriously unstable, with the most graphic content frequently removed by social media platforms before it can be preserved by investigators. How can new processes be devised, either among international criminal investigators or in partnership with outside actors, to ensure potential lead, linkage, and crime base evidence remain accessible for accountability? And then there is the scale problem: how can large datasets, whether on social media like YouTube, Facebook, Twitter, or Tencent, or in private archives being developed by non-profits, be efficiently combed for alleged crimes and relevant people? Are there ways to do so that are both efficient and effective, relying on algorithms to do at scale what humans cannot? And just as importantly, how can methods developed by journalists and other non-lawyers be adapted to the needs of courts — including satisfying relatively high standards of proof, preserving the chain of custody of online content, and identifying anonymous content creators to serve as potential witnesses?

Following numerous workshops and consultations with digital investigators, answers to some of these questions have recently emerged with the Berkeley Protocol on Digital Open Source Investigations,[7] released in English in

7 United Nations Office of the High Commissioner for Human Rights, 'Berkeley Protocol Gives Guidance on Using Public Digital Information to Fight for Human Rights', 1 December 2020, available online at https://www.ohchr.org/EN/NewsEvents/Pages/berkeley-protocol.aspx (visited 21 April 2021); see also Human Rights Center at UC Berkeley School of Law and United National Office of the High Commissioner for Human Rights, *Berkeley Protocol on Digital Open*

December 2020 and scheduled for release in Summer 2021 in all of the remaining languages of the United Nations. However, many open questions remain. The articles in this Special Issue are an attempt to share insights and lessons learned that are relevant to better understanding and advancing this fast-growing field.

2. Motivation for the Special Issue

Over the past decade, international criminal investigators have increasingly relied on digital technologies to support fact-finding and verification related to alleged international crimes. At first, the use of such tools was framed as entering a 'Wild West'. Practice included significant experimentation as legal investigators increasingly adopted and adapted methods and tools used by journalists, human rights actors, and others who had pioneered ways to comb large quantities of online information for data relevant to their research and investigations.

This special issue of the *Journal of International Criminal Justice* was motivated by an observation that digital technologies have become an established part of the investigation and prosecution of international crimes. This is evidenced by the professionalization of practice, as illustrated by the emergence of common standards for digital open-source investigations in the Berkeley Protocol, the turn towards incorporating digital investigation skills into legal education,[8] and the training of professionals.[9] Moreover, user-generated content has been introduced as evidence in international criminal trials not just before the ICC, but in domestic trials of atrocity crimes, as demonstrated in detail by several contributions to this special issue.[10]

Source Investigations, 2020, available online at https://humanrights.berkeley.edu/programs-projects/tech-human-rights-program/berkeley-protocol-digital-open-source-investigations (visited 21 April 2021).

8 Amnesty International has a 'Digital Verification Corps', teams of students that discover and verify online open source material for use in Amnesty investigations, based at Universities in Hong Kong, South Africa, Mexico, the USA, and the UK.

9 For example, the Institute for International Criminal Investigations and the Human Rights Center at UC Berkeley have collaborated to offer an open source investigation course for professionals across a variety of fields, including lawyers, investigators, analysts, law enforcement professionals, and investigative journalists. See Human Rights Center at UC Berkeley School of Law, *Trainings and Workshops*, available online at https://humanrights.berkeley.edu/resources/trainings-and-workshops (visited 21 April 2021). In 2020, Amnesty International launched a free-to-anyone two-part 'MOOC' on 'Open Source Investigations for Human Rights', hosted on the Advocacy Assembly platform, available online at https://advocacyassembly.org/en/courses/57/ (visited 21 April 2021).

10 K. Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands'; C. Gabriele, K. Matheson, R. Vazquez Llorente, 'The Role of Mobile Technology in Documenting International Crimes: The *Affaire Castro et Kizito* in the Democratic Republic of Congo', both in this Special Issue of the *Journal of International Criminal Justice, 2020*.

The maturation of the field is also demonstrated by the development of a rich scholarly literature.[11] Earlier research focused largely on the potential of technology in human rights investigations and the prosecution of international crimes,[12] particularly in the wake of the *Al-Werfalli* arrest warrant.[13] Now that this potential has become a reality, scholarly attention has turned to the practicalities of this 'digital turn' in international criminal investigations, with an in-depth analysis and critique of relevant procedures, and a realistic assessment of the benefits and pitfalls of developing practices. In this way, the literature on digital technologies and the investigation of international crimes appears to be following the same arc as the literature on international criminal justice in general — from an earlier 'faith-based' approach to the potentials of the system, to more rigorous (and perhaps, more realistic) evaluations and critiques.[14] That critical evaluation was seen as a necessary step in advancing international criminal law as a discipline,[15] and should be welcomed as moving the literature on new technologies and the investigation and prosecution of international crimes to the next stage of its development.

3. Structure of this Special Issue

Federica D'Alessandra and Kirsty Sutherland open this special issue with an article examining the role played by new technologies in the pursuit of accountability for international crimes. Drawing on extensive original research, the authors discuss the potential utility and challenges posed by the use of geospatial intelligence and remote sensing, open-source intelligence, financial intelligence, and modern documentation technologies, with a particular emphasis on 'third wave' UN accountability mechanisms, such as the International, Impartial and Independent Mechanism for Syria (IIIM–Syria).

