United Nations A/HRC/29/37

General Assembly

Distr.: General
24 April 2015

Original: English

Human Rights Council
Twenty-ninth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns

Use of information and communications technologies to secure the right to life

Summary

In the present report, submitted to the Human Rights Council pursuant to its resolution 26/12, the Special Rapporteur on extrajudicial, summary or arbitrary executions discusses the implications of information and communications technologies (ICTs) for the protection of the right to life.

The Special Rapporteur surveys existing applications of ICTs for promoting, protecting and monitoring human rights. While noting the potentially transformative role of "civilian witnesses" in documenting human rights violations and the challenges of using the evidence generated and transmitted by those witnesses — such as verification —, the Special Rapporteur considers how various international human rights mechanisms currently benefit from such material. He makes several recommendations, including that the Office of the United Nations High Commissioner for Human Rights appoint a specialist in digital evidence to assist it in making the best use of ICTs.

Contents

I. Activities of the Special Rapporteur

1. The Special Rapporteur last submitted a report to the General Assembly in October 2014. In that report (A/69/265), he focused on four topics relating to the protection of the right to life, namely, the role of regional human rights systems; less lethal and unmanned weapons in law enforcement; resumptions in the application of the death penalty; and the role of statistical indicators.

2. The Special Rapporteur submitted his previous report to the Human Rights Council in June 2014. In that report (A/HRC/26/36), he discussed the protection of the right to life during law enforcement and the need to bring domestic laws on the use of lethal force by the police in line with international standards. He also called on the Council to provide the outline of a legal framework on the use of remotely piloted aircraft or armed drones and to remain engaged on the matter of autonomous weapons systems.

A. Communications

3. The Special Rapporteur made observations on communications sent between 1 March 2014 and 28 February 2015, and on replies received between 1 May 2014 and 30 April 2015 (A/HRC/29/37/Add.5).

B. Visits

4. From 3 to 7 November 2014, jointly with the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez, the Special Rapporteur visited the Gambia (A/HRC/29/37/Add.2).

5. Follow-up reports on missions undertaken by the Special Rapporteur to India and Turkey are contained in A/HRC/29/37/Add.3 and 4, and the mission report to Papua New Guinea is contained in A/HRC/29/37/Add.1.

6. Since the submission of his previous report to the Human Rights Council, the Special Rapporteur has sent country visit requests to the Governments of Nigeria, Rwanda, Ukraine and Yemen. He thanks the Governments of the Gambia, Iraq and Yemen for their positive responses to his requests, and encourages the Governments of Egypt, Eritrea, Iran (Islamic Republic of), Nigeria, Pakistan, Rwanda and Ukraine to accept his requests for a visit.

C. Press releases[1]

7. The press releases set out below were issued by the Special Rapporteur between March 2014 and March 2015.

8. On 6 March 2014, the Special Rapporteur issued a joint statement on allegations of excessive use of force and violence against protesters, journalists and media workers in the Bolivarian Republic of Venezuela.

9. On 18 March 2014, he issued a joint statement on the events leading to the death of a Chinese human rights defender.

[1] Press releases of the Special Rapporteur are available from www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx?MID=SR_Summ_Executions.

10. On 30 May 2014, he issued a joint press statement on the decision by the Security Council not to refer the situation in the Syrian Arab Republic to the International Criminal Court.

11. On 12 June 2014, he issued a statement calling on the Government of Mexico to put an end to violations of the right to life in the country.

12. On 2 July 2014, jointly with other mandate holders, he called on the Government of Sri Lanka to stop the promotion of racial and faith-based hatred.

13. On 4 July 2014, he issued a joint statement calling on the Government of Nepal to amend the truth-seeking legislation that allowed for amnesties in cases of serious violations of human rights and humanitarian law.

14. On 8 August 2014, he issued a joint statement expressing grave concern over the escalating trend of arrest and sentencing of individuals in the Islamic Republic of Iran.

15. On 12 August 2014, he issued a joint statement expressing concern at the imminent danger of massacre faced by the Yazidi population and other minority communities exposed to attacks by the Islamic State in Iraq and Al-Sham (ISIS), in Iraq.

16. On 29 September 2014, he issued a joint statement on the possible adoption of Bill No. 85 of 2013, aimed at restructuring and expanding the scope of the jurisdiction of military courts in Colombia.

17. On 29 September 2014, he issued a statement urging the Government of Mexico to investigate the deaths of 22 people.

18. On 10 October 2014, he issued a joint statement calling on the Government of Mexico to investigate the disappearances of 43 students in the State of Guerrero.

19. On 26 November 2014, he issued a joint statement urging the President of the United States of America to support the fullest possible release of a report on Central Intelligence Agency interrogation practices.

20. On 5 December 2014, he issued a joint statement on the decisions of grand juries in the United States not to bring to trial the cases of police officers involved in two high-profile killings.

21. On 27 March 2015, he issued a joint press statement calling for the extradition or prosecution by Spain of those responsible for human rights abuses.

22. During the reporting period, the Special Rapporteur also issued joint statements on the death penalty in Bangladesh, Egypt, India, Indonesia, Iran (Islamic Republic of), Pakistan, Saudi Arabia, the Sudan and the United States.

D. International and national meetings

23. The activities carried out by the Special Rapporteur during the period from 26 March to 22 July 2014 are outlined in the report submitted to the General Assembly at its sixty-ninth session (A/69/265).

24. On 2 September 2014, the Special Rapporteur delivered an address on the death penalty to the Human Dimension Committee of the Organization for Security and Cooperation in Europe, in Vienna.

25. On 15 September 2014, he gave a lecture on autonomous weapons systems at the Stellenbosch Institute for Advances Studies, in South Africa.

26. On 18 and 19 September 2014, he participated in the World Health Organization and University of Cambridge Global Violence Reduction Conference 2014, at King’s College, Cambridge, United Kingdom of Great Britain and Northern Ireland.

27. On 22 September 2014, he participated in a panel discussion entitled “Ensuring the use of remotely piloted aircraft or armed drones in counter-terrorism and military operations in accordance with international law, including international human rights and humanitarian law”, organized by the Human Rights Council, in Geneva.

28. On 25 September 2014, he delivered a speech at the parliamentarian seminar on drones, organized by the Parliament of Norway, in Oslo.

29. From 29 September to 3 October 2014, the Special Rapporteur participated in the 21st annual meeting of the special procedures mandate holders, in Geneva.

30. On 8 and 9 October 2014, he participated in the international workshop on enhancing cooperation between United Nations and regional mechanisms for the promotion and protection of human rights, organized by the Office of the United Nations High Commissioner for Human Rights (OHCHR), in Geneva.

31. On 20 October 2014, he participated in a discussion at the University of Columbia, New York, that was co-sponsored by Columbia Law School Human Rights Institute, Rightlink, the Institute for the Study of Human Rights, the Human Rights and Humanitarian Policy Concentration of the School of International and Public Affairs and the Human Rights Law Review.

32. On 10 and 11 November 2014, he participated in the third Jakarta Human Rights Dialogue, on the right to life and a moratorium on the death penalty in the countries of the Association of Southeast Asian Nations (ASEAN), organized by OHCHR, the European Union and the Indonesian representative to the ASEAN Intergovernmental Commission on Human Rights, in Jakarta.

