Digital evidence as a means of proof before the International Court of Justice

Roscini, M.

DIGITAL EVIDENCE AS A MEANS OF PROOF BEFORE THE INTERNATIONAL COURT OF JUSTICE

Marco Roscini[1]

Abstract: This article discusses the use of digital evidence as a means of proof before the International Court of Justice (ICJ). The absence of specific Court rules and procedures for digital evidence (with the exception of Practice Direction IX *bis*) is not necessarily an obstacle to its production and evaluation before the ICJ, as the general evidentiary rules can also be applied to digital evidence. The article first looks at the rules on the production of documentary evidence and then examines the specific issues related to audiovisual evidence. Finally, it examines the admissibility of digital evidence unlawfully obtained by a litigant through unilateral transborder access to data. The article concludes that, even if specific regulation may be needed as to the specific way in which authenticity and accuracy of digital evidence are to be established, the particular facts of the case and the grounds of challenge can vary widely, and it is doubtful that any regulation could be sufficiently flexible to deal with this in advance.

Keywords: International Court of Justice, international courts and tribunals, dispute settlement, means of proof, digital evidence, international procedural law.

1. Introduction

'Evidence' is 'information … with a view of establishing or disproving alleged facts'.[2] It is different from 'proof' in that '"proof" is the result or effect of evidence, while

---

[1] Professor of International Law, University of Westminster. The article is based on developments as of January 2016 and all websites were last visited on that date. I am grateful to Russell Buchan, Simon Olleson and Nicholas Tsagourias for their comments on previous versions of this article. All errors and omissions are my sole responsibility.

[2] R Wolfrum, 'International Courts and Tribunals, Evidence', *Max Planck Encyclopedia of Public International Law* (OUP 2012), vol V, 552.

"evidence" is the medium or means by which a fact is proved or disproved'.[3] Digital, or electronic, evidence is any probative material stored or transmitted in digital form, i.e. as series of the digits 0 and 1, which can be used in legal proceedings before a court in order to prove a fact according to the required standard of proof.[4] It can be obtained from different sources including fixed computer hard drives, removable USB flash drives, mobile phones, satellites and the internet, and can have different forms, such as text documents (e.g. Word or Excel files, emails, instant messages and spreadsheets), maps, databases, digital images, video and audio files, GPS data, internet browser histories and metadata.[5] Digital evidence can be open access, i.e. accessible by everyone without passwords or encryption, or available only to authorized users.

In spite of its growing importance as a means of proof and the specific problems it presents, the use of digital evidence in inter-state litigation has been almost entirely neglected by international law scholarship.[6] The present article aims to contribute to fill this gap. As it is not possible to identify uniform evidentiary rules applicable to all cases and before all international courts, due to limited space this article only focuses on proceedings before the International Court of Justice (ICJ) and does not deal with digital evidence in proceedings before other international courts and tribunals or before domestic courts.[7] Its conclusions, therefore, cannot automatically be extended to them.[8]

---

[3] MJ Canavan, LJ Culligan, AO Ginnow, FJ Ludes, RJ Owens, *Corpus Juris Secundum: A Complete Restatement of the Entire American Law*, Vol 31A: Evidence (West Publishing, St Paul, 1964) 820.

[4] The standard of proof is 'the *quantum* of evidence necessary to substantiate the factual claims made by the parties' (JA Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice', (2009) 58 ICLQ 165). International courts, at least those of a non-criminal nature, normally determine the standard of proof applicable in each case, which can differ considerably according to the nature of the court and the case under examination.

[5] As has been observed, digital evidence may include 'the content of a transmission or, more frequently, the attributes of a communications activity, or "meta-data", that identifies and describes the content of a transmission and its management by an ICT [information and communications technology] resource' (I Walden, *Computer Crimes and Digital Investigations* (OUP 2007) 208).

[6] There are, however, a limited number of studies on the use of digital evidence before international criminal tribunals: see, among others, ED Macauley, 'The Use of EO Technologies in Court by the Office of the Prosecutor of the International Criminal Court', in R Purdy and D Leung (eds), *Evidence from Earth Observation Satellites. Emerging Legal Issues* (Nijhoff 2013) 217-240; Human Rights Center, 'Digital Fingerprints. Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (February 2014), <https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf>. Some of the International Bar Association (IBA) Rules on the Taking of Evidence in International Arbitration ('IBA Rules'), adopted in 2010, expressly address electronic documents (text at <http://www.ibanet.org/Publications/publications_IBA_guides_and_free_materials.aspx>).

[7] On the use of electronic evidence before domestic courts, see generally S Mason (ed), *International Electronic Evidence* (British Institute of International and Comparative Law 2008).

[8] The article also does not deal with the application of the attribution rules to establish state responsibility in the cyber context: on this, see M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 33-40.

