

# UKWELI

Investigating human rights violations

Main Book



AMNESTY  
INTERNATIONAL



# UKWELI

## Investigating human rights violations

Main Book

**AMNESTY**  
INTERNATIONAL



## ***Ukweli***

*Investigating human rights violations – Main Book*

© 2020 Amnesty International

ISBN: 9789064634673

Author of *Ukweli: Investigating human rights violations – Main Book*: Claire Beston, Human rights consultant

Design and layout: Dalia Elazab

Cover illustration: (C Design Studio) Shutterstock

Human Rights Capacity-Building Programme (HURICAP) staff at Amnesty International Netherlands oversaw and edited the publication for final usage.

This book is the main handbook of the *Ukweli* series. *Ukweli* is a Swahili word for “finding the truth”. This main handbook can be used in conjunction with other books in this series.

Published and distributed by:

Amnesty International Netherlands

Human Rights Capacity-Building Programme (HURICAP)

PO Box 1968

1000 BZ Amsterdam

The Netherlands

Email: [huricap@amnesty.nl](mailto:huricap@amnesty.nl)

PDF file available at [amnesty.nl/media/huricap/publications-overview-human-rights-capacity-building-programme](https://www.amnesty.nl/media/huricap/publications-overview-human-rights-capacity-building-programme)

All rights reserved. This publication is copyrighted but may be reproduced by any method without fee for advocacy, campaigning or teaching purposes, but not for resale. When doing so, please acknowledge Amnesty International Netherlands as your resource. For copying in any other circumstances, or for reuse in other publications, translation or adaptation, prior written permission must be obtained from the publishers. To request permission, or for any other inquiries, please contact [huricap@amnesty.nl](mailto:huricap@amnesty.nl)

## Table of contents

<b>List of abbreviations.....</b>	<b>7</b>
<b>Preface.....</b>	<b>8</b>
<b>About this guide .....</b>	<b>10</b>
<b>Acknowledgements.....</b>	<b>11</b>
<b>Chapter 1: Introduction to investigating human rights violations .....</b>	<b>14</b>
1.1 Why does investigating human rights violations matter? .....	16
1.2 Core principles of investigating violations .....	18
1.2.1 Accuracy.....	19
1.2.2 Credibility.....	19
1.2.3 Impartiality and non-discrimination .....	20
1.2.4 Do no harm .....	21
1.2.5 Informed consent and confidentiality.....	22
1.2.6 Integrating a gender perspective .....	23
1.3 Starting points: monitoring and contact building .....	24
1.3.1 Monitoring .....	24
1.3.2 Contact building.....	26
<b>Chapter 2: Introduction to the legal frameworks of human rights.....</b>	<b>28</b>
2.1 International legal framework.....	29
2.1.1 International human rights law .....	29
2.1.2 International humanitarian law.....	33
2.1.3 International criminal law .....	33
2.2 Regional legal frameworks.....	36
2.3 National legal frameworks .....	37
<b>Chapter 3: Planning your investigation.....</b>	<b>40</b>
3.1 Decide on the focus and scope of your investigation .....	42
3.2 Check the relevant legal frameworks/standards .....	44
3.3 Identify what information you need .....	44
3.4 Identify sources of information.....	46
3.4.1 Testimonial evidence.....	47
3.4.2 Physical evidence.....	49
3.4.3 Documentary evidence.....	50
3.5 Identify how you will collect the information .....	50
3.5.1 Key methods of information collection .....	51
3.5.2 Information collection plan .....	52
3.6 Avoiding bias in your investigation methodology .....	53

3.7 Integrating a gender perspective into your methodology and investigation planning.....	54
3.8 Consulting technical experts and background research.....	56
3.9 Make logistical preparations.....	57

## **Chapter 4: Security planning and preparation ..... 60**

4.1 Understanding the threats.....	62
4.2 Preparing a risk assessment and security plan.....	64
4.2.1 Preparing your risk assessment.....	65
4.2.2 Preparing your security plan.....	68
4.2.3 Before you travel/begin your field work.....	72
4.2.4 General safety and security practices for all investigations.....	73
4.3 Security when working in areas of armed conflict.....	73
4.3.1 Understanding the threats.....	73
4.3.2 Preparing risk assessments for conflict and post-conflict areas .....	75
4.4 Security considerations for high-risk groups .....	76
4.4.1 Security of women human rights investigators.....	76
4.4.2 Security of LGBTI human rights investigators.....	77

## **Chapter 5: Digital security, information and communications security ..... 78**

5.1 Understanding threats.....	79
5.2 Computer/account security.....	79
5.3 Information security.....	81
5.4 Communications security.....	82

## **Chapter 6: Identifying and documenting physical evidence ..... 88**

6.1 Identifying physical evidence: what to look for.....	90
6.2 Documenting physical evidence.....	91
6.3 Investigating in conflict settings.....	94

## **Chapter 7: Interviewing..... 98**

7.1 Interview preparations.....	99
7.1.1 Identifying interviewees.....	99
7.1.2 Safety and security.....	101
7.1.3 Means of documenting or recording the interview.....	102
7.1.4 Support and referrals for interviewees.....	104
7.2 Before you start the interview.....	105
7.3. Conducting the interview: process .....	108
7.3.1 Avoiding interview biases.....	110
7.3.2 Interview challenges.....	111
7.4 Conducting the interview: content .....	113
7.5 Closing the interview.....	118

7.6 Interviewing groups with specific considerations.....	119
7.6.1 Interviewing survivors of sexual violence.....	119
7.6.2 Interviewing children.....	120
7.6.3 Interviewing people with trauma / avoiding re-traumatization.....	122
<b>Chapter 8: Collecting documentary evidence.....</b>	<b>126</b>
8.1 Identifying and collecting documentary evidence.....	127
8.1.1 Identifying sources.....	127
8.1.2 Collecting documentary evidence.....	129
8.1.3 Protecting sources and those featured in photos/footage.....	130
8.2 Satellite imagery.....	131
8.3 Handling open source/online information.....	135
8.4 Verifying content posted on social media (user-generated content) .....	137
<b>Chapter 9: Verification and analysis.....</b>	<b>148</b>
9.1 Verifying information.....	149
9.2 Analysing your findings.....	151
9.3 Storing and categorizing your findings.....	153
9.4 Identifying patterns in human rights violations.....	156
<b>Chapter 10: Report writing.....</b>	<b>162</b>
10.1 Guiding principles.....	163
10.2 Report content .....	164
10.3 When to publish your report, and seeking a government response.....	174
<b>Chapter 11: Stress, trauma and burnout: managing the well-being of                     human rights investigators .....</b>	<b>176</b>
11.1 Identifying conditions and recognizing symptoms.....	178
11.2 Good practices for managing the impact of stress and trauma.....	181
11.3 Responding to symptoms.....	183
<b>Glossary.....</b>	<b>186</b>
<b>Annex 1: Reference materials, resources and tools – security of human                     rights investigators.....</b>	<b>192</b>
<b>Annex 2: Reference materials, resources and tools – digital security.....</b>	<b>196</b>
<b>Annex 3: Tools for verifying open source material, photos and videos .....</b>	<b>200</b>
<b>Annex 4: Types of interview questions.....</b>	<b>202</b>
<b>Annex 5: Sample interview guide.....</b>	<b>206</b>
<b>Annex 6: Incident report form .....</b>	<b>212</b>

## List of boxes, figures and tables

### Boxes

Box 1. Key terminology.....	12
Box 2. Forms of human rights monitoring.....	25
Box 3. Sources of international law.....	29
Box 4. Core treaties of international human rights law .....	30
Box 5. Applicability of international legal frameworks.....	36
Box 6. Regional human rights instruments.....	36
Box 7. Investigating multiple violations happening together.....	43
Box 8. The 5WH framework of human rights investigations.....	45
Box 9. Pre-departure checklist .....	59
Box 10. What is a threat?.....	62
Box 11. What is a risk?.....	64
Box 12. Examples of how security planning and preparation can reduce vulnerability to risk.....	64
Box 13. Essential reminders – before you travel.....	85
Box 14. Do(s) and don't(s) when documenting at the scene .....	93
Box 15. Informed consent.....	106
Box 16. Following up – details!.....	116
Box 17. The importance of small details.....	117
Box 18. Patterns that data does and does not show you – example .....	160

### Figures

Figure 1. Key steps in the human rights investigation process .....	16
Figure 2. The 5-step process of planning your investigation.....	41
Figure 3. Example of a risk analysis table .....	66
Figure 4. Ratings bands for assessing the risk .....	67
Figure 5. Using satellite imagery to document suspected mass graves in Syria and Burundi.....	132
Figure 6. Using satellite imagery to document the abduction of protesters in Sudan .....	142

### Tables

Table 1. Examples of mitigation measures.....	68
Table 2. Sample risk assessment and mitigation plan.....	70
Table 3. Sample categories for a case sheet .....	154
Table 4. Key details of incidents/cases in which you might identify patterns ....	157
Table 5. Outline of a human rights report.....	171
Table 6. Interview questions .....	203

# List of abbreviations

<b>CAT</b>	Convention against Torture
<b>ICL</b>	International Criminal Law
<b>IDP</b>	Internally Displaced Person
<b>IHRL</b>	International Human Rights Law
<b>IHL</b>	International Humanitarian Law
<b>LGBTI</b>	Lesbian, Gay, Bisexual, Transgender, Intersex
<b>NGO</b>	Non-governmental Organization
<b>PTSD</b>	Post-traumatic Stress Disorder
<b>UN</b>	United Nations
<b>VPN</b>	Virtual Private Network
<b>WHRD</b>	Woman Human Rights Defender



# Preface

This guide is a revised and updated version of the Human Rights Capacity-Building Programme (HURICAP) *Ukweli: Monitoring and Documenting Human Rights Violations in Africa: A Handbook*, published in 2000. This new guide reflects the significant developments that have been made in methods and tools for investigating human rights violations over the last 20 years, as well as the emergence of new technologies that have completely changed how we receive, collect and share information, and how human rights investigators can protect themselves. However, these technologies have also introduced new threats to those seeking to protect human rights, and to their information.

Over the last two decades, some countries have made progress in rights protections. For instance, countries have emerged from long-running conflicts or lengthy periods of authoritarian rule characterized by multiple violations, and have introduced legal protections for minority rights or loosened restrictions on women's basic rights.

However, despite some successes in the last 20 years, and the ongoing struggle of many individuals, activists and organizations, in many parts of the world the protection of human rights has deteriorated: civic space is shrinking, and threats to democracy and human rights are increasing. Governments have retreated from their historic commitments and rolled back protections of citizens' basic rights; new conflicts have arisen, characterized by ever-more extreme levels of violence against civilians, which have caused new refugee crises met with apathy or even hostility from destination countries and the wider international community; and climate change increasingly fuels human rights violations and affects the ability of millions of people to enjoy basic rights including access to clean water, adequate shelter and healthcare, and is set to create millions of new refugees in coming decades.

The vast expansion of the internet, social media and digital technologies has created new opportunities for gathering information, exposing violations and expressing solidarity, but has also brought with it high levels of online abuse, often-unchecked incitement of hatred and infringement of privacy rights. The proliferation of inaccurate information disseminated online has jeopardized accurate reporting; the continued harassment of independent media in many countries exacerbates the situation.

In this context, the role played by human rights defenders continues to be absolutely critical. Human rights organizations and activists continue to denounce human rights violations, fight impunity, seek justice for victims, and attempt to change repressive and discriminatory systems and practices through human rights monitoring and investigations, human rights education, lobbying, advocacy and strategic litigation,

and through providing services where the state is not willing or able to do so. In some parts of the world, human rights civil society has grown considerably over the last 20 years. But human rights defenders frequently continue to undertake this work at great risk to themselves as the space in which human rights defenders operate increasingly shrinks. New technologies bring new threats of surveillance, interception of information and the identities of sources, and the intimidation and harassment of activists.

However, despite unprecedented challenges, people across the world continue to show that their thirst for justice, dignity and equality – for themselves, their communities and for others – will not be extinguished.

## About this guide

This book provides detailed guidance to human rights activists and organizations on conducting accurate and high-quality investigations into possible human rights violations. The accuracy and reliability of information collected and reported through human rights investigations is essential to their impact. The findings of high-quality and credible investigations can influence policy and practice; provide admissible evidence for court cases; advocate for justice, remedy and assistance for survivors and victims of violations and accountability for perpetrators; and generate pressure on duty bearers.

This guide provides detailed information on each stage of planning and conducting investigations into possible violations, verifying your findings and writing human rights reports. It explains techniques, skills and considerations relevant to each aspect. Examples and tools are used to illustrate the skills and processes involved, which investigators can adapt to their needs.

In light of the shrinking space worldwide for human rights defenders and the increasing risk of repercussions against their sources, the guide emphasizes safety and security planning for investigators, sources and the work itself, including secure digital, information and communications practices. The final chapter covers the critical aspect of managing the well-being of human rights investigators.

This handbook is accompanied by – and can be read in conjunction with – several thematic handbooks that provide detailed information and guidance relevant to investigating specific violations. These include handbooks on investigating enforced disappearances and on investigating torture and cruel, inhuman or degrading treatment or punishment, as well as a number of other thematic issues.

All the resources available in the series can be accessed here:

- [amnesty.nl/media/huricap/publications-overview-human-rights-capacity-building-programme](https://amnesty.nl/media/huricap/publications-overview-human-rights-capacity-building-programme)

The Human Rights Capacity-Building Programme (HURICAP) of Amnesty International Netherlands has worked with African civil society organizations in building human rights capacity for more than 20 years. Following the successes of working with African civil society, HURICAP started operating in the Middle East in 2016. A key part of this work has been in strengthening the knowledge and skills of local human rights organizations and activists to monitor, document, and report on human rights violations and abuses. This handbook draws on this experience.

# Acknowledgements

This handbook was written by Claire Beston, a human rights researcher and consultant. It was reviewed by members of the HURICAP team at Amnesty International Netherlands (notably Ellen Vermeulen, Yuhniwo Ngege, Liana Rodrigues and Wim de Regt). The design and layout were created by Dalia Elazab, and reviewed by Maylis Fabrissin, finance and administration assistant at HURICAP.

### **Box 1. Key terminology**

#### **Human rights violations**

A distinction is often made between human rights violations (when state actors are the main perpetrators) and human rights abuses (committed by non-state actors). However, this publication uses the term “human rights violation” to refer to both situations, namely, whether state or non-state actors are the perpetrators (see definitions of violations and abuses in the Glossary).

#### **Human rights investigators or human rights defenders?**

Human rights investigators are a type of human rights defender. This manual and other HURICAP materials in this second series use the term “human rights investigator”, as the series focusses on the investigation aspect of human rights work, to provide guidance to the defenders and activists who carry it out.

#### **Survivors and victims of human rights violations**

There is much debate about whether the term “victim” or “survivor” should be used to refer to people who have experienced certain human rights violations, particularly rape and other forms of sexual violence, and torture. Survivors/ victims themselves argue for both terms. Some materials tailor their use to the violation. For example, in the guide *Ukweli: Investigating Torture* in this series, the term “victim” is used to denote a person who has died as a result of torture, while “survivor” refers to someone who experienced torture but survived. In the guide *Ukweli: Investigating Enforced Disappearances*, “survivor” is used to refer to an individual who has been released from a period of enforced disappearance, while “victim” refers to someone in an ongoing situation of enforced disappearance as well as their family members.

This Main Book uses the term “survivors and victims” to refer to people who have experienced human rights violations, with the exception of sexual violence, for which we use “survivors” throughout. Therefore, the use of “victim” does not only denote someone who has died as a result of a violation.

# Chapter 1

Introduction to investigating  
human rights violations

Investigations entail identifying and collecting information in order to establish if a human rights violation, or series of violations, has occurred. **All allegations and reports of violations must be investigated before they are shared or published** in order to verify what took place and whether it constituted a human rights violation. Investigating seeks to establish **if** the incident occurred and **how** it occurred, and – if possible – **who** was responsible. Before you can state that a violation has taken place, you need to be able to report the details of what happened: investigating seeks to establish those details. The process of investigating can also reveal underlying issues and associated violations.

Many allegations of human rights violations are false, exaggerated or inaccurate. The investigation process seeks to distinguish facts from rumours or hearsay. Thoroughly investigating and verifying the specific details of violations ensures that you only report accurate information. This is key for establishing and maintaining the credibility of your work.

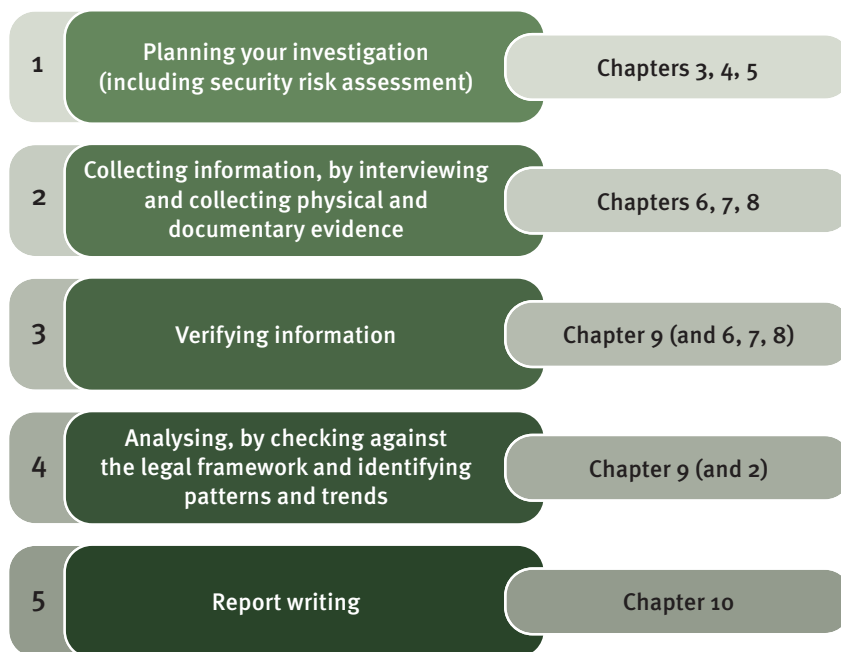
Human rights investigations are most effective when they combine a variety of information from multiple sources. As much information and detail should be collected as possible. This significantly strengthens your ability to verify what happened – through cross-checking the consistency of multiple sources – and will enable you to draw strong findings from your investigation.

You will (or might) need to:

- Gather information from first-hand (testimonial) sources, which is likely to include interviewing survivors, victims or witnesses of violations as well as other sources, including perpetrators if possible.
- Conduct a site visit to examine and document physical evidence.
- Identify types of documentary evidence to examine and make a record of or photograph, such as medical records, charge sheets, police records, photos or audio-visual material, satellite imagery or geographic information systems (GIS) data, official statements, statistics, maps.
- Seek expert opinions on certain aspects of the information.
- Gather information from secondary sources such as reports from other organizations, the UN or regional bodies, media articles, academic journals and numerous others.

This handbook outlines the following phases of investigating one or more possible human rights violations:

**Figure 1. Key steps in the human rights investigation process**



The current chapter of this handbook describes the need for and principles of monitoring and documenting violations. Chapter 2 introduces the legal frameworks that investigators need to refer to. The final chapter of the book deals with the well-being of human rights investigators.

### **1.1 Why does investigating human rights violations matter?**

Investigating human rights violations is the process of identifying, collecting, verifying and recording information about an event or series of events. When collected and verified, this information can be used to expose violations, seek redress for survivors and victims and accountability for perpetrators, and to bring about changes in policy and practice, in order to help end ongoing violations or impunity.

Accurate reporting is critical to the success of these efforts: it is an essential foundation for all human rights campaigning, advocacy and lobbying. Producing impartial, accurate reports will also build the legitimacy and reputation of you and your organization. Investigating and documenting violations serves at least six purposes. Each is described in turn below.



### **Taking immediate action**

In cases of suspected arbitrary arrest or detention, enforced disappearance, torture and similar violations, the survivors, victims and/or their relatives may need immediate assistance. This might include trying to establish the whereabouts and well-being of the victim (for example in police stations, military camps or other detention centres), filing a petition for habeas corpus (requiring the detained person to be brought before a judge or court to determine if the detention is lawful or if the person should be released) or seeking medical assistance. Establishing and verifying the facts surrounding such violations is an essential element of taking immediate action to help survivors, victims and their families.

### **Seeking redress and remedies**

A common motivation to investigate and document the facts about human rights violations is to help survivors/victims and their relatives seek justice through legal action and/or to obtain redress for victims. International human rights law gives victims of violations the rights to truth, justice and compensation. Justice and redress might be sought at the national, regional or international levels. Investigating and documenting human rights violations ultimately seeks to ensure that violations do not go unnoticed or unpunished and do not reoccur. The facts are also needed in order to seek medical, psychosocial, and other relief and rehabilitation for the victims.

### **Changing policies and laws**

Human rights violations are frequently investigated and documented to highlight state practices that violate or fall short of their obligations under international human rights law, with the aim of pressuring state actors (the duty bearers) to comply with the obligations they have signed up to. These efforts seek to change laws and policies that are inconsistent with international human rights law and standards. They might seek to end ongoing violations or prevent future violations.

### **Changing the authorities' behaviour and attitudes**

Human rights activists also aim to influence or change the behaviour, practices, attitudes and perceptions regarding human rights of officials such as policy makers, the judiciary, security services, the military, heads of militias or armed groups, local leaders (such as chiefs) and religious leaders. Efforts to influence people in positions of power to respect human rights are much more impactful when supported by clear, accurate and unbiased information.

### **Raising public awareness**

Publishing information about human rights violations also raises awareness among the public and the media, which can create public scrutiny and/or pressure on duty

bearers and perpetrators to end violations, hold perpetrators to account or prevent future violations, for instance through protests, critical media coverage, loss of political support/votes and other means. Publishing information can also attract attention from – and mobilize – the international community including governments and multilateral organizations, non-governmental organizations (NGOs) and other actors, which can exert pressure on duty bearers through different channels. Raising wider awareness can also generate solidarity for survivors, victims and their families.

### **Having a deterrent effect**

Some human rights investigators conduct systematic visits or observations of certain events or locations based on indications that violations might take place. This includes detention centres, criminal trials, demonstrations and elections. The presence of investigators can sometimes have a deterrent effect: actors may behave differently if there are witnesses to their actions. Identifying patterns of violations (see Section 9.4) is key to deciding if (and where) systematic monitoring is required.

## **1.2 Core principles of investigating violations**

A set of core principles should guide and inform every action and decision taken during human rights investigations. These apply to each stage of the processes laid out in this guide:

- accuracy
- credibility
- impartiality and non-discrimination
- do no harm
- informed consent and confidentiality
- integrating a gender perspective

Observing these principles will help to safeguard the security and well-being of the people you interact with in your work, particularly survivors and victims, as well as your own well-being. Adherence to these principles will also strengthen the quality of your work and enhance your reputation. This in turn will help you build trust with your contacts, including survivors and victims, and may increase your influence with state actors and other stakeholders.

These considerations apply to every stage of your work. This guide details specific instances in which these principles apply during the process of documenting violations. For example, *Security planning and preparation* includes details on using security risk assessments to ensure that you do not put the people you interview at risk of further harm; *Planning your investigation* covers integrating a gender perspective into your methodology and plans; *Interviewing* contains guidance on how to safeguard the confidentiality of your interviewees, and avoid re-traumatizing (that is causing further

harm to) people who have been subjected to traumatic experiences; and *Verifying information* contains guidance on ensuring the accuracy and credibility of your reporting.

### 1.2.1 Accuracy

Accuracy is the backbone of investigating violations. Before making public any claims that human rights violations have taken place, human rights investigators and organizations must be certain that what they claim happened did in fact take place.

Robust investigation and verification techniques are key to ensuring the accuracy of your information. Many reports of human rights violations are false or exaggerated. Unverified details must not be included in your reporting. Thorough investigations distinguish fact from rumours and hearsay. This involves identifying and collecting information from a wide variety of sources, and a rigorous assessment and verification of this information – through corroborating sources and consulting with technical experts – to establish a detailed picture of what took place. Being aware of your own and other people's biases is also important for safeguarding the accuracy of your work. In this way, accuracy is linked to impartiality (see below).