33. On 10 December 2014, he spoke at the launch of *The War Report 2013: Armed Conflicts and their Consequences*, organized by the Geneva Academy of International Humanitarian Law and Human Rights, in Geneva.

34. On 6 February 2015, he spoke at the ninth meeting of the Security Forum, entitled “From drones to killer robots”, organized by Webster University in collaboration with the United Nations Institute for Disarmament Research, in Geneva.

II. Use of information and communications technologies to secure the right to life

A. Background[2]

35. Given that many of the norms of international law concerning the right to life have broadly been settled, the work relating to protecting this right often concerns disputed facts or even the availability of facts. Individuals commit violations of the right to life not because they believe it is justifiable, but because they believe they will not be called on to justify themselves. That places a premium on fact-finding and evidence.

36. Because of the expertise that fact-finding requires, the development of human rights methodologies has hitherto gone hand in hand with the professionalization of human rights.[3] It has evolved over what has been characterized as three generations of communities involved in international human rights monitoring, each with its own methods. First, there was the systematic

[2] The Special Rapporteur thanks the Centre of Governance and Human Rights, University of Cambridge, in particular Ella McPherson and Thomas Probert, for their valuable research support. As part of the research, descriptions of many of the applications and projects discussed have been collated and are available from http://ictandhr.tumblr.com/.

[3] Molly K. Land, “Networked activism”, *Harvard Human Rights Journal,* vol. 22 (2009), pp. 205–43.

review of available information by a distinguished group of lawyers on behalf of intergovernmental organizations; second, came the fact-finding revolution, led by large international human rights non-governmental organizations (NGOs), that dramatically broadened the field but remained attached to witness interviewing, which offers first-hand and very detailed accounting, but which can be very time consuming and vulnerable to interference and selection biases. Over time, the methodology of the second generation was incorporated into the practices of the first generation, including the special procedures of the Human Rights Council. Now, however, the field is being transformed again by a diverse and growing array of digitally enabled actors — the third generation —, including witnesses, monitors and activists, characterized by greater flexibility of fact-finding methodology and output.[4] Each generation has broadened the base of those who participate in human rights investigations. No generation has invalidated earlier work, but it is important that each is able to draw on the strengths of the others without compromising its own capacities.

37. It has become clear that information and communications technologies (ICTs) — the hardware and software that facilitate the production, transmission, reception, archiving and storage of information — can play an increasing role in the protection of all human rights, including the right to life. Information harnessed in this way can be used to secure accountability, but the technology can also ensure visibility or mobilize support for persons in immediate danger.

38. In his daily work of identifying and assessing claims about unlawful killings, the Special Rapporteur, like many others in the field, is increasingly dependent on information mediated through technology. See, for example, the use of video material taken with cell phones during the civil war in Sri Lanka to press both the State and the international community for fuller investigation of the widespread violations of many human rights, including the right to life, alleged to have occurred (A/HRC/17/28/Add.1). Similarly, in preparing the report to the Human Rights Council on the safety of journalists, it became clear how salient citizen journalists and civic media had become through their use of technology to highlight and document violations around the world (A/HRC/20/22 and Corr.1).

39. Increasing digital capacity is greatly enhancing the ability of ordinary people to participate in human rights monitoring. Digital ICTs create opportunities for pluralism that can democratize the process of human rights fact-finding, as well as offer mechanisms of social accountability that citizens can use to hold States and others to account.[5] Social media have created a wealth of opportunities for civilians to highlight human rights violations that they have witnessed, often unmediated by formal intergovernmental or non-governmental structures. This has far-reaching implications for the established power relations in human rights monitoring as there is a much wider community of human rights monitors at work than ever before. It also presents opportunities in contexts that might otherwise be closed to scrutiny. In circumstances where the physical presence of human rights investigators can be a challenge, the sensitive use of ICTs can help to avoid information austerity about situations that are of great interest to the human rights community.

40. However, the development of ICTs should not be viewed as an unqualified good in terms of the protection of human rights. Opportunities for States to carry out surveillance on and interfere in the work of civil society have multiplied in the digital space, and the Council should be vigilant concerning the dangers as well as the affordances of ICTs.[6] The use of technology by human rights activists and others can expose them to a range of risks, of which many may not be aware.

[4] Philip Alston “Introduction: third generation human rights fact-finding”, *Proceedings of the Annual Meeting of the American Society of International Law*, vol. 107 (April 2013), pp. 61–62.

[5] Molly K. Land and others, *#ICT4HR: Information and Communication Technologies for Human Rights* (World Bank Institute, 2012).

[6] The Special Rapporteur notes that, at its twenty-eighth session, the Human Rights Council decided to appoint a special rapporteur on the right to privacy in the digital age.

41. In order to fully realize the potential of ICTs for human rights work, it is necessary to address the issue of the digital divide in terms of both access and literacy. On the one hand, ICTs facilitate pluralism within human rights work, allowing amateurs to complement professionals; on the other hand, however, they can create new lines of inclusion and exclusion that often correspond with pre-existing barriers to access to resources and power, such as language, education, affluence or gender.[7] Moreover, in addition to providing opportunities to speak, pluralism is also about being heard. Being heard by human rights fact-finders may depend on one's ability to produce verifiable information, which can in turn be determined by one's digital literacy and digital footprint.[8] The greater availability of digital information on human rights violations in one context or region may lead to such violations being prioritized over more egregious but less visible violations elsewhere.

42. It is clear that, if used sensibly, ICTs can enhance the protection of human rights, including the right to life. Various parts of the wider United Nations system have been investing significant time and resources into accommodating the affordances of ICTs into their methods of work. The Office for the Coordination of Humanitarian Affairs and the Department of Peacekeeping Operations have been developing advanced techniques for crisis monitoring and mapping. The International Criminal Court has undertaken a review into the way it handles digital evidence. Nonetheless, it still seems that the full potential of these new tools has not been systematically investigated and internalized by the human rights community (see A/65/321, paras. 3–10).

43. In the present report, the Special Rapporteur considers how ICTs present, in particular, opportunities and challenges for the core modalities of human rights work, that is, promotion, protection and monitoring or fact-finding to ensure accountability should a violation occur. Although the impact of ICTs and social media on advocacy spaces has been explored elsewhere, it will be briefly discussed here, as will the role of technology in facilitating physical protection and the necessary security measures for safety in a digital environment, which are both significant from the perspective of the mandate. The Special Rapporteur will then address the question of using ICTs to collect information concerning violations, which can foster accountability, exploring the challenges faced, including the challenge of verification. Finally, the Special Rapporteur will consider the extent to which digital evidence is currently used within parts of the international human rights machinery.

B. Promotion and advocacy

44. Greater capabilities for information sharing and communication present obvious and now widely used opportunities to disseminate information about human rights, either generally, as education, or as more focused advocacy in support of legislative or policy changes, or calling for investigation or accountability concerning individual cases. Human rights organizations can supplement traditional communication strategies using mainstream media, by targeting the public directly.