This article's purpose is to address certain issues that may arise from the production of digital evidence before the ICJ.[9] It will start with a discussion of the application of the ICJ rules on documentary evidence to digital documents. It will then analyse the specific problems related to the production of digital audiovisual evidence in ICJ proceedings. Finally, the last Section will examine whether digital evidence unlawfully acquired through transborder access to data is an admissible means of proof before the Court. The article will focus on the contentious jurisdiction of the Court: indeed, there are no detailed evidentiary rules for advisory proceedings and Article 68 of its Statute provides, as a general rule, that '[i]n the exercise of its advisory function the Court shall further be guided by the provisions of the present Statute which apply in contentious cases to the extent to which it recognises them to be applicable'.[10] Furthermore, the article will primarily look at proceedings in the merits: the nature of most preliminary objections as to admissibility of a claim before the ICJ is such that they will not normally turn on a detailed assessment of the evidence.[11] In any case, when deciding on preliminary objections, the Court does not normally rule on the evidence as such, but rather proceeds to assess the objection on the assumption that the allegations in the claim are true.

2. Digital evidence as documentary evidence

[9] Digital evidence could be useful not only to establish state responsibility for cyber operations, but also in other disputes, including those on border delimitations. On all the means of proof available to the ICJ to attribute cyber operations to states, as well as on questions related to burden and standards of proof, see M Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations', (2014-2015) 50 *Texas International Law Journal* 233 ff.

[10] Art 68, ICJ Statute (text at <http://www.icj-cij.org/documents/?p1=4&p2=2>). Under art 102(2) of the Rules of Court, in determining whether the rules for contentious proceedings are applicable the Court needs to take into account 'whether the request for an advisory opinion relates to a legal question actually pending between two or more States'. If so, the Court is required to first ascertain the views of the states involved before making any written statements and annexed documents accessible to the public (art 106) and the disputing states are entitled to appoint a judge ad hoc in relation to the advisory proceedings (art 102(3)). The text of the Rules of Court is at <http://www.icj-cij.org/documents/index.php?p1=4&p2=3&>. It should be noted that, while advisory proceedings are normally divided into written and oral phases as in contentious ones, the Court could dispense with both should it consider that it possesses sufficient information to give the advisory opinion (A Riddell and B Plant, *Evidence before the International Court of Justice* (British Institute of International and Comparative Law 2009) 388). In general, the Court does not engage in an in-depth discussion of the admissibility or probative weight of the documents used as evidence in advisory proceedings: it has been observed, therefore, that 'the concept of proof itself seems out of place in the context of the Court's advisory jurisdiction' (ibid, 397).

[11] Any preliminary objections as to Court's jurisdiction or as to the admissibility of a claim will normally be dealt with as incidental proceedings in accordance with art 79 of the Rules of Court, with the proceedings on the merits being suspended, although the Court can decide to join an objection to the merits where 'the objection does not possess, in the circumstances of the case, an exclusively preliminary character' (art 79(9)).

In the absence of a customary international law of evidence, whether or not digital evidence may be used before an international court depends entirely on the procedural rules of each court, which differ considerably from one to another. Rules on the production of evidence before the ICJ are contained in the ICJ Statute (Articles 48-52), the Rules of Court (adopted in 1978 according to Article 30 of the Statute), and the non-binding Practice Directions additional to the Rules for use by states appearing before the Court, first issued in 2001 and subsequently amended.[12] With the exception of Practice Direction IX *bis*, none of these documents explicitly refers to digital evidence. There is also no exhaustive list of the means of proof available to parties to cases before the Court or any indication of their different probative weight.[13]

As a commentator has observed, '[t]he International Court of Justice has construed the absence of restrictive rules in its Statute to mean that a party may generally produce any evidence as a matter of right, so long as it is produced within the time limits fixed by the Court'.[14] The basic rule, then, is that all evidence is, in principle, admissible.[15] As to the probative value of the evidence so produced, in *Nicaragua* the Court solemnly emphasized the principle of the free assessment of evidence, stating that 'within the limits of its Statute and Rules, [it] has freedom in estimating the value of the various elements of evidence'.[16] In other words, the ICJ is free to request or admit any evidence, including that in digital form, and to give it the probative value it deems appropriate.

Digital evidence belongs to the broader category of documentary (as opposed to oral) evidence, which includes 'all information submitted by the parties in support of the contentions contained in the pleadings other than expert and witness testimony',

---

[12] All the above documents are reproduced on the Court's website at <http://www.icj-cij.org/documents/index.php?p1=4>.

[13] The statutes and rules of international criminal tribunals, on the other hand, provide for more specific evidentiary rules (Wolfrum (n 2) 567-569).

[14] DV Sandifer, *Evidence Before International Tribunals* (University Press of Virginia 1975) 184. A general requirement of good faith can be said to apply to the taking of evidence by the parties (see, eg, Preamble, IBA Rules (n 6) para 3).