Governments and others look for methodological flaws with which to discredit human rights reports, and the individuals who compile them. Reporting inaccurate information will undermine the credibility of your organization, meaning that your future reports may not be trusted, and may put you and your colleagues at risk.

Accuracy is achieved by:

- recording, checking and verifying details;
- collecting information from a variety of sources.

### 1.2.2 Credibility

The principle of credibility is about being accepted as or believed to be true, real or honest. You and your work must be perceived to be credible so that the information you release publicly (in reports, statements, media interviews, and so on) is accepted as accurate and reliable. This will increase the likelihood that it will be used and cited by other actors including the media, other organizations, the UN, governments and international bodies. Credibility helps to expose violations, influence decision makers, increase pressure on perpetrators and achieve other outcomes.

It is also essential that survivors, victims and witnesses perceive you as credible and trustworthy. This is key to gaining the necessary trust for people to discuss sensitive information and experiences with you. When investigators and their organizations are deemed to be credible, witnesses and others with information are more likely to come

forward. When you engage with people, it is essential to be clear about the nature of the work and your organization, how you will use the information, and what assistance you can or cannot provide.

Reporting only accurate information is central to establishing and safeguarding the credibility (and therefore the impact) of your work and your organization. The accuracy of all the information you receive needs to be thoroughly verified before you report it. Credibility is therefore strongly linked to the principles of accuracy and impartiality.

You can also increase the credibility of your reports by clearly explaining your methodology – how you collected and analysed the information, and how you reached conclusions and identified patterns of violations.

Credibility is achieved by:

- being accurate;
- transparently explaining the purpose and methods of your investigation;
- being impartial.

### 1.2.3 *Impartiality and non-discrimination*

Impartiality entails being non-partisan and guarding against advancing any particular political, sectarian or other agenda. For human rights investigators, this means not supporting or opposing any government or political system, or taking sides in an international or domestic conflict, but objectively assessing the human rights practices of all relevant parties and documenting human rights violations that take place regardless of the nature of the government, political opposition or armed group, the nature of the conflict, the ideology of the perpetrators or the beliefs of the victims.

Impartiality also involves documenting violations and engaging with survivors, victims and other actors without discriminating on the basis of nationality, race, ethnicity, political opinion or status, religion, gender or other characteristics.

Taking an impartial approach to your investigations is vital to ensuring the information you collect is accurate and unbiased. Being perceived as impartial is also essential to your credibility and therefore the impact of your investigation and recommendations. It will also be key to some people's willingness (or refusal) to talk to you. In some contexts, demonstrating impartiality may be important for the safety and security of the investigators, your organization and your sources.

To ensure you are impartial, you must be aware of your own biases and the impact of your political beliefs, ethnicity or religion on your human rights work. You must thoroughly investigate and scrutinize all information: never make assumptions or

conclusions about events or actors before you have confirmed the facts. Also be aware of potential biases or agendas when engaging with survivors, victims, alleged perpetrators and other contacts. If it is safe to do so, seek to give alleged perpetrators or responsible authorities the opportunity to respond to a summary of the findings of your investigations.

Impartiality is achieved by:

- looking for information from different parties, victims and perpetrators, without any discrimination;
- being aware of possible biases.

#### 1.2.4 *Do no harm*

The principle of “do no harm” involves ensuring that the people and cases you engage with are not put at risk of further harm because of your work. This requires anticipating possible risks to survivors, victims, witnesses and other contacts, and to yourself, and taking steps to avoid them.

Harm can be direct or indirect, physical, psychological or social. The risk of retaliation is real in many places where survivors and victims speak out about what happened to them. Re-traumatization of survivors and victims is a real risk if interviews are conducted badly; where certain violations are subject to social stigmatization, survivors and victims are at risk if their identity and experiences are exposed. Investigators face risks including arrest, harassment and physical danger in some contexts.

The principle of “do no harm” should be considered throughout the process of planning and conducting your investigation and when reporting violations. Such considerations could influence decisions on *whether* and *what* you investigate; *where* you conduct field missions, as well as *when* and *how*; *who* you interview, *where* and *how*; and *how* you store, communicate and report the information you gather. This principle is particularly important when working with vulnerable groups such as children or marginalized individuals or communities.

A key way to incorporate the principle into your work is to conduct thorough security planning. But it also relates to how you treat survivors and victims of violations and people experiencing trauma; obtaining informed consent before interviewing; and the secure storage, transfer and communication of information.

Collecting information is essential to documenting human rights violations, but this should never be done at the expense of anyone’s security or well-being, including your own. If the likelihood of harm resulting from your actions is too high, change, postpone or cancel your plans.

The principle of do no harm entails:

- anticipate possible risks to survivors, victims, witnesses and other contacts, and to yourself;
- take steps to avoid those risks (security risk management, safe storage of information);
- prudent interviewing;
- obtaining informed consent before interviewing and photographing.

### *1.2.5 Informed consent and confidentiality*

Informed consent is a fundamental principle of ensuring the safety of everyone involved in your investigations and respecting their right to make decisions about their participation. This principle requires that anyone you interview, or who otherwise shares information with you, gives their consent to do so based on a thorough understanding of the purpose of their involvement and providing information, how that information will be used, and the potential security and other implications of doing so, and based on an understanding of the voluntariness of the process. Informed consent must be provided for each specific way in which an individual might be involved or their information used (such as separate consent for conducting an interview, and for taking photos). Informed consent must be given by each individual: it cannot be provided on behalf of a group by a “representative”.

Confidentiality is about not disclosing the identity and personal details of survivors, victims, witnesses and other sources of information, and safeguarding these details. This is a precaution to prevent sources of information from experiencing further harm for having reported such evidence. Confidentiality may apply to the identity of sources (such as names, families, locations) or the details of an incident or case. Interviewees may consent to you publicly disclosing details of their case, but in most cases they are likely to prefer (and/or you might decide) to withhold their identity due to concerns about repercussions, stigmatization or simply to protect their (right to) privacy.

There are limits to confidentiality in human rights work, however, as the purpose of collecting information from people is to use it to document violations. Respecting confidentiality in this sense means ensuring that information is only used in the way(s) to which interviewees and contacts have given their consent, and ensuring that any identifying details are concealed.

Breaching confidentiality could put interviewees and sources of information at serious risk of harm. At a minimum, it will undermine trust and make people less likely to talk to you or provide you with information in the future. Having adequate physical and digital

security protections in place for your office and your digital information storage and communications systems is an essential element of protecting confidentiality.

Confidentiality is achieved by:

- informed consent;
- not disclosing personal details in (public) reports;
- interviewing people discreetly;
- safe storage of information.

### 1.2.6 Integrating a gender perspective

Human rights violations affect men and boys, and women and girls, differently. They are targeted in different ways, have different vulnerabilities, and participate in and experience incidents in different ways. Gender determines what is expected, allowed and valued in a woman or man in a given context. In most societies there are differences and inequalities between women and men in decision-making opportunities, responsibilities assigned, activities undertaken, and access to and control over resources.

Integrating a gender perspective into your work involves considering, investigating and analysing how violations affect men and boys, and women and girls differently. Such a perspective helps to understand (less visible) power relations and patterns of discrimination, and to uncover human rights violations that specifically or disproportionately target or affect women and girls, or men and boys. “Specifically” means violations that happen to someone *because of* their gender – for example laws that deny women the right to own property *because* they are women. “Disproportionately” means the violation is *mostly* perpetrated against a particular gender, but also affects the other gender. For example, sexual violence disproportionately affects women and girls, while forced recruitment into armed groups disproportionately affects men and boys. Integrating a gender perspective also means considering how women and girls or men and boys experience the same violation differently, or are subject to different violations in the same context. Sometimes multiple layers of violations and injustice underpin the particular violation(s) you are investigating.

Including a gender perspective is crucial for properly understanding violations and accurately documenting all violations that have taken place in a given context. Doing so can help to ensure that women’s rights issues receive adequate attention in your investigations. In the past, human rights violations against women and girls have frequently been under-documented as a result of the subordinate status frequently assigned to them within families, communities and societies.

Gender considerations need to be incorporated not only into *what* you investigate but *how* you investigate it. This includes considering gender when mapping possible sources of information, your methodology and plans for investigations, anticipating and planning for challenges resulting from gender-related biases, and cultural norms and assumptions that you may have to navigate, for example in societies where social and cultural attitudes towards women might inhibit your ability to interview them about violations.

How to integrate a gender perspective:

- interview men and women;
- investigate how violations affect them differently;
- adapt your investigation approach to gender considerations.

### 1.3 Starting points: monitoring and contact building

#### 1.3.1 Monitoring

For many human rights investigators, the starting point for investigations is ongoing monitoring work. This is the process of observing and collecting information on a general situation or issues or situations of possible human rights concern over an extended period of time. Information is collected from a range of sources on a regular or systematic basis. During monitoring work, information and reports are gathered from a network of contacts, and from regularly checking the news media, social media and other sources. This work uncovers information, allegations and indications that human rights violations may have occurred, which are then confirmed and detailed through investigations.

If you are conducting monitoring on an issue, you should build trust with the communities or individuals who might be affected by the issues you are focusing on, in part because they might be sources of information. Developing a network of contacts and being known to monitor a certain issue means that your contacts will report incidents of possible violations directly to you.

Monitoring usually either focusses on a specific issue (such as incidents of police killings, harassment of journalists, enforced disappearances); a specific case/situation of an individual victim or group of victims (for example, discrimination against a minority ethnic group, a community at risk of forced eviction); a conflict situation; or the general human rights situation in a certain geographic area (region/country).

When you identify (or are alerted to) reports or indications that possible violations have taken place or continue to take place, you must investigate these reports to find out



if a violation did actually happen – and to establish exactly what happened – before you publicize anything or take any action. **All information gathered during monitoring must be verified through thorough investigations.**

### Box 2. Forms of human rights monitoring

- **Demonstration monitoring:** Entails observing the conduct of security forces and specific groups during demonstrations with the aim of determining whether the methods used by the security forces are necessary and/ or proportionate. This might include interviewing persons involved in the demonstrations or the security force response, either at the scene or afterwards. Demonstration monitoring is important where there is a previous pattern of violations.
- **Court/trial monitoring:** This involves observing a judicial proceeding to determine whether it complies with national and international standards for fair trials. It is not possible to conduct trial observation in all situations. For instance, some trials take place behind closed doors. Others might be open to the public but it might be too dangerous for you, or the defendants, to attend. (See Amnesty International's *Fair Trial Manual* [2nd Edition, 2014] for detailed guidance on fair trial standards and what to look for when observing trials.)
- **Prison/detention centre monitoring:** This involves visiting prisons /detention centres to observe the conditions of detention, facilities (for example provision of healthcare), and if possible, interviewing detainees about their treatment and conditions. Be aware that you may not be able to interview detainees in private (see below on interviewing), and detainees could face repercussions for speaking to you, even if they are seemingly permitted at the time. Your visit might also involve asking to see official records (for example of admissions, releases, and others). In many situations, human rights investigators are not permitted access to detention facilities; limited access might be permitted in some countries.

Monitoring can also entail direct observation. This involves going to situations where you think human rights violations *may* occur or *are likely* to occur. This can serve different purposes: collecting primary evidence by becoming a first-hand witness yourself, possibly photographing or recording incidents as they occur, collecting testimonial evidence (interviewing sources/victims/witnesses) at the scene, and recording or photographing physical evidence. Such situations may include an ongoing protest movement or demonstration, trial, electoral campaigns or activities in detention centres.

### *1.3.2 Contact building*

Building and maintaining a wide network of contacts plays a crucial role in effectively monitoring and investigating human rights violations.

- Contacts can alert you to the occurrence of possible violations or provide information about incidents involving possible violations, provide analysis or contextual information about a situation, offer specialist expertise relevant to assessing certain violations or details, help to corroborate information and help to identify a pattern in violations.
- Your network can help identify and establish contact with first-hand sources of information to interview during investigations.
- Maintaining a wide network of contacts is essential to the safety and security of yourself and your colleagues because it makes it more difficult for you to be targeted by hostile entities. Contacts can provide you with security-related information (including before you travel to conduct a field investigation), act as local check-ins (see below), can react if anything happens to you (for example, demand your release if you are arrested) or represent you (lawyers), and provide solidarity and other support.

Collecting information from a wide variety of sources and interviewing people with a range of perspectives is essential to the accuracy of your investigations and reporting, as discussed in detail below. Therefore, it is important that your network of contacts reflects this variation. This will help to minimize bias in your work. This is especially important when working in highly divided or politicized contexts, such as areas with ethnic divisions or in conflict settings.

Contact building is an ongoing process throughout your work. In all situations, but particularly in sensitive contexts, it takes time and regular contact to build trust. It can also take time to establish the reliability of the contacts, and to assess whether they have any political or other agendas. However, even with trusted contacts, all information received from any source must be verified. Contacts can unknowingly provide inaccurate information; others may do so intentionally.

# Chapter 2

Introduction to the legal  
frameworks of human rights

Human rights are guaranteed under international, regional and national law. The work of human rights investigators is firmly situated within these legal frameworks. Before you begin any investigation into one or more possible human rights violations, it is important to understand how that violation is defined in law, which might include international human rights law (IHRL), international criminal law (ICL), international humanitarian law (IHL), regional law, national legislation, and with reference to other international and regional human rights standards. It is also essential to know what your government's legal obligations are in relation to that right.

## 2.1 International legal framework

Human rights are protected in a number of areas of international law – IHRL, IHL (the laws governing armed conflict), ICL (which deals with individual responsibility for the most serious violations of human rights and humanitarian law), and other areas of law specific to particular issues or groups, such as international refugee law or labour law. The main sources of international law are treaty law and customary international law (see Box 3).

### Box 3. Sources of international law

**Treaty law:** Treaties, conventions, covenants and protocols are international legal instruments that **impose binding legal obligations on states that are party to them**. A state can become party to a treaty through ratification, accession or adherence, which means it voluntarily decides to be bound by the provisions of the treaty. By becoming parties to international treaties, states take on obligations and duties under international law to respect, protect and fulfil the rights enshrined in them.

**Customary international law:** International obligations arise from state practice – where a certain practice is widely upheld by the international community, and when there is a conviction in the international community that the practice is required as a matter of law, it becomes law “by use”. Customary international law comprises norms that are **binding on all states** independent of their treaty obligations.

### 2.1.1 International human rights law

IHRL is the primary source of protections and guarantees of human rights at the international level. This body of law stipulates the rights of people (rights holders) and the obligation of the state (duty bearer) to ensure that these rights are fully enjoyed. When states become party to human rights treaties, they take on obligations to respect, protect and fulfil the rights contained therein.

The obligation to *respect* means that states must refrain from interfering with or curtailing the enjoyment of human rights. The commitment to *protect* requires states to protect individuals and groups from human rights abuses committed by non-state actors. The obligation to *fulfil* means that states must take positive action to facilitate the enjoyment of human rights.

The Universal Declaration of Human Rights of 1948 is a central source of human rights law. The declaration itself is not legally binding, but it significantly influenced the content of the core IHRL treaties, and some of its provisions are considered to constitute customary international law as they are widely accepted and practised by states. The main body of IHRL is contained in core human rights treaties of the United Nations (UN) (see Box 4).

#### **Box 4. Core treaties of international human rights law**

International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)

International Covenant on Civil and Political Rights (ICCPR)

International Covenant on Economic, Social and Cultural Rights (ICESCR)

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)

Convention against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment (CAT)

Convention on the Rights of the Child (CRC)

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW)

International Convention for the Protection of All Persons from Enforced Disappearance (CPED)

Convention on the Rights of Persons with Disabilities (CRPD)

The full texts of these treaties are available on the website of the UN High Commissioner for Human Rights: [ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies](https://www.ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies). Many other treaties and legal documents constitute additional sources of human rights law.

- Treaty law is binding on states that are party to (have ratified) the instrument. However, in some cases, states make a reservation or declaration related to a specific article of the treaty they are ratifying.

- ▶ *When applying international law in your investigations and reporting, you need to check which treaties your government has signed up to. This will confirm whether your government has obligations under that treaty.*
- ▶ *You can check which treaties your government is a state party to in this table: [indicators.ohchr.org](https://indicators.ohchr.org), which also shows reservations or declarations made by states at the time of ratification.*

- Some treaties have been expanded by the addition of one or more optional protocols, which states must ratify separately. The link above shows the status of states' ratification of all human rights treaties and their optional protocols.
- Some IHRL provisions are considered to amount to customary international law as they are widely accepted and practised by states. This includes the prohibition on torture, meaning that all states are bound by that norm, irrespective of whether they have ratified the Convention against Torture (CAT).
- Article 4 of the International Covenant on Civil and Political Rights allows states to temporarily suspend ("derogate") some rights in exceptional circumstances of a "state of emergency", which threaten the life of a nation, subject to official notification and other conditions. Such measures are strictly limited to the extent required.
- However, some rights are non-derogable in any circumstances – meaning they cannot be suspended even in a state of emergency. These rights include the right to life; the prohibition of torture or other cruel, inhuman and degrading treatment or punishment, and of medical or scientific experimentation without consent; the prohibition of slavery, slave trade and servitude; the right to recognition before the law (which therefore amounts to a prohibition on enforced disappearance); and freedom of thought, conscience and religion.
- IHRL applies in periods of armed conflict as well as peacetime. IHL (covered below) applies additional obligations on the belligerent parties relevant to the conduct of hostilities.

- ▶ *Further guidance on the applicability of relevant standards is available at: [ohchr.org/sites/default/files/Documents/Publications/Chapter05-MHRM.pdf](https://ohchr.org/sites/default/files/Documents/Publications/Chapter05-MHRM.pdf)*

## UN human rights mechanisms

The UN system includes a range of mechanisms to monitor states' implementation of human rights law. These include:

### Treaty bodies

- Each of the core UN human rights treaties has a committee of independent experts that monitors its implementation by state parties. These committees are known as UN treaty bodies. For example, the Committee against Torture oversees the implementation of the CAT, and the Human Rights Committee oversees the implementation of the International Covenant on Civil and Political Rights.
  - States are required to periodically report on steps they have taken to implement the treaty. Civil society can submit parallel reports on a state's adherence to its treaty obligations. Based on these reports and other relevant sources of information, the treaty body will issue recommendations on further measures to be taken by the state to enhance its compliance with the treaty.
  - Most treaty bodies can also receive complaints from individuals residing in a state party who claim their rights have been violated, if those states have acceded to the individual complaints mechanism. Treaties contain different criteria for the admissibility of complaints. For most, this includes a requirement that domestic remedies have been exhausted before referring a complaint to the international level.
- *For more information, including on mandates and working methods, see: [ohchr.org/en/treaty-bodies/videos-about-treaty-bodies](https://www.ohchr.org/en/treaty-bodies/videos-about-treaty-bodies)*

### Universal Periodic Review

- This mechanism of the UN Human Rights Council reviews the human rights situation of all UN member states every 4–5 years. States submit a report on their compliance with their international human rights obligations, and detail their main human rights initiatives and challenges. Again, civil society can submit parallel reports and suggest recommendations. The Universal Periodic Review Working Group issues recommendations at the end of the review.
- *See: [ohchr.org/en/hr-bodies/upr/upr-home](https://www.ohchr.org/en/hr-bodies/upr/upr-home)*

### UN special procedures – special rapporteurs and working groups

- These are independent experts or groups of experts mandated by the UN Human Rights Council to monitor, advise and report on specific human rights issues or situations. These include special rapporteurs and working groups. They can examine and issue reports on rights or situations under their mandate, conduct country visits (at the invitation of the state in question), and send communications and urgent appeals to states on individual cases/situations of concern. The mandate of each procedure is different, and therefore, there are a number of ways in which civil society can engage with special procedures.
- *For further information on the different mandates, see: [ohchr.org/en/special-procedures-human-rights-council](https://www.ohchr.org/en/special-procedures-human-rights-council) (country mandates and thematic mandates); also click on the right bar “How to submit information”.*

### 2.1.2 International humanitarian law

IHL – also known as the laws of war – stipulates the rules and principles that regulate the protection of people and the conduct of hostilities during armed conflict. IHL seeks to protect people who are not participating in hostilities – civilians, as well as civilian objects including schools and hospitals. It also contains protections for certain combatants, including those who are no longer participating in hostilities because they have been wounded or captured. IHL also sets out standards of humane conduct, and limits the means and methods of conducting military operations. Its central purpose is to limit, to the extent feasible, human suffering in times of armed conflict.

IHL sets out rules applying to international armed conflicts and non-international armed conflicts. While only limited provisions apply to domestic conflicts, customary international law is considered to apply in all conflicts. Grave breaches of the Geneva Conventions and of Protocol I amount to war crimes – see below.

IHL remains applicable during conflicts and is binding on states, but human rights law does not address the obligations of non-state armed groups, which are not parties to the treaties (only states can ratify and become parties to treaties). Since customary IHL applies to all parties to a conflict, it imposes some duties on non-state armed groups to respect certain rights.

- *The principal instruments of IHL are the four Geneva Conventions of 1949 and their two Additional Protocols of 1977 which can be found here: [oas.org/dil/introductory\\_course\\_on\\_international\\_humanitarian\\_2007\\_IHL\\_instruments.pdf](https://oas.org/dil/introductory_course_on_international_humanitarian_2007_IHL_instruments.pdf)*
- *The International Committee of the Red Cross (ICRC) has also compiled a database of customary international law which can be found here: [ihl-databases.icrc.org/customary-ihl/eng/docs/home](https://ihl-databases.icrc.org/customary-ihl/eng/docs/home)*

### 2.1.3 International criminal law

ICL deals with individuals' criminal responsibility for the most serious violations of human rights law and humanitarian law. This means that, while IHL obligations fall to states, under ICL individuals can be held criminally liable for their acts and omissions.

- *The central instrument of ICL is the Rome Statute of the International Criminal Court (1998): [icc-cpi.int/Publications/Rome-Statute.pdf](https://icc-cpi.int/Publications/Rome-Statute.pdf)*

ICL applies to state and non-state actors accused of perpetrating, ordering, aiding and assisting, or facilitating the commission of the most serious violations of IHL and IHL. Under the Rome Statute, criminal responsibility is also attributed to military commanders for crimes perpetrated by forces under their effective command, who knew (or should have known) that such crimes were being committed, and failed to take action.



The three main areas of crimes covered by the Rome Statute are genocide, war crimes and crimes against humanity.

### Genocide

- The Rome Statute defines genocide as “any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such: (a) Killing members of the group; (b) Causing serious bodily or mental harm to members of the group; (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; (d) Imposing measures intended to prevent births within the group; (e) Forcibly transferring children of the group to another group.”

### War crimes

Serious violations of IHL constitute war crimes.

- Article 8 of the Rome Statute describes the acts that constitute war crimes. Most war crimes are perpetrated against non-combatants and civilian populations. They include killing, torture, deportation, rape, the taking of hostages, forced labour, wilfully causing great suffering or serious injury, and the extensive destruction of property.
- War crimes can only be committed during periods of armed conflict. They may be individual and isolated acts: for example, one case of rape in connection to an armed conflict could be a war crime.

### Crimes against humanity

The Rome Statute defines crimes against humanity as acts which have been “committed as part of a widespread or systematic attack,” “directed against a civilian population” and committed according to “a state or organizational policy”.

- The Rome Statute defines 11 types of acts that can constitute crimes against humanity when committed under these circumstances, including murder, extermination, enslavement, enforced disappearance, deportation or forcible transfer of population, torture, rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization or any other form of sexual violence of comparable gravity, and persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender or other grounds that are universally recognized as impermissible under international law.
- “Part of a widespread or systematic attack” means that a single incident of one crime can be a crime against humanity when committed as part of a wider attack involving the commission of other crimes. For example, one act of murder can be a crime against humanity when carried out in conjunction with rapes, torture, and other acts as part of a widespread or systematic attack.

- Crimes against humanity can be committed at any time, including peacetime and periods of armed conflict or other situations of violence.

