TOAEP | Torkel Opsahl Academic EPublisher

Quality Control in Preliminary Examination: Volume 2

Morten Bergsmo and Carsten Stahn (editors)

PURL: http://www.legal-tools.org/doc/6706c9/

E-Offprint:

Alexa Koenig, Felim McMahon, Nikita Mehandru and Shikha Silliman Bhattacharjee, "Open Source Fact-Finding in Preliminary Examinations", in Morten Bergsmo and Carsten Stahn (editors), *Quality Control in Preliminary Examination: Volume 2*, Torkel Opsahl Academic EPublisher, Brussels, 2018 (ISBNs: 978-82-8348-111-2 (print) and 978-82-8348-112-9 (e-book)). This publication was first published on 6 September 2018. TOAEP publications may be openly accessed and downloaded through the web site www.toaep.org which uses Persistent URLs (PURLs) for all publications it makes available. These PURLs will not be changed and can thus be cited. Printed copies may be ordered through online distributors such as www.amazon.co.uk.

This e-offprint is also available in the Legal Tools Database under PURL http://www.legal-tools.org/doc/6706c9/. It is noteworthy that the e-book versions of *Quality Control in Preliminary Examination: Volumes 1 and 2* contain more than 1,000 hyperlinks to legal sources in the Database. This amounts to a thematic knowledge-base that is made freely available as an added service to readers.

Front cover: *Alberto Gandolfi inspects his fresco of Hugo Grotius in Florence. Trained for years in fresco painting and restoration, including at the Accademia di Belle Arti di Firenze, he employs the fresco techniques used since the 1400s in Florence, including preparing ingredients such as the lime plaster himself. An exceptional level of quality control of the preliminary stages is required for the paintings to stand the test of time. Photograph: © CILRAP 2017.*

Back cover: *Section of a Roman street close to where the Statute of the International Criminal Court was negotiated, paved with 'sampietrini' cobblestones of trimmed, black basalt-cubes. When each stone is precisely cut and placed, they make up a robust and attractive whole, with the ability to withstand pressure and inundation. Preliminary examination is similarly made up of numerous small steps, each of which should be undertaken with proper quality control. Photograph: © CILRAP 2018.*

34

Open Source Fact-Finding in Preliminary Examinations

Alexa Koenig, Felim McMahon, Nikita Mehandru and Shikha Silliman Bhattacharjee*

34.1. Introduction

In national and international criminal jurisdictions, preliminary examination refers to a pre-investigative stage of prosecution during which available information is examined to determine whether a threshold for further engagement is met. In the context of the International Criminal Court ('ICC'), the Office of the Prosecutor ('OTP') makes an informed determination about whether there is enough information to proceed to a full investigation.

Article 15(3) of the Rome Statute sets the threshold for determining whether the available evidence is sufficient, requiring a "reasonable basis" to advance to investigation.[1] In making this determination, the OTP must grapple with all of the information at its disposal, including both tradi-

* **Alexa Koenig** (J.D., Ph.D.) is the Executive Director of the Human Rights Center and Lecturer-in-Residence at the UC Berkeley School of Law; **Felim McMahon** (M.A.) is the Technology and Human Rights Program Director at the UC Berkeley School of Law; **Nikita Mehandru** (B.A., Claremont McKenna College) and **Shikha Silliman Bhattacharjee** (J.D., Ph.D. candidate) are researchers affiliated with the Human Rights Center. The authors thank Caitlin Hoover and Michelle Lee for their research support and Lindsay Freeman for her feedback on earlier drafts of this chapter.

1 Office of the Prosecutor ('OTP'), International Criminal Court ('ICC'), *Policy Paper on Preliminary Examinations*, 2013 ('OTP 2013'), para. 24 (http://www.legal-tools.org/doc/acb906/). As explained in the introductory remarks, the Paper "describes the OTP's policy and practice in the conduct of preliminary examinations, that is, how the Office applies the statutory criteria to assess whether a situation warrants investigation. The paper is based on the Rome Statute […], the Rules of Procedure and Evidence […], the Regulations of the Court […], the Regulations of the Office of the Prosecutor, the Office's prosecutorial strategy and policy documents, and its experience over the first years of its activities. [The Paper reflects] an internal policy of the OTP. As such, it does not give rise to legal rights, and is subject to revision based on experience and in light of legal determinations by the Chambers of the Court" (paras. 19, 20).

tional and newer forms of evidence. Such data streams include a wide range of digital sources that can be accessed through open source investigations – that is, online investigations that involve combing through publicly accessible resources for information related to potential crimes.[2]

Since the OTP does not have full investigative powers at the preliminary examination phase,[3] rigorous collection and analysis of open source information can play a significant role in shaping preliminary examination outcomes. Open source investigation and analysis can be used to authenticate existing information and discover new materials and sources.[4]

According to the OTP, preliminary examinations are governed by established internal standards, including standard formats for analytical reports, specific methods of source evaluation, consistent practices for measuring internal and external coherence, and a commitment to using information from diverse and independent sources as a means of bias control.[5] As information ecologies evolve, these standards must continuously adapt to the range and scale of available open source materials.

The OTP routinely uses open source information in preliminary examinations and, accordingly, has taken steps to grapple with a rapidly evolving context. These measures include engaging in meetings, workshops, and bilateral conversations with human rights organizations to discuss the range of scientific and digital technologies that can assist the Office in its use of open source materials. Among other considerations, these conversations have focused on harnessing data via remote sensing and satellite imaging, as well as how to manage the 'coming storm' of potential evidence from social media – a storm that has arguably arrived.[6]

---

2 For the purposes of this chapter, 'open sources' include news media, academic publications, public reports, social media as well as online video and image sharing services. Clive Best, "Open source intelligence", in Françoise Fogelman-Soulié (ed.), *Mining massive data sets for security: advances in data mining, search, social networks and text mining, and their applications to security*, IOS Press, Amsterdam, 2008, pp. 331-344.

3 OTP 2013, para. 12, see *supra* note 1.

4 Alexa Koenig, *The New Forensics: Using Open Source Information to Investigate Grave Crimes*, Human Rights Center, 2018 (forthcoming).

5 OTP 2013, para. 32, see *supra* note 1.

6 Human Rights Centre, UC Berkeley School of Law, "Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court" (http://www.legal-tools.org/doc/a95842/). *Idem*, "Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court" (http://www.legal-tools.org/

The ICC is far from alone in these conversations. In this digital age, methodologies for discovering, verifying and analysing information from open sources have changed rapidly, including in the context of journalism, policing, and government intelligence. Investigative journalists are experimenting with more efficient ways of using social media and embracing new technologies to monitor global events. Human rights organizations like WITNESS are training activists in how to document atrocities with an eye to maximizing court admissibility and the weight of any videos they produce.[7]

Reflecting these recent developments, the question at the heart of this chapter is: "how can evolving practices around the use of online open source information be harnessed to improve the quality of preliminary examinations at the ICC?". This issue, which resides at the intersection of international criminal justice, human rights, and law and technology scholarship, has yet to be adequately addressed in legal and academic analysis. Finding an answer, we argue, is particularly important in the context of our rapidly expanding digital information ecosystem, in which information sources and transmission practices are continuously evolving.