45. Websites, for example, are used by intergovernmental and non-governmental organizations, as well as States, to make information about human rights norms or legal standards available to the widest possible audience. In previous reports, the Special Rapporteur underlined the importance of clear and publicly available legal frameworks for preventing arbitrary killings through the use of force or the application of the death penalty (A/HRC/26/36 and A/67/275).[9] ICTs clearly enable States to be more transparent towards their populations and the international community.

[7] A. Trevor Thrall, Dominik Stecula and Diana Sweet, "May we have your attention please? Human rights NGOs and the problem of global communication", *International Journal of Press/Politics,* vol. 19, No. 2 (April 2014), pp. 135–59.

[8] Ella McPherson, "Advocacy organizations' evaluation of social media information for NGO journalism: the evidence and engagement models", *American Behavioral Scientist*, vol. 59, No. 1 (July 2014), pp. 124–48.

[9] See also www.use-of-force.info.

46. In addition to providing information digitally, many human rights organizations have developed expertise in using social media quickly and directly to engage members of the public. ICTs may create new educational opportunities that foster environments supportive of human rights. In Kenya, the PeaceTXT initiative sent peace-promoting text messages to registered subscribers with the aim of de-escalating potential conflicts. Elsewhere, NGOs have used secret filming to expose extreme cases of bigotry and harassment in order to sensitize public.[10]

47. Digital ICTs can thus facilitate the widespread visibility of human rights, at least among those connected through social media. Applications such as AiCandle or Pocket Protest allow users to sign petitions, write e-mails or receive human rights information using their mobile or smartphones and are particularly useful for urgent mobilizations.[11] Messages can also be amplified using platforms such as Thunderclap. Ultimately, such strategies can succeed in getting a case or issue on the public agenda.[12]

48. Questions remain as to whether these affordances are markedly changing advocacy dynamics for the better. Campaigns compete for attention in an ever-proliferating information context and are accessible — at least in the first instance — only to the digitally literate.[13] Meanwhile, the brevity of the messages and real-time culture of Twitter may preclude or simplify coverage of complicated situations and the drivers of virality can sit uneasily with human rights evidence.[14] Social networks are effective at increasing participation, in part because they lessen the motivation that participation requires, which can lead to shallow or fickle forms of activism (so-called “clicktivism”).[15] However, some have argued that such seemingly insignificant moves are significant in their accumulation, demonstrating a “supportive environment” and “drawing awareness”.[16]

C. Prevention and protection

49. ICTs can contribute to the prevention of violations of the right to life, by State or non-State actors, in a variety of ways. First of all, alert applications can provide physical and digital protection to potentially vulnerable groups, including human rights defenders. While that enables networks to take advantage of digital connectivity, the very same connectivity is a risk for those vulnerable to digital snooping or other forms of surveillance. Secondly, there is need for education on digital security and safety. Surveillance can, however, also be a preventive mechanism, and tactics ranging from live-streaming demonstrations or police operations to using satellite imagery will be discussed below.

[10] Cynthia Romero, “What next? The quest to protect journalists and human rights defenders in a digital world”, conference report, Freedom House, Mexico City, (February 2014), https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf.

[11] See Amnesty International UK, “What is pocket protest?” (June 2013), www.amnesty.org.uk/what-pocket-protest.

[12] See Jiva Manske “Case studies: concrete examples of compelling and strategic use of social media”, *New Tactics in Human Rights* (9 May 2013), https://www.newtactics.org/comment/6124.

[13] Thrall, Stecula and Sweet, “May we have your attention please?” (see footnote 7).

[14] Dustin N. Sharp, “Human rights fact-finding and the reproduction of hierarchies” (6 June 2014), *Social Science Research Network*, http://papers.ssrn.com/abstract=2341186.

[15] Malcolm Gladwell, “Small change: why the revolution will not be tweeted”, *The New Yorker* (4 October 2010), www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

[16] Stephanie Vie, “In defense of ‘slacktivism’: the Human Rights Campaign Facebook logo as digital activism”, *First Monday,* vol. 19, No. 4 (April 2014), http://firstmonday.org/ojs/index.php/fm/article/view/4961.

1. Alert applications

50. Various organizations are developing alert applications that activists, journalists and others can use to send a signal that they are in danger. For example, Amnesty International developed a "panic button" application — disguised as an ordinary utility — that allows users secretly to activate an alarm by sending a text message, and, optionally, geolocation data, that can be sent to pre-selected contacts by rapidly pressing the power button of the phone. When activists or journalists are attacked or detained, their phones are often taken for the lists of contacts they store. The hidden application will continue to broadcast alerts, which are not only calls for help but also warnings to the person's contacts that they should take security precautions themselves.[17] Other applications or devices have been developed with the same objective.[18]

51. Such applications respond to the challenges posed by a lack of information and time lags, which can restrict efforts to protect individuals at risk. Practitioners believe that there is an approximately 48-hour window after an individual is detained or threatened during which a large-scale response is most likely to have the greatest effect. There are numerous examples worldwide in which mass response to detention — coordinated using social media or otherwise — has persuaded authorities to recalculate the merits of keeping an individual in custody.

52. The new technologies thus fit into wider and long-standing strategies of communicating with a trusted network when at risk and mobilizing a wide community to respond vocally or visibly to an arbitrary act against an individual. It is important, however, to bear in mind the potential risks of such technology which could become the basis of identification and targeting.

2. Importance of digital security

53. While they provide additional capabilities for those working on human rights issues, ICTs can present a number of additional risks, and to mitigate those risks, persons potentially at risk of violations, including human rights defenders, should take the requirements of digital security seriously. Digital security can include software to scan computers for spyware, resources such as Security in-a-Box, as well as digital security helplines or forums.[19]

54. Activists can communicate more securely using virtual private networks, encryption programmes or Tor, a browser designed to increase the anonymity of Internet users. Nonetheless, developers and trainers should caution users that full privacy and anonymity online is never guaranteed. The risk of digital insecurity should also be weighed by larger international human rights actors, both intergovernmental and non-governmental, with regard to their interactions with smaller organizations or individuals.

55. Evaluating the merits and demerits of secure digital encryption does not fall squarely within the mandate of the Special Rapporteur. However, it is certainly a complex issue, with the demands of human rights investigation pulling in both directions, that becomes an issue of concern to this mandate holder when digital insecurity leads directly to victimization, including the threats or actual commission of extrajudicial killings. The use of mainstream social media platforms to share human rights information can pose security risks both for "civilian witnesses" and their subjects.

3. Monitoring for protection

56. The proliferation of surveillance and recording afforded by ICTs not only greatly enhances the opportunities to hold individuals to account, as will be discussed below, but can also prevent the

[17] See https://panicbutton.io/.

[18] BBC News, "Smart bracelet protects aid workers" (5 April 2013), www.bbc.com/news/technology-22038012.