### Other relevant international treaties and sources of international human rights protections

- Convention Relating to the Status of Refugees (1951) and Protocol Relating to the Status of Refugees (1967): [unhcr.org/about-unhcr/overview/1951-refugee-convention](https://www.unhcr.org/about-unhcr/overview/1951-refugee-convention)
- Conventions of the International Labour Organization. Eight “fundamental conventions” set out international standards of principles and rights at work, which are legally binding on ratifying states. “Recommendations” also serve as non-binding guidelines: [libguides.ilo.org/c.php?g=657806&p=4649148](https://libguides.ilo.org/c.php?g=657806&p=4649148)
- UN declarations, recommendations, guidelines, bodies of principles and codes of conduct on a range of subjects further enshrine human rights standards. These sources are not legally binding, though some provisions of some instruments may be considered to amount to customary international law. These instruments are considered authoritative as they have been recognized by the UN member states. These include:
  - Standard Minimum Rules for the Treatment of Prisoners (Mandela rules): [unodc.org/pdf/criminal\\_justice/UN\\_Standard\\_Minimum\\_Rules\\_for\\_the\\_Treatment\\_of\\_Prisoners.pdf](https://www.unodc.org/pdf/criminal_justice/UN_Standard_Minimum_Rules_for_the_Treatment_of_Prisoners.pdf)
  - Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment: [ohchr.org/sites/default/files/Documents/ProfessionalInterest/bodyprinciples.pdf](https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/bodyprinciples.pdf)
  - Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Istanbul Protocol): [ohchr.org/sites/default/files/documents/publications/training8rev1en.pdf](https://www.ohchr.org/sites/default/files/documents/publications/training8rev1en.pdf)
  - Code of Conduct for Law Enforcement Officials: [ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials](https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials)
  - Basic Principles on the Use of Force and Firearms by Law Enforcement Officials: [ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement](https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement)
  - The Minnesota Protocol on the Investigation of Potentially Unlawful Death: [ohchr.org/sites/default/files/Documents/Publications/MinnesotaProtocol.pdf](https://www.ohchr.org/sites/default/files/Documents/Publications/MinnesotaProtocol.pdf)
  - Declaration on the Elimination of Violence against Women: [ohchr.org/en/instruments-mechanisms/instruments/declaration-elimination-violence-against-women](https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-elimination-violence-against-women)
  - Declaration on the Protection of All Persons from Enforced Disappearance: [ohchr.org/en/instruments-mechanisms/instruments/declaration-protection-all-persons-enforced-disappearance](https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-protection-all-persons-enforced-disappearance)

### Box 5. Applicability of international legal frameworks

- IHL applies during periods of armed conflict. Different provisions apply to international and non-international armed conflicts. IHRL applies at all times (including during periods of armed conflict), though some rights are derogable in times of emergency, subject to official notification.
- IHL is binding on states party to the relevant treaties. Customary international law is binding on all states.
- ICL applies to individual responsibility relating to the commission of the most serious violations of IHRL and IHL.

## 2.2 Regional legal frameworks

Human rights are also enshrined and enforced through regional instruments and mechanisms. Africa, the Americas, Europe and the Arab states all have regional human rights instruments. These are legally binding for the states that have ratified them.

### Box 6. Regional human rights instruments

- African Charter on Human and Peoples' Rights, adopted by the Organization of African Unity, now the African Union, came into force in 1986: [au.int/sites/default/files/treaties/36390-treaty-0011 - african charter on human and peoples rights e.pdf](http://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf)
- American Convention on Human Rights, adopted by the Organization of American States, entered into force in 1978: [treaties.un.org/doc/Publication/UNTS/Volume%201144/volume-1144-I-17955-English.pdf](http://treaties.un.org/doc/Publication/UNTS/Volume%201144/volume-1144-I-17955-English.pdf)
- Arab Charter on Human Rights, adopted by the Council of the League of Arab States, entered into force in 2008: [ohchr.org/sites/default/files/Documents/Issues/IJudiciary/Arab-Charter-on-Human-Rights-2005.pdf](http://ohchr.org/sites/default/files/Documents/Issues/IJudiciary/Arab-Charter-on-Human-Rights-2005.pdf)
- Association of Southeast Asian Nations (ASEAN) Declaration of Human Rights, adopted in 2012: [asean.org/asean-human-rights-declaration](http://asean.org/asean-human-rights-declaration)
- European Convention for the Protection of Human Rights and Fundamental Freedoms, adopted by the Council of Europe, entered into force in 1953: [coe.int/Documents/Convention\\_ENG.pdf](http://coe.int/Documents/Convention_ENG.pdf)

These regional treaties largely reflect the core provisions of IHRL, but some go further than the international level. For example, the African Charter on Human and Peoples' Rights enshrines the rights of individuals as well as peoples as collectivities.

Regional mechanisms in the African, American and European systems oversee or enforce the implementation of the legal statutes.

- Africa: the African human rights system is established under the African Union. The main mechanisms are the [African Commission on Human and Peoples' Rights](#) and the [African Court on Human and Peoples' Rights](#). The commission uses a number of special mechanisms including Special Rapporteurs and Working Groups. The court has jurisdiction over cases and disputes relating to the interpretation and application of the African Charter and other relevant human rights instruments ratified by the states concerned.
- Americas: the inter-American system for the protection of human rights exists under the umbrella of the [Organization of American States](#). The main mechanisms are the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights. The commission oversees several rapporteurships and one special rapporteur. The court can hear cases submitted to it by the commission or by a state party to the convention.
- Arab states: the Arab Human Rights Committee was established in 2009 to oversee compliance with the Arab Charter on Human Rights.
- Europe: the leading regional arrangements for protecting human rights in Europe are the [European Convention on Human Rights](#) and the [European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment](#), and corresponding mechanisms such as the [European Court of Human Rights](#) and the [European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment](#). The European Court of Human Rights has jurisdiction over Council of Europe member states that have opted to accept the court's jurisdiction. Once a state has done so, all court decisions involving the state are binding.

Each mechanism has different criteria regarding who can engage with it, how and under what circumstances. Their websites contain useful information about their working methods and how to engage with them.

Most, if not all, of the regional mechanisms require that you have exhausted domestic legal remedies before you refer a case to them.

### 2.3 National legal frameworks

Human rights are also protected in national constitutions and other national legislation. In ratifying an international treaty, a state undertakes as a matter of law that its national arrangements (its constitution, laws, budgets, policies and practices,

and so on) will comply with that standard. If a state's national legislation or practice fall short of the human rights standards to which it has agreed, this constitutes a violation of its international legal obligations and commitments. Most state constitutions enshrine human rights (often in a Bill of Rights) within additional legislation, policies and procedures, giving force and effect to these rights.

States follow different practices in incorporating international treaties into their domestic legal structures. In some countries, international and regional human rights treaties automatically become part of national law. Thus as soon as the state has ratified or acceded to an international agreement, that agreement is directly applicable within its national legal system. In other countries, additional national legislation must be passed before international treaties have the force of law. Some national constitutions stipulate that if national law is in conflict with an international treaty, the treaty provisions shall prevail.

National law may also contain other provisions relevant to the protection – or absence of protection – of human rights. In some instances, protections of human rights in national law are stronger than those in international treaties. For example, many states prohibit the death penalty, which is not explicitly prohibited under IHRL. However, national law may also contain provisions that enshrine discrimination or other violations of rights – such as prohibiting women from inheriting property.

A range of oversight and enforcement mechanisms may be in place to monitor and act upon adherence to national and international law. These might include oversight bodies such as National Human Rights Commissions, Ombudsman's Offices and Independent Police Complaints / Oversight Bodies.

Some legal systems have processes of habeas corpus and/or amparo, which give individuals access to a court to challenge the lawfulness of a detention, or protect them from certain violations.

- When applying human rights legal frameworks in your work, always check the status of both national and international law on the right(s) in question.
- Be familiar with oversight mechanisms in your country, including their mandates and working methods.
- Understand any extraordinary processes included in your national legal framework such as habeas corpus or amparo procedures where they may be relevant to your work.

# Chapter 3

## Planning your investigation

This chapter deals with the first phase in the investigation process: **planning your investigation**.

**Proper planning of any human rights investigation is essential to its effectiveness.** This involves obtaining as much evidence as you can and establishing reliable findings, while protecting the safety and security of everyone involved.

Planning and preparing your investigation consists of the following elements, each of which is discussed in turn below:

- Deciding the focus and scope of your investigation;
- Identifying the relevant legal standards;
- Identifying what information you need;
- Identifying the possible sources of that information;
- Identifying the methods you will use to collect the information;
- Checking for any bias in your investigation methodology (including integrating a gender perspective);
- Security planning, including digital aspects (this is addressed in Chapters 4 and 5);
- Making logistical arrangements;
- Consulting technical experts and conducting background research.

These elements can be summarized as a 5-step planning process:

**Figure 2. The 5-step process of planning your investigation**



### 3.1 Decide on the focus and scope of your investigation

When planning an investigation into a possible human rights violation or series of violations, the first step is to identify what your investigation will cover. You will always need to be flexible regarding information and situations that arise during the investigation, but you should have a good idea at the beginning of what you aim to achieve.

As it is not possible to investigate everything, you will need to define the focus and scope to ensure your investigation is effective.

Consider the following issues:

- **Thematic focus:** What alleged violation or interconnected violations are you going to investigate? Many cases involve the violation of a number of different rights (see Box 7).
- **Type of case:** Are you investigating an individual case or multiple cases?
- **Geographic focus:** Which area are you looking at – one region/the whole country?
- **Timeframe:** What time period does your investigation cover? If a series of violations may have occurred over a prolonged period, are you looking at the whole period / all incidents? Or only those alleged to have taken place in the last year?
- **Resources:** What can you realistically achieve with the time and resources you have?
- **End goal:** What do you intend to do with the information? This will also inform the scope and depth of your investigation. For example, do you plan to take immediate action to assist victims of violations or their families? (For example, if you want to assist a family whose relative has been forcibly disappeared by approaching the authorities to seek the disappeared person, you need a lower standard of certainty, less information and time is an urgent factor, meaning your investigation will have limited scope.) Do you plan to publish a report? (This will require a higher level of certainty and therefore a more in-depth investigation, and more time to collect the information.) If you are investigating a pattern of violations, you will need to verify each case (with multiple sources for each) and examine a sufficient number of cases to be able to confidently conclude that there is a pattern.
- **Context:** What context will your investigation take place in? This might influence what you are able to do or focus on, and where you will be able to investigate in person (for example, during an armed conflict or context of severe political repression).

► *If you are investigating multiple cases, it is very important to examine whether there are any patterns between the cases (see Chapter 9).*



**Box 7. Investigating multiple violations happening together**

A number of violations might occur in the same circumstances or incident, or be connected. One violation might provide the context for other violations to occur. For example, if someone is arbitrarily arrested, they might also be subjected to prolonged detention without charge, or torture or inhumane treatment; forced evictions might give rise to the unnecessary use of force by security services, cruel, inhuman or degrading treatment, sexual violence or other violations, and may lead to loss of access to education and other economic, social and cultural rights.

**Your investigation should try to establish all the violations that have happened** in relation to an incident or series of incidents, to the fullest extent possible given your available time and resources.

For example, torture often occurs in conjunction with a range of other violations. Therefore, when investigating information about an allegation of torture, you also need to determine if other violations may have occurred by considering the context in which the torture took place. For example, was the victim detained? If so, was the detention lawful? Were international standards of due process and fair trial met? Did the conditions of detention meet international standards? **If you only investigate the torture allegation, you risk missing key information about related violations.**

Multiple *layers* of violations also often occur at the same time – and contribute to or reinforce each other. This is particularly the case where certain groups are subjected to discrimination and with gender-based violence. For example, during displacement caused by conflict, women and girls may experience multiple layers of violations with several perpetrators, including: indiscriminate killing and targeting of civilians (non-gender specific), sexual violence by combatants (disproportionately targets women and girls), denial of access to services in displacement (which may be due to gender-based discriminatory practices), domestic violence (often increases in times of conflict/displacement, affects women and girls disproportionately), and rejection or stigmatization by community because of rape/sexual violence they experienced (non-gender specific stigmatization, though majority of survivors are women and girls).

While it is impossible to know or anticipate in advance all the violations that might have occurred in a given context, it is important to be aware of the possibility of related violations so you are open to these during your investigation.

You might become aware of other possible violations while observing physical evidence or reviewing documentary evidence, or interviewees might reveal unexpected information during interviews.

### 3.2 Check the relevant legal frameworks/standards

Your investigation will need to establish whether the alleged incident did occur and if so, whether it constitutes a human rights violation or an ordinary crime. This determination requires considering two sets of questions:

1. What are your government's legal obligations in relation to the violation?
  - What are the relevant provisions in national law?
  - How is the right in question protected in a regional human rights instrument? Is your state a party to that treaty?
  - How is the right in question protected under relevant international human rights, humanitarian, criminal and refugee treaties? Is your state a party to these treaties (meaning they have a legal obligation to uphold their provisions)? Did it register any reservations at the time of ratification?
  - How is the right in question protected under customary international law, which applies to all governments regardless of whether they have ratified any relevant treaties?
  - Is a state of emergency in place, and have certain rights been formally derogated from (where derogation is permitted)?
  - Is an international or non-international armed conflict occurring? Which areas of IHL apply? Is the right in question a principle of customary IHL?
2. Are you trying to investigate/document abuses by non-state actors? If so, what law and standards apply to those actors?
  - What provisions in national law relate to the rights in question?
  - Are the rights in question enshrined in areas of IHL or ICL that apply to non-state actors?
  - What are the particular state obligations to protect rights holders from abuse by non-state actors?

### 3.3 Identify what information you need

In all investigations, you should aim to obtain as much detail as possible – and from as wide a variety of sources as possible. This is crucial to confirming what happened, and whether or not it constitutes a human rights violation. Obtaining detailed information can also reveal other related violations. Box 8 summarizes the details you need to gather in order to establish if the incident happened, how it happened, and that it constituted a violation.

### Box 8. The 5WH framework of human rights investigations

The details you need to collect vary depending on the type of violation you are investigating. However, to establish if a violation has taken place, all investigations should **try to answer the central questions** of “**Who did What to Whom, When, Where, How and Why?**”

- **Who** is/are the perpetrator(s)? **Who** is/are the survivors/victims?
- **What** did the perpetrators do (act/violation)?
- **When** did the incident(s) take place?
- **Where** did the incident(s) occur?
- **How** did it happen (details of the incident)?
- **Why** did the incident(s) occur (motivation behind the incident)?

For example, investigating suspected arbitrary arrests would involve looking for the following details:

- *Who* – Who made the arrests? (Security services? Which branch? How many of them? Under official state orders?)
- *What* – What happened? What was the basis of the arrests? Was there an arrest warrant? Was violence / unnecessary / excessive force used? Were the arrested people (arbitrarily) detained? For how long, and so on?
- *To Whom* – Who was arrested? How many? What were their identities (ethnicity, profession, political affiliation, activity at time of arrest (for example during a demonstration))? Depending on the violation, these details might be very relevant to the reason for the arrests.
- *When* – When were the arrests made? When (if at all) were the individuals taken before a court? When were their families informed, if at all? When were they released (if at all)?
- *Where* – Where did the arrests happen? Where were the arrested people detained?
- *How* – How were the arrests carried out? Was violence involved? Was it disproportionate/unnecessary?
- *Why* – What was the reason for the arrests? Why were the victims targeted?

### Investigation checklist

You may want to prepare a checklist of issues to cover in your investigation and interviews. For example, a checklist to investigate an allegation of torture might list the following areas to cover:

1. **Circumstances leading to torture?** (Took place in a detention setting?  
Circumstances of the detention? (Who was detained, by whom, when, where,

- duration, why (reasons for arrest), lawful (followed due process)? If not in a detention setting, in what circumstances?))
2. **Details of victim/survivor...?** (Identity, gender, age, ethnicity (if relevant), employed/studying, political affiliation (if relevant), and so on.)
  3. **Details of perpetrator?** (Police, guards, other? How did the interviewee know? Uniform? Language spoken (if relevant)?)
  4. **Details of the act(s) of torture**
    - i. **What** (What happened exactly? Physical/psychological torture? Any treatment received?)
    - ii. **When** (What time of day/night? Always at the same time of day (if more than one incident)? At which point in the detention (early stages, throughout, and so on)?)
    - iii. **Where** (In an interrogation room, in the cell, another location?)
    - iv. **How** (Implements used? (Which ones? How were they used / on which part of the body?) Injuries sustained?)
    - v. **Why** (Reasons given/accusations made or particular insults that indicate motivation? Particular questions asked? Could link to motivation to extract information, confessions, or to force the incrimination of others.)
  5. **Details of the detention centre** (Where, size, what types of prisoners detained there, and so on.)
  6. **Conditions in detention** (if detained) (Size of cell, number sharing cell, provision of food, water, bedding, healthcare, sanitation, access to daylight, exercise.)
  7. **Circumstances of release from detention** (if relevant).
  8. **Torture allegation reported?** To who? If medical attention was sought, is a medical report available?
  9. **Injuries /scars?** At the time? Now? With consent, take photos of any injuries/scars.
  10. **Any relevant documents?** (Such as charge sheet, release papers, medical report.)
  11. **Information on other prisoners/other violations?** (Others tortured? (For example, saw/heard other torture, cell mates shared experiences, and so on), identity of other prisoners (lawfully arrested/ detained)?)

Checklists are also particularly useful to ensure that all members of a team are gathering information on the same aspects of the case(s).

### 3.4 Identify sources of information

Multiple sources and types of information can provide evidence to establish a picture of what happened/is happening in one or more cases, and whether or not a violation has taken place. Gathering information from multiple sources can also provide an alternative perspective on what happened or disprove certain aspects of the alleged incidents.

There are three main types of evidence:

- testimonial evidence
- physical evidence
- documentary evidence

You should aim to collect information from as wide a variety of sources as possible. If multiple different sources corroborate your findings, this helps confirm the accuracy of the information. However, the type of information that might exist/be relevant will vary according to the nature of the violation being investigated, and not all types of evidence will be accessible in all investigations.

#### 3.4.1 *Testimonial evidence*

**Survivors/victims and witnesses:** The most important sources of testimonial evidence will be people who directly experienced, were involved in, or witnessed violations, or experienced, were involved in or witnessed incidents in the run-up to or aftermath of a violation, and therefore have **first-hand information** of one or more aspects of what occurred. This includes **survivors and victims** of the violation, **perpetrators/officials who played a role** (including issuing orders), and **witnesses** who saw or heard an incident, **medical staff** who were involved in treating injuries, **lawyers** who were involved in representing cases and others who were directly involved.

**Note:** First-hand information means the information is original to the source: they have not obtained it from anyone else.

It is important to establish how sources of testimonial evidence know certain details. Some people might report information they have received second hand, as if they witnessed it directly themselves.

**Other sources:** People who did not directly experience or witness the incident(s) may nevertheless have some information relevant to your investigation. Sources may have witnessed other details that are relevant to the case or the context in which it took place, such as events leading up to or after the incident in question. This sort of information might come from sources including family members or friends, or representatives of a group to which the survivor/victim belonged (political, religious, or other).

Other sources can include **technical and professional experts** who can provide important contextual information, or interpret or confirm details of cases, such as injuries or cause of death (medical staff, forensics experts), types of weapons used (ballistics/weapons expert), and so on.

Testimonial evidence is mostly collected through interviewing (see Chapter 7), and might also be gathered from written expert reports/assessments. In investigations of

certain types of violations, it might also be collected from affected communities through surveys, mapping exercises, focus group discussions or digital platforms (see *Chapter 8: Collecting documentary evidence*), though these methods are not appropriate for investigating all types of violations.

### Examples of people who might have first-hand evidence related to a violation

- Survivors, victims, witnesses of violations.
- Medical professionals, mortuary staff (could have treated victims, seen bodies, and so on).
- Family members, neighbours, work colleagues (could have witnessed violation or key incidents in the lead-up to the violation).
- Prison staff (could have witnessed (ill-)treatment in detention, could confirm the detention of a disappeared person, and so on).
- Other officials who played a role in the case.
- Members of police/security forces/armed opposition groups (perpetrators or witnessed perpetration of violations by colleagues).
- Lawyers representing individuals/communities, judicial officials (could have first-hand experience of aspects of trying to follow due process in arrest/detention proceedings, or court proceedings).
- Journalists (may have witnessed the violation while reporting, for example at a demonstration).

**Note:** Do not assume someone will be a first-hand witness. For example, family members might have very little information about what happened. Only individuals who personally experienced or witnessed an event or incident can be a source of primary information.

### Examples of other testimonial sources who may not have witnessed a violation directly but have information relevant to the case or context

- Family members of survivors/victims.
- Local human rights activists who may have investigated similar cases or have information on the context.
- Members or officials of security forces.
- Technical expert witnesses (forensics experts, weapons experts, environmental scientists, medical experts, and so on).
- Representatives (formal or informal) of any group the survivor/victim belonged to (for example, political, activist community, student group, religious, social, ethnic or other group).

- Lawyers who have case information, or who have experienced other similar cases, local / national officials.
- Journalists (for example who investigated the violation).
- Community, traditional or religious leaders, youth leaders, women leaders.
- Members of political parties, civil rights groups, trade unions, ethnic groups, and so on.
- UN, international and local NGOs, legal associations, such as those who work in the area or have reported on similar issues.
- Teachers.

**Note: Actor mapping:** List all the actors who might be relevant to a violation (survivors/victims, witnesses, family members, community leaders, perpetrators, police officer receiving the report, senior commanders giving orders, policy makers, and so on) to identify potential sources of information to interview. Also consider the relationship between the perpetrators and the victims to help understand the power dynamics that might underpin the violation.

### 3.4.2 Physical evidence

Physical evidence includes marks of violations left on humans, buildings or the physical landscape. For example, scars or injuries left on people, damage or destruction of buildings and land from conflict, bombing, environmental damage from wilful or neglectful practices, destruction of houses, property, hospitals, and health centres and food sources. Physical evidence could also include objects relating to a violation such as weapons or remnants of certain types of weapons/ballistics.

- *Physical evidence should be documented, photographed and/or filmed during field investigations if it is safe to do so (see Chapter 6 on documenting physical evidence).*

#### Examples of physical evidence of possible violations

- Physical (corporeal) evidence – scars, wounds, injuries
- Blood stains
- Damaged or demolished buildings
- Damaged infrastructure (hospitals, water sources, schools)
- Transport means left behind
- Weapons or ammunition/bullet casings, shrapnel, shell casings
- Mass graves (evidence of large areas of disturbed ground/aerial footage of same)
- Polluted water sources
- Burnt crops

### 3.4.3 Documentary evidence

Documentary evidence includes official and unofficial documents, audio-visual materials, statistics and other types of information that confirm or demonstrate an aspect or detail of an incident. These might include legal and medical documents; photographs and footage of incidents or the aftermath, including from content shared on social media and uploading platforms; official statements; written security force orders/correspondence; and scientific analysis/reports (for example of samples).

- *Documentary evidence is collected through multiple channels including from survivors, victims, witnesses and technical experts; from ministries and other government offices or courts; or through online research. It can also be commissioned, through freedom of information requests (see Chapter 8 on collecting documentary evidence).*

#### Examples of documentary evidence

- Police and court records: arrest warrants, charge sheets, court/trial documents, written evidence, rulings
- Official reports/statistics
- Hospital or morgue records, medical records, autopsy reports
- Official letters/papers (such as security force orders, correspondence or other official correspondence)
- Medical reports
- Mapping of affected areas/communities
- Photographs, aerial photographs, video footage, sound recordings – of incidents, aftermath, wounds/injuries, physical signs of violations on people, buildings and landscapes
- Correspondence/emails (written or received by victims/witnesses (for example threats, summons)
- Academic/scientific testing of (contamination/pollution) samples
- (Repressive) legislation

### 3.5 Identify how you will collect the information

When you have identified what information you need, and what the sources of that information might be, you can determine what methods you will use to collect the information. This will vary according to the type of violation you are investigating and what kind of information you are seeking to collect. Your approach might also be determined by the accessibility of information or the geographic location.



### *3.5.1 Key methods of information collection*

**Field visits:** Visiting the sites where (alleged) violations occurred to document or photograph physical evidence. As well as observing physical evidence, you might also conduct interviews (and possibly focus groups) during field visits. In some circumstances, interviewees might be in different locations to the physical evidence – for example, with displaced individuals or communities.