Bringing together international criminal justice and human rights scholarship and practice, this chapter raises critical issues, including quality control, related to the use of open source information in preliminary examinations. Section 34.2. of this chapter outlines the historic use of open source information to show how the comparatively recent use of such data by the OTP fits into the larger context of information gathering for effective prosecution. This section describes shifts in available types of open source information and maps the transition from military, political, and diplomatic uses of open source intelligence – with governments as the primary agents of retrieval, extraction, and analysis – to our contemporary context. This context is driven by the relatively recent proliferation of smartphones, social media, and other networked public repositories as civil society has increasingly emerged as an agent in both intelligence gathering and information generation.

doc/84e097/). *Idem*, "First Responders: An International Workshop on Collecting and Analyzing Evidence of International Crimes" (http://www.legal-tools.org/doc/bf0b24/). *Idem*, "The New Forensics: Using Open Source Information to Investigate Grave Crimes" (http://www.legal-tools.org/doc/e7b0b9/).

7 WITNESS, "Video as Evidence Field Guide" (https://www.legal-tools.org/doc/a1c088-1/).

Section 34.3. discusses the factors the OTP weighs when using information derived from open sources to support preliminary examinations and explains how open source material can strengthen the preliminary examination process. It opens by discussing three core principles that are supposed to guide that process: (1) independence, (2) impartiality, and (3) objectivity.[8] Next, consistent with the Policy Paper on Preliminary Examinations released by the OTP in 2013, the section considers three statutory factors that guide preliminary examination processes: (1) jurisdiction, (2) admissibility, and (3) the interests of justice. Finally, this section addresses the implications of open source information for three policy objectives at the preliminary examination phase: (1) transparency, (2) ending impunity through positive complementarity, and (3) the prevention of crimes. In the context of each of these factors, this chapter discusses the implications of open source information gathering for quality control standards in preliminary examination. We argue that effective methods for gathering and rigorously analysing open source information are essential to the preliminary examination process and, if optimally conducted, present significant opportunities to improve associated outcomes.

34.2. The Rise of Open Source Investigations for Intelligence Gathering and Human Rights Monitoring

Governments have long utilized open source information in military, political, and diplomatic contexts to shed light on events happening at a distance. Significant shifts in the types of open source information collected by governments have occurred with the proliferation of new information technologies, often motivated by and thus concurrent with periods of political unrest and war. Three distinct eras in the evolution of open source intelligence include: (1) newspaper-based intelligence gathering during the Crimean War (1853–1856); (2) the use of journals and foreign broadcasts during World War II (1939–1945); and (3) the mining of print, radio, television and telephonic communication during the Cold War, and later for human rights monitoring.

A fourth and more recent stage in the evolution of open source information gathering has been driven by the relatively recent proliferation of smartphones, social media, and other networked public repositories –

[8] OTP 2013, p. 7, see *supra* note 1.

including academic and legal communities on portals such as Academia.edu and LinkedIn, as well as social media sites such as Facebook, YouTube, and Twitter. This stage is distinct from the first three because private actors, rather than governments, have emerged as dynamic players in both information generation and intelligence gathering. This expansion of access to the production, dissemination, and collection of open source information has disaggregated and arguably democratized information production and usage.

This history is instructive for at least two reasons. First, the evolving nature of open source information calls for similarly evolving strategies for information collection and verification. Thus, developing rigid policies that cannot accommodate new forms of media will be counterproductive. Second, this history suggests that existing practices governing authentication of open source information that were developed in relation to government-dominated phases of open source intelligence may need rethinking.

34.2.1. Brief History of Open Source Intelligence: 1853 to Present

The Crimean War (1853–1856) – provoked by Russian expansion into the Danube principalities then under Turkish control – positioned Russia against Britain, France, the Ottoman Empire, and Sardinia. Historians of the Crimean War have marked the legacies that this conflict left for future international conflicts. They note the role of nationalism in driving such conflicts, the forming of alliances between world powers, the widespread use of railways as supply lines, and the use of modern warfare, including trench warfare and machine guns.[9]

Equally important, the Crimean War was also the first major global conflict to be covered by wartime correspondents and photojournalists.[10] Thus, this period witnessed the birth of the modern military-media relationship, a distinction largely attributed to the work of British journalist William Howard Russell from *The Times.* Prior to the Crimean War, junior army officers filtered information about wartime activities from battlefronts through letters to newspaper editors. Conversely, Russell, a civilian reporter, unleashed unbridled criticism of the war directly from his posi-

9 "The Crimean War", in *BBC News*, 29 March 2011.

10 *Ibid*.

tion on the frontlines, revealing the awful living conditions of soldiers and the occasional incompetency of army leadership. Coverage of sinking troop morale and experiences by embedded journalists like Russell provided an early source of open intelligence. With Russian and British spies using newspapers to track what was happening around the world, Russell's war coverage became a valuable source of information. This shift in the military-media relationship and the stream of information it produced led then-Russian Emperor Nicholas I to remark: "I have no need of spies, I have the *Times* of London".[11]

A second significant moment in the evolution of open source information occurred during World War II when the United States government systematically invested in developing open source intelligence capacity. As early as 1939, the Princeton School of Public and International Affairs developed the Foreign Broadcast Monitoring Service, which was brought under the ambit of the Federal Communications Commission. On 25 February 1941, President Franklin Delano Roosevelt designated $150,000 from his emergency fund to monitor foreign broadcasts for intelligence purposes.[12] Following the attack on Pearl Harbor in December 1941, the Foreign Broadcast Monitoring Service was renamed the Foreign Broadcast Intelligence Service, responsible for tracking foreign short-wave radio signals to extract intelligence.[13]

Meanwhile, the Roosevelt administration had also established the Office of the Coordination of Information, tasked with analysing information collected abroad.[14] In June 1942, the Office of the Coordination of Information became the Office of Strategic Services, directed to conduct both espionage against the Axis powers and in-depth research and analysis on designated national enemies and their capabilities.[15] The Office's Research and Analysis Branch collected newspaper clippings, journals, and radio broadcast reports from around the world that could provide valuable

[11] David Murphy, *Ireland and the Crimean War*, Four Courts Press, Dublin, 2014, p. 174.

[12] Central Intelligence Agency, "Early Beginnings" (http://www.legal-tools.org/doc/0c9562/).

[13] Central Intelligence Agency, "Impact of Pearl Harbor Attack" (http://www.legal-tools.org/doc/669689/).

[14] Central Intelligence Agency, "A Look Back … Gen. William J. Donovan Heads Office of Strategic Services", 31 December 2009 (available on the Agency's web site).

[15] Central Intelligence Agency, "A Look Back … Gen. William J. Donovan Heads Office of Strategic Services", see *supra* note 16.

intelligence.[16] Obituaries of soldiers or navy officers in German newspapers, for instance, could include images of battleships and bomb craters that facilitated an understanding of German technologies, some of which were reverse engineered for American use.[17]

In 1946, following the war's conclusion, first the Office of Strategic Services and then the Foreign Broadcast Intelligence Service were dissolved. Their respective roles were concentrated in the Central Intelligence Agency ('CIA'), established under President Truman by the National Security Act.[18]

During this period, the Soviet Union gained parity with intelligence operations in the United States. The Ministry of State Security (MGB) was one of the USSR's many iterations of intelligence agencies, and played a prominent role during World War II. It was succeeded by the Committee for State Security (KCG), which served as the Community Party's watchdog, with the added objective of monitoring domestic counterintelligence efforts.[19]

In addition to the expanded *number* of organizations collecting open source information, the Cold War era witnessed an explosion of new *means* for intelligence gathering, specifically radio, television, and real time phone communication. It was towards the end of this third era, in the late 1980s, that the US military first coined the term 'OSINT' to reference open source intelligence.[20] Scrutiny of foreign press, propaganda, and radio initiated during World War II was extended and expanded, not only by the United States but by all other major national government players.[21] One inside source at the time remarked in response to this enormous growth that, "in aggregate, open sources probably furnish the greater part

16 Cameron Colquhoun, "A Brief History of Open Source Intelligence", in *Bellingcat*, 14 July 2016.

17 *Ibid*.