[19] Resources provided through such programmes as New Tactics in Human Rights (www.newtactics.org) provide spaces for online knowledge exchange on various aspects of human rights work, including digital security.

commission of violations. Awareness of surveillance can have a significant deterrent effect if coupled with credible accountability regimes, as demonstrated by the use of closed-circuit television surveillance to deter crime. Belief in this deterrent effect is so strong that some activists have been known to pretend to film events, even though their phone battery was dead, as a strategy against abduction or arrest.[20]

57. Perhaps the most directly applicable example of this, and one that addresses a core interest of the Special Rapporteur — the excessive use of force by law enforcement — is the use of body-worn cameras by police officers. A recent study of the use of such technology in California, United States, found that officers' use of force dropped by 59 per cent on the introduction of the cameras, and complaints concerning excessive force dropped by nearly 90 per cent.[21] Other trial projects, involving the use of smartphones as body-worn cameras that transmit video, audio and geolocation information, are being run in Brazil, Kenya and South Africa.[22]

58. Just as the preventive impact of closed-circuit television works best where there is cognition of its presence, some argue that body-worn cameras deter violations because of their institutionalized use, whereby the police must issue a warning that incidents are being recorded, which creates cognition of surveillance among both police and civilians.[23]

59. Concerns exist around possible violations of the right to privacy that body-worn cameras may generate, leading to suggestions that they be turned off upon entering a home or when speaking with victims. Others consider that individual officers should not have control over their cameras, so as to reduce opportunities for selective documentation.[24] Concerns also exist with respect to access to and secure storage of the footage. Although questions remain to be answered, many feel that the deterrent effect of police body-worn cameras warrants further deployment.[25] Linked with the potential advantages of the police recording themselves is the equally important protection of citizens' right to record the police.

60. If body-worn cameras bring surveillance to the micro level of interpersonal interactions, at the opposite end of the spectrum is the surveillance potential of remote sensing imagery, either from satellites or drones. Initiatives such as the Satellite Sentinels Project and Amnesty International's Eyes on Darfur campaign have highlighted the possibilities of such mechanisms. Raising awareness among potential perpetrators that vulnerable areas are being watched could deter violations, or at least those that are visible remotely.[26] However, such surveillance is expensive and

[20] Stephanie Hankey and Daniel Ó Clunaigh, "Rethinking risk and security of human rights defenders in the digital age", *Journal of Human Rights Practice*, vol.5, No. 3 (November 2013), p. 543.

[21] Barak. Ariel, William A. Farrar and Alex Sutherland, "The effect of police body-worn cameras on use of force and citizens' complaints against the police: a randomized controlled trial", *Journal of Quantitative Criminology* (November 2014).

[22] Graham Denyer Willis and others, "Smarter policing: tracking the influence of new information technology in Rio de Janeiro", *Igarapé Institute Strategic Note 10* (November 2013); see also the Smart Policing initiative, http://en.igarape.org.br/smart-policing/.

[23] The effect of cognition of surveillance was perhaps most memorably elaborated by Jeremy Bentham, but its criminological effects, as well as its potential dangers, have not been technologically realized until recently.

[24] Bracken Stockley "Public support for police body cameras – but who controls on/off switch?" *The justice gap* (March 2014), http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/.

[25] Robert Muggah, "Why police body cameras are taking off, even after Eric Garner's death", *IPI Global Observatory* (11 December 2014), http://theglobalobservatory.org/2014/12/police-body-cameras-eric-garner/; see also Alexandra Mateescu, Alex Rosenblat and Danah Boyd, "Police body-worn cameras", Data & Society Research Institute Working Paper (February 2015), www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf.

[26] Nathaniel A. Raymond and others, "While we watched: assessing the impact of the satellite sentinel project", *Georgetown Journal of International Affairs* (26 July 2013),

can involve rather arbitrary decisions about which communities or places to monitor. As with other surveillance methods, the deterrent effect of the technology is connected to both awareness of its existence (making the accompanying media campaign significant) and the credible threat of punitive measures.[27]

61. Those surveillance methods use the threat of accountability in the future to condition behaviour in the present. It is potentially also possible to exploit the capacities of ICTs to use information from the (recent) past to influence what happens in the present. Social media analysis could predict hotspots of human rights violations in real time. For example, the Hatebase database collects data on the vocabulary and incidence of hate speech on social media based on the correlation between hate speech and the risk of genocide and is used to predict regional violence.[28]

62. There are limitations, however, to the possibilities of ICTs as early warning systems. Although "big data mining", i.e. collecting large amounts of data, has a record of being good for conflict prediction and prevention, it has been less effective for analysis and actionable transmission.[29]

63. Big data mining and remote sensing work for the prevention of human rights violations also raises methodological and ethical concerns. For example, vulnerable populations could be put at risk by the remote documentation, and thus identification, of their locations and situations.[30] Moreover, potential inaccuracies in the statistical analysis of human rights data arise from selection bias, duplication and constraints on data capture.[31]

4. Towards digital due diligence

64. The application of surveillance to prevent violations of human rights may be so effective as to imply that States with the capacity to take advantage of them have a responsibility to do so. Cameras have been used in police vehicles and interrogation rooms and consideration might be given to other contexts in which such surveillance could have a preventive effect (for example, prisons), subject to the limitations imposed by other rights, such as the right to privacy.

65. Other affordances of ICTs can be harnessed by States to fulfil their responsibilities concerning prevention or precaution. For example, there have been instances of States using text messages or calls to warn civilian populations before launching air raids. The recording devices on certain advanced weaponry offer the potential for greater oversight, but that will require more transparency.

66. In the digital space, however, the responsibility of due diligence extends beyond States. Human rights monitoring organizations — both intergovernmental and non-governmental — need to give thought to the consequences of their correspondence or use of information. Traditional understandings of "informed consent" may need to be revisited.

http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/.

[27] Patrick Meier, "Will using 'live' satellite imagery to prevent war in the Sudan actually work?" *iRevolutions* (30 December 2010), http://irevolution.net/2010/12/30/sat-sentinel-project/.

[28] See http://www.hatebase.org/.

[29] Sheldon Himelfarb, "Can big data stop wars before they happen?" (United States Institute of Peace, 25 April 2014), www.usip.org/publications/can-big-data-stop-wars-they-happen.

[30] See, for example, Harvard Humanitarian Initiative, "The Signal Program on Human Security and Technology" (2013), http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program.

[31] See the work of the Human Rights Data Analysis Group, https://hrdag.org/coreconcepts/.

D. Monitoring and fact-finding

67. As noted above, the particular nature of violations of relevance to this mandate place a premium on fact-finding. Human rights organizations have developed rigorous fact-finding methodologies, not least to protect the credibility of their evidence, and thus their reputations. ICTs and the user-generated content they facilitate have broadened and democratized the process of fact-finding by empowering both spontaneous and solicited "civilian witnesses." The most challenging dimension of this evolution is balancing democratization with a continued, perhaps heightened, requirement for authority and thus for verification of digital evidence.

1. Civilian witnesses and video evidence

68. The advantages of video evidence have been appreciated by campaigners for several decades, at least since the Rodney King incident in the early 1990s. The re-purposing of private closed-circuit television footage for public investigations has become commonplace.[32] At the international level, the conviction by the International Criminal Court of Thomas Lubanga, which admitted video footage of interviews of child soldiers who had been impressed into his militia, proved that video recordings could be used to fill an evidentiary gap.[33] Of course, it is not only witnesses or subjects of violations who are producing such information, but also perpetrators. Moreover, information does not have to be shared publicly for it to be useful to human rights investigations.