11 For an overview of the issues related to open-source investigations, see S. Dubberley, A. Koenig and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability* (Oxford University Press, 2020). In addition to the contributions to this special issue, see, for example, R. Hamilton, 'User-Generated Evidence', 57 *Columbia Journal of Transnational Law* (2018) 1; L. Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', 41 *Fordham International Law Journal* (2018) 283; and the contributions to an *ICC Forum* discussion on the 'Cyber Evidence question', 2020, available online at https://iccforum.com/cyber-evidence (last visited 21 April 2021).

12 See e.g. P. Alston and S. Knuckey (eds), *The Transformation of Human Rights Fact-Finding* (Oxford University Press, 2016); M.K. Land and J.D. Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018).

13 Second Warrant of Arrest, *Al-Werfalli* (ICC-01/11-01/17-13), Pre-Trial Chamber I, 4 July 2018. See further E. Irving, 'And So It Begins … Social Media Evidence in an ICC Arrest Warrant', *Opinio Juris*, 17 August 2017, available online at http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/ (visited 21 April 2021).

14 C. Stahn, 'Between 'Faith' and 'Facts': By What Standards Should We Assess International Criminal Justice?' 25 *Leiden Journal of International Law* (*LJIL*) (2012) 251; D. Robinson, 'Inescapable Dyads: Why the International Criminal Court Cannot Win', 28 *LJIL* (2015) 323.

15 D. Robinson, 'The Identity Crisis of International Criminal Law', 21 *LJIL* (2008) 925.

Having set the scene, the rest of this issue is divided into three sections. The first looks at the use of new technologies in international criminal investigations. The second is composed of field notes detailing practitioner experiences to illustrate how new technologies are beginning to be used in practice. The third examines the use of new technologies at trial.

A. Investigations

Lindsay Freeman opens the investigations section with a discussion on the changing nature of the modern battlefield, and how the increasing adoption of military AI — and the emergence of the 'battlefield of things' — may affect military investigations in the future. Yvonne McDermott, Alexa Koenig, and Daragh Murray then discuss the cognitive and technical biases that may impact open-source investigations, particularly at the information gathering and analysis stages, and propose a number of steps to mitigate these effects. Next, Alexa Koenig and Ulic Egan address the online investigation of sexual violence. They present three key insights, suggesting that open source investigation may be refined to better respect and protect the interests of survivors by considering contextual issues, including the identity of the investigators and victims; integrating a gender and intersectional analysis into online investigation planning; and being thoughtful about consent, privacy, trauma, and control.

B. Field Notes

To open the 'field notes' section, Chiara Gabriele, Kelly Matheson, and Raquel Vazquez Llorente present a case study on the landmark *Affaire Castro et Kizito* case in the Democratic Republic of Congo. This was the first case internationally to admit digital photography captured using the eyeWitness app, and the authors analyse five key lessons learned. Elena Radeva then draws on her experience as a Digital Evidence Analyst Consultant at the IIIM–Syria to discuss how computer vision techniques can play a key role in the management of exceptionally large digital evidence sets. She presents the results of a number of different tests performed by IIIM–Syria to examine the utility of 'unsupervised clustering' and 'supervised object recognition' techniques. Giancarlo Fiorella, Charlotte Godart, and Nick Waters then draw on their extensive experience conducting open-source investigations for Bellingcat to highlight two key vulnerabilities in open-source research: the impermanent nature of digital evidence, and its susceptibility to dis/misinformation campaigns. They present a number of practices that can be incorporated into the investigative workflow in order to mitigate risk.

C. Trials

Lindsay Freeman and Raquel Vazquez Llorente begin the 'trials' section with an examination of the ICC's rules of criminal evidence and procedure. The

authors assess whether these rules are appropriate with respect to the use and handling of digital evidence, and the specific characteristics of the internet and other dissemination channels. Karolina Aksamitowska then looks at the prosecution of international crimes in Germany, Sweden, Finland, and The Netherlands, analysing how digital evidence — and particularly online open-source materials — have been used in international criminal prosecutions in national courts. Sarah Zarmsky closes this section with an examination of the use of digital reconstruction technology in domestic and international cases. While highlighting the key role that this technology can play in helping legal audiences understand a crime scene, the author notes a number of issues — such as problems with equality of arms, and the weight given to realistic but potentially inaccurate reconstructions — that should be considered and addressed if digital reconstructions are to be more widely used.

The special issue closes with reviews of two books that have recently made important contributions to the technology and international criminal justice field. In the first, Guido Acquaviva reviews 'Autonomous Weapons Systems and International Law: A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains', by Daniele Amoroso. In the second, Ruwadzano Patience Makumbe reviews 'Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability', edited by Sam Dubberley, Alexa Koenig, and Daragh Murray.

4. Conclusion: From the Wild West to the Golden Age, and Where to Next?

The pieces in this special issue, individually and taken together, make a notable contribution to the scholarly literature on new technologies and their place in the investigation and prosecution of international crimes. They come at a time when ongoing trials, in both international and domestic criminal justice systems, are reaping the benefits of technological developments — a far cry from the 'Wild West' of experimentation that defined earlier practice.

The coming era could be seen as a 'Golden Age' for technology-assisted international criminal investigations. There is a risk that emerging threats from cyberattacks and the perceived ubiquity of 'deepfakes' may lead to a wider distrust of digital evidence in future legal proceedings. More likely, however, is the possibility that — as the technology that threatens to shatter our trust in digital and open-source evidence develops — so too will courts' abilities to deal with those threats. That may be a topic for another special issue in a couple of years' time. For now, however, we as editors thank our authors for contributing their outstanding research to this volume; Antonio Coco and Urmila Dé for patiently guiding us through the process; and the people utilizing, developing, and managing these new technologies in their everyday practices. We hope that this special issue will help to inform their work and start a conversation on important current and future developments.