[15] There are, however, limitations to this general principle: see Riddell and Plant (n 10) 153-158. The Court does not hold specific preliminary proceedings in order to assess the admissibility of the evidentiary materials produced by the litigants unless they are specifically challenged by a party: what it does is consider any issues arising from the production of such evidence together with its probative value (Riddell and Plant (n 10) 53).

[16] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits), [1986], ICJ Rep, para 60. See also *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, [2005], ICJ Rep, para 59.

whatever its form.[17] Most national legislation does not discriminate between electronic evidence and physical evidence: '[w]hile approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence'.[18] Electronic documents, therefore, are in principle equivalent to paper documents, and electronic mail equivalent to traditional postal mail.[19]

While there is no formal hierarchy between different means of proof, the ICJ has taken a civil law court approach and has normally given primacy to documentary over oral evidence.[20] The Court has the power to call upon the parties to produce any documents it deems necessary or to seek such evidence itself,[21] but it has generally refrained from doing so and has relied on that spontaneously produced by the litigants.[22] Indeed, all documents not 'readily available'[23] must be produced by the interested party: certified copies of any document relied upon by the parties in support of their contentions in the pleading must be annexed to the original of the pleading.[24] As already noted, unless the other party challenges the authenticity of the evidence the Court is likely to assume that the digital evidence produced is authentic, and will not go through any formal process of authentication.[25]

---

[17] Wolfrum (n 2) 558. The IBA Rules define a 'document' as 'a writing, communication, picture, drawing, program or data of any kind, whether recorded or maintained on paper or by electronic, audio visual or any other means' (IBA Rules (n 6) Definitions).

[18] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (February 2013), at XXIV, <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

[19] Cybex, *The Admissibility of Electronic Evidence in Court* (2006), 28-29, <https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf>.

[20] A Aguilar Mawdsley, 'Evidence Before the International Court of Justice', in R St John Macdonald (ed), *Essays in Honour of Wang Tieya* (Nijhoff 1994) 543.

[21] Articles 49-50 of the ICJ Statute, art 62 of the Rules of Court.

[22] But see *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua)*, Judgment of 16 December 2015, para 41 <http://www.icj-cij.org/docket/files/150/18848.pdf>.

[23] Art 56(4) of the Rules of Court.

[24] Art 50(1) of the Rules of Court. All documents, be they annexed to the pleadings, additional or supplemental, must be filed with the Court's Registry in two certified copies and 125 non-certified additional copies (S Talmon, 'Article 43', in A Zimmermann, C Tomuschat, K Oellers-Frahm, CJ Tams (eds), *The Statute of the International Court of Justice. A Commentary*, 2nd ed. (OUP 2012) 1117-1118). Electronic copies of paper documents can also be accepted (ibid, 1099; Riddell and Plant (n 10) 165). It is the agent that certifies the copies. The IBA Rules contain further guidance on the production of electronic documents and provide that '[d]ocuments that a Party maintains in electronic form shall be submitted or produced in the form most convenient or economical to it that is reasonably usable by the recipients, unless the Parties agree otherwise or, in the absence of such agreement, the Arbitral Tribunal decides otherwise' (IBA Rules (n 6) Art 3(12)(b)).

[25] According to a UK House of Lords report, the original of a digital document is 'the data first recorded in memory' (Select Committee on Science and Technology, *Digital Images as Evidence* (HL 1997-98, 64-I) para 2.3).

If the authenticity is challenged, it is for the litigant producing the evidence to prove its reliability.[26] In particular, it will have to demonstrate authentication and chain of custody of the digital evidence in question. Authentication aims to determine that digital evidence has not been altered or manipulated and can occur through external indicators such as live witnesses, expert testimony or other documentary evidence, or internal indicators, like timestamps and metadata.[27] Chain of custody is '[t]he movement and location of … evidence, and the history of those persons who had it in their custody, from the time it is obtained to the time it is presented in court'.[28]

The challenged digital evidence's probative weight will depend on the demonstration by the litigant that it is authentic, accurate and complete, that its sources have been securely identified and that it has not been compromised.[29] A litigant, however, may refuse to explain the sources and procedures through which it obtained the digital evidence it has submitted:[30] while there are no sanctions for this, the litigant in question will bear the risk that the evidence is excluded or given reduced weight and that the facts it claims will not be considered sufficiently proved.

According to Article 56 of the Rules of Court, '[a]fter the closure of the written proceedings, no further documents may be submitted to the Court by either party except with the consent of the other party' or, in the absence of such consent, if the Court, after hearing the parties, deems the document necessary.[31] Article 56(4), however, introduces

---

[26] Talmon (n 24) 1121. There is no specific procedure before the ICJ to challenge the authenticity of documents.