69. While information from civilian witnesses has long been a cornerstone of human rights fact-finding, it has traditionally been gathered by professionals. Either professionals or their trusted contacts would be present during the production and transmission of information from witness to fact-finder during an interview, for example. ICTs enable civilian witnesses autonomously to produce and transmit information.

70. At its most spontaneous, civilian witnessing can occur through widely available consumer tools or platforms. The ubiquity of smartphones enables the capture of visual and auditory information, which can be easily transmitted through digital channels such as social media platforms. The benefit of those production and transmission strategies is that they do not require any particular expertise; the drawback is that they may limit the metadata (such as source, place and time of production) which could be instrumental to verifying the information. Alternatively, applications such as InformaCam and EyeWitness are specifically designed to enhance the metadata supplied with photographic or video information and to maintain the chain of custody.[34]

71. A number of NGOs are already offering training courses to citizen witnesses and trainers on how to produce and transmit material with stronger evidentiary value. WITNESS, Amnesty International, Tactical Tech and the Open Society Justice Initiative are all conducting such activities on a global or regional scale. The training may concern both personal protection issues, such as those concerning digital security, discussed above, and practical information about the kind of detail to capture in witness videos (such as licence plates, uniform numbers or landmarks) and how to share them.[35]

[32] See, for example, Daoud Kuttab, "Video technology exposing Isreali violations in the West Bank", *Al-Monitor* (8 July 2014), www.al-monitor.com/pulse/originals/2014/07/israel-palestine-cctv-camera-footage-occupation-settlers.html.

[33] Matthew Shaer, "The media doesn't care what happens here: can amateur journalism bring justice to Rio's favelas?" *The New York Times* (18 February 2015), www.nytimes.com/2015/02/22/ magazine/the-media-doesnt-care-what-happens-here.html.

[34] See information about Informacam, https://guardianproject.info/informa/; and New Perimeter, "eyeWitness to atrocities", www.newperimeter.org/our-work/access-to-justice/eyeWitness.html.

[35] See, for example, Kelly Matheson, "Video as evidence: basic practices", *Witness blog* (16 February 2015), http://blog.witness.org/2015/02/video-as-evidence-basic-practices/.

2. Crowdsourcing information

72. Somewhere between the traditional methods of soliciting information from civilian witnesses and the spontaneous production and transmission of information by civilian witnesses are the practices of crowdsourcing and crowdseeding. Crowdsourcing involves turning over tasks to a large, unspecified group recruited through an open call but that is not necessarily representative, as such calls privilege the participation of those with resources such as technology, money and time. Crowdseeding is a form of bounded crowdsourcing whereby participants can be randomly sampled for representativeness and equipped with the technology and resources necessary for gathering information. A relationship develops over time between chosen witnesses and the project, with the credibility and trust that such a relationship entails.[36]

73. Besides potentially widening the scope of human rights work, involving civilian witnesses as a crowd could strengthen the effect of human rights advocacy through greater participation and awareness as well as potential corroboration.[37] However, there are risks. By publicly mapping information, crowds may jeopardize vulnerable populations. The techniques may also be used against the human rights community, for example to perform “human intelligence tasks” such as matching faces to photographs of protests.[38]

3. Satellite evidence

74. Satellite footage can have a transformative impact on human rights work. Central to the deterrent effect of satellites is the knowledge that, should a violation occur, somebody is going to use the footage to expose it. For example, earlier this year, fact-finders at Amnesty International and Human Rights Watch undertook “change detection” analysis of satellite images of two towns in north-eastern Nigeria that revealed extensive fire damage. The information was cross-referenced with eyewitness testimonies to establish that the fires were part of militant attacks in which hundreds were killed. Although that linking was important because, on their own, satellite images do little to establish culpability and causality, the case highlights the benefits of remote sensing for hard-to-reach areas.[39]

75. Satellite evidence can be combined with other digital processes, such as social media mapping, in order to better convey information. Reports on the origins of missile or artillery attacks or the impacts of drone strikes have relied on satellite photography.[40]

76. At present, much of the satellite imagery relied on for human rights work is owned by commercial operators. This means that, for satellite imagery to be available, there must be a commercial interest in the area and no cloud cover; also, the imagery will tend to be of low resolution. Military-grade satellite imagery has broader coverage and higher resolution, but there is often a reluctance to share information (rather than classified imagery itself) with human rights investigators, even when national security is not at stake.

[36] Patrick Meier, “From crowdsourcing crisis information to crowdseeding conflict zones (updated)”, *iRevolutions* (10 July 2012), http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/.

[37] Molly Beutz Land, “Peer producing human rights”, *Alberta Law Review,* vol. 46, No. 4 (2009), p. 1115.

[38] Jonathan Zittrain, “The Internet creates a new kind of sweatshop”, *Newsweek* (7 December 2009), www.newsweek.com/internet-creates-new-kind-sweatshop-75751.

[39] Christoph Koettl, “The story behind the Boko Haram satellite images”, *Amnesty International UK/Blogs* (17 January 2015), www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images.

[40] Bellingcat, “Origin of artillery attacks on Ukrainian military positions in Eastern Ukraine between 14 July 2014 and 8 August 2014” (17 February 2015), www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/; and Forensic Architecture, “Drone strikes: investigating covert operations through spatial media”, www.forensic-architecture.org/case/drone-strikes/.

E. Evaluating evidence collected using information and communications technologies

77. The flood of information from civilian witnesses can only have evidentiary potential if the information can be gathered and evaluated. It is therefore important that human rights organizations be able to integrate that information into their traditional methods of research and analysis, especially given the importance of reporting credibility. However, evaluating digital content produced by civilian witnesses can be a challenge, including with regard to the identification of relevant information, and verification and storage of that information. Technological developments as well as initiatives in information evaluation practices may help to address those challenges.

1. Problem of volume

78. The proliferation of digitally produced and transmitted civilian witness information means that identifying relevant information can be an overwhelming task. Using networks to crowdsource the filtering process can be an intermediary step, but it will likely be necessary to harness the analytical affordances of digital ICTs to address their own "signal-to-noise ratio" problem. One way is through the automated cleansing of large datasets of potentially relevant information. For example, CrisisNET aims to collect and standardize real-time digital crisis data from thousands of sources so that researchers can search quickly and efficiently.[41] Although machines cannot replace human expertise in the evaluation of human rights information — for assessing the relevance of information for evidence is an ultimately subjective task —, technology can help human rights monitors to concentrate on the most important material. More research is needed in this regard.

79. There will probably always be a need to curate digital content for monitoring and consumption by a wide audience of interested parties. Such curation will involve a combination of automation and traditional fact-finding or verification skills. One successful model is the WITNESS Human Rights Channel, which uses material that is verified in partnership with the social media news agency Storyful.

2. Problem of transience

80. Because much of the material of relevance to human rights investigations could be online for only a very limited time (owing to pressures either on the uploader or the platform not to host content of a certain type),[42] it is important that investigators have the capacity to capture all the information that might be needed and to store it securely. The development of guidelines for national investigators as well as human rights monitors should be a priority.[43]

81. The storage of material for human rights investigations can be a security risk for activists. Applications such as Eyewitness and International Evidence Locker have been designed to allow witnesses to upload evidence to a cloud-based repository and to use or delete it as best suits their circumstances. Those applications also allow secure transmission of information to target audiences while maintaining the metadata of the information as well as the information itself. Nonetheless, collaboration between investigators and technology corporations will remain a vital consideration.