18 Central Intelligence Agency, "A Look Back … Gen. William J. Donovan Heads Office of Strategic Services", see *supra* note 16.

19 Encyclopedia Britannica, "KGB" (available on its web site).

20 Florian Schaurer and Jan Störger, "The Evolution of Open Source Intelligence (OSINT)", in *Intelligencer: Journal of U.S. Intelligence Studies*, vol. 19, no. 3, Winter/Spring 2013 (available on AFIO's web site).

21 Stephen Mercado, "Sailing the Sea of OSINT in the Information Age", in *CSI Studies*, vol. 48, no. 3, 14 April 2007 (available on the Agency's web site).

of all information used in the production of military intelligence on the Soviet Union".[22]

These public information sources provided near real time access to sites of conflict and other remote events. In the United States, the CIA developed innovative approaches to intelligence gathering, including the use of overhead surveillance systems to collect images of weapons and operational sites.[23] Signal intelligence ('sIGINT') collectors eavesdropped on military exercises, and were deployed covertly in the air, under sea, and within the USSR.[24] The Council of Ministers of East Germany for State Security mined 1,000 Western magazines, hundreds of books, and twelve hours of West German daily radio and television programming.[25] The US publication *Aviation Week* served as a particularly valuable source, fueling East German intelligence gatherings of recent US developments in aerospace.[26] New media forms not only expanded government use of open source intelligence during the Cold War era but facilitated the creation, collection, and use of visual documentation by a variety of stakeholders seeking accountability for government misconduct – including ever-increasing numbers of human rights advocates.

Reflecting on US-North Korea relations at the time, Donald P. Gregg explained, "it is a well-known phenomenon in the field of intelligence that there often comes a time when public political activity proceeds at such a rapid and fulminating pace that secret intelligence, the work of agents, is overtaken by events publicly recorded".[27] Gregg's assessment of the immediacy of press coverage anticipated the next stage in the evolution of open source intelligence, when nongovernmental actors emerged as participants in both information generation and intelligence gathering.

---

22 *Ibid*.

23 Clarence E. Smith, Central Intelligence Agency, "CIA's Analysis of Soviet Science and Technology", in Gerald K. Haines and Robert E. Leggett (eds), *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, 2003, chap. 4 (available on the CIA's web site).

24 *Ibid*.

25 Schaurer and Störger, see *supra* note 23.

26 Mercado, see *supra* note 24.

27 Donald P. Gregg, "A Long Road to P'yongyang", in *Korea Society Quarterly*, Spring 2002, vol. 3, no. 1, p. 7.

This third era is marked by the accelerated creation of visual and print- based documentation of human rights abuses by organizations such as the New York Civil Liberties Union, American Civil Liberties Union ('ACLU'), Amnesty International, and Helsinki Watch – a precursor to Human Rights Watch. For instance, in order to document police violence, ACLU staff, armed with movie cameras, posted themselves in buildings overlooking protest sites during the Vietnam war. Aryeh Neier, former director of the ACLU and founder of Human Rights Watch, recalled that when he began working at the ACLU in the mid-1960s, protestors "could not produce witnesses or evidence other than their bruises to support [police brutality] complaints". Addressing this evidentiary gap, lead attorney for the New York Civil Liberties Union, Police Practices Project, Paul Chevigny, used a 'moviola' film editing tool to comb through footage, frame by frame, and capture police abuses. In one instance, Chevigny used segments from a film to clear charges against approximately 600 demonstrators, establishing that police who claimed to have arrested activists were, in fact, providing false testimony against those activists. These practices, developed at the New York Civil Liberties Union, were embraced by the ACLU in the early 1970s. In a landmark case, the ACLU used activist footage to clear charges against 13,000 demonstrators and to secure damages.[28]

Amnesty International similarly used open source information to support their investigations and produce publicly accessible data for use by others. Established in Britain in 1961 to provide amnesty for prisoners of conscience, by 1963, Amnesty International had founded an international secretariat and expanded its mandate to include global engagement.[29] The Amnesty staff, comprised almost entirely of volunteers, "regularly scanned [foreign newspapers] for information about those imprisoned", developed detailed reports, and filed prisoner-specific information on index cards. During their first year in operation, Amnesty volunteers, many housed in universities, produced approximately 1,200 prisoner histories. These histories were made available to the press and other interest-

[28] Aryeh Neier, *Taking Liberties: Four Decades In The Struggle For Rights*, Public Affairs, New York, 2003, p. 19.

[29] For a brief overview of the transition from the domestic orientation of the United States based civil rights movement into an international human rights endeavour, see *ibid*.

ed bodies,[30] a practice that facilitated frequent partnerships between Amnesty and news outlets, including the BBC.[31] Amnesty International also published research in journals and newsletters.[32] Now operating in around 70 countries, Amnesty International both consumes and produces publicly-accessible data for use in a range of human rights campaigns and initiatives.[33]

By 1978, production of publicly accessible data was directed at monitoring compliance with international agreements and legal standards. Helsinki Watch was established in 1978 to support citizen groups formed throughout the Soviet bloc to monitor government compliance with the 1975 Helsinki Accords.[34] Helsinki Watch later morphed into a series of regional 'Watches' to monitor abusive governments in disparate parts of the world, eventually collectivizing into Human Rights Watch. The Human Rights Watch mandate, to monitor and document abuse, expanded in the 1990s to tracking violations of humanitarian law.[35] Today, the Human Rights Watch International Justice programme works closely with the ICC, other international and hybrid tribunals, and national courts to bring justice to perpetrators who have committed war crimes and crimes against humanity.[36]

By the late 1980s, in concert with the rise of these large non-governmental organizations, smaller civil society organizations had also begun using still and video cameras to document human rights abuses. In 1988, while on a humanitarian tour with a group from Amnesty International, activist and musician Peter Gabriel used his Sony Handycam to record survivor stories. A few years later, in 1991, a bystander captured the brutal beating of Rodney King, an African-American male, by Los Angeles police. The footage hit television and sparked condemnation and riots that lasted days. In 1992, inspired by these two events, Gabriel established the non-governmental organization WITNESS to train activists

30 Amnesty International, *First Annual Report 1961-1962*, Temple, London, 1962, p. 5.

31 *Ibid*., p. 11.

32 *Ibid*., p. 10.

33 Amnesty International, "Who We Are" (available on its web site).

34 Human Rights Watch, "History" (available on its web site).

35 *Ibid*.

36 Human Rights Watch, "International Justice" (available on its web site).

around the world in the effective use of video documentation for human rights purposes.[37]

By this time, the Internet had dramatically changed the accessibility of a wide range of public information. In military information gathering contexts, an emergent pool of information online necessitated a fresh look at the use of non-classified information for military purposes. Increasingly, videos, photographs and satellite imagery, including images collected through remote sensing by drone, were being used not only for military, political and foreign policy purposes,[38] but to support legal accountability. One particularly notable example is the use of perpetrator footage in the now-infamous Skorpions case at the International Criminal Tribunal for the former Yugoslavia ('ICTY').[39] The footage was passed along from activists to ICTY prosecutors, and ultimately used to help establish the killings that were alleged to have occurred, who committed them, and how.[40] Increasingly, video content generated in conflict zones began to be used as evidence in war crimes cases around the world. As that content began to flood the internet, new opportunities emerged for both accessing and analysing such resources.