**Interviews:** With survivors, victims, witnesses and other sources who may have first-hand evidence/details of violations; with technical experts to inform understanding or to confirm details or aspects of accounts; and with other secondary sources who might have information relevant to your investigation. Interviews can take place anywhere (during field visits, in your office, or anywhere else), as long as it is safe for both the interviewee and the investigator.

**Collection of documentary evidence including online (open source) information:** As above, documentary evidence might be collected through many channels, including from witnesses and experts, through online research, and through generating evidence by commissioning the use of technologies like satellite imagery. (The relevance of these different types of evidence is explained in detail in Chapter 8.)

**Direct observation:** You might use direct (in-person) observation as part of your investigation of a specific violation, which involves you personally observing situations to monitor whether any violations occur. For example, if you are investigating a case involving politically motivated arrests (for example of journalists, opposition politicians) you might attend trial hearings to observe if due process rights are being respected. Alternatively, if you are investigating alleged violations in the context of an ongoing protest movement you might attend some of the protests to witness and/or photograph or record incidents, interview witnesses at the scene, and so on.

**Focus groups:** Semi-structured discussions on a specific problem or area of interest with a small group of people. These can be held with affected communities, survivors, victims and witnesses. This approach can be used to collect first-hand information from affected communities or contextual information / community perceptions that might be relevant to your investigation.

- Focus groups can be useful in certain situations and for investigating some violations, such as contexts in which a community as a group have been affected by an issue (such as environmental pollution of water sources).
- Focus groups can be a useful first step in building trust with a community, and understanding the context in which violations may have occurred, before conducting individual interviews.

- Focus groups can also be helpful with vulnerable groups – for example, when gathering information from children, talking in a small group may make them more comfortable. When collecting information on highly sensitive topics such as sexual violence, while some survivors will not wish to talk in front of a group, others may gain solidarity and confidence from being in a small group of fellow survivors.
- Focus groups must be approached with caution in human rights investigations: group dynamics will influence who talks more/less and may affect what some participants say. For instance, some may feel pressured to agree with other participants. Be aware that the individual organizing the group may select participants to give you a certain impression. Therefore, in general focus groups are not suited to investigating some violations, and must not be used to collect detailed individual accounts.

**Participatory/community-led approaches:** Community-led mapping and research directly involves community members in collecting information. This can enable communities to explain how they are affected by an issue, and eliminate investigators' perceptions/bias of what are the key issues. When facilitating community-led approaches, it is essential to be sensitive to dynamics within communities (power dynamics/marginalization of certain groups such as women, youth). Frequently, certain figures/groups will be dominant, and may seek to speak on behalf of the entire community while representing only a narrow constituency. You must ensure that participatory approaches are genuinely representative of all the relevant demographics of the community.

**The use of focus groups and community-led approaches highly depends on the situation and the type of violation you are investigating** (see cautions above).

### *3.5.2 Information collection plan*

Decide which information collection methods are relevant and feasible based on the type of violation you are investigating and the context in which the possible violations occurred and the descriptions of the methods explained above. Decide what is possible, realistic and safe – for you and for your sources. Keep in mind that sometimes it simply will not be possible to collect the information.

To develop your information collection plan, consider the following questions:

- Is there a possibility there may be physical evidence?
- If so, are field visits possible? Is it safe to travel to the relevant areas? Will you need to request permission to access certain regions/areas or specific locations? What equipment might you need to take with you?
- Where are the survivors/victims and witnesses located? Will you be able to access those locations?

- How will you identify and approach potential interviewees? How will you arrange interviews? Where will they take place? Will you need interpreters?
- What other contacts might have information and/or be able to connect you with survivors or witnesses?
- Do you need to obtain or commission satellite imagery?
- You could ask a trusted contact to collect certain evidence for you or to conduct certain interviews for you and transmit the information via secure channels. If it is safe for them to do so, local contacts might also be able to record footage or take photos.
- If individuals/communities are not willing to speak to you, identify intermediaries trusted by local people to either build trust for you to do the work, or to collect information / conduct interviews on your behalf and pass the information to you securely.
- If you cannot access a location because of hostility to human rights or your own or your organization's high profile, send in someone who is not known to be a human rights investigator.
- Can you identify and interview people who have left the area – such as refugees or internally displaced persons (IDPs), former detainees /prisoners, or see if people from the area can come to you instead?
- If local authorities are denying you access to a specific location, try going to another level of authority to request access.
- If relevant to the type of violation, look at the possibility of obtaining satellite imagery or use Google Earth to do some basic imagery research (see Chapter 8).

### 3.6 Avoiding bias in your investigation methodology

When creating your methodology (what information you will collect and how you will collect it), you need to take steps to avoid bias in your investigation – that is to prevent one perspective or a preconception from excessively influencing it. This may lead to a lack of balance in the information collected, which could prevent you from establishing exactly what happened, or establishing everything that happened – that is revealing associated violations or underlying dynamics in the context. Bias compromises the accuracy and objectivity of the information.

Bias can come from:

- The personal views, perceptions or assumptions of the investigator;
- A narrow selection and lack of variation in your sources of information;
- Your selection of interviewees;
- Individual sources might also be subject to personal biases – meaning they could have a preconceived idea that led them to interpret something in a certain way, or might have a political or personal agenda.

These will all influence the type of information you collect.

Obtaining as many types of evidence from as many different sources as possible, encompassing different perspectives and experiences, is essential to verifying your information and limiting bias in your investigation.

Questions to consider when developing your methodology:

- Is there variation in your types of information (mix of first-hand, documents, other evidence)?
- Is there variation in your sources of information/channels for identifying and contacting first-hand sources?
- Are all your first-hand sources from the same group or share the same key characteristic? For example, are they all from the same ethnic group, party to a conflict, village, opposition political party? Are they all men?
- Who may have a different account of what took place?
- Is it safe to seek the perspective of the alleged perpetrators? This can be done through a “right to reply” – presenting a summary of your initial findings to the authorities/alleged perpetrators to enable them to respond to the allegations. This should be pursued whenever it is safe to do so as part of ensuring the impartiality of the investigation, to gather alternative perspectives, and because the authorities might also provide useful information.

📌 **Note:** *Bias in selecting interviewees and bias in interviewing are addressed later in this handbook.*

### **3.7 Integrating a gender perspective into your methodology and investigation planning**

Human rights violations can affect women and girls, men and boys differently. Gender-based violence involves harm that is directed against a woman or girl because they are a woman or girl, or against a man or boy because of being a man or boy. This type of violence also includes violence directed at an individual due to the way they express their gender or because of their gender identity.

The majority of gender-based violence is directed against women and girls, based on the traditionally recognized binary genders (male and female). Some violations are gender specific (solely targeted at one gender); others disproportionately affect women and girls or men and boys.

Gender can also determine how women and girls or men and boys experience the same situations and violations: they may be vulnerable to different violations in the same context. For example, in a conflict setting where sexual violence by armed groups is disproportionately affecting women and girls (women and girls are the survivors/

victims in the majority of incidents), men and boys may be disproportionately affected by forced recruitment into armed factions.

Women and girls also have different health and security needs than men and boys. For instance, pregnant or lactating women need access to maternal health care, which may not be available to refugees or IDPs.

Integrating a gender perspective into your analysis of a situation helps to:

- Understand power relations and less visible patterns of discrimination;
- Reveal and document human rights violations that specifically or disproportionately affect women and girls or men and boys when other (more visible) human rights violations occur;
- Reveal how gender hinders women (as compared to men) from claiming their rights.

To effectively understand, investigate and document these differences, **it is essential to integrate a gender perspective when planning your investigation focus and methodology.**

Think about all the ways in which gender might affect peoples' experiences of the situation or violation you are investigating:

- Does the violation affect men and boys and women and girls differently?
- Are there aspects of the issue that only affect men and boys, or only affect women and girls, or that affect one group significantly more than the other? Does one group have specific needs in the situation (such as pregnant or lactating women)? Do power dynamics affect one group's ability to enjoy their rights in the situation or create, underpin or entrench additional violations?
- Are underlying gender power dynamics contributing to people's experiences of the issue or making them vulnerable to associated violations?
- What information will you look for? Do you have the right sources to ensure that you collect information on how the issue is affecting women and girls as well as men and boys? If not, do you need to identify additional sources?
- Does the investigator/one of the investigation team need to be a woman? (Female survivors of sexual violence may prefer to be interviewed by a woman.) Do you need a team member with expertise in interviewing children (who have experienced gender-based violence)?
- Might socio-cultural dynamics obstruct you from talking to women and girls? (In some contexts, pressures from the family or community, shame or fear can inhibit women and girls from talking. Women and girls might be willing to talk while male family or community members may try to prevent them from doing so for a range of reasons. Investigating in these contexts might require additional trust building in order to address barriers.)

- Do socio-cultural attitudes associated with gender roles affect how a violation is perceived (for example if it is considered a violation or not, if/how a violation is spoken of or not, and so on)?
- If women and girls are reluctant to discuss sensitive topics such as sexual violence, might they find it easier to discuss in a small group (focus group) of fellow survivors, instead of individual interviews?

### 3.8 Consulting technical experts and background research

Before you begin your investigation, consider if it would be useful to consult technical experts, and whether you need to do any further background research about the context in which the alleged violations occurred and in which your investigation will take place, for example via your contacts and through desk/online research. This could be particularly helpful if you are investigating in a context that you are less familiar with.

**Technical experts:** If it is relevant to the issues you are investigating, consult technical specialists in relevant areas (such as forensic experts, weapons experts, doctors, lawyers, environmental scientists) if possible.

- Experts might be able to advise you on what to look for in relation to specific violations – what information to collect, details that you should ask survivors, victims and witnesses about, or what to photograph during your field research.
- Whenever possible, arrange for the experts to review/analyse the relevant information you collect, including reviewing photos and confirming specific details of testimonies that have been securely anonymized, and confirming/interpreting details.

**Background research on contextual information:** You might gather contextual information from your previous work, contacts and published/online sources. You may want to look at secondary sources on the violation, such as media or NGO reports.

This can:

1. Provide important details about the underlying historical, political, social and economic dynamics of the context in which the alleged violation took place. Since such contextual factors can be extremely relevant to how or why a violation occurred, it is important to understand them. These underlying dynamics could also influence survivors' and victims' ability to access justice, health care, and so on after violations have occurred.
2. Provide relevant detail for planning and preparing your investigation, such as up-to-date knowledge of alleged violations, relevant actors, political dynamics, refugee or IDP locations, security concerns, information about the accessibility of certain locations, local languages or dialects for which you may need an

interpreter, or security issues that need to be included in your risk assessment and planning (see Chapter 4).

3. Make you aware of other sources to speak to or who might be able to assist you with establishing contact with communities, or other aspects of your investigation.

Consider:

- historical context (past violations, past conflicts)
- political context (political tensions/affiliations)
- social indicators (access to health care, access to education, educational levels, access to land, working conditions)
- economic indicators (unemployment rate, primary source of livelihoods)
- demographic indicators (ethnic make-up, refugees, IDPs)
- geographical context (climate, infrastructure, geographic accessibility)

### 3.9 Make logistical preparations

You might have to travel during your investigation for a range of activities, for example to identify and document physical evidence; identify and interview survivors, victims, witnesses; collect/record documents and photos from survivors, victims and witnesses, medical/morgue reports, police station/prison records/admissions data and other documentation; or to observe detention centres/prisons, trials, demonstrations. Before you go, you need to consider and arrange the following preparations.

#### Seeking permission/informing the authorities

Before going on a field visit, find out if you need to seek official permission to access a certain area or location. For example, institutions such as detention centres and prisons will require written permission from the relevant authorities, and to access most refugee camps you either have to seek permission or at least inform the authorities of your visit. In conflict-affected contexts, it can be necessary to obtain the permission of the party in effective control of the territory (see Chapter 4). It can also be an essential matter of security to do so. Security personnel at checkpoints may not be willing to grant access without official permission, even if written permission is not officially required.

Applying for permission usually has to be done in writing and can take time. Allow sufficient time for this in advance of any field visit.

If it is not essential to seek permission to get access, decide whether to inform the authorities of your field visit. There can be advantages and disadvantages of doing so. As this has security implications, it should preferably be an organizational decision. Adapt your risk assessment accordingly. **Never inform the authorities of the identity of anyone you will meet or interview.**

## Equipment

Do you need any equipment to record/document what you find?

- Camera/smartphone camera, video camera, voice recorder (with spare memory cards for security purposes);
- Encrypted USB stick, encrypted laptop, encrypted smartphone;
- Means of measuring size and distances (such as a measuring tape to measure physical features/damage, and so on);
- Additional phone (to reduce risk of surveillance/interception of some calls, to present to security if demanded, to have a spare if one is confiscated, and so on).

You might also need other equipment for practical or security reasons. This might include:

- Satellite phone (for remote locations);
- First aid kit, trauma kit (for immediate triage of severe injuries).

## Logistics

Arrange your transport, driver (if relevant), accommodation, insurance (if possible) and money. For high-risk areas, use security advice from trusted local contacts, UN security reports and other sources.

- *Transport:* Means of transport should be reliable and safe. Pay extra attention to the condition of your vehicle and prepare the supplies you need – extra fuel, first aid kit, radio, drinking water, and so on.
- *Accommodation:* Do not save money on hotels; choose those that are most secure. When travelling with several colleagues, stay together in one place. Staying on the ground floor increases your vulnerability to theft as well as other threats (for example abduction).
- *Money:* Find out if you will have access to ATMs where you are travelling, or if you need to take enough cash with you to cover the expenses of your trip. If so, consider how you can carry this most securely.
- *Interpreters:* If needed, identify an interpreter through trusted contacts or other organizations.

## Referrals

Survivors and victims of some violations might require medical care or psycho-social support, including counselling, legal assistance/legal aid, or other types of support and assistance.

- Find out before beginning your investigation what organizations and agencies (local and international) provide these types of services in the investigation



location. Confirm if it is possible to direct people to these services if relevant, and confirm the process for doing so.

- You might also decide at this stage whether your organization is able/mandated and has the budget to provide people with financial support in order to access these services (for example, travel to the clinic).

#### **Box 9. Pre-departure checklist**

- Have prepared an investigation methodology or information collection plan – identified the information you need to prove or disprove the violation happened, sources/types of information and collection methods you will use.
- Have integrated gender considerations into the investigation focus and methodology.
- Have completed a risk assessment and security plan (see Chapter 4).
- Have organized the necessary logistics (accommodation, transport, insurance, interpreters).
- Have prepared an investigation checklist.
- Have relevant contextual information (political, religious, ethnic, socio-economic conditions).
- Have identified if specific thematic expertise is needed/have consulted relevant technical experts.
- Have obtained necessary permissions/decided whether to inform the authorities of the visit.
- Have provided a detailed itinerary and agreed a communications protocol with colleagues.
- Have the necessary equipment.
- Have installed the necessary encryption software on smartphones, USB sticks, laptops (see Chapter 4).
- Have prepared responses if questioned about the team's presence and activities.
- Have assessed the risks of interviewing people, and found alternative methods if it puts people at too much risk to interview directly.
- Have up-to-date information on the security situation – if it is not safe, do not go!

# Chapter 4

## Security planning and preparation

Investigating human rights violations or abuses can involve multiple risks to both investigators and their contacts (survivors, victims, witnesses and other sources). Security planning and preparation is therefore essential to your safety, the security of your sources and contacts, and the protection of the information that you collect. Security planning should be a cyclical – rather than linear – process that is constantly reviewed and improved before and during the investigation.

People are hostile to human rights investigations for a range of reasons. For instance, they may be implicated in the violations/crimes themselves, or they could feel their own power or reputation (or those of their institutions) would be threatened by the exposure of violations/perpetrators. They may also oppose such investigations due to self-interest, or because of entrenched social attitudes to certain issues/groups/genders, and so on. Entities hostile to your work may want to obstruct the investigation, discredit or undermine you or your organization, or intimidate or harm you or those who share information with you.

Human rights investigators are also at risk of incidental harm as a result of working in high-risk or volatile locations such as conflict-affected areas, or locations with a poor transport, health or communications infrastructure.

Hostility to human rights investigations can manifest itself in many different forms, including prevention of access to locations to conduct investigations, direct threats, arbitrary arrest, harassment or physical assault. A general hostility to human rights work can be sustained through restrictive laws, smear campaigns and more.

**Security planning and preparation are essential to avoid or mitigate possible harm to you (the human rights investigators), your contacts and sources, and to the work.** The principle of “do no harm” requires that you must anticipate and plan against risks to yourself as well as your sources and contacts. Adequate preparation is particularly essential when working in high-risk contexts such as conflict situations, which can change rapidly and unexpectedly.

Security planning also entails understanding the context of your work (in relation to political, social, environmental and other factors), understanding where opposition, obstruction or danger may come from and in what form, assessing the risk of those harms, and identifying measures to reduce the likelihood of harm and to prevent or minimize the impact if it does occur.

Security planning must be undertaken before all investigations, whether operating in high- or low-risk environments. This involves:

- Mapping/understanding what the threats are;
- Assessing the risk levels of those threats (in a risk assessment);
- Preparing risk mitigation measures and a security response plan.

## 4.1 Understanding the threats

### Box 10. What is a threat?

**Threats** are any events/issues that could potentially cause harm to you, your sources and contacts, or to the work. Threats might be deliberate, for instance to force you to cease your investigation (by threatening or arresting you, or blocking your access to a certain location), or silencing survivors/victims/witnesses from reporting their experience and exposing violations (through violence, arrest, confiscation of property). Threats might also be incidental (meaning, not related to the work specifically) from working in locations with high levels of road traffic accidents, exposure to diseases or contaminated water, and so on.

Threats vary significantly depending on the context you are working in, the issues you are working on and the technology you are using. This section discusses common threats to the work of human rights investigators.

### Threats to human rights investigators

Human rights defenders/investigators face a range of threats directly related to the work they do, resulting from hostility to human rights work in general or to the particular issues under investigation.

Direct threats include: arbitrary arrest, arbitrary detention (without charge), torture, sexual assault, prosecution on trumped-up charges, extrajudicial killing, enforced disappearance, injury, death, defamation, labelling (attempts to discredit you and your information), denial of freedom of movement and speech, theft, and revocation of registration/licence/press credentials/shutting down organization.

Incidental threats resulting from working in locations with a poor transport or health infrastructure include: road traffic accidents, breakdown and stranding in remote areas, and contracting water-borne, insect-borne and other diseases.

Threats to the well-being of the investigator resulting from the work (for example from operating in high-risk environments or exposure to grave human rights violations) include: stress, burnout, depression and vicarious trauma. Left untreated, these conditions can further compromise your security as they can affect decision making, concentration levels and relationships. They can also result in behaviours that can compromise your security, such as heavy drinking or substance abuse, or getting easily frustrated – which can in turn lead to poor decisions or unhelpful approaches. For example, responding to harassment at a military checkpoint in a confrontational

manner may worsen the situation. These are addressed in detail in Chapter 11, but measures to mitigate negative mental health impacts must be included as part of all security planning.

### **Threats to contacts (survivors/victims, witnesses, other sources, and their families)**

People who provide information to investigations face threats to try to prevent them from doing so, or can suffer serious repercussions for providing such information – as a punishment, to act as a deterrent to others, and/or to suppress reporting.

These include: arbitrary arrest, (arbitrary) detention without charge, torture, sexual assault, prosecution on trumped-up charges, extrajudicial killing, enforced disappearance, injury, death, loss of employment, education opportunities or livelihood, confiscation of property. Individuals who cooperating with investigators may also suffer from social repercussions from hostile community members or based on attitudes to gender roles or to speaking out. They may also be stigmatized for admitting to certain violations, or experience psycho-social harm including re-traumatization as a result of being interviewed.

There may also be incidental harm: for example, if sources travel on unsafe roads/in unsafe transportation through hostile checkpoints to meet you for the interview.

### **Threats to information**

Investigators' information is often the target of security threats – to obstruct the work or discover the identity of sources and contacts to silence or punish them. Threats to information come from both physical and digital sources.

These threats include: physical search/examination of computers, phones, cameras or other electronic devices (on the spot or following confiscation) by security services or other actors; digital/electronic surveillance – monitoring of phone calls/emails/instant messaging systems, computer hacking and installation of malware (spyware) on your devices (see Chapter 5); physical surveillance; and office raids.

### **Threats to the work**

Hostile entities might find different ways to disrupt your work or prevent it from taking place.

Threats include: expulsion from the investigation location, denial or revocation of travel permission, revocation of licence to operate/organizational registration/press credentials, defamation/discrediting and loss of credibility.

## 4.2 Preparing a risk assessment and security plan

### Box 11. What is a risk?

**Risk** is what happens when a threat is realized. It is measured by the severity of the potential impact multiplied by the likelihood/probability:

$$\text{Risk} = \text{Impact} \times \text{Probability}$$

The risks related to the confiscation of your laptop at a checkpoint include exposure of the names and addresses of contacts or other sensitive information that could lead to people being harassed, arrested or worse, and other sources losing confidence in sharing information with you. The risks of a road traffic accident are that you or your contacts suffer severe injury or death, the vehicle is damaged, thus restricting your movement, you are stuck in an insecure location, and so on.

Security planning entails two stages:

1. **Conduct a risk assessment:** Identify the threats that pose potential harm to you, your contacts and your work, and evaluate the likelihood that they will occur and the severity of their impact.
2. **Prepare a security plan:** Put mitigation measures in place to reduce the potential damage of the most likely and most severe risks.

### Box 12. Examples of how security planning and preparation can reduce vulnerability to risk

- Soldiers at a checkpoint are aggressive and force you to open your equipment to search the contents. You had anticipated this threat in advance and had put in place the following preparations: your information is securely stored in a disguised (encrypted) file on your computer, you have no sensitive contact details in your phone, you have the requisite permission papers, and you have prepared your responses to difficult questions.
- You are under surveillance, but you have identified and put in place the following measures: you are using only secure communications channels (end-to-end encryption), you change your transport route every day, you meet your contacts at different locations each time, you communicate meeting/ interview arrangements through trusted intermediaries, your colleague knows your itinerary at all times and you check in with them twice a day.

- You are operating in a conflict situation that could flare up at any point. In advance, you have put in place the following arrangements: you have the necessary permissions, you have radio equipment and are on the security alert radio frequency, you have registered with the relevant security body in order to receive security alert notifications, and you have a well-maintained vehicle in which the driver keeps the engine running while you do your work.

**Such mitigation measures reduce the vulnerability of yourself, your contacts and the work by reducing the potential negative impact of these situations.**

#### *4.2.1 Preparing your risk assessment*

##### **Identify the threats**

- Consider and list all possible threats that could affect your own safety and security and that of your contacts and sources, as well as threats to the information and the work. Consider everything from threats arising from a hostile political context (arrest, assault), surveillance, social stigmatization of survivors, digital threats to communication, seizure/confiscation of information (devices, recordings), health risks, localized conflict, poor road conditions, theft, natural disaster, and so on.
- Think about each destination of field work and all of the activities to be conducted, and the possible threats involved. Remember to consider threats arising from logistical arrangements, for example at the hotel, on the road, at border crossings and those related to using interpreters.
- Remember that in addition to hostility from the security services or other state institutions, your work might also face threats from non-state actors including companies, organized crime entities, and individuals or communities who may object to the team's presence or to community members sharing information with the team.
- To identify and understand the threats, gather information on possible changes in the situation (threats) in the relevant location(s) from trusted contacts, background research, governmental advice, UN or NGO security advice (such as the United Nations Department for Safety and Security).
  - Example 1: You know that the security services are hostile to your work. You identify that this could result in attempts to access your information or reveal the identity of your sources through a range of channels: monitoring of phone calls and emails, installation of malware on your computer; physical surveillance; searching or bugging your hotel room; harassment; and confiscation of digital devices when you come into contact with security services during travel (at the airport, border crossing, checkpoints).

- Example 2: You are travelling to a conflict-affected area. You find out from local contacts that one of the warring parties has set up multiple checkpoints and sometimes closes roads entirely. Your contacts also tell you that the conflict flares quickly and is unpredictable. You identify threats of possible harassment/physical harm and compromising of your devices/information/luggage when you go through checkpoints; possible denial of access to certain locations; possible attack on the road. (In order to make the requisite preparations, you would need to find out from contacts: Do you need particular permissions, do you need to travel in a convoy, do you need particular supplies for the vehicle, driver and team? Do you need particular communications equipment?)