[41] See http://crisis.net/about/.

[42] Madeleine Bair, "Navigating the ethics of citizen video: the case of a sexual assault in Egypt", *Arab Media & Society*, vol. 19, (2014), http://arabmediasociety.com/?article=844.

[43] Resources exist to guide activists concerning the archiving of their material, for example, see http://archiveguide.witness.org/. The Office of the Prosecutor of the International Criminal Court is currently finalizing guidelines for investigators.

3. Problem of verification

82. Although sometimes raised as a major impediment to the embrace of digital evidence, verification is not a new issue: it concerns the conventional institutional need to establish the credibility of a source and the accuracy of its information before acting on or staking one's reputation to a claim. While the nature of the information being verified and the specific techniques are shifting rapidly as ICTs evolve, the fundamentals of verification remain constant: identifying and corroborating the content and provenance of information received.

83. Verification usually involves checking the origin, source, time and place of the information in question, as well as the chain of custody. Fact-finders must take time to establish the identity of the source, assess the file for metadata indicators, then cross-reference those with other sources. A new set of methods, often referred to as information forensics, is emerging, but many elements of the process still require human expertise and painstaking checks, akin to old-fashioned investigation.

84. The witness may provide information concerning the time, place and content in an interview, or, alternatively, may include that information in the file. The former method underlines the importance of cross-fertilization between the methodology of the second and third generations of fact-finding and the extent to which the sources of one can bolster the authority of the other, while the latter can occur either during the production process, for example by verbalizing the location and date, or through the transmission process. The information may also be evident through physical landmarks (such as road signs or geological features), weather conditions, clothing, weapons or dialect captured in the digital file, or it may also be identified through the metadata automatically embedded in the file, such as the time stamp. That information can be corroborated and cross-referenced against other digital files and evidence, including satellite images. Several videos of the same incident can be time synced so as to provide a multiperspective video timeline.[44]

85. Recognition of the need for expertise concerning digital verification is growing. The more knowledge about information forensics that human rights fact-finders have, the more comfortably and quickly they will be able to use digital information from civilian witnesses. The *Verification Handbook*, published in 2014, quickly became a reference point for humanitarians and human rights fact-finders.[45]

86. Increasing verification knowledge among civilian witnesses is likely to ease the verification process. WITNESS, for example, provides a guide on what information to include in videos documenting human rights violations.[46]

87. Another strategy to facilitate verification is through initiatives that support either the provision of information for verification or the evaluation of that information. Such initiatives have been referred to as "verification subsidies" and may incorporate human participation or designed technologies.[47] Applications such as InformaCam automate the addition of verification cues at production and prompt their inclusion during transmission. Alternatively, the power of the crowd can be used retrospectively, as is done, for example, with Veri.ly.[48] Alternatively, Checkdesk, a

[44] See, for example, the Rashomon Project, http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/.

[45] Craig Silverman (ed.) *Verification Handbook: An ultimate guideline on digital age sourcing for emergency coverage* (European Journalism Centre, 2014), http://verificationhandbook.com/.

[46] See "A field guide to enhancing the evidentiary value of video for human rights", http://verificationhandbook.com/book/appendix.php.

[47] Ella McPherson,**Error! Hyperlink reference not valid.** "Digital civilian witnesses of human rights violations: easing the tension between pluralism and verification at human rights organizations" in Lind (ed.), *Producing Theory 2.0: The Intersection of Audiences and Production in a Digital World*, vol. 2 (forthcoming 2015).

platform designed for individual newsrooms, allows for collaborative and transparent verification among members of a bounded crowd.

88. While the technical difficulty of verification should not be exaggerated, its importance cannot be overstated. If used by a human rights organization, unverified material can lead to the degradation of the organization's credibility, but hoaxes can also create combustible situations — so-called "digital wildfires" — that can lead to violence.[49] Many States already have laws limiting freedom of expression for reasons such as incitement of violence or panic, but they are struggling with how to apply those laws effectively to online activities. Any regulation in that area will remain complex and controversial; it has been suggested that the online community itself must fill the gap, with important roles for community curators and moderators.[50] The Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance reported to the Human Rights Council in 2014 on the complex challenges for his mandate posed by the Internet and social media (A/HRC/26/49). In addition to pointing out policies developed by some of the major social media sites, he also highlighted the importance of civil society initiatives.

4. Using digital evidence

89. Most of the information that can be captured through the streams described above is "convenience data", but its value to a human rights investigation cannot always be immediately assessed. Moreover, it is important not to privilege images as much can also be learned from blogs or micro-blogs, which can be used to corroborate other sources.

90. While verification subsidies potentially speed up the verification process, using them requires digital literacy about verification among human rights fact-finders and civilian witnesses. It is unclear how knowledge about producing and transmitting information effectively, safely and ethically for evidence will be diffused among civilian witnesses, particularly those who are acting in a truly spontaneous manner. Pre-emptive steps to train human rights monitors will favour the prepared, but it is often the accidental witnesses who are best placed to be truly informative.

91. For that reason, organizations such as WITNESS advocate for the standard inclusion of an "eyewitness" or "proof" mode, resembling InformaCam, in preloaded photo and video applications on smartphones and in social media platforms.[51] The inclusion of those features in mainstream applications and platforms means that civilian witnesses are more likely to know about them and thus to use them.

F. Use of information and communications technologies by human rights mechanisms

92. Thus far, the present report has addressed the applications of ICTs in human rights work in general, rather than their use by the international machinery for the protection of human rights. It is important that the international community be open to these new methodologies, otherwise advocacy organizations and civilian witnesses will find it difficult to take full advantage of existing accountability mechanisms. As noted above, technological evidence must not be seen as

[48] See Victor Naroditskiy, "Veri.ly – getting the facts straight during humanitarian disasters", (August 2014), www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters.

[49] This issue was raised in the World Economic Forum *Global Risks* report, 8th ed. (2013), pp. 23–27.

[50] See Lee Howell, "Only you can prevent digital wildfires" (8 January 2013), www.nytimes.com/2013/01/09/opinion/only-you-can-prevent-digital-wildfires.html.

[51] Sam Gregory "How an Eyewitness mode helps activists (and others) be trusted", *WITNESS Blog* (3 March 2014), http://blog.witness.org/2014/03/eyewitness-mode-helps-activists/.

the endpoint — without meaningful accountability it is just more sound and fury — and it is therefore vital that official channels designed to facilitate accountability for human rights violations be open to this type of evidence.

93. The broader United Nations community has invested in harnessing the potential of ICTs, particularly in the area of crisis information management (A/69/517). The United Nations Office of Information and Communications Technology has, in conjunction with the ICT4Peace Foundation, coordinated the Crisis Information Management Advisory Group, which has become a forum to discuss technological developments in humanitarian aid and crisis information management.[52] The Office for the Coordination of Humanitarian Affairs (OCHA) has reviewed the impact of ICT-enabled networks on humanitarian relief and has, since then, undertaken a number of collaborative projects to take advantage of the power of the crowd.[53] Meanwhile, the Global Pulse project is a major undertaking on the humanitarian impact of big data.[54]

94. In 2014, the Department of Peacekeeping Operations requested the Expert Panel on Technology and Innovation in United Nations Peacekeeping to recommend ways in which technology and innovation could enhance their operational effectiveness. The panel issued its final report in February 2015,[55] in which it recommended that, among other things, the Security Council create a special technical mission to use technical audio, visual, monitoring and surveillance technologies to inform decision-making.