34.2.2. The Shifting Nature of the Internet: Web 1.0 to Web 2.0

The fourth era in the evolution and use of open source information – the one we are in today – is meaningfully distinct from the first three stages in part because individual (as opposed to organizational) actors have emerged as central participants in both the process of information generation and intelligence gathering. This is largely due to the availability of open source information on the Internet. This evolution can be described as a transition from exploiting the first generation of Internet-based re-

37 Peter Gabriel, "WITNESS", available at *PeterGabriel.com*.

38 Steven Livingston, *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention*, Joan Shorenstein Centre on the Press, Politics and Public Policy, John F. Kennedy School of Government, Harvard University, 1997.

39 Alexa Koenig, Keith Hiatt, and Khaled Alrabe, "Access Denied? The International Criminal Court, Transnational Discovery, and The American Servicemembers Protection Act", in *Berkeley Journal of International Law*, 2018 (forthcoming) (discussing the use of video as evidence in international courts).

40 *Ibid*.

sources on Web 1.0 (the 'readable' phase of the Internet) to discovering materials available during its next, 'writable' stage: Web 2.0.[41]

During the early years of the Internet, Web version '1.0' was a relatively static place from which users could access information from a limited number of sources. While version 1.0 facilitated access to news reports, public statements and official websites, academic articles, and human rights reports, these sources – available at a comparatively limited scale – tended to be relatively stable and attributable to particular national or international sources, and therefore more easily authenticated. While Web 1.0 made it quicker and easier to find information related to an investigation when compared with analogue sources, the type of information available online was not radically different from what could otherwise be found in a physical library. The ways in which Web 1.0 data and resources were used were also similar to engaging with traditional information sources.

The Internet has since evolved to become a more dynamic environment, one that permits significant interaction between users and sites, and features a greater diversity of resources, including citizen journalism, social media, and data derived from social science to hacktivism to leaks. Referred to as 'Web 2.0', this writable world of expanded online open source information presents new opportunities and challenges. Web 2.0 is marked by an exponential expansion of online content that includes "profile pages, public messages, digital photographs, video, chat transcripts, [and] private messages"[42] and the enabling of two-way communication between user and platform, and between user and user.

This next generation of the Internet was driven in part by the proliferation of smartphones, social media, and networked public repositories, such as digital archives, during the first two decades of the twenty-first century. Today, Web 2.0 open sources are increasing exponentially. For instance, as of early 2017, there were reportedly more hours of citizen footage documenting the Syrian war than had taken place during the war

41 Riaan Rudman and Rikus Bruwer, "Defining Web 3.0: opportunities and challenges", in *The Electronic Library*, 2016, vol. 34, no. 1, pp. 132–154 (discussing the evolution of Web 1.0 to 2.0 as well as the emergence of later versions).

42 Christopher Boehning and Daniel Toal, "Authenticating Social Media Evidence", in *New York Law Journal*, 2002, vol. 248, no. 65, p. 2.

itself.[43] In addition to volume challenges, this next generation requires new approaches to assessing veracity, since sources may be transitory, manipulated and/or lack attribution. Importantly, the repeat sharing of content hinders the potential to identify an incident's veracity by potentially obscuring its source. Since metadata – information about the content – can be stripped away, it may be difficult to corroborate critical information about the videographer, uploader, time, date and place. These features of Web 2.0 sources require new modes of retrieval, extraction and analysis – including new methods for source verification and credibility assessment.

Importantly for legal accountability, version 2.0 has also facilitated access to information about human rights abuses and alleged war crimes. For example, in 2007, rising fuel prices in Myanmar combined with decades of political oppression and human rights abuses by the Burmese government triggered massive demonstrations.[44] Termed the 'Saffron Revolution', civilian video footage documented daily protests despite government attempts to suppress Internet access.[45] In 2009, the Green Revolution in Iran was marked by millions of young Iranians sharing real-time videos from Tehran.[46] Twitter and Facebook served as platforms to document the revolution and encourage international observers to stand in solidarity. The movement helped instigate the advent of citizen journalism, with news from civilians reaching the masses before many, if not most, traditional media outlets.[47] While citizen journalism and mobilization through networked public repositories was perhaps most visible during this Arab Spring period of democracy building,[48] around the same time

43 Andy Greenberg, "Google's New YouTube Analysis App Crowdsources War Reporting", in *Wired*, 20 April 2016.

44 Human Rights Watch, "Crackdown: Repression of the 2007 Popular Protests in Burma" (http://www.legal-tools.org/doc/058507/).

45 "Burmese Government Clamps Down on Internet", in *New York Times*, 28 September 2007.

46 Cameron Colquhoun, "A Brief History of Open Source Intelligence", see *supra* note 19.

47 Jared Keller, "Evaluating Iran's Twitter Revolution", in *The Atlantic*, 18 June 2010.

48 Philip N. Howard and Muzammil M. Hussain, *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Oxford University Press, New York, 2013. Gadi Wolfsfeld, Elad Segev, and Tamir Sheafer, "Social Media and the Arab Spring: Politics Comes First", in *International Journal of Press/Politics*, 2013, vol. 13, no. 2, pp. 115-137 (finding that social media activity tends not to lead political protest activity but to follow it).

'user generated content' was also streaming out of South and Central America, Africa and Asia.

A rise in citizen journalism has been evident even in countries that lag in access to technology. Midia Ninja in Brazil, for example, has been challenging traditional media outlets that have historically been monopolized by powerful Latin American families. Promoting independent journalism, in June 2013 Midia Ninja's citizen journalists were on the ground with citizens protesting Brazilian government spending and education policies.[49] YouTube quickly became one of the primary platforms for sharing relevant video and providing a counter narrative to that disseminated by major broadcasting corporations.

Compared with Web 1.0 open sources, which are relatively static, Web 2.0 sources are dynamic, may be transitory, lack attribution, and/or may increase or spread quickly. By August 2017, as many as 300 hours of video footage were being uploaded to YouTube every minute, a number that continues to rise.[50] Thus, the challenge for activists has become less about how to get information about what is happening in various regions of the world, than to find *relevant* data – to separate the 'signal' from the 'noise.'[51]

By the start of the second decade of the twenty-first century, video footage was not only being increasingly uploaded, but sent from human rights activists directly to courts with the objective of strengthening prosecutions, including at the ICC.[52] Simultaneously, OTP investigators began meeting with human rights organizations to discuss the range of scientific and digital technologies that could assist the court in generating the critical lead, linkage and corroborative evidence needed to identify witnesses, strengthen witness testimony, and pursue successful prosecutions. These conversations focused on harnessing data via remote sensing and satellite

49 Hivos, "Ninja, the rise of citizen journalism in Brazil", 13 August 2013.

50 Danny Donchev, "37 Mind Blowing YouTube Facts, Figures and Statistics – 2017", Fortunelord.

51 For a discussion of source verification and spatial relevance of YouTube footage on the Syrian war, see Michael Storm, Nadine Fattaleh, and Violet Whitney, "Conflict Urbanism: Aleppo Seminar Case Study, Spatializing Syria's YouTube War" (available on the web site of Columbia University).