### Assess the risk

To determine the level of risk, assess the severity of the impact of the threat (if it occurred) against the likelihood of it taking place. For example, a threat that is unlikely to occur is low risk, even if its consequences would be serious.

- Go through the possible threats you have listed, assess the likelihood of each one happening and the seriousness of the consequences if it did happen.
- A risk analysis table helps to visualize the risk level of a certain activity or ongoing threat (Figure 3). It assesses the severity of the impact if the threat does occur (Impact – A) against the likelihood that it will occur (Likelihood – B).

**Figure 3. Example of a risk analysis table**

IMPACT (A)	Very high (5)	(5)	(10)	(15) Example: Being assaulted; confiscation of laptop	(20) Example: Getting arrested and detained (without access to lawyer)	(25)
	High (4)	(4) Example: Natural disaster	(8) Example: Break-in to hotel room	(12)	(16)	(20)
	Medium (3)	(3)	(6)	(9)	(12)	(15)
	Low (2)	(2)	(4)	(6) Example: Defamation in newspaper	(8)	(10)
	Very Low (1)	(1)	(2)	(3)	(4)	(5)
		Very Low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
LIKELIHOOD (B)						



Severity of threat/impact (A)	Likelihood of occurrence (B)
<ol style="list-style-type: none"> <li>1. <b>Very Low</b> (for example: small discomfort, minor injury, minor damage, self-help recovery)</li> <li>2. <b>Low</b> (for example: minor delay or inconvenience, temporary discomfort, small injury)</li> <li>3. <b>Medium</b> (for example: possible reputational damage, intimidation, delay or inconvenience, violence, injury)</li> <li>4. <b>High</b> (for example: severe injury, arrest, violence, loss of livelihood, employment (contacts))</li> <li>5. <b>Very High</b> (single or multiple)</li> </ol>	<ol style="list-style-type: none"> <li>1. <b>Very Low</b> (almost never)</li> <li>2. <b>Low</b> (occurs rarely)</li> <li>3. <b>Medium</b> (possibly could occur, but uncommon)</li> <li>4. <b>High</b> (recurrent but not frequent)</li> <li>5. <b>Very High</b> (occurs frequently)</li> </ol>

- When you have plotted identified risks into the table, note the “score” achieved for each risk through multiplying the impact and the likelihood. This can be assessed in a ratings bands table – see Figure 4. This can guide you in making decisions about activities and risks.

**Figure 4. Ratings bands for assessing the risk**

Ratings Bands (A x B)				
Very Low risk (1-5)	Low risk (6-8)	Medium risk (9-12)	High risk (15-20)	Very High risk (25)
Should not disrupt activities or field travel but take necessary precautions.	Should not disrupt activities or field travel but take necessary precautions.	Proceed with caution. Take all sensible mitigation measures and maintain regular contact routine.	Consider cancelling the field visit or certain activities planned. Implement robust mitigation measures and have strict contact routine.	Cancel field visit or specific activity planned. Look for alternative methods to carry out the work without putting anyone at excessive risk.

### 4.2.2 Preparing your security plan

#### Prepare mitigation measures

- When you have identified the significant risks in your work, identify measures for each that will reduce its likelihood and/or reduce the harm it would cause if it does occur. Table 1 lists mitigation measures that help reduce your vulnerability to the risk and increase your capacity to respond effectively.
- You are also responsible for identifying and implementing mitigation measures to reduce risks to your sources and contacts (see Chapter 7).

**Table 1. Examples of mitigation measures**

Topic	Examples of mitigation measures
Digital and communications security	<ul style="list-style-type: none"> <li>• Digital security preparations – for example installing encryption software, getting spare memory cards for cameras and uploading non-sensitive photos</li> <li>• Only using encrypted/secure communications channels and having secure communications routines</li> <li>• Surveillance evasion measures</li> <li>• Programming speed dial numbers into your phone or installing a panic button/instant alert system</li> </ul>
Physical security	<ul style="list-style-type: none"> <li>• Identifying safe journey routes</li> <li>• Providing your itinerary to a local contact</li> <li>• Putting in place an evacuation plan</li> <li>• Creating a code of conduct for all investigators/staff</li> <li>• Taking hostile environment training (for work in conflict and other high-risk contexts)</li> <li>• Taking self-defence training</li> <li>• Arranging travel in a convoy</li> <li>• Shared calendars and itineraries</li> <li>• Always travelling in teams of at least two people</li> </ul>

	<ul style="list-style-type: none"> <li>• Door stops for your hotel room door (stops anyone from being able to force their way in)</li> <li>• Continuous monitoring of the security situation</li> </ul>
<b>Medical emergency</b>	<ul style="list-style-type: none"> <li>• Health insurance and vaccinations</li> <li>• Accessing professional mental health assistance</li> <li>• Take first aid training, take a first aid kit/trauma kit when you travel</li> </ul>
<b>Support network</b>	<ul style="list-style-type: none"> <li>• A lawyer on standby to act for you in the event of arrest</li> <li>• Arranging a check-in/buddy system</li> <li>• Having a network of local contacts on standby to assist in the event of an incident</li> </ul>
<b>Other mitigating measures</b>	<ul style="list-style-type: none"> <li>• An emergency fund (for lawyers' fees, bail money, and so on)</li> <li>• Standard operating procedures/minimum requirements for vehicle travel</li> <li>• Preparation of responses in the event of interrogation: mental preparation can reduce the stress of an incident</li> </ul>

- **Information and communications security measures** for electronic and physical storage of information and secure communications are paramount to protect your contacts/sources and the work itself (see Chapter 5 for detailed guidance on information and digital security).
- If the mitigation measures are not sufficient to reduce the likelihood or consequences of activities that fall into the “very high risk” category of the risk analysis table, the activity should not be undertaken.

Table 2 provides an example risk assessment and security plan.

Table 2. Sample risk assessment and mitigation plan

Threat	Likelihood	Possible risks	Impact	Mitigation measures
Road traffic accident	High	Death, injury, stranding (including in insecure locations)	High	<p>We will only travel in vehicles that meet required safety standards; use drivers recommended by trusted contacts in the area.</p> <p>We will make sure the vehicle has the necessary equipment (spare tire, jack, wheel wrench, spare fuel, first aid kit) and supplies (drinking water, food, and so on).</p> <p>We will not travel after dark (unless there is an emergency).</p> <p>We have emergency messages/contact numbers prepared in our phones.</p> <p>We have identified nearby medical facilities for accessing medical assistance if needed; health insurance is in place.</p>
Surveillance	High	Exposure of sources, causing risk of repercussions against sources/ contacts, information compromised/ confiscated by security forces/ other hostile entities	High	<p>We will change our interview location each day, leave accommodation at different times each day, take indirect routes to interviews; only use trusted drivers and interpreters; encrypt all digital devices before travel; use secure communication channels wherever possible.</p> <p>We will not mention the names of sources or make meeting arrangements over phone or email, use code</p>

				<p>words if possible and make arrangements through secure channels and trusted intermediaries.</p> <p>We will type, encrypt and destroy all hard copy notes the day of interviews; consider using a lookout while conducting interviews (to watch for security forces / informants); consider asking a trusted local contact (with a lower profile) to do interviews and bring the information to us securely.</p> <p>We will not leave any hard copy information or any devices in unsecured locations (such as hotel rooms).</p>
--	--	--	--	--

### Prepare response plans

- Part of reducing the potential damage inflicted by an incident is identifying in advance the steps that will be taken if an incident occurs – meaning knowing in advance who you will call, what they will do when you call them, where the nearest hospital is, and so on, so that you can respond effectively and efficiently.
- For high-risk threats, identify an incident **response plan** which lays out the steps and arrangements that you or your colleagues will follow if the threat materializes, for example if you are arrested or conflict breaks out/flares during field travel.
- Think what steps would need to be taken in these situations and make the necessary preparations in advance. Two examples are provided below.

#### *Incident response plan: risk of arrest*

You were aware of a risk of arrest while carrying out your work. You put in place a range of mitigation measures including a twice-a-day check-in with a colleague, pre-identification of a lawyer who has agreed to represent you in case of arrest, and providing your colleague with your trip itinerary and contact details of your lawyer and local contacts.

If you miss check-in, your colleagues will:

- Try to contact you;
- If unsuccessful, immediately call a trusted local contact who will confirm if you are at your hotel;
- At the same time, your colleague will contact other local contacts who may have information about your whereabouts;
- If unable to locate you, your colleague will contact the lawyer, who will try to locate you at police stations;
- If necessary, your colleague and the lawyer will coordinate to prepare a habeas corpus petition.

#### ***Incident response plan: escalation of conflict***

You are working in a conflict-affected area where you knew there was a chance the conflict could flare at short notice. You put in place a range of mitigation measures which included ensuring access to regular security updates, adequate equipment and an evacuation plan with the necessary assistance agreements in place (for example from the UN). You also know where you have to be to evacuate, and how to make sure you are aware of the evacuation order; if relevant/needed, obtain all necessary permissions or consent.

Your evacuation plan covers the following details:

- The immediate steps to take after a decision to evacuate are...
- Evacuation will take place by... (air, road, and so on – details: for example if by road, via which route?)
- Evacuation will be facilitated by or in conjunction with... (UN, embassy, and others – if by road in convoy, who will coordinate convoy)
- The contact point for evacuation will be...
- Their contact details are...
- In the event we cannot reach them, we contact...
- If we need to take shelter while awaiting evacuation, this will be at... (location)

#### ***4.2.3 Before you travel/begin your field work***

- Review your risk assessment and security plans: are the risks to yourself or others too high to make the field investigations viable? If your presence on the scene carries too many dangers for yourself or others, identify alternative means of collecting information (for example, rely on a trusted local contact to bring possible witnesses outside the area), or delay the activity until it is safe to do so.
- If you decide to go ahead with your field work, implement all the mitigation measures you have identified in your security plan; prepare your secure information storage methods (ensure encryption software is installed on phones,

computers, USB sticks (see Chapter 5 for detailed guidance on digital security)); prepare your responses regarding the reasons for your visit/your activities in case of questioning by security forces, and so on; compile a list of emergency local contacts (including nearest doctor, hospital) to be carried at all times.

- Draw up a communications routine: designate a colleague/trusted contact who you will check in with according to an agreed plan – for example a phone call or text message at a designated time once/twice a day, or every two days (frequency will depend on the level of risk in the location to be visited). Agree a response plan that the designated contact will follow if you fail to check in.

Working environments in all contexts can change very quickly. Security assessments and plans need to be re-examined frequently.

#### *4.2.4 General safety and security practices for all investigations*

- Invest adequate time in carrying out a risk assessment and identifying mitigation measures to put in place for the investigators, sources and information.
- Have staff check-in systems (or a “buddy system” with a friend or family member if you are working independently) where your designated colleague or “buddy” knows your movements/itinerary at all times; check in with them according to a designated schedule; have a response plan in place if you fail to check in.
- Do not travel alone to insecure areas.
- Use panic button or security alert systems, pre-programme alert messages or speed dial numbers into your phone so you can immediately notify colleagues if you are in danger.
- Take self-defence training and hostile environment training (wherever possible).
- Maintain a strong network of contacts: potential aggressors know a larger and more vocal group will resist or respond to any incident involving you.
- Have standard operating procedures for staff operating in high-risk environments, for transport and movement routines, including minimum standards for vehicles/ vehicle maintenance.
- Establish an emergency fund that can cover expenses such as medical bills, bail and legal expenses in the event of arrest.
- Seek counselling or other mental health support if needed.

### **4.3 Security when working in areas of armed conflict**

#### *4.3.1 Understanding the threats*

The increased threats faced when working in conflict-affected areas include getting caught up in hostilities, the presence of mines or unexploded ordnance, a breakdown of law and order, and a general situation of instability and violence. Conflict situations involving several different armed groups can pose particular challenges to safety and

security as it can be more challenging to understand where a (potential) threat comes from. Human rights investigators can (potentially) become direct targets of one or more belligerent parties.

### **Access and impartiality**

Civil society groups operating in a conflict-affected area are particularly vulnerable to accusations of a lack of neutrality or impartiality. To gain access to conflict-affected areas, particularly frontline areas, for security reasons it can be necessary to seek the permission of, and possibly be escorted by, one party to the conflict. This can lead to perceptions of bias that can increase security threats from some parties. It can also make it very challenging to interview witnesses, as you will not have the necessary time or privacy to protect people's confidentiality. General levels of trust also tend to be lower in societies affected by conflict.

Travelling with or getting permission from a party to the conflict increases the likelihood that you will only be permitted to document certain things or have access to certain people, which creates bias in the information you collect.

If you travel with armed groups or seek their logistical support this can also lend them recognition. Being dependent in any way on a party to the conflict makes it difficult and dangerous to impartially investigate abuses committed by that group.

Remaining impartial during armed conflict can be challenging. For example, armed groups fighting a repressive government may be supported by local communities, including local human rights investigators. In some contexts, local communities are forced to support an armed group. A warring party can manipulate or tamper with information on violations for political purposes.

These issues can be a threat to your reputation, which may impact your ability to work.

### **Polarization**

Conflict environments are often highly politicized and polarized, which makes carrying out investigations more difficult and more dangerous. You may be accused of taking sides, or face pressure to do so. Negative labelling, intimidation and intentionally damaging human rights investigators' reputations are common in polarized societies. Parties to the conflict and their supporters may go to great lengths to shame you or your sources, or to manipulate or destroy evidence of abuses committed.

In these environments you need to exercise extra caution about possible bias, and the credibility and reliability of sources and the information they provide.

### **Media and information in conflict areas**

Press freedom is often restricted during armed conflict. It might be censored or



obstructed by the authorities or armed groups controlling territory, or manipulated for military or political purposes. Journalists may also self-censor for security reasons, or lack impartiality. Other information coming out of conflict-affected areas is also often censored, biased or manipulated. This makes planning for field work more difficult, as information from different sources might be conflicting.

### **Communication and lack of access to information**

Access to means of communication such as phone networks and the internet may be limited in conflict settings.

#### *4.3.2 Preparing risk assessments for conflict and post-conflict areas*

Your risk assessment before travelling to a conflict area is particularly essential.

- As with all risk assessments and security plans (discussed above), list all possible threats (to yourself, your contacts and your information).
- **Seek expert advice:** get up-to-date information from military experts, organisations specialised in NGO safety and security, and other informed sources. Find out:
  - What are the current dynamics of the conflict? What is the level of hostilities – has there been recent fighting/military activities in the area to which you are travelling? What is the latest security situation report in the area? Are there land mines in the area? Are there checkpoints? How many are there, and where are they? What are the lines of authority in the area?
  - Do you need to travel anonymously/conceal the purpose of your visit? What might local people's reactions/attitudes be towards human rights investigators? Would an investigator from a particular ethnic group or with a certain political profile be more safe/less safe?
- Identify and implement mitigation measures and develop response plans for serious incidents/situations. Have an exit/evacuation plan – make sure you know exactly what you will do if you need to get out of the area urgently, and put all the necessary arrangements in place. Know where the medical providers are in the area and establish any necessary arrangements to have access in case of need.
- If access to the scene and your presence there is too dangerous, identify alternative means of collecting the information. For example, a trusted local contact may be able to contact possible witnesses and request them to meet you outside the area, or conduct interviews for you and send transcripts through secure information channels.
- When considering the possibility of an escort (if it is optional – it may be imposed by the de facto authorities), think through the consequences – will it jeopardize your impartiality, and will people still trust you?

Before working in a conflict-affected area:

- Monitor the security situation daily to ensure you get immediate information if it changes. Try to establish a network of reliable local contacts.
- Ensure you have sought permission, if necessary, from those controlling the territory you are accessing.
- Make thorough logistical preparations: register with the UN or any NGO security information/alert providers; ensure you have appropriate communication methods (for example a 2-way radio) and are aware of the relevant channels for security information and updates; ensure your mode of transport is reliable, in good condition and well equipped with a reliable driver (if relevant); take first aid/trauma kits.
- Operating in a conflict situation can entail increased risk to information. Digital security measures must be prepared and installed on devices in advance.
- If possible, take hostile environment training.
- Ensure colleagues know your whereabouts at all times and have a strict check-in system.
- Such contexts are subject to change at very short notice. You must always be ready to change your activities, plans or evacuate immediately.

## **4.4 Security considerations for high-risk groups**

### *4.4.1 Security of women human rights investigators*

It may be easier for women to move around and connect with people, as they are more easily trusted, facilitating access to information. However, women human rights investigators generally face significantly higher risks of sexual aggression, as well as certain types of violence, discrimination and prejudice. In many contexts, women human rights investigators are more vulnerable to being threatened directly or through their families than their male colleagues. Some people may consider their work socially or culturally unacceptable or believe that it defies gender-specific roles, based on sexist or misogynistic ideas. This can lead to a lack of support, resistance, or hostility from their relatives or communities. Gender-related violence may occur within their organizations.

These factors also increase the risks to women human rights investigators from other threats because it reduces their resources and capacity to protect themselves against risks and respond to incidents, and may be an additional source of stress.

- Specific gender-related threats must be considered and included in risk assessments and mitigation measures, and response plans identified and put in place.
- Mitigation measures could include: security trainings tailored to women human rights investigators, self-defence training, a strong network of women human

rights investigators and supportive contacts, heightened security routines – such as regular check-ins for women human rights investigators, panic button or alarm technology, avoiding work/movement alone, particularly in remote locations, and (depending on the context and personal preferences) teaming investigators, ideally in male-female pairs.

#### *4.4.2 Security of LGBTI human rights investigators*

Lesbian, gay, bisexual, transgender and intersex (LGBTI) human rights investigators face heightened levels of aggression, stigmatization and discrimination. They are particularly at risk of sexual violence by both state and non-state actors. In many contexts, discrimination and the lack of social or cultural acceptance of LGBTI people can isolate LGBTI investigators and further increase the risk that they will be targeted. Moreover, LGBTI people face increasing persecution through “anti-homosexuality laws” that have (re-)emerged in recent years in some contexts. Same-sex relations are criminalized in many countries and are even punishable by death in some. A lack of support from relatives or their communities can further isolate LGBTI people and activists. Many are also denied support and solidarity from human rights organizations that avoid LGBTI issues.

- Specific threats related to or based on sexual orientation and gender identity must be considered and included in risk assessments, and mitigation measures and response plans must be identified and put in place. Heightened security measures are essential for LGBTI investigators.
  - Mitigation measures could include: increased security routines, self-defence training, regular check-ins, avoidance of traveling or working alone particularly in remote areas, a network of contacts, activists and lawyers who can provide legal representation or solidarity, protective accompaniment or action in case of an incident, an emergency fund to cover legal and other costs, and strict confidentiality protocols regarding the identity of investigators.
- 📌 *For further detail on all issues covered in this chapter, see Annexes 1 and 2 for reference materials, resources, and tools relating to the safety and security of human rights investigators, including digital security.*

# Chapter 5

Digital security, information  
and communications security

Secure storage and transfer of information and secure communications practices (digital and non-digital) are essential to protecting the security of your sources, information and yourself.

As discussed above, entities hostile to your work might try to access your information, intercept your communications, or monitor your online activities to disrupt or suppress your work, harass you and/or discover the identity of your sources in order to threaten them into silence or to punish them for disclosing information, deter further cooperation and to act as a deterrent to others. If hostile entities are aware of your itinerary (from accessing your information or intercepting calls and emails in which arrangements are discussed) this will increase the risk of harm to sources and yourself.

### 5.1 Understanding threats

Before all investigation activities, it is essential to be aware of the threats. Threats to your information can come via monitoring/interception of telephone and electronic communications (email, internet-based communication channels, and so on), hacking your computer by installing “malware” (software intentionally designed to cause damage) and accessing/manipulating files, physical examination of your phone, computer, other electronic devices (for example at police stations, checkpoints, airports, border crossings, where security personnel may search your devices), bugging of hotel rooms or other locations, searching of offices, homes and hotel rooms for contact lists, notes, documents and other evidence.

New applications for digital technology are being developed all the time that can help protect and support human rights investigators in their work. New tools and software for electronic surveillance, interception and disruption are also constantly developing and are used by hostile governments and security forces and others.

- *Annex 2 contains reference materials and guides on digital security. For installation guides and information on more applications that can help increase your digital security, visit Surveillance Self-Defense ([ssd.eef.org](https://ssd.eef.org)) or Digital FirstAid ([digitalfirstaid.org](https://digitalfirstaid.org)).*

The security practices explained below should be applied systematically to any communications or information storage you use in the course of your investigation. Install any necessary software on devices before you begin collecting information and before traveling to locations where your devices/information might be at risk.

### 5.2 Computer/account security

**Create strong passwords or passphrases on all your devices and for all your accounts**

A strong password should be long and complex, contain capital and lowercase

letters, symbols and numbers; never use names/birth dates that can easily guessed/deciphered; use different passwords for each account/application; change passwords regularly. Increasingly, passwords are being crafted as passphrases. This is highly recommended as they are more complex and easier to remember. Ideally passwords/passphrases should be changed every six months although the introduction of two-step verification process (see below) for most online accounts – if turned on – eliminates the need to change passwords.

- Think of something that is easy for you to remember – for example the first line of your favourite song, quote or story and introduce characters like uppercase letters, numbers and symbols. Alternatively, use password management software, such as **KeePass** (for your computer), **MiniKeePass** (for your smartphone), **LastPass** and **Bitwarden**, which stores all your account/app passwords for you so you do not have to remember them. Such software has a web version that guarantees access to accounts even when your device crashes.
- If you log into accounts on a public computer (such as in an internet café), change the passwords of the accounts immediately afterwards: the computers may contain software that records passwords.
- Use two-factor (two-step) authentication for your accounts to make it much more difficult for someone to get unauthorized access. This requires that you have a password and a second proof of identity when you sign in to an account (such as an SMS sent to your phone with a log-in code). While the two-step authentication process is currently recommended as the safest way to secure your account, always remember that savvy hackers could develop ways around it.

**Protect your computer from viruses, Trojan horses and malicious software (malware),** such as spyware, which infiltrates your device to steal your data and sensitive information.

Attachments and links can infect unprotected computers with viruses (which can damage, steal or destroy information) and malware (or spyware) software (which can gather information from a computer over the internet and send it to third parties). Viruses can also get onto your computer from an infected device (such as a USB stick or portable hard drive). Spyware can also be installed remotely by someone in the vicinity of your computer (for example if working in the same Wi-Fi environment).

#### **To avoid malware:**

- Update your computer operating system and all applications regularly. If you have a reliable internet connection, switch on automatic software updates.
- Install anti-virus tools (and anti-malware), though if you are using Windows 8 or above, Windows Defender already contains anti-virus software.

- Only download applications from trusted websites. If using a phone, only download from the Google Play Store (for Android devices) or iOS App Store (for iPhones).
- Do not open email attachments or links from unknown senders, including those sent through WhatsApp and SMS.
- Use a secure (private) internet connection whenever possible.
- For all non-secure internet connections, such as over open Wi-Fi (which does not need a password or is managed by unknown or untrusted third parties), ensure you use a virtual private network (VPN) application and enable it.

### 5.3 Information security

#### Encryption – protecting sensitive files on devices

Encryption locks or hides files from unauthorized access, even if someone has access to your devices (laptop, USB stick, external hard drive, phone, and others) physically or electronically (through spyware). Encryption is **essential to protect sensitive files from hostile surveillance and interference**. It makes files inaccessible to people who do not have the password or encryption key. Encrypted files can be disguised to avoid detection – for example, an encrypted file containing a Word document can be made to look like a picture (JPEG) file to someone searching your computer or other device.

- There are a number of free encryption tools. Most computers and phones have full disc encryption tools like **BitLocker** (for Windows) and **File Vault** (for Mac computers). **VeraCrypt** can be used to encrypt specific files and folders.
- Note that in some countries, encryption is illegal.
- Install encryption software on your devices before you travel to locations where your devices/information may be at risk.