[27] A Ashouri, C Bowers and C Warden, 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts', (2014) 11 *Digital Evidence and Electronic Signature Law Review* 118. Timestamps are sequences of characters or encoded information that identify when a certain event is recorded by a computer (which does not necessarily coincide with the time of the event itself).

[28] BA Garner (ed), *Black's Law Dictionary*, 10th ed (2014) 277-278.

[29] The Special Tribunal for Lebanon, for instance, declined a request by the Defence to admit into evidence two alleged US diplomatic cables found on the Wikileaks website. The Tribunal looked at other cases that dealt with Wikileaks documents and concluded that '[t]he judicial trend is …not … towards admitting Wikileaks documents into evidence', although cross-examination on the contents of the documents is admissible (*Prosecutor v Salim Jamil Ayyash et al*, Special Tribunal for Lebanon, STL-11-01, Trial Chamber, Decision on the admissibility of documents published on the Wikileaks website, 21 May 2015, paras 33-34). The Tribunal found that the Defence had failed to prove that the Wikileaks documents were authentic US diplomatic cables and that they accurately described the events they referred to (ibid, para 40). In fact, the sworn testimonies of two witnesses had denied their content (ibid, para 42).

[30] In the *Tolimir* case, for instance, the Prosecutor of the International Criminal Tribunal for the former Yugoslavia (ICTY) presented evidence that the United States provided under the condition that the procedures through which the evidence had been obtained would not be discussed (*Prosecutor v Tolimir*, IT-05-88/2, Trial Judgment (12 December 2012) para 68).

[31] Art 56(1) and (2). Silence by a litigant is considered consent. Practice Direction IX states that the litigants should refrain from submitting new documents after the conclusion of the written proceedings and that, in the absence of the consent of the other party, requests in that sense will be accepted by the Court only exceptionally. The production of additional documents not included in the pleadings *before*

an exception to this rule and provides that reference may be made in the oral proceedings to documents not formally produced during the written proceedings providing that they are 'part of a publication readily available'. Practice Direction IX *bis*, adopted in December 2006, takes note of the fact that documents can now also be published in digital form and provides that 'readily available' publications are any documents 'available in the public domain … in any format (printed or electronic), form (physical or on-line, such as posted on the internet) or on any data medium (on paper, on digital or any other media) [that] should be accessible in either of the official languages of the Court' and which it is possible to consult 'within a reasonably short period of time'.[32] In case the other litigant objects to the reference to a document in the oral proceedings, 'the matter shall be settled by the Court'.[33] Publications 'readily available' on the internet, then, may be referred to by the litigants in the oral proceedings without prior notice to the Court or the other litigant. The fact that documents on the internet can be accessed by anyone could make a potentially enormous amount of information 'readily available': as has been observed, this 'would increase uncertainty in proceedings and does not allow a party to prepare its cases effectively without notice of the documents on which the other party would rely'.[34] It is submitted, however, that not all internet publications are *ipso facto* 'readily available'. As Article 56(2) of the Rules of Court makes clear, the availability of a document is not to be assessed *in abstracto*, but in relation to the Court and the other litigant in each specific case. When assessing whether an internet publication is 'readily available' in a particular case, the Court should take into account factors like, for instance, the language in which it is written, whether the document is in a widely available format (like MS-Word and PDF), whether it is open access and whether it has been suitably indexed by a popular search engine.[35] It is also worth pointing out that the fact that a publication is 'readily available' does not necessarily render the concerned facts public knowledge of which the Court may take judicial notice: it only relieves the party from

---

the closure of the written proceedings is not subordinated to the consent of the other litigant or the authorisation of the Court (Talmon (n 24) 1117).

[32] Practice Direction IX *bis* (2)(i) and (ii).

[33] Practice Direction IX *bis* (4).

[34] A Riddell, 'Report on the Oral Proceedings in the *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*: Selected Procedural Aspects', (2007) 20 *Leiden Journal of International Law* 426. In the oral proceedings in the *Bosnian Genocide* case, the Agent for Bosnia and Herzegovina tried to refer to a newspaper article available online on the website of the newspaper in his cross-examination of a witness, but the respondent objected to this and the President suggested that the Agent for Bosnia and Herzegovina change the course of his cross-examination (ibid, 427-427).

[35] Practice Direction IX *bis* (2)(i)(ii).

the burden of having to produce the publication during the written proceedings.[36] The facts, however, still need to be proved.