52 For an overview of the various kinds of evidence that video footage can provide, see WITNESS, "Video as Evidence Field Guide", see *supra* note 10.

imagery, as well as how to manage vast quantities of potential evidence derived from smartphones and social media.[53]

Responding to challenges associated with source verification and credibility assessment, groups like WITNESS and Videre est Credere began training activists in how to document atrocities with an eye to maximizing the court admissibility and weight of any video they produced.[54] Investigative journalists also began experimenting with how to use new technologies, including social media, to monitor global events. For example, the founders of Storyful in Ireland figured out how to scoop major media outlets by collecting open source information from Twitter, Facebook, and other social media platforms, and then systematically verifying and authenticating the information they harvested to maximize its reliability. Human rights activists and legal investigators have since adopted many of these methods to more effectively search publicly accessible resources,[55] sometimes using crowdsourcing to conduct the labor intensive work of digital discovery, verification, and authentication of online open sources.[56]

34.3. The Use of Open Source Information to Advance Preliminary Examinations at the ICC

The preliminary examination process at the ICC is rooted in Article 15 of the Rome Statute, which describes the powers of the Prosecutor. A preliminary examination can be initiated in three ways: (1) on the basis of information sent to the court about crimes within its jurisdiction;[57] (2) via a declaration lodged by a State accepting the exercise of jurisdiction by the

53 Human Rights Centre, UC Berkeley School of Law, "Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court", "Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court", "First Responders: An International Workshop on Collecting and Analyzing Evidence of International Crimes", and "The New Forensics: Using Open Source Information to Investigate Grave Crimes", see *supra* note 9.

54 WITNESS, "Video as Evidence Field Guide", see *supra* note 10.

55 Bellingcat, "About" (available on its web site). Amnesty International, "Digital Verification Corps-Citizen Evidence Lab", available at https://citizenevidence.org.

56 In this context, verification refers to investigating the accuracy of the information while authentication refers to verifying whether the item is what it claims to be.

57 Rome Statute of the International Criminal Court, 17 July 1998, in force 1 July 2002, Article 14 ('ICC Statute') (http://www.legal-tools.org/doc/7b9af9/).

Court;[58] or (3) based on a referral from a State Party[59] or the United Nations Security Council acting under Chapter VII of the United Nations Charter.[60] In the case of a declaration or a referral, the preliminary examination process begins immediately. Otherwise, the Prosecutor is acting *proprio motu*, or on her own initiative based on information about crimes within the jurisdiction of the court.[61]

The Policy Paper on Preliminary Examinations, released by the OTP in 2013, details how a preliminary examination may be initiated, describes its phased approach, and outlines the activities that the Office may carry out during the process. It sets out general principles that are required of the Office in the conduct of its preliminary examination: independence, impartiality and objectivity. It also addresses jurisdiction, admissibility, and the interests of justice – three statutory factors that guide the preliminary examination process.[62] Finally, the Paper identifies three policy objectives for the Office in conducting its preliminary examinations: enhancing transparency, ending impunity, and preventing crimes.[63]

The ultimate objective of the preliminary investigation is to determine whether there is a basis to proceed to a full investigation. ICC judges have interpreted the standard of proof required to open an investigation as a "sensible or reasonable justification" to believe that a crime falling within the jurisdiction of the Court "has been or is being committed".[64] Judges have furthermore indicated that not all of the information available to the Prosecutor must "point towards only one conclusion", adding that such information cannot be expected to be comprehensive or conclusive during a preliminary examination.[65]

---

58 *Ibid*.

59 *Ibid*.

60 *Ibid*.

61 OTP 2013, para. 4, see *supra* note 1 (laying out the various ways in which a preliminary examination can be initiated).

62 ICC Statute, Article 53(1)(a)–(c), see *supra* note 62.

63 OTP 2013, paras. 93–106, see *supra* note 1.

64 ICC, Situation in the Republic of Kenya, Corrigendum of the Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, ICC-01/09-19-Corr, 31 March 2010, paras. 34, 35 (http://www.legal-tools.org/doc/f0caaf/).

65 OTP 2013, para. 11, see *supra* note 1.

Article 15(1) of the Rome Statute leaves open the types of data that can be relied upon during the preliminary examination phase, noting simply that such data should comprise "information on crimes within the jurisdiction of the Court". The 2013 Policy Paper reiterates the breadth of information upon which the Office may rely, stating that it may initiate a preliminary examination "taking into account *any* information on crimes within [its] jurisdiction".[66]

Similarly, the Statute does not limit the sources from which information can be received or solicited. Such information can come "from States, organs of the United Nations, intergovernmental and non-governmental organizations, or other reliable sources".[67] While the 2013 Policy Paper does not specifically mention individuals, unaffiliated persons could also be relied upon by the OTP insofar as they are reliable sources. Additionally, the Prosecutor "may receive written or oral testimony at the seat of the Court" in assessing the "seriousness" of information already in her possession. The OTP can therefore receive, gather or solicit information from almost any source during the preliminary examination phase. This provides the Office with a wide scope and strong incentive to use open source information.

Regardless of how a preliminary examination is initiated, the effective gathering and rigorous analysis of open source information is essential to the process. Since the Office does not "enjoy full investigative powers"[68] during preliminary examination, it is limited in the methods it can employ. The Office may send requests for information to reliable sources and may conduct field missions with the aim of analysing information, but these visits must be limited to collecting further information.[69] Accordingly, the value of open source information in the overall information-seeking context is at its apex at this point in the proceedings. Furthermore, optimum gathering and processing of open source information

66 *Ibid.*, para. 73 (emphasis added).

67 ICC Statute, Article 15(2), see *supra* note 62.

68 OTP 2013, paras. 12–13, see *supra* note 1.

69 For instance, field missions were conducted in Colombia, Guinea, Nigeria, and elsewhere. See Ignaz Stegmiller, "Article 15(2)-Additional information", in *Commentary on the Law of the International Criminal Court*, available at https://cilrap-lexsitus.org/clicc/content/15-2-additional-information (citing ICC, *Report of the Activities of the Court*, 21 October 2013, ICC-ASP/12/28, paras. 72, 74, 77 (http://www.legal-tools.org/doc/b22709/)).

has a greater relative impact during the preliminary examination phase than during the investigation phase, when the full spectrum of State co-operation measures can be activated.

The Office's policy and practice is therefore especially well developed with regard to the use of open source information during preliminary examination, during which open-source approaches are used to gather information about possible crimes, assess information in the Office's possession, and identify further sources of information. The degree to which the Office can rely on open source information does not seem to be limited by either the Rome Statute or Court policy or practice. This wide ambit reinforces the idea that open source information can play a positive role in both triggering and determining the outcome of a preliminary examination.[70]

34.3.1. Guiding principles

The use of open source information in preliminary examination is bound only by the necessity to analyse the information in line with the principles of independence, impartiality and objectivity. These general principles,[71] derived respectively from articles 42, 21(3), and 54(1) of the Rome Statute, define how such information is to be assessed.

34.3.1.1. Independence

Article 42 of the Statute states that the Office shall "act independently of instructions from any external source" and "shall not be influenced or altered by the presumed or known wishes of any party".[72] In the case of a State Party or United Nations Security Council referral, and in relation to

[70] Although not explicitly stated in the Policy Paper, it seems theoretically possible for a preliminary examination to be initiated entirely on the basis of information collected from open sources by the Office of the Prosecutor. In practice, it would be extremely rare for a situation to become the subject of an investigation, a preliminary examination, or a preventive statement without the office receiving any related communications or interacting with an external actor. However, the Rome Statute and Policy Paper do not rule out the possibility that the Office might open a preliminary examination, or even a full examination, on the basis of information derived entirely from its own open source collection and analysis, nor does it limit the degree to which the Office may rely on such information in issuing preventive statements.

[71] OTP 2013, para. 25, see *supra* note 1.

[72] *Ibid.*, para. 26.