#### Photos – encryption/secure storage

- Install software on your devices (laptop/phone) that can securely store/hide photos and footage.
- Several apps hide photos, folders and applications with password protection. **CameraV** allows secure (encrypted) sharing and storing of photographs and videos. **Vaulty App** allows users to store images and videos from a phone's photo gallery in a secure password-protected vault. **KeepSafe Photo Vault App** has a decoy gallery that can be opened using a fake password to hide other photographs and files (it does not encrypt the files).
- Automatically uploading photos to a cloud server such as Google Photos allows you to recover them easily if you lose your device. However, be aware that such servers do not provide full privacy and security as the data might in exceptional cases be accessed by third parties – for example hackers, governments and the technology companies themselves.

- Take a spare memory card, uploaded with non-sensitive images, which you can leave in the camera while moving around; hide the memory card with sensitive images.

### **Destroy sensitive information – wiping**

Be aware! When you have encrypted files (hidden them in your computer/phone) or when you have deleted files from your device and emptied the recycle bin, traces of the documents might remain. Recovery software can recover information that has been deleted but not wiped.

- Run a cleaning software on your devices to remove all traces of deleted documents/files.
- Use a tool like Eraser to over-write or “wipe” information – this permanently destroys files and any traces of the information.

## **5.4 Communications security**

### **Emailing / internet-based communications**

Most email, instant messaging and voice communication systems (such as Gmail, Yahoo, Facebook Messenger, WhatsApp) are not entirely secure. Any communication through the internet (including internet searches) carries information such as metadata (where the email, message or internet search originated, where it is going, the IP address of the user, date, time), and content information (what was searched for or sent). Governments and hackers may either be able to access the former (when end-to-end encryption is enabled) or the latter (in other cases).

Therefore, sending data through the internet always poses a risk to the security of the information. **Be extremely cautious when communicating sensitive information over the internet.** Complete privacy can never be guaranteed.

However, a number of tools can help you communicate more securely over the internet:

- Use encrypted email when possible, for example **Protonmail** or **Tutanota** (these work only when both sending and receiving ends have an account with that service). **RiseUp** is another secure email, designed for activists.
- Try to send as little sensitive information over email as possible. When possible, arrange with your colleagues and contacts about how sensitive information will be communicated. Decide on code names to refer to sources, sensitive information, and so on.
- Whenever possible, use a safe (private) connection when communicating, logging onto websites and downloading information. Do not access or send sensitive



information when using a public Wi-Fi connection/public computer, unless you are using VPN (see below).

- Do not send emails to large groups of receivers in the “to” or “cc” recipient lines. Even if the email’s content is not sensitive, displaying all email addresses is poor security practice and a breach of your contacts’ privacy. This also applies to messaging apps like WhatsApp: exercise caution when sending sensitive information over such platforms, and avoid sending to (large) app groups. (See more below, under phone security.)
- Erase your browsing history or use a browser like Firefox Focus (for smartphones), which automatically erases the browsing history once you close the browser.

### **Social media**

Exercise caution when posting information online. Privacy settings can help prevent certain information from becoming public, but do not stop unauthorized access to your personal details and data. When you post online, the network/platform owns the content: you lose your property rights to it.

Only share information related to your work on social media if strictly necessary, if you have given due consideration to the security implications and if you have the informed consent of any relevant/affected persons.

- Think about the information you are sharing online: is it necessary to share online? Will it put you or your contacts at risk? Who can access this information?
- Sensitive information (including personal information such as birth dates, phone numbers, addresses, family members, sexual orientation, education) should be kept private.
- Change your settings to “friends only” (Facebook) or “protect your tweets” (Twitter) to control who can see what you have posted online. Also think about what information your contacts can share about you with others.
- Disable automatic location sharing on updates, photos and videos which may reveal information about your whereabouts.
- Connect only to people you trust and verify their identities.

### **When using unsafe internet connections**

- Use a VPN service if you have to use an unsafe (public) Wi-Fi network. This can encrypt your information so that the network owner cannot see your activity/websites visited.
- VPNs are very useful for investigators working in countries with internet censorship: they enable you to access blocked websites and apps.
- There are many free VPN services (such as uProxy and Psiphon). Some work better in different countries. If using free VPN, be aware that some can collect your data.

### Phone security (mobile phones and smartphones)

All regular phone calls and SMS messages are unsafe. Mobile network providers have complete access to all text and voice messages sent and received via their network (giving governments easy access to private calls and text messages). All phones can also be easily be tapped (by governments or others trying to get unauthorized access to information) – through the SIM card, through the phone itself or by remotely installing tapping software. Some tapping software can record information when the phone is switched off. A mobile phone is only really “off” when the battery is taken out, as it regularly sends out a signal to the nearest antenna, even when it is switched off. This makes it possible to track the location of the phone/user. All information stored on the memory of the phone itself can be accessed even when the SIM card or memory card is removed.

- If you think your phone is likely to be tapped or traced, buy one with a removable battery. Where there is a high risk of tapping, replace both your phone and SIM card regularly.
- Use an internet-based messaging service with end-to-end encryption. This means only the sender and receiver can read the messages. At the time of writing, Signal is the safest messaging service.
- Use encryption software to encrypt voice and video calls and protect against interception. At the time of writing, Jitsi Meet is the safest. Make sure you are using a secure Wi-Fi connection when using these services.
- Do not share sensitive information over phone calls or SMS.
- Delete messages to and from sensitive contacts after you have sent or received them; tell your contacts to do the same with messages from you. Signal has a “disappearing messages” function that you can set to automatically delete messages after sending or reading them.
- Ensure strong passwords on your phone and for the applications installed on it.
- Information on your phone should be backed up regularly and stored in an encrypted file on a computer.
- Research which services/software work best, and are not illegal/banned, in each country you work in, as this can vary.

**Box 13. Essential reminders – before you travel****Information security**

- Encrypt! Use encryption software on your laptop, phone, USB sticks and external hard drive. This enables you to hide files from anyone who wishes to search the contents of your computer and other devices, and to use secure channels to communicate with sources, arrange interviews, and so on.
- Install malware protection on your phone, computer, tablet and other devices to protect against the installation of spying software (which can be installed remotely, for example by someone sitting in the same café while you are using your computer).
- When moving around with sensitive information/during field investigations, even if the files are encrypted, it is safer to take them off your computer altogether: save notes/documents/other information onto an encrypted USB stick that is easier to hide in your clothing or luggage.
- Remove (and hide) the memory/SD cards in cameras and voice recorders and replace with the spare (with non-sensitive content).
- Do not leave any sensitive information (notepads, documents) or communications devices in insecure locations (such as hotel rooms). Carry them with you at all times. Ensure devices are encrypted.
- Scan notes and documents and save in secure/encrypted locations. Destroy handwritten notes.
- Make sure your computer and smartphone are password or passcode protected.
- To minimize the risk of losing important information, use the **3-2-1 principle**: keep at least **three** copies of important files in at least **two** different places, with at least **one** copy in a different geographical location. Make sure files are secured with passwords, encryption or physical locks in all locations.

**Communications security**

- Only use communication channels with end-to-end encryption to communicate with contacts/sources/colleagues, arrange interviews and communicate anything about your investigation.
- Be aware at all times of the possibility of surveillance of communications, whether through email, telephones or spyware on your computer. Avoid discussing sensitive issues and names of sources over email or phone; use code words or phrases instead, particularly when arranging interview dates, times and locations. Agree with colleagues in advance on code words and phrases, or passwords for exchanging encrypted messages.

- Store contacts' / interviewees' contact details in an encrypted file: do not store sensitive contacts in your phone's contact list. Memorize two or three of your most important contact numbers (colleagues, key contacts) in case you need to call in an emergency.
- Remember that the person you are communicating with (and their phone/ email, and other) might be under surveillance. If there is a risk the person you are phoning/emailing is under surveillance, do not say who you work for, and do not write from your organizational email address (if you have one). Use a VPN (or Tor, see [torproject.org](https://torproject.org)) to disguise the IP address of your device (where it is connecting to the internet) and therefore disguise where you are sending your email/message from.
- Delete Signal, SMS, and other messages to and from interviewees and other sensitive contacts as soon as you have sent or received them so that there is no visible trace of these communications on your phone. Tell interviewees and contacts to do the same – delete all messages to and from you on their phones as soon as they have read or sent them. Transfer important messages or photos to encrypted files, for example on your computer.

# Chapter 6

Identifying and documenting  
physical evidence

Documenting physical evidence involves identifying and recording where potential violations have left physical traces on people, buildings, infrastructure or the landscape. It might also entail observing whether certain services and facilities are being provided in fulfilment of people's rights – for example, whether a refugee camp has adequate access to sanitation facilities, or a prison meets international standards on detention conditions. In some investigations, there may be no (known) physical evidence or you may not be able to access it.

Collecting physical evidence as part of your investigation could take you, for example, to:

- sites of bombings, conflict
- mass graves
- sites of forced evictions, house demolitions, destruction/confiscation of property
- refugee/IDP camps
- sites of pollution of local food or water sources
- morgues

When investigating at the scene of possible violations, make use of local knowledge. Get help from any local contacts: they are very likely to know people in the area and surrounding communities. Local people often have a lot of information, for example about where certain incidents occurred, the location of possible evidence/objects, military movements in the area, and so on. This can help you safely find relevant information.

🔍 **Note:** *Never make assumptions when collecting physical evidence: the presence of apparent evidence that violations have taken place does not prove who perpetrated those violations. Remember also that some evidence can be planted for political and other reasons.*

🔍 **Tip:** *Where you cannot access locations, either because you are denied access or because it is too dangerous to do so, you may be able to obtain images of some locations from others living there or through the use of satellite imagery (see Chapter 8.2 for more detail on using satellite images in your investigation).*

## 6.1 Identifying physical evidence: what to look for

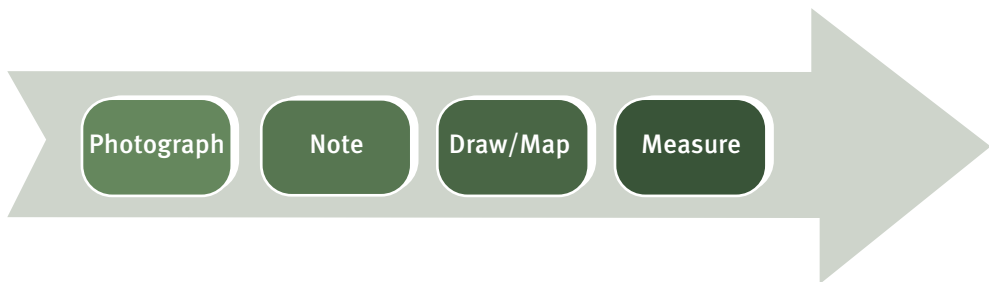
This will depend on the violation you are investigating, but physical evidence might include:

1. **Physical marks left on bodies** left by torture, ill-treatment, sexual violence and other violence that you might document (record notes/photograph) as part of the evidence, with the informed consent of the individual. This type of physical evidence is usually documented during interviews rather than at the scene of a violation.
2. **Bodies/human remains** might be physical evidence where someone has been killed or died as a result of a violation. Human bodies must be documented (recorded/photographed) with great sensitivity to the dignity of the victim and consideration for their family members – if their identity is known. Where the family is known, victims' bodies should never be documented or recorded without their permission.
3. **Graves (including mass graves):** if a grave or suspected grave is concealed, you can never be certain of its contents. However, an area of disturbed ground in a location where people have been disappeared, or killings are known to have taken place, could lead to the identification of a suspected mass grave. Likewise, unusual trends in the creation of graves – for example, a rapid increase in the number of graves in a graveyard near a military installation where detentions are taking place might indicate extrajudicial executions. Some graves might be exposed – revealing information about their contents. Satellite imagery can also be very helpful in identifying grave locations (see Chapter 8.2 for more detail on using satellite images).
4. **Physical marks left on buildings or the landscape** might provide evidence and details about violations. Examples might include: bomb damage, bullet holes, munition craters; mass grave sites; destruction of (permanent/non-permanent) housing; burnt villages, buildings, crops, land or property; polluted water and soil, including from oil spills.
5. **Physical remnants/material items** providing evidence or details about violations might include: weapons, bullet casings, ammunition, casings or fragments of munitions and unexploded ordnance, abandoned or damaged vehicles, items of clothing/uniform, documents.
6. **Details of buildings or locations where violations are alleged to have taken place,** such as a building that has reportedly been used to unofficially detain people. If you have access to buildings/locations of interest, note the details – about the location, surroundings, size of rooms, and so on. When observing official detention centres/prisons, refer to the specific international legal standards relating to conditions of detention.

7. **Provision, access and distance to services**, including in refugee/IDP settings. For example, you may investigate the provision of and access to education, sanitation and health facilities, and the logistical, financial and security considerations associated with accessing them. Pay particular attention to the safety and security of women and girls (especially within and near refugee and IDP camps, for example safety/risk when accessing water, sanitation facilities, venturing outside for commodities, and so on).
8. **Contextual information**: even where there is no physical evidence, contextual characteristics might be very relevant to understanding the details of an incident, including how it occurred and confirming or verifying the accounts of survivors, victims or witnesses. For example, documenting the details of buildings, locations or landscapes, and other, including descriptions, distances/proximity to other relevant points.

## 6.2 Documenting physical evidence

Documenting physical evidence involves the following four steps:



### Photograph

- Where possible, and if it is safe to do so, take photos of the physical evidence – such as damage to buildings, property, livelihood, objects such as bullet and munitions casings, documents, personal possessions, and so on.
- Only take photos if it will not put you or others at risk. Authorities/security forces are often hostile to taking photos. Check the environment thoroughly before taking photos, and then do so discretely.
- Wherever necessary, seek the permission or informed consent of all people involved, including the family members of victims and the owners of property, vehicles or other things you want to document. Do not take any photos or footage that put victims at more risk – for example by revealing the identity of people involved.
- Take three sets of photos:
  - a. Wide angle: Take photos that show the whole location, a building, piece of



evidence, grave or other feature in relation to the surroundings. Include in the frame any nearby landmarks or features of the landscape (buildings, trees, and so on): this will help prove the location of the evidence and its relation to other features of the landscape that might be relevant to the passage of events. If relevant, also include in the frame other pieces of evidence at the location to illustrate the position of pieces of evidence in relation to each other.

- b. Medium range: Frame photos to show the whole item, building, room or other piece of evidence (vehicle, ammunition, item of a uniform).
  - c. Close-up: Of any small pieces of evidence, for example ammunition casings or small details such as writing, numbers, markings. Put a reference number in the shot so that you know what close-up photos relate to.
- If you have a scale marker/measuring tape, put it in the shot to show the size/scale of what you are photographing. Take two images of the picture – one with the scale marker and one without (“clean”). If you do not have a measuring tape, use an identifiable object (for example, a pen, car) to indicate size. Demonstrating the size is important as part of the evidence and might be useful for later identification by an expert – for example, for unidentified munitions and so on.
  - As soon as possible, save the photos/footage to an encrypted location (in your phone, laptop, USB stick) and delete it from the photo gallery on your phone. If possible, send it through an end-to-end encrypted email platform or app to a colleague (WhatsApp is the most common, but as with all such apps, it is important to bear in mind that the quality of photos can be significantly compromised), or upload it to a secure cloud location (through, for example, OneDrive or Google Drive). Alternatively, if you have a spare memory (SD) card, transfer it into your phone and hide the other securely.
  - Ensure the date and time on your camera are accurately set and show the time when you began recording. Make a separate note of the date, time and specific location when you take each photo or piece of footage so you can identify them later.

### Note

Make detailed notes about what you see. Depending on what you are documenting, this may include:

- Where you are / where the physical evidence is located.
- A description of the site, its features, approximate distances between features.
- Detailed description of the (possible) evidence found (in the eight categories laid out in Section 6.1).
- The location of the evidence in relation to surrounding features of the area/landscape.

- The scale/extent of the damage (measure if relevant/possible – see below). For example, if a village has been burnt, count the remains/sites of houses, to document how many were affected.

### **Draw**

Draw a (rough) sketch or map of the site. This is an essential record of where evidence was found in relation to other evidence/features of the location for you to refer to after you leave the site. It also may be part of the evidence in itself – analysis of the location of evidence might also provide clues to what happened.

- Mark on your map all the details you can see.
- Mark on the map any measurements (see below) of features and distances between evidence/points of interest.
- Mark on a map the location of the pieces of evidence. Include any reference numbers you allocated to the evidence when photographing (as above).
- Mark north on the map (most mobile phones have a compass feature).

### **Measure**

- Measure any relevant features, distances including the scale of the damage (for example a possible mass grave, bomb damage) or objects of interest (munitions shells, equipment, and so on).
- If you do not have a measuring tape in your kit, count and make a note of the number of your steps/paces – you can measure your step later to give you an approximate size of the area.

### **Collect: environmental cases only**

- Where relevant, collect samples of environmental pollution. Only do this if you have the necessary arrangements in place to have the sample properly tested (for example by a local university department) *and* you have been advised by an expert on how to collect a viable sample.
- If possible, get the scientist/expert to collect the samples themselves.
- Do not take any other forms of physical evidence away from any scene.

#### **Box 14. Do(s) and don't(s) when documenting at the scene**

- NEVER touch munitions, explosive devices or any other remnants of war.
- NEVER touch human remains or attempt to remove them or exhume a grave unless you are professionally qualified to do so.
- Securely save information collected on a regular basis throughout your field visit. If you have a secure channel to do so, communicate it to another

trusted source before you move to another location in case your devices are taken from you.

- Be ready and flexible to change plans at short notice. When a situation is tense or unpredictable, remain aware of your surroundings at all times and be conscious of the overall mood; do not hesitate to leave a scene if you feel that something is wrong.
- Regularly reassess the level of surveillance you are experiencing (that you are aware of). If it is too intrusive, meaning there is a high likelihood that the identity of your interviewees will become known to the authorities, or there appears to be a physical danger to you, do not continue with the investigation.
- Field investigations will often generate large amounts of additional information as well as more leads that investigators would like to further explore. Decisions may have to be made on the spot depending on priorities, the situation, safety and security considerations, as well as your budget.

### 6.3 Investigating in conflict settings

#### Accuracy / impartiality

When investigating in a conflict situation, it is often necessary to get the permission of, and sometimes be accompanied by, the party to the conflict that controls the territory you are entering. Thus there is a heightened risk of bias in your information/interview sample. There is also an increased likelihood of misinformation from sources promoting one cause or another.

While active and former combatants may try to manipulate information or provide false information, they may also be genuinely willing to share (potentially sensitive or even incriminating) information, because of trauma, loss of faith, combat fatigue or other reasons. In many conflict situations, the line between “perpetrator” and “victim” can be blurred, and perpetrators of violations/abuses may have suffered violations/abuses themselves.

#### Physical safety at the scene

- Do not go to an area where there is a risk of active conflict, including shelling, mortar attacks or bombing, unexploded ordnance, mines or boobytraps, unless you have received security training in recognizing and responding to risks.
- If visiting a post-conflict site, do not go until the relevant military or civilian personnel have confirmed it is safe to access the area. Be aware of the possibility of explosive remnants of war, mines and booby traps (see explanations below).

- Local populations are often well informed about the nature and location of threats, and can therefore provide you with valuable information to help avoid them.

*Explosive remnants of war:* These include unexploded ordnance (explosive devices that failed to detonate on impact) and abandoned explosive ordnance (unused devices that have been left behind). Artillery shells, grenades, mortars, rockets, air-dropped bombs and cluster munitions fall into this category.

Look out for and avoid unexploded and abandoned ordnance at all costs. NEVER touch explosive devices, chemical waste or other munitions.

*Mine fields:* Mines can be either above or below ground. Where the presence of a minefield is known, there will be warning signs – either official signs (skull and cross bones, “Danger”) or signs placed by the local community. These often include crossed sticks, knotted grass, objects hanging from tree branches or on sticks pushed into the ground (such as empty plastic bottles, rags), or broken branches blocking a path. Never intentionally enter a minefield. If you become aware that you are in a minefield, if you have security support from a local (NGO/UN) contact, do not move: phone/radio them for assistance. If not, try to retrace your *exact steps* the way you came in, slowly and carefully, one person at a time.

*Booby traps:* Armed groups often leave booby traps behind in the locations where they have been forced to retreat. Any item can (and will) be boobytrapped, for example doors, chairs, refrigerators, toys and graves. If possible, avoid any area recently evacuated by retreating forces until it has been declared safe by the army, the UN or another appropriate entity.

### Identifying and documenting physical evidence in conflict settings

Physical evidence might include:

- damage to buildings and the landscape including the impact of bombs, other explosive devices and bullets;
- damage to/destruction of hospitals, schools and other civilian infrastructure;
- damage to/destruction of civilian houses, villages, crops (if so, how many, extent of damage, method of destruction (bombing, fire), and so on);
- injuries/burns sustained by the local population;
- dead bodies (if so, characteristics – uniforms, approximate age, gender, race, ethnic groups);
- blood spatter;
- physical evidence of the types of weapons/munitions used (weapons, bullet casings, ammunition, fragments of munitions and unexploded ordnance left behind);
- evidence of prohibited weapons (such as certain types of bombs and use of

chemical weapons) – casings of prohibited devices, burn patterns on buildings and on people, other injuries/impact on people.

**Note:** Many national armed forces have (a small number of) specific, allocated weapons. Thus evidence of those weapons may help determine the level of involvement of members of the armed forces in some incidents/settings (for example, types of ammunition used in the standard-issue assault rifle of the armed forces).

### Interviewing in conflict contexts

In conflict areas, members of the military and armed groups can provide valuable information. While each conflict situation is different, you may find individual soldiers/combatants (and people in non-combatant roles in national forces and armed groups) who are willing to talk or share information while still on active duty. Some may even come forward themselves to share information. Members of national forces will likely have to speak off the record. Others may be imprisoned or injured and in a hospital. This can make it easier to find soldiers/combatants to talk to, if they are willing to talk.

Interviewing (active and former) soldiers and combatants is difficult and not without risk, but it can help create a more complete picture of the conflict situation, command responsibility and group structure, details of attacks, and motivations behind certain attacks and violations (see Chapter 7).

# Chapter 7

## Interviewing

Identifying and interviewing first-hand sources of information who have directly experienced or witnessed possible violations (survivors, victims, witnesses and – if possible – perpetrators) is one of the most important and effective approaches human rights investigators can use to collect information. Obtaining detailed accounts of events is central to establishing a clear picture of exactly what happened.

Conducting an informative human rights interview that does not further harm the interviewee requires careful preparation and good analytical and communication skills. This involves knowing what information you need, how to ask questions that elicit the necessary details, how to follow up on key points mentioned during the interview to ensure an accurate and detailed version of events, and how to engage with someone who may have experienced or witnessed a traumatic event. Interviewing can be emotionally difficult for the interviewer as well as the interviewee.

## 7.1 Interview preparations

Good preparation is essential to conducting an effective interview that collects all the relevant information without further harming the interviewee. If you are unprepared, you are likely to overlook key questions and therefore miss important information about an incident that would help determine if a violation has occurred, and may put yourself or your contacts at risk.

Preparation for your interviews involves:

- identifying your interviewees
- safety and security planning
- planning the logistics – deciding the interview setting, the means of documenting/recording the interview, arranging interpreters (if needed)
- preparation for referrals

### 7.1.1 *Identifying interviewees*

You can use a number of channels to contact interviewees and/or to identify additional interviewees:

- Use your network to help you identify and/or establish contact with potential interviewees you have identified during the planning stage.
- Contact local human rights organizations, journalists or academics who have reported on the issue, or local figures who have spoken in the media about it, and ask if they can introduce you to interviewees.
- Use a “snowballing” approach: ask interviewees if they know other witnesses/people affected by the issue and if they can introduce you (where a violation has affected a group, rather than an individual).

Survivors, victims and witnesses might be unwilling to talk due to fear, lack of awareness of the point of human rights work or other reasons. Family members, local authorities, and others may harass or otherwise dissuade people who want to talk to human rights investigators due to socio-cultural attitudes to speaking out or to gender roles, because they themselves are implicated in the violations or for other reasons.