3. Specific issues related to the production of digital audiovisual evidence

Documents also include audiovisual materials.[37] There are no specific rules for this type of materials in the ICJ Statute or Rules of Court and they are therefore produced and assessed in accordance with the general rules applicable to all documentary evidence. Digital photographs, maps, graphics and other visual evidence can be submitted in hard copy as annexes to the written pleadings in accordance to the procedural rules for the submission of documents. The resources that cannot be turned into hard copy documents can be presented to the Court during the oral proceedings.[38] A copy of all audiovisual evidence constituting a 'document', however, should normally be deposited in the Registry together with the pleadings before the closure of the written proceedings.[39] If this has not been done and there is no consent of the other litigant to its production, the evidence may be admitted only if the Court deems it necessary or if the document is part of a readily available publication.[40]

Although this largely depends on the issue in the case, the Court has generally attached less probative weight to audiovisual materials than to written documents. The Court has been particularly concerned with the authenticity of audiovisual evidence and the purpose of its production.[41] To address these concerns, Practice Direction IX *quater* provides that '[a] party's request to present audio-visual or photographic material must be accompanied by information as to the source of the material, the circumstances and date of its making and the extent to which it is available to the public. The party in question must also specify, wherever relevant, the geographic co-ordinates at which that material was taken'. Authenticity and authorship of digital audiovisual evidence may be difficult to establish with sufficient certainty: think, for instance, of videos uploaded on YouTube or pictures appearing on Instagram or Twitter. In fact, digital images are not real pictures, but data that need to be interpreted and processed. Metadata indicating the time the image was captured and the location of the scene can be manipulated and,

[36] M Benzing, 'Evidentiary Issues', in Zimmermann, Oellers-Frahm, Tomuschat and Tams (n 24) 1241.
[37] Wolfrum (n 2) 558-559; Talmon (n 24) 1116.
[38] Riddell and Plant (n 10) 284.
[39] Art 56(1) of the Rules of Court. On when audiovisual materials constitute 'documents' in the sense of art 56 of the Rules of Court, see Talmon (n 24) 1140-1141.
[40] Art 56(2) and (4) of the Rules of Court.
[41] Riddell and Plant (n 10) 287.

unlike in traditional pictures, the manipulation is not easily identifiable.[42] In consideration of this problem, some NGOs have developed mobile device 'applications' for citizen policing that record geolocation and other important information and allow the user to upload pictures and videos. The eyeWitness Project, for instance, has created and released an 'app' produced by the International Bar Association and the legal services of LexisNexis where digital evidence of international crimes can be safely stored.[43] The 'app' permits capture of photos and videos with embedded metadata showing the place and time of the collection and confirming that no alteration has taken place. After submission, the images and related data are encrypted and stored in a database, where they are analysed by legal experts who then liaise with relevant international, regional and national jurisdictions to ensure that the images are used to bring to justice those who have committed international crimes.[44] Even though these applications have been developed with criminal law proceedings in mind, they (and similar ones) may be useful also before the ICJ.

Digital images and maps can also be taken remotely by satellites. Remote sensing, or Earth Observation (EO), is 'the science of extracting information from an object through the analysis of data acquired by a sensor that is not in direct contact with the area'.[45] Like any other documentary evidence, satellite imagery and maps may be presented by the litigants or requested by the Court under Article 49 of its Statute. In the oral proceedings in the *Kasikili/Sedudu Island* case, for instance, Judge Ranjeva requested satellite images from both litigants in order to assist the Court in its deliberation.[46] In *Cameroon v. Nigeria (Preliminary Objections)*, Nigeria submitted to the ICJ a satellite image of the disputed area to demonstrate its location.[47] In *Qatar v. Bahrain*, Qatar produced several satellite images although Bahrain contested its analysis of an image of the shoal of Qit'at Jaradah and the method by which it had been created. [48] In *Oil Platforms*, the United States submitted images from US reconnaissance

[42] M Williams, 'Satellite Evidence in International Institutions', in Purdy and Leung (n 6) 201.
[43] The 'app' is available at <http://www.eyewitnessproject.org>.
[44] K Covert, 'An eye for atrocity? There's an app for that', *National*, 9 June 2015, <http://www.nationalmagazine.ca/Blog/June-2015/An-eye-for-atrocity-There-s-an-app-for-that.aspx>.
[45] AC Nuñez M, *Admissibility of Remote Sensing Evidence Before International and Regional Tribunals*, Innovation in Human Rights Monitoring Working Paper (August 2012), 2, <http://www.amnestyusa.org/pdfs/RemoteSensingAsEvidencePaper.pdf>.
[46] *Case concerning Kasikili/Sedudu Island (Botswana/Namibia)*, Pleadings, CR1999/3, 69. In its Counter-memorial, Botswana had already submitted several satellite images and had relied on them in its arguments ([1999], ICJ Rep, paras 29, 36).
[47] *Case concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v Nigeria: Equatorial Guinea Intervening)* (Preliminary Objections), Pleadings, CR 1998/1, para 30, <http://www.icj-cij.org/docket/files/94/4833.pdf>. The image was not relied on by Nigeria in the merits phase, although it annexed other satellite images to its Counter-memorial.
[48] *Case Concerning Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v Bahrain)*, Pleadings, CR 2000/9, 51, <http://www.icj-cij.org/docket/files/87/5467.pdf>.