Article 15 communications, the Office "is not bound or constrained by the information" it receives. It may seek further information from "reliable sources" and all information is "subject to critical analysis and evaluation".[73]

In practice, Article 42 not only permits but reinforces the importance of effectively using open source information to corroborate existing information and to identify further sources. The principle of independence also requires the Office to develop and apply consistent and defensible standards in analysing and evaluating information received from outsiders, supplementary information received at the request of the Office, and information gathered from open sources.

34.3.1.2. Impartiality

The principle of impartiality is rooted in Article 21(3) of the Statute, which states that the Court shall interpret and apply the law "without any adverse distinction founded on grounds such as gender, age, race, colour, language, religion or belief, political or other opinion, national, ethnic or social origin, wealth, birth, or other status".[74] According to the Policy Paper, this requires the Office to "apply consistent methods and criteria, irrespective of the states or parties involved or the person(s) or group(s) concerned".[75] The principle of impartiality thus reinforces the need to develop and apply a methodology around open source information and information collection more generally that does not unfairly disadvantage persons or groups based on unequal access to modern information and communication technologies.

In developing preliminary examination methodologies in relationship to a wide range of open source information, impartiality as a governing principle requires continued attention to ensuring that the use of open source information does not disadvantage persons on the basis of their being on the wrong side of the digital divide or otherwise poorly represented. The Policy Paper states that the OTP "seeks to ensure that […] all relevant parties are given the opportunity to provide information".[76] The

[73] *Ibid.*, para. 27.

[74] *Ibid.*, p. 7, fn. 15.

[75] *Ibid.*, para. 28.

[76] *Ibid.*, para. 33.

principle of impartiality and the wider requirements of Article 21(3) therefore stand as a corrective to an over-reliance on digitally derived open source information.

The principle of impartiality also points to the importance of governmental organizations, the UN system, non-governmental organizations, civil society, and other 'first responders' in rendering situations and their complexities visible to criminal jurisdictions. Further, it reinforces the importance of systematically accessing mass communication platforms associated with modern information communication technologies that are increasingly being used by underrepresented groups in order to identify and integrate their experiences and perspectives.

34.3.1.3. Objectivity

The 2013 policy paper derives the principle of objectivity from Article 54(1), which provides that the Office will "investigate incriminating and exonerating circumstances equally". The Paper notes that, because the information assessed in preliminary examinations is mainly from external sources, the OTP will pay "particular attention to the assessment of the reliability of the source and the credibility of the information".[77]

Today, organizations seeking to make objective use of all available resources must assess information from a diverse range of sources including information from State organs, political and military actors, professional news organizations, media activists, hacktivists, citizen journalists, ordinary citizens and untrained eyewitnesses. A far richer and more diverse stream of information is available than ever before, including detailed real-time information. This presents a challenge not just in terms of source evaluation, but also in terms of source identification and the corroboration and verification of available data.

The Policy Paper notes that "the Office uses standard formats for analytical reports, standard methods of source evaluation, and consistent rules of measurement", checking "internal and external coherence" and "drawing information from diverse and independent sources as a means of bias control".[78] As discussed in the previous section, methodologies around the discovery, verification and analysis of relevant information

[77] *Ibid.*

[78] *Ibid.*

from open sources have changed rapidly in the context of journalism, policing and in the world of intelligence. As the information ecosystem evolves, the formats, methods, and rules of the Office will need to adapt to respond to those changes. It is thus incumbent upon the Office to equip itself with the latest skillsets in terms of handling data streams from open sources.

In service of the principle of objectivity, the Office is also presented with an opportunity and a challenge in relation to the volume, variety, and relatively unstable nature of open source information. Online investigations require fact gatherers to grapple with ever larger quantities of information, while valuable information often appears, disappears, or is replicated in real time, with varying degrees of fidelity. In ensuring that the use of open source information is in line with the principle of objectivity, the OTP can draw on the experience and activities of a range of actors outside the Court, including from the fields of journalism, human rights, and law enforcement.

34.3.2. Statutory Factors

The OTP analyses three statutory factors when determining whether to proceed with an investigation: jurisdiction, admissibility, and the interests of justice.[79] Each analysis can benefit from open source information to varying degrees. The 2013 Policy Paper examines each of the factors in turn and situates them within a four-phase filtering process. For analytical purposes, each stage focuses on a distinct statutory factor. Following this framework, the remainder of this section explores how open source information can inform an assessment of whether statutory factors are met.

34.3.2.1. Phases 1 and 2: Jurisdiction

Phase 1 – the "pre-preliminary examination phase"[80] – consists of an assessment of information received via Article 15 communications whereby outsiders send information to the court for consideration.[81] This sifting of material during the Article 15 process distinguishes between communications related to matters manifestly outside the jurisdiction of the Court,

79 Each factor is set out in ICC Statute, Article 53(1)(a)–(c), see *supra* note 62.

80 Amitis Khojasteh, "ICC Statute Article 15", Centre for International Law Research and Policy (https://www.cilrap.org/cilrap-film/15-khojasteh/).

81 In 2016, the OTP received nearly 600 Article 15 submissions. *Ibid*.

which are dismissed, and those pertaining to matters already under preliminary examination, under full investigation, or forming the basis of an existing prosecution, which are forwarded to the relevant team.[82] Those that do not fit in these two categories are then subject to an "independent and objective" two-step analysis, the first step being factual and the second legal, to see if the alleged crimes potentially fall within the jurisdiction of the Court and thus whether further engagement is warranted. According to the 2013 Policy Paper, "[those situations] deemed to require further analysis will be the subject of a dedicated analytical report which will assess whether the alleged crimes appear to fall within the jurisdiction of the Court and therefore warrant proceeding to the next phase. Such communications shall be analysed in combination with open source information such as reports from the United Nations, non-governmental organisations and other reliable sources for corroboration purposes".[83]

Between mid-2012 and mid-2017, situation analysts produced nearly 40 such reports, each of which relied on information derived from open sources. Of them, two resulted in investigations, including allegations against United Kingdom forces in Iraq and an inquiry into the situation in Burundi. As of summer 2017, analysts were considering Article 15 submissions that focused on allegations as varied as forceful evictions in Cambodia, the ill treatment of asylum seekers in Australia, and extrajudicial killings in the Philippines.[84]

The reports ultimately provide the basis for moving to phase 2, "the formal commencement of a preliminary examination". Phase 2 includes those Article 15 submissions that survive phase 1 analysis, as well as any referrals from a State Party, referrals from the United Nations Security Council, or declarations by non-State Parties. In addition to any infor-

82 The final category is for matters that are not manifestly outside the jurisdiction of the Court or subject to ongoing examination, investigation or prosecution and which therefore warrant further analysis and thus may provide the basis for a preliminary examination. Communications deemed to be manifestly outside the Court's jurisdiction may be revisited in light of new information or circumstances, such as a change in the jurisdictional situation, so these are retained. Amitis Khojasteh, *ibid*.

83 OTP 2013, para. 79, see *supra* note 1. This third category of submissions that 'warrant further analysis' are known as 'WFA communications'. They are not subject to the "reasonable basis" standard; instead, the applied standard is whether any alleged crimes "appear to fall within the jurisdiction of the court". Khojasteh, see *supra* note 80.

84 Khojasteh, *ibid.*

mation provided by these external actors, the phase 2 process can be supported by testimony received at the seat of the Court and open source information.[85] Like phase 1, phase 2 aims to identify whether potential cases fall within the Court's jurisdiction.