- Take time to build trust and explain your work to individuals or communities.
- Being introduced by someone individuals or communities already know (for example religious, community or prominent women leaders) can help establish the trust necessary for people to share sensitive information with you.
- If people want to speak but face opposition from family/community, try to arrange separate interviews (in person, on the phone or over the internet), enabling them to speak out if they wish to do so without putting them at risk.
- Ensure that you have an appropriate gender representation among interviewees. When investigating issues/in contexts that affect both women and girls and men and boys or people with a different gender identity, or issues that affect different genders in different ways (for example armed conflict situations, during displacement), you must interview representatives of all groups affected.
- Be sensitive to the fact that if an individual has already been interviewed by others they may be reluctant to be interviewed again (talking about difficult experiences can be tiring or upsetting, or they might not understand why it is necessary to repeat the same details). If someone has had to repeat the same account several times, this can affect the quality of the information in several ways. For example, an interviewee might skip parts of the story, or think they know what you want to hear based on what they have been asked before. You should explain why it is necessary to conduct another interview on the topic. For instance, say things like “I’m sorry I have to ask you the same questions”, but never force someone to talk if they do not want to.

### **Interviewing state officials**

It is important to interview state officials wherever possible. Doing so can help you maintain impartiality and avoid bias in your findings. Officials might also provide a different perspective on what happened. The reaction of government officials will be part of your investigation – to determine the official response to the incident. Officials’ knowledge of and attitude towards the alleged violation might indicate the government’s attitude/response to the violation and to upholding those rights more widely. Officials sometimes, intentionally or unintentionally, provide important information.



## Avoiding bias in the selection of interviewees

Be careful to avoid bias when selecting your interviewees. Use a number of different channels/contacts to identify interviewees. Otherwise, you can end up with a selection of interviewees who all have the same perspective, come from the same group or location, share the same political opinion, or are subject to other conscious or sub-conscious biases. This can significantly compromise the accuracy of your information and lead to an inaccurate picture of what took place.

Other biases can also influence the selection of interviewees, including:

- **Stereotyping:** making assumptions about a person or a group of people based on gender, race, ethnic group, religion or another factor.
- **Common characteristics:** interviewers may unconsciously select interviewees based on shared characteristics (between the interviewer and interviewees).
- **Gender:** female interviewees are frequently excluded – either by the interviewer in identifying interviewees, or by the individuals and communities putting forward interviewees.

### 7.1.2 Safety and security

The safety and security of an interviewee can never be fully guaranteed. However, risks can be minimized through proper planning and preparation, as covered in Chapter 3. Security considerations should influence the choice of location of the interview, communications practices when arranging the interview, selection of an interpreter, your and the interviewee's mode of travel to the interview, the methods of recording the interview and how information gathered in the interview will be stored.

Remember: A testimony, no matter how important, must never put the respondent – or their relatives – at risk.

- Revisit your security assessment and mitigation plans for interviewees. Are they sufficient? Do they need updating based on new information or changed circumstances?
- Make sure your information storage methods are sufficiently secure.
- It is usually preferable to physically meet people to conduct interviews, but if this may put you or your interviewees at risk, consider conducting your interviews using an encrypted channel such as Signal, or ask a trusted intermediary to conduct them for you and securely send you the transcript and any additional documentation.
- When arranging the interview, either directly or through a trusted contact, and/or at the beginning of the interview, consult the interviewee on any risk they believe they are currently facing and whether reporting their testimony might increase or

exacerbate that risk. Consult the interviewee on any security measures they think can be taken in order to conduct the interview with a maximum level of protection.

- You will need to remain aware of your surroundings before and throughout the interview. Be alert to any changes in the context or anything suspicious that occurs.
- Security planning needs to take into account the mental and emotional well-being of the interviewee, for example the risk of re-traumatization, particularly if they have experienced trauma or belong to a vulnerable group such as children (see Section 7.6 on interviewing specific groups, and on avoiding the re-traumatization of interviewees).

### **Interview setting**

Interviews should be conducted in a private, safe and comfortable place. The interviewee may wish to suggest a location they feel comfortable with.

- Agree on the location and time with the interviewee. Think about the accessibility of the venue, and ensure the location and time of day chosen does not affect the interviewee's security during arrival or departure. For instance, does the interviewee have to travel far to get there/pass through checkpoints/will they have to travel back at night and so on.
- Use secure communications channels to arrange the time and location of interviews, or organize in person (including through trusted contacts) if possible.
- If it is necessary to meet in a public place (for example, because your office/the interviewee's home is under surveillance, or if you are interviewing in a refugee camp or prison), try to find as discreet a location as possible. Make sure the interviewee is comfortable with the setting. Sit apart from other people and watch out for anyone trying to listen to the conversation, photograph or record you and the interviewee together.
- Where there is a risk of surveillance, do not arrive at or leave the location at the same time as the interviewee. Do not take a direct route to the interview location.
- If you have to interview the same person several times, use a different location each time.

#### *7.1.3 Means of documenting or recording the interview*

- When deciding how you will record the interview, think about the security context. Will there be an immediate threat to the interview record afterwards – for example, will you have to pass through a checkpoint where your information/devices might be vulnerable to being checked/confiscated? Which means of recording can you most safely store afterwards?
- Protect interviewees' identities in your notes/labelling of files. Allocate a number

to interview notes and digital files, and keep a separate record in a secure location of which interviewee each number corresponds to.

### Audio (or video) recordings

- If you want to make an audio recording of the interview, you must get the informed consent of the interviewee at the beginning of the interview (see Box 15). Explain fully how the recording will be used, and any security implications.
- Avoid video recording, unless there is a specific reason to do so (for example, you might use the video in public advocacy), in which case you must have informed consent specifically for this, based on a full understanding of the purpose and risks to the interviewee (and a full assessment of the risks yourself).
- Audio and video recordings enable the interviewer to replay the interview and write it out in detail afterwards, but present increased security risks. Recording interviews can also affect responses as it can make people more conscious of their answers, particularly when talking about sensitive topics such as sexual violence.
- If you are using a voice recorder, you will still need to make brief notes during the interview of points you need to return to.
- Encrypt your recording device **before the interview**. When the interview is finished, immediately save the recording in an encrypted location before leaving the interview setting. If you have a voice recorder with a removable memory/SD card, immediately save the recording to the SD card, delete it from your device, and hide the card somewhere safe. Make sure your device has music or podcasts on it to make it appear it is for personal use (see Chapter 5 on digital security).

### Handwritten notes

- When writing notes, write the precise words the interviewee uses, including writing your notes in the first person “I”. For example “I had just left the student committee meeting when the police van pulled up next to me. One of the policemen jumped out and threw me to the ground.” This makes your notes an accurate record to refer back to, and enables you to use direct quotes in a report.
- If you are taking handwritten notes in a context where there might be surveillance or you might come into contact with the security services (for example at checkpoints), type up your notes as soon as possible – preferably the same day as the interview – and then destroy them.
- If you do not have time to type up the notes before exposure to the risk of surveillance or confiscation (for example if you may encounter a risk while leaving/travelling away from the interview), photograph them and save the photo files in an encrypted location on your computer or USB stick, or send the photos through secure (encrypted) channels to a trusted colleague to store securely. Destroy the notes properly: do not just put them in a bin from which they can be easily

removed. For example, burn them or rip them into many pieces.

- If possible, store notes (and any other documents/photos, and so on) on an encrypted USB stick, which you can hide more easily than a computer (for example in your clothing, luggage, vehicle).

### Interpreters

- If you are not fluent in the language in which the interviewee talks most freely, use interpreters recommended by trusted contacts, wherever possible.
- When interviewing on sensitive topics related to sexual or gender-based violence, use an interpreter of the same sex as the interviewee (and the interviewer).
- Ensure you have a common understanding of key concepts and terminology before you start the interview.
- Give interpreters clear instructions that they should only provide a literal translation of what the interviewee says without adding anything. Interpreters can be biased in their interpretation of what the interviewee said, that is, give their own version/understanding of it intentionally or unintentionally, for different reasons. The objectivity and accuracy of the translations are essential to the reliability of the interview. Interpreters may also add (unsolicited) contextual detail when they think it is relevant and helpful.
- Give interpreters clear instructions on confidentiality and security considerations. They can jeopardize interviewees' confidentiality and security if they share information about them with anyone else.
- Remember interpreters might also experience security threats as a result of being involved in the work. Make sure the same security protections are in place for them as for investigators and interviewees: protect their identity, use secure channels to communicate with them, and avoid arriving and leaving interview locations at the same time.

#### *7.1.4 Support and referrals for interviewees*

It may be necessary to reimburse interviewees' travel costs to attend the interview. If so, confirm a realistic amount: paying five or ten times the actual cost of transport amounts to paying for interviews, which creates an incentive for people to provide false or irrelevant information.

---

**Remember: Never pay for an interview.** This carries a high risk of distorted or even false information.

---

Interviewees may come with needs and/or expectations of assistance. At the start of the interview, be transparent about the assistance you and your organization can and cannot provide. Be clear that any referral or assistance is not dependent on the person giving testimony.

Where required and feasible, you might refer survivors and victims in need of medical treatment, counselling or legal aid to agencies that can provide assistance and support services. This might include hospitals, legal aid centres, survivor/victims/child/trauma support groups, NGOs, counselling services and safe houses.

- Before the interview, check what services are available in the area that you could recommend/refer interviewees to.
- You may want to contact the agency in advance to confirm it is possible for you to direct people to them.
- Decide if you would be able to assist with the costs of the interviewee travelling to access services or make a report (for example to a police station) if this falls within your organizational mandate and your budget. If so, make sure you have the right amount of money with you at the interview(s). Your organization may require you to get a receipt for this signed by the interviewee.
- Consider the possible security implications of referring survivors and victims.

## 7.2 Before you start the interview

### Interview set-up (who is present?)

- Interviews should generally be conducted on a one-to-one basis (plus an interpreter if necessary), unless the interviewee requests the presence of another person (friend, relative, NGO representative). Some interviewers like to work in pairs, where one leads on asking the questions and the other takes notes. Think about the dynamics before you decide on this, especially if using an interpreter: talking to three strangers can be intimidating.
- If you are interviewing children, in most cases it will be appropriate to have a family member or guardian present. See Section 7.6.2 for more detail on interviewing people under 18.
- Do not allow anyone else to observe the interview. Even if these are friends and family members, the presence of others can inhibit an interviewee from talking or influence what they say.
- Women and adolescent girls should be interviewed by women, where possible. The necessity of this will depend on local cultural norms and practices. Women interviewers are particularly necessary (though not always) when interviewing female survivors of sexual and gender-based violence and issues that affect women and girls disproportionately, including harmful traditional practices.

### Opening the interview

- Properly introduce yourself and your organization including its mandate.
- Introduce the interpreter and explain their role.

- Before the interview begins, respondents must give their informed consent to be interviewed and for their information to be used (see Box 15).
- If the interviewee gives their consent to proceed, explain the structure of the interview and the information/details you would like to ask about. Inform the interviewee that you may need to ask some questions that might be difficult.
- Agree on one or two grounding techniques that the interviewee can use to help them relax if they get upset. Such techniques might include having a break for a cup of tea, listening to music, calling a sibling/friend (see Section 7.6 on interviewing people with trauma for more detail on grounding techniques).
- Inform the interviewee approximately how long the interview will last.
- **Inform the interviewee that they can stop and withdraw their consent at any time during the interview.**

#### Box 15. Informed consent

You must obtain informed consent from every interviewee before you interview them. Informed consent means they agree to participating, based on a full understanding of what the process involves and what the implications are.

If you want to record the interview you must obtain specific consent for that. Similarly, if you want to take photos, or might publicly use photos or documents the interviewee gives you, you must obtain specific consent for each of these processes.

To obtain informed consent:

- Provide the interviewee with full details of the purpose of the interview and how the information might be used. Offer realistic assessments of what the possible outcomes might be.
- Explain the possible risks and benefits of providing testimony.
- Explain the protections and possible limitations of confidentiality (see below).
- Explain that your interpreter follows the same confidentiality guidelines (and make sure that they do).

On the part of the interviewee:

- Informed consent should be based on a full understanding of the information you have given about the interview, use of the information, the potential risks, and the voluntariness of providing information.
- The interviewee must be sufficiently competent to comprehend the implications of their participation and consent to an interview. Assessing an

interviewee's competence to provide informed consent can be particularly difficult when working with children, people with mental health or learning challenges, or traumatized survivors, victims or witnesses. Such assessments must be made on a case-by case-basis and should always be in the best interest of the interviewee.

- Before interviewing children (under 18 years old), the informed consent of a parent or caregiver should be obtained.

Be alert to whether participation is indeed voluntary. Witnesses or survivors/ victims may have been pressured by others into giving a statement, even if they deny that this is the case. If an individual is receiving aid or assistance (such as during a humanitarian response), they may feel obliged to provide information in return for this aid – especially if interviewees were referred to you by an NGO that is providing them with assistance. People sometimes find it difficult to distinguish between one organization and another, and may give consent believing they are talking to the organization they already know.

**Confidentiality** is a core principle of human rights investigations. Interviewers must protect the information and personal details they collect from interviewees for reasons of security and privacy. There are, however, some limits to confidentiality as information from testimonies is often used in reports or for advocacy purposes.

- Explain to the interviewee that the information they provide will be treated confidentially. This means that their name and identifying details will not be shared with anyone outside of your organization, but it may be discussed with team members. No detail will be shared with other colleagues/people who are not part of the team. Explain that security measures are in place to ensure that the information is stored securely. If requested by the interviewee, describe these measures.
- Explain, however, that the information from their testimony might be used in a report or other publication. Make it clear that if the details of their case are highlighted in a report or other form of action, personal identifying details will be withheld, and a pseudonym will be used. Stick to using a pseudonym even if the interviewee wants to use their real name. High-profile cases (where the identity of the interviewee is already widely known) could be an exception.
- Informed consent implies that the interviewee understands and agrees to certain information being used (anonymously) in reports or other actions. Agree on what information can be used and how (in reports, with third parties, and so on) and any restrictions on the use of this information.

- If relevant, ask interviewees whether their information can be shared with third parties, such as the police, UN or other investigative teams. Ensure they fully understand the purpose and potential implications of sharing information with third parties.
- Note that some survivors/victims who want to pursue justice may be prepared to waive confidentiality.

**Remember:** Protecting the confidentiality of your sources requires having robust security protections in place for your physical and digital information storage, and undertaking secure planning for the interview – protecting information about the date, time and location.

Confidentiality also applies to documentary evidence. Any use or publication of evidence (including photos and audio-visual footage) in your reporting work must be based on careful consideration of the security of the source, and must conceal any identifying details (this is covered in further detail in Section 8.1).

### 7.3. Conducting the interview: process

#### Attitude and body language

- Maintain an open, empathetic attitude throughout the interview. This is essential to establishing trust with the interviewee.
- Pay attention to your tone of voice, the pacing of your speech and your body language to avoid appearing judgemental, pitying, disbelieving or impatient. Ensure your facial expressions do not show shock, horror or disgust about what is being shared.
- Sit at the same eye level as the interviewee, and maintain direct eye contact as much as possible. If you are sitting at a table, try to not sit directly opposite the interviewee, as this can be intimidating.
- Keep the tone of voice conversational.
- Use active listening. This means fully concentrating on what is being said rather than just passively “hearing” the content. Active listening also involves observing as well as hearing, for example to the interviewee’s body language and emotional state. Active listening is a way of supporting the interviewee: when people are talking to you about difficult things, it is important that you are seen to be listening. This shows that you are interested and are understanding what the interviewee is saying; it will make them more at ease and encourage them to continue. This can be communicated through verbal and non-verbal language: say things like “yes” and “ok”, slightly nod your head, and most importantly, maintain frequent eye



contact while the interviewee is speaking (including when taking notes).

- Show empathy. Use phrases such as “I know this is difficult to talk about”, “I’m sorry that I have to ask you the following question, but I need to ask the detail about...” Repeating the interviewee’s own words to summarize what they have said or when asking follow-up questions can help to build trust.
- Observe the interviewee’s body language to gauge whether they are becoming upset (see Section 7.3.2 on what to do if someone becomes upset, and Section 7.6.3 on interviewing people with trauma).

### Interviewing with an interpreter

- Look and speak directly to the interviewee (not to the interpreter) and make sure the interpreter also looks at and speaks directly to the interviewee (the tone and body language of the interpreter is as important as that of the interviewer).
- Use “you” to address the interviewee directly – “What did you see?”, rather than “What did he/she see?” to direct the question to the interpreter and make sure he or she does the same when translating the response: “I saw...” Not “he/she saw...” This is essential for the accuracy of the interpretation and the interview as a whole, and ensures you maintain direct communication with the interviewee, not with the interpreter.
- Ensure that the interpreter is aware of his/her tone of voice, pacing and body language.

### Using an interview guide

If you are using an investigation checklist or interview guide, as suggested in Chapter 3, make sure that this is kept to an **extremely short list of bullet points** – based on the who did what to whom, when, where, how and why questions. You can have this as a checklist on the table, but avoid longer guides in the interview. Using an interview guide can help to ensure that you do not forget to ask about important details. This can be particularly useful if you have limited experience with interviewing. Having the right questions in your mind comes with practice.

Annex 5 contains an example of a comprehensive guide to the content of the whole interview. This longer version will help you prepare the interview and make your list of bullet points in advance. For inexperienced interviewers, it is helpful to read the guide in Annex 5 before you conduct each interview.

However, this full interview guide **should not be used in the interview**. This can make you less open to other details and information that might emerge during the interview, affect your communication and body language with the interviewee (discussed below), give you too much control over the interviewee’s narrative and interrupt the flow of conversation.

Even a short interview checklist can have these effects. **Remember: an interview guide is a reference point, not a questionnaire.** If you do use one, you must:

- Be flexible in the way you conduct the interview to allow the interviewee to tell their story in the order that is most relevant or comfortable to them.
- Be flexible and let the interviewee talk about additional things if they want to; follow up on items of interest that emerge during the interview. **You have to be alert and think quickly while conducting interviews to react to whatever information emerges.**
- Keep the tone conversational: you cannot do this if you are simply reading questions from a questionnaire.

### *7.3.1 Avoiding interview biases*

Even the most experienced interviewer will face certain biases, which are preconceptions that can influence the questions you ask as well as your interpretation of the interviewee's answers. It is difficult to completely avoid biases, but you must be aware of them and can take steps to minimize them.

Common biases in interviewing include:

- **Stereotyping:** This refers to generalized assumptions about a person or a group of people based on their gender, race, ethnic group, religion or other factor. It can cause you to treat different groups in different ways: you might make judgements about the relevance of information/observations shared by a person from a certain group.
- **Gender bias:** Interviewees may be treated differently based on their gender. For instance, you may ask them different questions and make assumptions about what they will know, and about the reliability and relevance of their information based on their gender (or how they choose to express it).
- **Emotional involvement:** Becoming emotionally involved or overly affected by the content of the interview can influence your ability to make informed assessments and credibly collect data.
- **Trauma:** If interviewees are traumatized, this can lead to difficulties recollecting events or cause them to speak incoherently. Biases can occur if you think the interviewee's testimony is less reliable as a result, if you oversimplify questions or do not ask the interviewee the same questions as others because of their trauma.
- **Inconsistency in questioning:** When you ask different people different questions due to their personal characteristics (overlaps with stereotyping and gender bias).
- **Contrast:** This bias can occur when you compare interviewees with each other – for example, this can lead to believing that interviewees who are eloquent are more credible than those who are shy or softly spoken.

Addressing or minimizing biases is essential to the accuracy of your information gathering and analysis.

- Approach all interviewees in the same way.
- Never make assumptions about an interviewee or their testimony. Remember that an individual's characteristics or history have no bearing on the relevance or credibility of their information.
- Ask all interviewees the same basic questions about the same aspect of the investigation/violation (based on the who did what to whom, when, where, how and why questions).
- Remember: an interviewee who has difficulties in remembering, or who lacks coherence in their narrative, is not necessarily lying.
- Use grounding techniques to reduce the impact of stress on the interviewee.

### 7.3.2 Interview challenges

**Dates and times:** Pay attention to dates and times and the sequence of events. This can be challenging in areas where people are less familiar with referring to calendar days, or where a different calendar is used. If an interviewee does not know the date when something happened it can help to reference specific days (in a person's weekly schedule) such as market days, or events such as national/religious holidays, local elections. Some examples: "Did the attack on the village happen before or after Eid?" "Roughly how many days before/after?"

**Interviewees may become upset or angry** when talking about distressing experiences. Often, a human rights interview is the first time that survivors/victims have talked about what happened to them. Talking about experiencing or witnessing violations can be therapeutic and helpful for survivors, victims and witnesses in the medium to long term. Yet in the short term, verbalizing what happened can be very emotional. Some interviewees may show signs of trauma or post-traumatic stress disorder.

- If an interviewee becomes upset, pause and give them time.
- Be prepared to just sit and wait if the interviewee is crying.
- After a pause appropriate to their level of distress, ask if they would like to take a break, use a **grounding technique** to help them feel better or stop the interview.

🕒 *See Section 7.6.3 for more detail on signs of trauma, interviewing people who are traumatized, grounding techniques and avoiding re-traumatization.*

Be aware that:

- Survivors, victims and witnesses may appear unreliable. They may hold back some aspects of their experiences to avoid painful memories, embarrassment or shame. They may be unable to remember parts of their experience, or might

confuse locations or the timing of events. Trauma, time and other factors can affect memories of events. Interviewees might also add more details as they come to mind later in the interview and/or when they feel more trusting towards you (the interviewer). Remember that this does not mean they are unreliable or dishonest.

- Survivors, victims and witnesses may exaggerate. This could be unintentional, for example due to trauma. Some may feel under pressure (from themselves or others) to ensure that their story makes an impression and is believed. This does not mean that the story is untrue, but it may mean that some elements of the testimony need to be checked and clarified.
- Some interviewees may not give you all the relevant information. A range of reasons, including shame, embarrassment, or fear for their safety and security could cause interviewees to adjust or withhold crucial information.
- There may be a political agenda. Opponents/supporters of the government or an armed group may have a vested interest in maximizing/minimizing the number and severity of allegations of human rights violations or abuses. It is also possible that false witnesses come forward, for example in a bid to protect or accuse someone.
- Where the individual's story seems unclear or inconsistent with what you already know about the pattern of that violation, it is important to find out why in order to clarify – not doubt – their story. Do not probe too hard, as this could be interpreted as not believing them.

#### **Things to remember when interviewing:**

- Make sure you have allowed enough time for the interview: interviewees may have long and complicated stories to tell. A thorough human rights interview is likely to take a minimum of 1–1.5 hours, and possibly longer.
- Be patient: interviewing can be frustrating for both interviewers and interviewees. When an interview is taking so long that the interviewee is uncomfortable (when there are numerous aspects to cover), try to make a follow-up arrangement.
- Be empathic, supportive and non-judgemental.
- Be sensitive to differences in (local) language, communication practices and social dynamics that could influence how questions are understood or answered. Make sure you, the interpreter and the interviewee have the same understanding of key words or concepts. You can do this by asking “do you mean...?” or by summarizing what the interviewee has said in order to confirm you have understood it correctly.
- Interviewees may not be able to answer some questions. This does not mean that their account is unreliable. Trauma, time elapsed and other factors influence a person's memory. They may also have simply not observed certain details at the time of the incident(s).
- Interviewees may also be unwilling to answer some questions. You can try once to

explain why it is important to have that detail, but you must not force someone to talk about something they do not want (or are unable) to talk about. This does not mean their account is unreliable.

- Limit the number of times you repeat questions, even if you are unclear, as this may come across as questioning people's memory or integrity.
- Do not rush. A thorough interview on a complicated topic could take up to several hours.
- Never tell an interviewee what another respondent has said. Apart from breaching confidentiality, this can put the interviewee under pressure to support the same narrative and may lead to biases or misinformation.
- Confirm that the interviewee witnessed or experienced the acts themselves: interviewees sometimes share a testimony they have heard from someone else. This is often not intentionally misleading but results from being eager to share information they have heard.

## 7.4 Conducting the interview: content

### Personal/biographical details

Collect basic biographical details at the beginning of the interview. Keep these to a minimum to avoid intimidating the interviewee.

- Confirm basic biographical details: name, age (date of birth), gender, where they live, nationality (if relevant, for example with refugees). You may also want to ask about their employment/student status, and living arrangements (size of household, and so on) (the interview guide in Annex 5 contains a fuller list of biographical questions that could be relevant).
- Ask for the interviewee's contact details/phone number and how to contact them in the future if more information is needed.

**Note:** If you are taking handwritten notes in a location where there is a risk of search or confiscation of your notepad/belongings, put a number in the notes instead of the name of the interviewee. Note the name of the interviewee and the number of the corresponding interview notes in a separate location.