satellites to refute Iran's claim that there were no missiles in the Faw area and supported the images with expert testimony during the oral proceedings in the merits.[49] The United States, however, refrained from submitting high resolution satellite images for national security reasons, but argued that reducing the resolution of the original images had not affected their integrity.[50] In the end, the Court did not find the images sufficiently clear.[51] In the *Bosnian Genocide* case, the ICJ relied on a UN report that based its findings, *inter alia*, on satellite photos.[52] Georgia also relied on satellite imagery to prove that Russian forces were present in the disputed region and that ethnic cleansing was occurring there.[53] In *Pulp Mills*, Argentina referred to various satellite images showing the concentration of chlorophyll in the River Uruguay.[54] In *Aerial Herbicides Spraying*, Colombia submitted extensive satellite evidence, using false colour renderings to show vegetation, in some cases overlaid with the GPS tracks of the spray flights.[55] In *Certain Activities (Costa Rica v. Nicaragua)*, Costa Rica relied on satellite imagery in order to show that Nicaragua had dug the *caño* and cleared vegetation.[56]

Like any other audiovisual evidence, satellite images and maps must be presented by the litigants either as annexes to the written pleadings or during the oral proceedings: in the latter case, they may be excluded because of the opposition of the other litigant.[57] This is so unless the satellite images are 'readily available' in the sense of Article 56(4) of the Rules of Court, for instance when they can be easily found on the internet as in the case of Google Earth images. In *Nicaragua v. Honduras*, Honduras produced a satellite image in the oral proceedings arguing that it should not be considered a 'new document' because it was readily available on the internet.[58] It is not clear whether the Judgment accepted Honduras's claim.

---

[49] *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits), Counter-Memorial and Counter-Claim of the United States of America, 23 June 1997, 48-49, <http://www.icj-cij.org/docket/files/90/8632.pdf>.
[50] *Oil Platforms*, US Counter-memorial and Counter-claim (n 49) 49, footnote 125.
[51] *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits), [2003], ICJ Rep, para 58.
[52] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Merits), [2007], ICJ Rep, para 229.
[53] *Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Georgia v Russian Federation)*, Pleadings, CR 2008/22, 48-50.
[54] *Pulp Mills on the River Uruguay (Argentina v Uruguay)*, [2010], ICJ Rep, para 248.
[55] *Aerial Herbicide Spraying (Ecuador v Colombia)*, Counter-memorial of Colombia, vol I, 29 March 2010 <http://www.icj-cij.org/docket/files/138/17548.pdf>; Rejoinder of the Republic of Colombia, vol II, 1 February 2012, Annex 6, Expert Report by Dr. Barry M. Evans, 129 ff. <http://www.icj-cij.org/docket/files/138/17566.pdf>.
[56] *Certain Activities (Nicaragua v Costa Rica)* (n 22) paras 80-81.
[57] Art 56 of the Rules of Court.
[58] *Territorial and Maritime Dispute between Nicaragua and Honduras in the Caribbean Sea (Nicaragua v Honduras)*, Pleadings, CR 2007/8, para 56. Nicaragua had also produced a satellite image that was allowed by the Court as 'readily available' ([2007], ICJ Rep, para 12). It can also be recalled that, in the

Satellite evidence is the result of a process that includes several stages: raw data are collected by satellites and sent to ground stations, where they are processed and made available in digital form as well as enhanced, if need be, through the use of computers.[59] If the raw data, at least in their initial stage, cannot be modified, manipulation can occur at the interpretation stage and may be difficult to detect.[60] In practice, however, the certificate of authenticity from the Agent is taken at face value unless challenged. Commercially available satellite imagery was simply submitted identifying its source and the date of the image (with a certification from the Agent as to its authenticity) in both *Aerial Herbicides Spraying* and *Costa Rica v. Nicaragua* (especially in Costa Rica's second provisional measures application). In *Aerial Herbicide Spraying*, in particular, Colombia's satellite imagery was annexed to an expert report by the geographer who had created the images, which explained the process undertaken to create them. However, the chain of custody was limited to stating that he had received the images from the commercial provider and that he had subsequently performed the relevant manipulations.[61]

Litigants could of course disagree on the accuracy and reliability of satellite imagery, both in relation to how the image was constructed from raw data and to how the image was interpreted.[62] In such cases, the parties will normally put forward competing expert evidence on the question.[63] Indeed, even though, according to Article 50 of the ICJ Statute, '[t]he Court may, at any time, entrust any individual body, bureau, commission, or other organization that it may select, with the task of carrying out an enquiry or giving an expert opinion',[64] it will normally decide any issue on the basis of parties' evidence, rather than engaging its own experts to carry out independent analysis.[65] The ICJ could also in the future consider hiring a permanent expert or a panel

---

Palestinian Wall Advisory Opinion, the Court relied on a map available on the Israeli Ministry of Defence's website in order to establish the existing and proposed route of the security fence in the Palestinian Territories (*Legal consequences of the construction of a wall in the occupied Palestinian territory* (Advisory Opinion [2005] ICJ Rep para 80).