Findings from phase 2 are documented in an 'Article 5 report' to the Prosecutor that clarifies the Court's jurisdiction. When considering whether the Court has jurisdiction, the Office must consider temporal, territorial or personal and subject-matter jurisdiction over crimes that have been or are being committed. In accordance with Article 53(1), the required standard of proof during phase 2 is a "reasonable basis" to believe that such crimes have occurred.[86] Open source information, as touched on below, can be helpful in analysing whether the requisite standard can be met.

34.3.2.1.1. Temporal Jurisdiction

The temporal jurisdiction of the Court applies from the date of the Rome Statute's entry into force (1 July 2002); the date of entry into force for a particular State Party (when ratified later); the date specified in a United Nations Security Council referral; or a declaration by a State pursuant to Article 12(3) accepting the exercise of the Court's jurisdiction.

Given the clarity of these options, it is difficult to imagine a situation where the Office might have to rely on open-source information to make an assessment of its temporal jurisdiction. Summaries of the application of this statutory factor *tend* to be short and refer only to legal facts such as the date a State deposited its instrument of ratification of the Rome Statute, or the dates specified in a United Nations Security Council referral or State declaration.

34.3.2.1.2. Territorial or Personal Jurisdiction

Territorial or personal jurisdiction is determined by whether a crime specified in Article 5 has been committed "on the territory or by a national of a state party".[87] In most instances, establishing a person's nationality and analysing the statutory factor of personal jurisdiction can be done with

[85] OTP 2013, paras. 79–80, see *supra* note 1.

[86] *Ibid*., para. 36.

[87] *Ibid*., para. 40.

reference to official records and will not require the Office to rely on open sources.

However, the role of foreign fighters acting as combatants can complicate this assessment. In such instances, open source information may play a role. For example, social media sources were specifically mentioned by the Prosecutor in her 2015 statement on alleged crimes committed by ISIS, which focused on the question of the Court's personal jurisdiction over foreign fighters in Iraq and Syria who were nationals of State Parties. In her statement on the alleged crimes committed by ISIS, the Prosecutor noted that: "A few [foreign fighters] have publicised their heinous acts through social media".[88] In this particular assessment, there was a wealth of open source information on the role of foreign fighters from States Parties in Iraq and Syria, including videos of French nationals who joined ISIS in burning their passports and videos of atrocities.

In this particular situation, since ISIS was primarily led by nationals of Iraq and Syria, which are not States Parties, the Office concluded that the jurisdictional basis for prosecuting those most responsible was too narrow to proceed. However, in other instances, it is entirely possible for open source research to indicate that State Party nationals are in fact those most responsible for atrocity crimes in a situation *not* covered by territorial jurisdiction. For instance, it may be possible to use open source information to establish the facts around the involvement of foreign fighters in specific incidents and perhaps even their place within command structures. In other words, it is conceivable that open source information could, in the future, be instrumental not only in gathering information about the crime base but also in throwing light on leadership structures in complex organizations for purposes of ascertaining personal jurisdiction.

In addition to the type of investigation described above, there are other instances where open source information collection and analysis could inform determinations of territorial jurisdiction. For example, geolocation techniques can be used to anchor and verify the locations depicted in videos that show troop movements or alleged criminal activity. Geolocation is now a standard means to corroborate a video obtained from

[88] ICC, "Statement of the Prosecutor of the International Criminal Court, Fatou Bensouda, on the alleged crimes committed by ISIS", 8 April 2015 (http://www.legal-tools.org/doc/b1d672/).

open sources and can contribute heavily towards both source and content evaluation.[89]

34.3.2.1.3. Subject-Matter Jurisdiction

With regard to subject-matter jurisdiction, the Court is limited to assessing the crimes set out in Article 5: genocide, crimes against humanity, war crimes, and the crime of aggression. An analysis of whether there is a reasonable basis to believe that such crimes have been committed will consider "underlying facts and factors", "contextual circumstances", "patterns of similar conduct […] aimed at a protected group", alleged perpetrators, the "role of the individual, group or institution" and their "link with the alleged crime", as well as the mental element of any alleged crime(s).[90] While a detailed assessment is beyond the scope of this chapter, the potential for open sources to support each of these factors is worth exploring in further research.[91]

34.3.2.2. Phase 3: Admissibility

Phase 3 of the preliminary examination process focuses on admissibility, and whether discovered data supports the necessary gravity and complementarity assessments.[92] At this stage, the Office will continue to collect information relating to its subject-matter jurisdiction, in particular where new or ongoing crimes are alleged to be taking place.

---

89 Craig Silverman, *Verification Handbook: A definitive guide to verifying digital content for emergency coverage*, European Journalism Centre, Maastricht, 2014, p. 39 (discussing use of satellite imagery for verification). Sam Dubberley, "In the Firing Line: How Amnesty's Digital Verification Corps changed official narratives through open source investigation", in *Medium*, 18 May 2017.

90 OTP 2013, paras. 38–39, see *supra* note 1.

91 In a June 2017 presentation in The Hague, a situation analyst from the OTP suggested the value of information provided by external actors, such as survivors and non-governmental organizations, to the second phase of the preliminary examination process. She noted how helpful it would be for those actors, when sending information to the ICC or posting online, to provide the "who, what, when, where, and how" underlying a particular atrocity, as opposed to focusing on the impact of any alleged crimes. In addition, she stressed that those external actors could improve the quality of information for ICC purposes by using and declaring a clear and consistent method of information collection and analysis, as well as preserving and providing primary sources. Matilde Gawronski, "ICC Statute Article 15", Centre for International Law Research and Policy (https://www.cilrap.org/cilrap-film/15-gawronski/).

92 OTP 2013, para. 42, see *supra* note 1.

In determining admissibility, the Office must consider three things: gravity, complementarity, and the interests of justice in the context of specific cases that might be pursued.[93]

Two questions for defining potential cases have been identified by the Pre-Trial Chambers: (1) What groups or persons involved in a situation; and (2) What alleged crimes are likely to become the focus of a future investigation? In practice, the Office has made its admissibility assessment based on an assessment of which persons or organizations bear the "greatest responsibility for the most serious crimes"[94] related to a situation. As discussed below, open source data can inform an analysis of the crimes that may have been perpetrated, who was involved, and whether the national system – under the complementarity process – has jurisdiction instead of the ICC.

34.3.2.2.1. Complementarity

A complementarity assessment is concerned with determining whether the relevant national system is willing and/or able to investigate and prosecute the potential cases identified by the OTP in its preliminary examination, in which case the ICC does not have jurisdiction. First, the Office looks at whether national proceedings are taking place in relation to the potential cases it has identified. If they are, the Office asks whether "the focus is on those most responsible for the most serious crimes committed"[95] and whether the proceedings are "vitiated by an unwillingness or an inability to genuinely carry out the proceedings". In assessing any potential unwillingness to conduct genuine national proceedings, the Court asks whether the investigation or prosecution is being undertaken to shield somebody from ICC jurisdiction; whether there has been an unjustified delay; and whether national proceedings are being conducted independently and impartially.

Much of this information may be obtained through a careful review of online, public sources. For example, the OTP can obtain useful information via open sources about the ability of a national justice system to carry out proceedings, including whether a "substantial collapse or una-

93 *Ibid.*, para. 43.

94 *Ibid.*, para. 45.

95 *Ibid.*, para. 49.

vailability" means it is incable of being successful.[96] In making such an assessment, the 2013 Policy Paper indicates that the Office will consider evidence of a lack of adequate protection systems for victims; the absence of a legislative framework; and a general paucity of resources.