95. The United Nations human rights mechanisms have not completely ignored the advances of ICTs. Several of them have created successful social media presences as part of their promotional engagement strategies and campaigns to reach millions of users worldwide. Although the promotional uses of digital ICTs are significant, the Special Rapporteur will now consider the engagement of various international and regional human rights mechanisms that use ICTs for fact-finding and accountability.

1. Special procedures and other mechanisms of the Human Rights Council

96. This report was in part motivated by the Special Rapporteur's investigation of video evidence of executions at the end of the civil war in Sri Lanka (see A/HRC/17/28/Add.1, appendix). In that instance, the Special Rapporteur was able to provide impetus to a broad coalition pressing for accountability by independently seeking out technical experts to comment on the metadata of the videos, the ballistics of the weapons shown in the videos and the movement of the bodies. Given the rapid developments in the field, it is quite possible that such expertise is easier to find today, however, the capacity of OHCHR has not changed greatly. Special procedures mandate holders would benefit from in-house technical knowledge for selecting the best experts for specific tasks.

97. As noted above, the verification of user-generated content is fundamental to reaping the advantages of ICTs in terms of broadening access to and the scope of human rights work. However, it is important that verification not be viewed as a barrier to the use of digital evidence. The technical difficulty of verification is sometimes exaggerated and used as an excuse not to engage with such evidence. Verification should be demystified within the international human rights machinery, so that the advantages offered by digital evidence can be more fully embraced.

98. With respect to the dangers of ignorance concerning digital security, it is noteworthy that many Human Rights Council mechanisms encourage individual contact through insecure generic email addresses, with no warnings concerning security or suggestions of alternatives. While offering

[52] See http://ict4peace.org/crisis-information-management-advisory-group-cimag-retreat/.

[53] OCHA Policy and Studies Series, *Humanitarianism in the Network Age: including world humanitarian data and trends 2012*, (2013), https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

[54] See http://www.unglobalpulse.org/.

[55] See http://www.performancepeacekeeping.org/offline/download.pdf.

such contact points is a laudable effort to broaden access to its mechanisms, the Council is arguably failing in its duty of care by failing to adequately warn individuals or groups of the potential risks that they may be taking.

99. Of course, the impression should not be given that the special procedures of the Council are closed off to information from the new data streams discussed in the present report. Indeed, much of the NGO reporting on which special procedures' communications are based derives information from such sources. However, the fact that the Council is not yet open to weighing such evidence or reporting places it at risk, over the coming years, of isolation from the broader human rights community with which it has done so much to engage in the past.

2. National and international commissions of inquiry

100. Various national investigations have made use of digital evidence. The finding that the death of Ian Tomlinson during a demonstration in London in 2009 was an unlawful killing hinged on a witness video that was tracked down and handed over to the Independent Police Complaints Commission by an investigative reporter. Also, the ongoing inquiry into the shootings at Marikana, South Africa, received ostensibly probative video evidence that the South African Human Rights Commission has had synchronized by a technological expert.[56]

101. At the international level, OHCHR has partnered with the Operational Satellite Applications Programme of the United Nations, and with various external partners on an ad hoc basis, to use both satellite and video evidence in the work of international commissions of inquiry.[57] As discussed above, when combined with other techniques of human rights monitoring, satellite imagery can provide extremely valuable information for inclusion in reporting to the Human Rights Council.

102. The Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea made use of both satellite imagery and clandestinely recorded videos and photographs in order to demonstrate the existence of several political prison camps (see A/HRC/25/63). The Commission relied on the videos and photographs to the extent that they could confirm their authenticity, and, with respect to satellite imagery, on commercially available footage. The Commission noted that higher resolution satellite imagery produced by more technologically advanced States would, almost certainly, have provided further information. Unfortunately, despite requests, those images were not made available to the Commission (see A/HRC/25/CRP.1, para. 60–61).

103. The Independent International Commission of Inquiry on the Syrian Arab Republic has also made use of a certain amount of satellite and digital material, as one might expect from a body monitoring one of the most documented conflicts in history.[58] In conducting its special inquiry into the AlHoula killings, for example, the Commission examined satellite imagery to review access points to an area where killings had occurred, as well as to review statements made by interviewees and to assess claims that the Government had razed civilian areas in Damascus and Hama.[59] The Commission mentioned instances where it had received or found video evidence supporting allegations of torture or other forms of ill-treatment or footage of killings, but noted when it could not verify those recordings.[60] Video material has also been directly gathered by the United Nations Supervision Mission in the Syrian Arab Republic and referred to in reports of the

[56] See the "Written submissions of the South African Human Rights Commission regarding 'Phase One'" in the Marikana Commission of Inquiry (29 October 2014), www.sahrc.org.za/home/21/files/SAHRC%20PHASE%20ONE%20FINAL%20WRITTEN%20SUBMISSIONS.pdf.

[57] See http://www.unitar.org/unosat/.

[58] See Marc Lynch, Deen Freelon and Sean Aday, *Syria's Socially Mediated Civil War* (United States Institute of Peace, 2014).

[59] See A/HRC/21/50, annex IV; and A/HRC/22/59, annex XIII, para. 18.

[60] A/HRC/21/50, annex VIII, para. 31; A/HRC/22/59, annex V, para. 22.

Commission.[61] The Commission also undertook preliminary reviews and conducted forensic analyses of 26,948 photographs allegedly taken between 2011 and 2013 in government detention facilities.[62] In more recent reports, the Commission cited a number of videos that had been created and distributed by ISIS; those videos have been a challenge to the current methodology of using videos only to substantiate events for which there are other witness testimonies, but the Commission has given them weight as confessions.[63]

3. International criminal accountability

104. Information derived from digital sources has become increasingly important to international tribunals, including several of those established during the 1990s, and now also the International Criminal Court. In assessing the importance of such evidence to moving forward its work, the Court has been proactive in establishing working methods that can accommodate such evidence. In 2012 and 2013, the Court encouraged partners to exchange ideas and expertise on strategies to improve the capacity of investigators and prosecutors to gather and analyse digital evidence concerning serious international crimes.[64]

105. One of the recommendations from that process was that the Office of the Prosecutor should "hire specialists trained in advanced cyberinvestigation techniques and familiar with cutting-edge technologies" and who would have "experience and credentials specific to digital investigations, including computer and smartphone forensics, online investigations, data storage and management, advanced cyberinvestigation techniques, and superior knowledge of digital security." It was suggested that this would "go a long way toward building a robust in-house capacity for vetting digital data and extracting quality evidence."[65] On the basis of that consultation, the Office of the Prosecutor appointed a specialist in the verification of digital material to work as a "cyberinvestigator", as part of its team of other investigators from legal and law enforcement backgrounds.