[59] Williams (n 42) 200-201.

[60] Williams (n 42) 211.

[61] *Aerial Herbicide Spraying (Ecuador v Colombia)*, Rejoinder of the Republic of Colombia, vol II, 1 February 2012, Annex 6, Expert Report by Dr. Barry M. Evans, 129 ff. <http://www.icj-cij.org/docket/files/138/17566.pdf>.

[62] Riddell and Plant (n 10) 292.

[63] In *Pulp Mills*, the ICJ was critical of the use of expert counsels by the parties and reminded them that, in oral proceedings, 'those persons who provide evidence before the Court based on their scientific or technical knowledge and on their personal experience should testify before the Court as experts, witnesses or in some cases in both capacities, rather than counsel, so that they may be submitted to questioning by the other party as well as by the Court' (*Pulp Mills* (n 54) para 167).

[64] See also art 67 of the Rules of Court.

[65] The Court has been reluctant to appoint experts under art 50 of its Statute. See, eg, the rejection of the suggestion that the Court appoint an expert in *Certain Activities (Costa Rica v. Nicaragua)* (n 22) para 226.

of advisors that could assist it in the evaluation of digital evidence. It would not be the first international court to do so: in 2013, the Office of the Prosecutor of the International Criminal Court (ICC) hired an expert in digital forensics for its Scientific Response Unit to improve its ability to collect and analyse digital evidence.[66]

4. Is illegally obtained digital evidence admissible?

While remote sensing from satellites is generally not deemed to be a violation of international law,[67] the legality of unauthorized 'transborder access'[68] by the investigative authorities of a state to data stored in another state is dubious. In addition to issues related to data protection and the privacy of any individuals whose data are accessed, transborder access is an 'exercise of power'[69] by a state performed on the territory of another state whenever the data are stored in computer systems physically located on the territory of that state, even if the data are accessed remotely.[70] Article 32 of the 2001 Budapest Convention on Cybercrime addresses the problem and provides that '[a] Party may, without the authorisation of another Party: a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'.[71] It has been suggested that at least the first case

[66] Human Rights Center (n 6) 5.
[67] The matter, however, is not uncontroversial: see R Purdy, 'Pulling the Threads Together and Moving Forward', in Purdy and Leung (n 6) 413-415. The UN Principles Relating to Remote Sensing of the Earth from Space, adopted by the General Assembly in 1986, state that remote sensing activities must be conducted 'in accordance with international law, including the Charter of the United Nations, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, and the relevant instruments of the International Telecommunication Union' (Principle III, GA Res. 41/65, 3 December 1986). The document does not address privacy issues, as the technology in use at the time it was adopted did not raise concerns in this sense (Purdy (n 67) 418).
[68] The expression includes, in addition to access, copying and seizing (A-M Osula, 'Accessing Extraterritorially Located Data: Options for States', CCDCOE, 2015, 18, <https://ccdcoe.org/multimedia/accessing-extraterritorially-located-data-options-states.html>).
[69] *The Case of the S.S. "Lotus" (France v Turkey)*, Judgment No. 9, 1927, P.C.I.J., Series A, No 10, 18.
[70] J Bourguignon, 'La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat', in Société Française pour le Droit International, *Internet et le droit international, Colloque de Rouen* (Pedone 2014) 362. One commentator has argued that 'the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty' (W Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *Naval War College International Law Studies* 129).
[71] The text of the Convention is in (2002) 41 *International Legal Materials* 282 ff.

identified in Article 32, that of publicly accessible data (ie without the need for passwords or authorisations), reflects customary international law.[72] On the other hand, Article 32(b) seems to be opposable only to parties to the Cybercrime Convention.[73] Under customary international law, outside the case of open source data, the consent of the affected person (be it the user or the internet service provider or another subject) is not sufficient to allow unilateral transborder search by foreign authorities: the competent organs of the territorial state must authorise the search, without which transborder access is a violation of the sovereignty of the territorial state.[74]