34.3.2.2.1.1. National Investigations that Shield Alleged Perpetrators

Even when a national investigation has commenced, complementarity is not satisfied if the Office concludes that the investigation is a sham, for example, if it was commenced to shield one or more alleged perpetrators. The OTP's 2013 Policy Paper lists indicators that suggest a person at the heart of a potential ICC case is being deliberately shielded by a State. These include manifestly insufficient steps taken towards prosecution; deviations from standard practices and procedures; ignoring evidence or giving it insufficient weight; intimidation; findings that are irreconcilable with the evidence; inadequacies in charging and in the application of modes of liability; flawed forensic examinations; failures related to disclosure; fabricated evidence; manipulated or coerced witness statements; undue admission or non-admission of evidence; lack of resources; and failure to co-operate with the Court.[97]

Open source investigative techniques can provide information on many of these indicators. For instance, information on the more difficult-to-ascertain, such as deviations from procedure or intimidation, may be available via national non-governmental organizations. Open source monitoring can supplement such sources. Given that potential ICC cases tend to be high-profile, there is likely to be significant reporting and other online information available to the OTP in near real time.

In the absence of information from a local non-governmental organization, assessing whether there has been an unjustified delay can be greatly assisted with open source information. For example, open sources can help the Office understand the context in which a potential case is playing out as well as the actors involved and their relationships. In addition, official government information accessed through open information portals can feed into an assessment of the national process, including the

96 *Ibid.*, para. 56.

97 *Ibid.*

allocation of resources and other organizational factors, even in the absence of co-operation with the ICC.

34.3.2.2.1.2. Independence and Impartiality of National Proceedings

Indications of the independence of national proceedings include the involvement of State organizations or personnel in alleged crimes; the structure of the criminal justice system; appointments and dismissals impacting on proceedings; the application of immunities and privileges; and political interference and corruption. The *indicia* of impartiality can include connections between the accused persons and the authorities charged with proceedings and "public statements, awards, sanctions, promotions or demotions, deployments, dismissals or reprisals in relation to [the] investigative, prosecutorial or judicial personnel concerned".[98]

Open sources, especially news reports, but also information publicly available via social media, can shed light on negative indicators regarding the independence and impartiality of those involved in national proceedings. In the absence of the collation of such information by national actors or other relevant organizations, or in a situation where there is no co-operation from local authorities, the OTP can access much relevant information online.

34.3.2.3. Phase 4

If the admissibility and jurisdiction requirements are met, the preliminary examination moves to phase 4, during which the OTP considers the interests of justice and produces what is known as an Article 53(1) report.[99] There is a presumption that any investigation will be in the interest of justice "unless there are specific circumstances which provide substantial reasons to believe that the interests of justice are not served by an investigation at that time".[100] As part of this assessment, the OTP is particularly charged with considering the gravity of the alleged crimes and the interests of victims, as well as the views of "community, religious, political or tribal leaders, States, and intergovernmental, and non-governmental or-

98 *Ibid.*

99 *Ibid.*, para. 80. See also OTP, *Policy Paper on the Interests of Justice*, 2007 (http://www.legal-tools.org/doc/bb02e5/).

100 OTP 2013, para. 67, see *supra* note 1.

ganisations".[101] Assuming there is no justice-based reason to prevent moving to an investigation, the resulting report will include an initial legal characterization of the alleged crimes within the jurisdiction of the Court and a basic statement of the facts, detailing the places the alleged crimes took place, the time or time period in which they took place, and the persons or groups involved.

Open source information may be quite helpful to both the interests of justice assessment and the Article 53(1) report. In the CILRAP-conference in The Hague in June 2017 titled "Quality Control in Preliminary Examination: Reviewing Impact, Policies and Practices", an OTP analyst emphasized the importance of thinking through what both the OTP could do internally – and what modifications external actors could make – to enhance the quality of the preliminary examination process. She noted the potential value of systematically soliciting the impressions of survivors and other stakeholders as to what they perceive as satisfying the needs of 'justice' in a particular situation in order to determine whether a case at the ICC would potentially compete with (and/or support) those interests. While she proposed creating a survey to gather those perspectives, a systematic combing of open source materials could fulfill a similar function and/or be used to support any survey that might be employed.[102]

34.3.3. Policy Considerations

In addition to contributing to decisions around whether to launch a full investigation, the 2013 Policy Paper mentions other potential uses of open source information. Specifically, the Paper outlines an "early warning function" as within the Office's mandate, noting that the OTP "systematically and proactively collect[s] open source information on alleged crimes that appear to fall within the jurisdiction of the Court" in order to gauge potential spikes in violence around the world.[103] The monitoring of open sources is thus seen as central to the Office fulfilling not only its mandate to combat impunity but to prevent future violence, with the Policy Paper noting that such monitoring will "allow the Office to react promptly to upsurges in violence by reinforcing early interaction with States, interna-

[101] *Ibid.*, para. 68.

[102] Gawronski, "ICC Statute Article 15", see *supra* note 94.

[103] OTP 2013, para. 104, see *supra* note 1.

tional organisations and non-governmental organisations in order to verify information on alleged crimes, to encourage genuine national proceedings and to prevent reoccurrence of crimes". Thus, the Policy Paper foresees that open source information may be used in preparing and issuing "public, preventive statements"[104] that put perpetrators 'on notice' and encourage national jurisdictions to act.

34.4. Conclusion

As indicated above, significant changes in the means of information dissemination, especially online, have facilitated the sharing of data related to core international crimes. Much of this information is publicly accessible. The growing quantity and quality of online sources – and practices of harvesting information derived from those sources – has considerable potential to strengthen the quality of information feeding into the preliminary examination stage of situations that are being considered by the ICC. Ultimately, open source-derived information is an under-utilized resource that is quickly expanding in importance. When considering standards and initiatives for improving the quality of preliminary examinations, a careful look at the open source fact-finding process is essential.

[104] *Ibid.*

Publication Series No. 33 (2018):

Quality Control in Preliminary Examination: Volume 2

Morten Bergsmo and Carsten Stahn (editors)

This is the second of two volumes entitled *Quality Control in Preliminary Examination*. They form part of a wider research project led by the Centre for International Law Research and Policy (CILRAP) on how we ensure the highest quality and cost-efficiency during the more fact-intensive phases of work on core international crimes. The 2013 volume *Quality Control in Fact-Finding* considers fact-finding outside the criminal justice system. An upcoming volume concerns quality control in criminal investigations. The present volume deals with 'preliminary examination', the phase when criminal justice seeks to determine whether there is a reasonable basis to proceed to full criminal investigation. The book promotes an awareness and culture of quality control, including freedom and motivation to challenge the quality of work.

Volumes 1 and 2 are organized in five parts. The present volume covers 'The Normative Framework of Preliminary Examinations', 'Transparency, Co-operation and Participation in Preliminary Examination', and 'Thematicity in Preliminary Examination', with chapters by Shikha Silliman Bhattacharjee, Cynthia Chamberlain, Matthew E. Cross, Elizabeth M. Evenson, Shannon Fyfe, Gregory S. Gordon, Alexander Heinze, Jens Iverson, Dov Jacobs, Alexa Koenig, Mark Kersten, Shreeyash U Lalit, LING Yan, Asaf Lubin, Christopher B. Mahony, Felim McMahon, Nikita Mehandru, Chantal Meloni, Mutoy Mubiala, Jennifer Naouri, Ana Cristina Rodríguez Pineda, Andreas Schüller, Usha Tandon, Pratibha Tandon, Vladimir Tochilovsky and Sarah Williams.

ISBNs: 978-82-8348-111-2 (print) and 978-82-8348-112-9 (e-book).