106. Recognizing the transient nature of much of the relevant material, the Office of the Prosecutor has adopted the practice of surveying digital evidence that is available when the preliminary examinations are opened. As noted above, the Court has developed guidelines for use by investigators concerning best practices with respect to the retrieval, storage and investigation of digital evidence, including the capture of websites and seizure of hard drives.

III. Conclusion

107. **ICTs have had a profound effect on the impact and character of human rights work. However, it is important that the process not be taken too far, especially in information-scarce environments, where it will be increasingly important to resist the temptation to privilege digital material. While new technology may raise expectations for information, it should be noted that traditional human rights monitoring and reporting make no claim to comprehensiveness, and neither should analysis of new ICT-enabled data streams. The latter should not be viewed as a shortcut, but rather as part of a complementary process that fits into pre-existing strategies used by human rights actors.**

[61] A/HRC/21/50, annex V, para. 14.

[62] A/HRC/27/60, para. 26.

[63] A/HRC/28/69 and Corr.1, annex II, paras. 21–25.

[64] See Human Rights Center, University of California, *Beyond Reasonable Doubt: Using scientific evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2012); and *Digital fingerprints: Using electronic evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2014).

[65] See Human Rights Center, *Digital Fingerprints*, p. 11 (see footnote 64).

108. **It is also important that ICTs be embraced with due acknowledgement of their risks. While in many cases, technology can be a vehicle for pluralism, issues of a digital divide remain. In order to benefit from digital protection measures, human rights defenders need to know about them. The digitally enabled promotion of human rights may contribute to a culture of awareness, but if promotion resources for those initiatives are diverted away from more traditional channels, this will be to the detriment of vulnerable groups who are not online.**

109. **It is also important to acknowledge the importance of ownership and control of the mechanisms of digital ICTs. The use of digital evidence often depends on the willingness of technology corporations to host, store and facilitate searches for this information. Moreover, in some States, access to externally owned commercial social media platforms, such as Twitter, Facebook and YouTube, are blocked. In others, entire communication networks have been shut down to suppress the flow of information.**

110. **Keeping up with digital literacy and paying for new technology can be difficult for human rights organizations. One solution would be collaboration between ICT specialists and human rights experts to develop, implement and even commercialize new applications for human rights, or to negotiate low-cost or free licensing for the use of existing solutions. Donors are interested in funding technological developments, but reportedly can focus more on the technology than on the training that is required to deploy it. However, technology can be useless or even dangerous without training. As one observer noted, "sooner or later, all technology problems become education problems."**[66]

111. **The collaborative framework can be extended further. Indeed, a wide range of organizations are willing to assist international human rights mechanisms in more fully benefiting from ICTs. Coordination efforts have been made in that regard, but it seems that the human rights community is currently far behind other international agencies — most notably in terms of crisis response — in fully realizing that potential.**[67]

112. **What is needed to support those United Nations human rights mechanisms that respond directly to evidence that is often gathered by third parties is in-house capacity to conduct a triage-like function on digital material, as an initial assessment of the likely value of the source, before passing it on to external experts for full verification or other technical assessment. Such a "first opinion" and liaison capacity within the secretariat of international mechanisms, including the special procedures, would encourage greater use of potentially valuable information.**

113. **Of course, technological advances in gathering evidence remain only as effective, in real terms, as the accountability mechanisms to which they contribute and which are, in large part, external to the technology. In that sense, the improved information streams offered by ICTs are necessary, but not sufficient, for better protection of human rights, including the right to life. That underlines the importance of international human rights mechanisms, including the Human Rights Council and its special procedures, being able to fully interact with such materials. Some human rights NGOs — the so-called "second generation" — are keeping pace with the innovations of the "third generation." It is vital that the "first generation" catch up**.

[66] Christopher Neu, "Mobile applications for atrocity prevention require mobile students", *TechChange*, (19 February 2013), http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/.

[67] In the humanitarian response context, Digital Humanitarian Network has produced two reports aimed at both sides of such partnerships: see http://digitalhumanitarians.com/content/guidance-collaborating-formal-humanitarian-organizations, and http://digitalhumanitarians.com/content/guidance-collaborating-volunteer-technical-communities.

IV. Recommendations

A. To the United Nations

114. **OHCHR should appoint, on a consultancy basis and as soon as possible, a digital content specialist to provide advice with respect to information received from or produced by civilian witnesses and to serve as an interface with external networks of expertise in that area. That should be seen as a stopgap solution to ensure quick movement on that front. At the same time, OHCHR should, with the assistance of the appointed specialist, set about establishing longer-term capacity.**

115. **As international commissions of inquiry and fact-finding missions are ad hoc bodies that are likely to receive a large and increasing quantity of digital evidence, consideration should be given to expertise for analysing such material in the staffing requirements for those mechanisms.**

116. **More broadly, OHCHR should take steps to improve awareness of and to familiarize its staff and processes at all levels with the requirements of digital security. That involves the development of minimum standards of due diligence with respect to the digital security of sources. Guidelines for United Nations staff on the ethics of using information from open sources, especially social media, should also be developed in consultation with relevant partners.**

B. To regional human rights mechanisms

117. **Regional human rights mechanisms should evaluate their capacity to receive and use digital material and to promote best practices in terms of digital security. Where necessary, they should liaise with OHCHR to increase that capacity.**

C. To States

118. **States should respect and, where necessary, protect the individual's right to make a recording of a public event, including the conduct of law enforcement officials, and to "record back" an interaction in which he or she is being recorded by a State agent.**

119. **States should consider measures that may be taken innovatively to use ICTs to prevent violations of the right to life by its agents, particularly the excessive use of force by law enforcement officers, or in custodial settings. That could include, but is not limited to, innovations such as body-worn cameras, with due consideration given to the necessary safeguards of the right to privacy.**

120. **States with advanced capacity to capture satellite imagery should consider providing at least derived information to international human rights mechanisms that have such needs, if necessary, on a confidential or non-attributable basis.**

D. To civil society organizations and academic institutions

121. **While remaining open to developments from a rapidly evolving field of technological innovation, civil society organizations should adopt an evidence-based assessment of the benefits of new ICT-enabled mechanisms. In collaboration with academics, they should concentrate resources on those areas where ICTs genuinely afford greater capacity, while maintaining the vital work they do using other, more traditional methods. Academics and human rights organizations should also collaborate to prioritize research in areas where it is needed most, for example to address the "volume challenge".**

122. **Those responsible for human rights curricula and training programmes should consider including modules on the effective use of ICTs to secure human rights. Larger organizations should continue to seek to assist those with more limited digital resources.**

E. To donors

123. **Donors should acknowledge that technological solutions to human rights problems can only be as successful as the training that accompanies them. In addition to expecting rigorous and honest appraisals of the utility and impact of new applications or devices, donors should also mainstream and support efforts to improve digital literacy and digital security awareness among those communities that most need it.**

F. To technology and software corporations

124. **Developers should favourably consider the inclusion of an "eyewitness" or "proof" function in mainstream camera applications that gives users the option to include the metadata and establish the integrity of the file, so as to make video evidence valuable, without the need to have previously downloaded a specialized application.**

125. **Social media platforms should devise a process whereby user-generated content that may be of relevance to human rights investigations, but that has been removed from platforms because of community standards, can remain available to fact-finders.**