Is digital evidence collected by a litigant through unauthorised transborder access admissible before the ICJ? There is no express rule in the Court's Statute providing that evidence obtained through a violation of international law is inadmissible.[75] It is also not a general principle of law, as it seems to be a rule essentially confined to the US criminal system.[76] As Thirlway argues, the rule in domestic legal systems is motivated by the need to protect the defendant against the wider powers of the prosecutor and its possible abuses: in inter-state litigation, there is no criminal trial and no dominant party, as the litigants are states which are formally in a position of sovereign equality.[77] In the *Corfu Channel* case, the United Kingdom claimed that its actions in Albania could be justified on 'a new and special application of the theory of intervention, by means of which the State intervening would secure possession of evidence in the territory of another State, in order to submit it to an international tribunal and thus facilitate its task'.[78] While the ICJ rejected this defence, it did not dismiss the evidence illegally obtained by the United Kingdom in Operation Retail; on the contrary, it relied on it in

---

[72] Council of Europe, *Transborder access and jurisdiction: What are the options?*, Report of the Transborder Group of the Cybercrime Convention Committee, 6 December 2012, 56 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8>; Bourguignon (n 70) 369-370; N Seitz, 'Transborder Search: A New Perspective in Law Enforcement?', (2004-2005) 7 *Yale Journal of Law and Technology* 38.

[73] The already mentioned Council of Europe Report concedes that, in relation to the situations covered in art 32(b), 'overall, practice, procedures as well as conditions and safeguards vary considerably between different States. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or "in the clouds" as well as national sovereignty persist and need to be addressed' (*Transborder access* (n 72) 58). *Contra*, but without much justification, see Seitz (n 72) 45.

[74] Bourguignon (n 70) 362-363; Osula (n 68) 7, 19.

[75] It has been argued, however, that evidence obtained through a *jus cogens* violation, for instance torture, should be deemed inadmissible (Wolfrum (n 2) 563).

[76] H Thirlway, 'Dilemma or Chimera? – Admissibility of Illegally Obtained Evidence in International Adjudication', (1984) 78 AJIL 627-28; N Hasan Shah, 'Discovery by Intervention: The Right of a State to Seize Evidence Located Within the Territory of the Respondent State', (1959) 53 AJIL 607-609. See *contra* Wolfrum (n 2) 563.

[77] Thirlway (n 76) 628-29.

[78] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* (Merits), [1949], ICJ Rep 34.

order to determine the place of the accident and the nature of the mines.[79] In fact, Albania never challenged the admissibility of the evidence acquired by the British Navy,[80] and the Court did not address the question. What it found was that the purpose of gathering evidence did not exclude the illegality of certain conduct of the United Kingdom.[81] In the digital context, by analogy this means that the fact that digital evidence is stored in the computers or servers located in another state does not entitle the interested litigant to access them without authorization from the competent authorities in order to submit the evidence in the proceedings. If the evidence is unlawfully collected, however, it is unlikely that it will be considered inadmissible by the ICJ on grounds of its illegality alone. The probative weight of the collected evidence will also not depend on whether it was collected legally or illegally, but on the demonstration of its authenticity and accuracy. While the Court's liberal approach with regard to the admissibility and probative value of evidence illegally collected may at first sight be seen as a possible challenge to international legality as it could encourage such practice, this should be seen in the context of the consensual characteristics of international litigation, where the disputants are states in a position of sovereign equality: as Thirlway observes, 'a state adducing evidence obtained by means that could be challenged would run the risk not merely of seeing the evidence in question excluded, but also of a finding of fact against it of, in effect, international responsibility on the basis of a purely incidental jurisdiction of a procedurally interlocutory nature. The inconsistency of such a structure with the basically consensual nature of international jurisdiction is flagrant'.[82]

5. Conclusions

As the ICJ approaches its seventieth anniversary, it is easy to predict that, with the progresses and wider availability of technology, digital evidence will be increasingly used before it. As has been seen, however, the production of digital evidence raises certain questions, some of which have been addressed in this article.

The fact remains that, apart from one exception, there are no rules or directions that specifically address the production and assessment of digital evidence in proceedings before the ICJ. *De lege ferenda*, should the production of digital evidence

[79] Hasan Shah (n 76) 606-607.
[80] Thirlway (n 76) 632.
[81] *Corfu Channel* (n 78) 34-35.
[82] Thirlway (n 76) 638-639.

in ICJ proceedings be specifically regulated, or should the general rules on evidence continue to apply to it? Although – as has been argued in this article - the absence of specific rules and procedures for digital evidence is not necessarily an obstacle to its production and evaluation, it is unquestionable that adopting specific regulations that take into account the peculiarities of digital evidence would help the ICJ judges and the litigants make a more effective use of this increasingly important means of proof. The Court, therefore, could amend its Rules or adopt Practice Directions specifically addressing issues related to digital evidence, as already happened with Practice Direction IX *bis*. Having said that, even if specific regulation may be needed as to the way in which authenticity and chain of custody of digital evidence are to be established, the particular facts of the case and the grounds of challenge can vary widely, and it is doubtful that any regulation could be sufficiently flexible to deal with this in advance.