If you are recording the interview, for security reasons start the recording only after you have gone through personal data information.

### Details of the interviewee's account

Start the interview by asking a few general, non-sensitive questions to help the interviewee feel more comfortable.

To begin discussing the incident(s), **use a broad, open question** that allows the interviewee to start wherever they want to in their story of what they experienced or witnessed. An open question to begin can simply be “Can you tell me about the incident...?” or “Can you tell me what happened when...?”

**Continue to use open questions during the interview** which enable the interviewee to **shape the narrative** and include details they think are important. Let respondents talk in a narrative as much as possible to ensure the flow of the interview. **Make notes of points/details you want to come back to in follow-up questions.**

However, sometimes it will be necessary to interrupt gently, for example if the interviewee is talking at length about things that are less relevant to the incidents in question. You need to strike a balance between enabling the interviewee to talk freely and guiding the conversation when necessary.

Open questions are the best way to obtain detail. Specific (closed yes/no) questions are useful for confirming specific details, but otherwise should be avoided. Asking too many closed questions will exert too much control over what the interviewee talks about and will cause you to miss important details that you are not aware of/fail to ask about.

► *See Annex 4 for guidance on different types of questions you can use in a human rights interview, and how to use them.*

**If using an interpreter**, make sure the interviewee pauses regularly in their narrative to allow the interpreter to translate (explain this at the start). If an interpreter translates long periods of speech (rather than shorter sentences), they are more likely to summarize, and miss out or forget key details, which affects the accuracy of the interview. Ask questions that are not so long that they require pauses, and when explaining informed consent and other details at the beginning of the interview, pause to allow the interpreter to translate.

**Ask follow-up questions later** in the interview to clarify statements or to obtain more specific details, or to fill in missing details. A follow-up question acknowledges what the interviewee said, using their own words as closely as possible, and then probes on a particular detail or what happened next. Interviewees may not be aware which details are important or relevant, and may unintentionally leave out valuable additional information (see Box 16 on follow-up questions and obtaining detail).

Try to **build a chronology of events**. Clarify the order in which things happened if necessary: interviewees might not tell their story in chronological order. Remember that there may have been many steps in the days, weeks and months leading up to the possible violations that may be vital to understanding what happened.

**Be flexible** to discussing events and asking questions in an order that makes sense with the interviewee's narrative. You must also be flexible enough to accommodate unexpected issues that come up during the course of the interview.

**Never avoid discussing sensitive topics (such as sexual violence, torture, the death/killing of a family member) because you think they are too difficult** for you or the interviewee.

- Be empathic but professional in the way you ask questions about these subjects.
- Be clear about why you need to ask detailed questions (for example on sexual violence, torture). Use supportive statements and acknowledge how difficult it is for the interviewee, such as “I’m sorry that I have to ask you these details but it is important to be exact about what happened...” or, “I know this is difficult to talk about, we can stop any time you need to...” (see Section 7.6.1 for more guidance on interviewing survivors of sexual violence).

Remember that interviewees **may also have information about related violations**. For example, when interviewing a former detainee, they may have information about other detainees, their identity and their treatment. This could help, for example, to document other violations in that detention centre, or even to locate someone who has been detained arbitrarily/incommunicado.

If something the interviewee says is **ambiguous or unclear**, ask a clarifying question to confirm the details. Using the interviewee's own words when checking if you have understood them correctly builds trust and helps them tell their story in their own way.

**Note:** Make sure the interviewee is telling you facts, not assumptions: clarify how they know certain details. For instance, if an interviewee states that the army was responsible for incident x, ask, “Why do you believe it was the army?” This might lead to key information such as “they were driving vehicle x – only the army has those vehicles” or “I recognized the man in command, his name is General...” Alternatively, the interviewee's response might show that the statement is an assumption (unconfirmed).

Interviewees may not know certain details. For example, they may not know how to recognize different branches of the security services to tell you who was responsible. But they might be able to tell you what colour the uniform was, or other features that will help you identify who was responsible.

**Clarifying such details (and avoiding assumptions) is essential for creating an accurate picture of what happened.** Small details might be the key to unlocking vital pieces of

information about the incident(s). The more detailed the information you collect, the easier it will be to corroborate details from different sources/accounts and draw strong conclusions.

The **who did what to whom, when, where, how** and **why** questions are central to obtaining all the details of an incident or series of incidents and establishing a chronological order of events. The box below illustrates examples of follow-up questions to ask based on a statement made by an interviewee in order to obtain all the relevant details.

#### **Box 16. Following up – details!**

Get a clear picture, clarify the details. This fictional example demonstrates the amount and type of detail you should be aiming to collect during an interview.

During an interview, an interviewee is telling you about the alleged extrajudicial execution of his brother. He says: “...*They came and they took my brother away and then they killed him. My mother went to ask what happened to my brother, but they told her she was not allowed to ask, and that if she wasn’t careful, she would also be in trouble...*”

Details that you need to obtain (through follow-up questions) might include: **Is it first-hand or second-hand information?** When your brother was taken away, did you see this, or did someone tell you about it? Also structure your questions using the framework of Who did What to Whom? When? Where? How? Why?

**WHO:** Who took your brother away? (If interviewee witnessed directly): did you know them? (If interviewee did not witness): who witnessed this, or how do you know who took your brother away? (If security services): do you know which security service? How do you know? Were they wearing a uniform? (Can you describe it?) What vehicle were they using? How many were they? Who did your mother ask about your brother’s fate (police station, local authorities, other)? Who did she speak to (rank/position of person)? Was anyone else arrested at the same time, for example any of your brother’s friends/colleagues/students?

**WHAT:** Did the people who took him away have an arrest warrant? Do you know the cause of death? Do you know the circumstances of his death? (In a detention centre/another location?) How did you find out that he was killed? Were there any witnesses to his death? Did any witnesses see his body?

**WHEN:** When was your brother taken away (date, time of day)? How long after that did you learn of his death? Do you know when he died? (How do you know



that?) When did your mother go to ask about him? (How long after he was taken away, or how long after you learnt of his death?)

**WHERE:** Where was your brother when they came and took him away? Do you know where he was taken? How do you know that? Do you know where his body is/was found?

**HOW:** What was the cause of death? How do you know? If told an official cause of death, is this confirmed? Is there a coroner's report/other medical report? Did anyone see the body? Were there any signs/marks on the body (which may indicate the cause of death)?

**WHY:** Was any reason given for the arrest/abduction? Did the people who took your brother away say anything at the time (accusation, insult, statements, questions)? If there was an arrest warrant, what was the charge? Were there any previous incidents that might indicate why your brother was targeted? Why do you think he was taken, and killed?

The interviewer should decide the best order to ask the relevant questions based on how the interviewee is telling the story.

### Box 17. The importance of small details

Small details can be essential in identifying aspects of what happened, the identity of perpetrators, and so on. They can lead you to details or revelations about what happened that you have not thought about. For example:

- Small details of a uniform can identify which branch of security services, and which specific company/unit was involved – a badge (insignia) on uniforms; epaulettes or other insignia of rank may show who was in command.
- Details of the vehicles driven might also be relevant to tracking perpetrators – the type of vehicle, colour, anything written/marked on it, type and detail of number plates.
- Small details can help to identify unknown locations (for example if someone was taken to an unknown place of detention). For instance, features in the landscape, approximate distances/time spent in vehicle on way to location, terrain (tarmac, murrum, other), noises heard in the vicinity – traffic, industrial noises, rural noises (cows, cockerels, and so on), muezzin/church bells.
- Small things that perpetrators said can give clues about the motivation of the incident.

## 7.5 Closing the interview

When you have finished your questions, check whether any other forms of evidence or information need to be collected.

**Photos:** Is there anything that would be relevant to photograph? Particularly with survivors of torture – does the interviewee have any physical injuries or scars that resulted from the violation(s)? If so, ask permission to photograph the injury, wound or scar. Informed consent must be sought specifically for this purpose. Explain how the image might be used, and how confidentiality will be protected. Photograph the injury/scar in a way that does not expose their identity.

**Documents:** Does the interviewee have any documents relevant to the violation, such as an arrest warrant, charge sheet, court documents, medical records, correspondence, photos? If so, ask permission to take a photo or make a copy of each one. Free scanning applications (for example Adobe) can be downloaded onto your phone. They are useful for scanning longer documents, such as legal or medical documents, as they compile all the images into a single file. Make sure the interviewee understands and agrees to how these documents can be used. Obscure/mark over their name (and any other identifying details, such as ID number) from the copies you make using an image edit function.

**Additional contacts:** Ask the interviewee if they know other people you should talk to who have knowledge of the incident.

### Ending the interview

- Take time to close the interview.
- Ask if there is anything else to add to the story you have discussed; then ask if there is anything else the interviewee wants to discuss or any questions they want to ask you. This could be related or unrelated to the interview. Allow time for this at the end: there may be additional details that you did not ask about, or the interviewee may want to bring up other issues.
- Confirm that they still give consent to use the testimony. Agree on how to contact each other for follow-up, if relevant.
- If relevant, mention facilities that can provide assistance and support (medical, counselling, or other). Check if the interviewee can access these services (for example, has the means to).
  - You may want to/it may be helpful to contact the agency yourself at the end of the interview to refer the interviewee (if they wish it).
  - Assist with the costs if you have the mandate/budget to do so and the interviewee requires support.
  - If referring children for support services, a parent, guardian or adult care giver

must give consent and must be involved in the referral process.

- Where relevant, provide the interviewee with your contact number or that of a relevant colleague to call in case of any issues, or to give to a family member to call if anything occurs to them. Advise the interviewee to have an alert SMS ready in their phone or to put your number on speed dial.
- Check if the interviewee is ready to close and leave. Do not leave if they are upset. Ask if they have friends and family they can talk to, and whether they would like to discuss measures they could take for emotional support.
- Thank the interviewee and acknowledge their contribution.

**Immediately store the interview record securely:** When the interview is finished, follow your pre-identified steps to securely store the interview record information to ensure the security of the interviewee, the information and yourself. Immediately upload any recordings, save in an encrypted location and delete from your devices; replace the SD card in your recording device and hide the card with the interview record; email the files to your colleague using Tutanota or Protonmail; photograph your notes and store the photos in an encrypted location, or type your notes as soon as possible, and store the digital file securely; destroy the handwritten notes; and wipe the memory of the file(s) on your laptop, phone or camera.

## 7.6 Interviewing groups with specific considerations

### 7.6.1 *Interviewing survivors of sexual violence*

**Sex of interviewer/interpreter:** When investigating sexual violence, the interviewer and interpreter should preferably be of the same sex as the interviewee. For some survivors and in some cultural contexts this will be essential.

**Sensitivity, stigmatization and confidentiality:** In many places, rape and sexual violence are still treated as taboo subjects and are socially stigmatized, for women, men and children. Rape and sexual violence against men may be even more highly stigmatized than that of women and girls. This can make survivors reluctant to talk about their experiences. The strictest protections of confidentiality are necessary when interviewing survivors of sexual violence. You may need to spend more time explaining the sort of details you need to ask, and why, and reassuring the interviewee that you will protect their confidentiality.

**Socio-cultural attitudes:** Be sensitive to the local community's socio-cultural attitudes to rape and sex, which can affect a survivor's willingness to talk, understanding of key concepts (such as what constitutes rape), and the way they respond to and recover from incidents.

Be aware of your own attitudes too. If you feel uncomfortable or embarrassed, this can

show for example in your body language, inability to maintain eye contact. This can create or reinforce the idea that sexual violence is too painful or shameful to discuss.

**Terminology:** Use biological terms to refer to body parts. If these terms are unfamiliar to the interviewee, then use local terms. Make sure you have a shared understanding of the terms. It is necessary to ask explicit questions about exactly what happened in incidents of sexual violence. Explain why you need such details, and acknowledge that it is difficult: “I’m sorry I have to ask you this but can you tell me...”

**Support:** Be sensitive and empathetic, but remain professional. As with all interviews on difficult topics, interviewees might need extra support when talking about incidents of sexual violence.

**Referral:** Survivors of sexual violence are often in need of medical assistance, counselling and other services. Be prepared with a list of organizations and individuals you can refer survivors to.

- *For more detailed guidance on documenting sexual violence, including interviewing survivors, see:*
  - *International Protocol on the Documentation and Investigation of Sexual Violence in Conflict: [gov.uk/government/publications/international-protocol-on-the-documentation-and-investigation-of-sexual-violence-in-conflict](http://gov.uk/government/publications/international-protocol-on-the-documentation-and-investigation-of-sexual-violence-in-conflict); and*
  - *WHO Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies: [who.int/publications/i/item/9789241595681](http://who.int/publications/i/item/9789241595681)*

### 7.6.2 Interviewing children

Children, especially younger children, should only be interviewed when absolutely necessary. If possible, only investigators qualified/experienced with working with children should interview them.

Essential principles for interviewing children are:

- In general, it is best to use a single interviewer. This is likely to be less intimidating and stressful for the child, and it is easier for the child to develop a rapport with a single person.
- The child should choose who, if anyone, they want to be present (this could be a parent, caregiver, sibling, friend or teacher). However, having parents in the interview can be difficult. Their presence may cause children to exaggerate or minimise what has happened to them, and parents have a tendency to distract children, and to answer questions for them. If parents need to be present to put the child at ease, you can ask them to sit where they are visible but out of listening distance.

- The best interest of the child is the most important consideration at all times.
- If the child chooses not to be accompanied, ask another interviewer/trusted adult to be present for child protection reasons, or interview in a location where you are separate but visible – see below.

**Informed consent:** You must obtain the informed consent of the child and their parents/ caregiver before interviewing them, though cultural attitudes will vary on the age when a child can be interviewed without parental permission. If a child has neither a parent nor caregiver, use your judgement to assess their ability to make an informed decision about participating in the interview. This will be based on their age, intellectual/ emotional capacity, willingness and their best interest as the primary consideration.

**Setting:** Choose a place that can put children at ease, particularly a place they are familiar with, and smaller, child-friendly spaces. Sit on the same level as the child/ children – including if they are sitting on the floor – in order to reduce the power imbalance between you and make the child feel more comfortable. Try to sit where you are separate from other people, but not isolated – for reasons of child protection. For instance, if you are outside, sit away from others but in view. If you are inside, leave the door of the room open.

Some children may prefer to speak one to one, while others may feel more comfortable in a small focus group. Groups can work well with children, unless you need to ask a child about a very personal experience. If interviewing in a group, aim for around 4 to 6 children – if there are too many, not all of them will get chance to speak. Ensure they are of similar ages (younger children will often be intimidated by older children and will talk less).

**Introduction:** Tell them who you are and what you are investigating; explain informed consent and confidentiality in language the child will understand. Ask the interviewee to introduce and say a bit about themselves – this can help to build their confidence to talk.

### Language and approach

- Adapt your language to the age of the interviewee. If you are unsure what is appropriate for their age, listen carefully to how they speak and use similar language and phrases.
- Be very aware of your tone and body language when interviewing children. If you treat the interviewee as a person who has important things to say, they will be more responsive and open in answering questions. Do not interrupt them: this can cause them to lose confidence in what they are saying.
- It can be very effective to use art/drawing to encourage and help children to represent their experiences of a certain event, especially with younger children.

Ask the child to draw a picture of the event and then explain the picture to you.

- If you are interviewing a (focus) group, get the children to discuss the event among themselves first. This can help encourage participants to talk and share more detail.
- If a child does not want to talk, never push them. Ask if they understand why you are asking them questions and if they have any questions for you; ask if there is any way you can make it easier for them. If not, stop the interview. It is better to stop as soon as possible to avoid making the child feel they have failed. When you finish the interview, make sure you end it properly – see below.

**Timing:** A child's concentration span is much more limited than an adult's, so long interviews are not possible. Limit the number of questions you ask. You also need to allow more time to gain children's confidence before beginning an interview, and spend extra time at the end to ensure the child is not feeling distressed about the interview and what has been discussed.

**Sensitive topics:** Approach the subject in an indirect way. For example, do not ask "tell me about when you were abused", but "I think you've had some very difficult experiences and you've done well to get through them, can you tell me about this". Or, "how did you feel on that day when the men came to the village?" Let the child control how they want to talk about the issue(s), listen carefully, empathize and give praise.

**Biases:** Be aware of your prejudices and biases when interviewing children – you may take their opinions and observations less seriously and may instinctively think you know more about a subject than a child does.

**"Suggestibility":** This is when an interviewee is influenced by what they believe the interviewer wants or expects them to say. Vulnerable people, including children, can be more influenced by suggestibility. Be very careful about putting words into children's mouths, even if they are having trouble explaining something.

**Ending:** Children may be excited or upset at the end of the interview. The interview may have given them a chance to speak about things they have never talked about before, because of socio-cultural attitudes to children or to sensitive topics, or for other reasons. Make sure you allow proper time for the interviewee to calm down at the end and support them in this. Ask if there are any questions they would like to ask you. Whenever possible, make sure there is a supportive adult who knows that the child has been discussing difficult topics and can help them after you have gone. Make sure the child is with another trusted person before you leave.

### *7.6.3 Interviewing people with trauma / avoiding re-traumatization*

The term "traumatized" is used here to describe individuals experiencing longer-term psychological distress as a result of experiencing or witnessing something that caused

extreme fear, horror, distress or physical pain. Their capacity to process and cope with what they saw or expressed may be overwhelmed, and their ability to manage daily life activities may be compromised.

Do not assume that a survivor, victim or witness is traumatized. However, an interviewee who has experienced or witnessed a violation may show signs of possible trauma. Traumatic experiences can cause people to display a wide variety of emotions including sadness, anger, anxiety, guilt or shame, as well as emotional displays that may be more difficult to understand in the circumstances such as smiles and laughter. The effects of trauma can be highly visible for some traumatized individuals, while others might appear to be absent-minded or unreliable.

During interviews, trauma might cause some people to exaggerate, but lead others to downplay crucial information. Traumatized individuals may speak in the third person as if to dissociate themselves from what happened; they may have trouble recollecting events or details, lack focus, share multiple versions of the same story, be incoherent, appear stable and balanced, or show all the above interchangeably.

### **Re-traumatization**

Re-traumatization refers to a situation in which the survivor, victim or witness re-lives (or re-experiences) a traumatic event. Re-traumatization can be triggered by many things including particular smells, certain sounds or voices, or certain situations. Interviewers can trigger re-traumatization through poor interview techniques, attitudes or expressions. For example, an interviewer could display an attitude that reminds the interviewee of the traumatic incident; force the interviewee to talk about something they do not want to discuss; get frustrated with trauma-related behaviour displayed by the interviewee; be overly controlling of the direction of the interview or frequently interrupt. This can make the interviewee feel helpless: traumatic events often involve the victim feeling powerless or overwhelmed.

The effects of re-traumatization can vary widely. Interviewees may show high levels of anxiety, stress, dissociation, panic, sweat profusely or shut down completely.

To minimize the risk that interviewees become distressed and the risk of re-traumatization:

- If possible, obtain some detail in advance about what the respondent has experienced so you are prepared for the sensitivities of the interview.
- Take time over introductions and build trust and a supportive environment in which the interviewee feels comfortable talking. Remain aware that it is very difficult for people to open up and talk about a traumatic event, particularly to a stranger.

- Be very clear from the beginning that it is likely you will ask difficult questions, which the interviewee may find upsetting.
- Ensure the interviewee understands that they can let you know at any time how they feel and when they need to take a break or stop the interview.
- Before the interview, or at any point during the interview, ask whether the interviewee has emotional support, such as a friend or family member who they trust and can talk to when upset, and ask whether they have talked to that person about what happened. Ask if they have things they do that help them feel better when they are distressed (known as grounding techniques). If they are not aware of any, you could help them to identify things that relax them or that they might find helpful. This could be simply drinking some tea, going for a walk, doing breathing or stretching exercises, playing little games, talking about different subjects to distract from the memory, or listening to music.
- Show empathy and support in your speech and body language. Acknowledge the difficulty of talking about what happened, and reinforce the interviewee's capacity to cope with the interview – for example, say “I know it must be very hard to talk about these things, I really appreciate you talking to me about these details...” Emphasize that what they are doing is important and valuable, and that there are people who care about what they have gone through and for their security and well-being. Avoid any emotional response: it is more helpful for the interviewee (and you) if you are calm, empathetic but professional.
- Never try to force someone to discuss something they do not want to talk about.

**If the interviewee becomes distressed during the interview,** pause and ask if they would like to take a break, use one of the grounding techniques you have discussed, or stop the interview. If a friend or relative is nearby, ask the interviewee if they would like to take some time with that person or have them present in the interview.

If it becomes clear that it is too difficult for an interviewee to continue, stop the interview immediately. However, even if you are cutting the interview short, take the time to finish properly. Discuss the grounding techniques again (ask if the interviewee wants to try one now), and ask who they can go to for support. Try to make sure a friend or family member is with them before they/you leave. If relevant, refer the interviewee to relevant organizations or services, such as health services, lawyers or counselling.

### **Impact on the interviewer**

Repeated exposure to violations through frequently interviewing survivors, victims or witnesses can also affect interviewers and lead to symptoms of vicarious trauma, stress or burnout. This can result in diminishing empathy or even irritation towards survivors and victims, and an inability to use judgement and make sensible and informed decisions, which can affect people's security and the credibility of data collection.



- *Interviewers and their organizations must take time to address their mental and emotional well-being (see Chapter 11 on managing the well-being of investigators).*

# Chapter 8

## Collecting documentary evidence

Documentary evidence can form a vital part of the information you collect when investigating human rights violations. Such evidence can provide key details on certain aspects of the case, help to corroborate and offer supporting evidence to a survivor's/victim's testimony, and in some cases can even provide unequivocal evidence that a violation happened.

A wide range of written materials and documents can contain information relating to violations, including records of aspects of the case, official orders relating to an incident, charge sheets, death certificates.

Photos and video footage can capture incidents, provide evidence or reveal vital clues about the identity of perpetrators or victims, methods used, locations and/or other aspects.

Satellite images can provide vital detail to corroborate on-the-ground sources (such as photographic and testimonial sources). They might help to identify or confirm locations, or the extent of damage, and may even provide information about inaccessible locations. Before and after images can prove the timeframes in which violations occurred.

Online/open source material: all three of the above types of evidence/information might be found in online sources, particularly content shared on social media and other user-generated content-based platforms.

## 8.1 Identifying and collecting documentary evidence

### 8.1.1 Identifying sources

A wide variety of documentary sources might provide details relevant to your investigation. These could include:

#### Documents

- *Police and court records and documents (arrest warrants, charge sheets, judgements, evidence submitted in court cases, court records):* Can provide details of arrests, charges and legal processes (or the lack thereof), serve as evidence of whether due process was observed, and whether trial proceedings were fair (met international standards), details of any police investigations into incidents, and other details.
- *Medical documents (medical reports/records, autopsy reports):* Can corroborate reports and details of torture and sexual violence, cause of death, and other information.
- *Security force orders, correspondence:* Can prove details about military operations, such as orders issued, who ordered/led operations, who had command responsibility on the day, and so on.

- *Eviction or demolition orders*: Can demonstrate that a forced eviction was ordered, by whom, who was in command on the day, and so on.
- *Official reports or statistics (numbers of children in detention, maternal deaths, conviction rates in rape cases, number of arrests under terrorism legislation, enrolment in education system)*: Can show government policy, action or inaction on issues of concern, and official responses to allegations of violations.
- *Data on the provision of services (such as health care, education) or the prevalence of certain types of violence disaggregated geographically or according to other indicators*: Can show discrimination, trends and other information.
- *Official budgets*: Can illustrate the absence or shortfall of government spending on certain issues, discrimination in the provision of services, and so on.

#### **Photos and video footage (including content shared online)**

- Can show incidents/violations occurring, the aftermath of violations, injuries to victims, method of killings, destruction and damage to buildings/the landscape and details about the victims, perpetrators, locations and methods, including small details that might help to identify perpetrators, such as insignia on uniforms, number plates on cars, serial numbers on weapons.

#### **Satellite imagery/photos**

- Can provide visual evidence of violations that leave a physical impact on buildings and the landscape or show the physical impact over a wider geographic area (for example, destruction of villages, bombing of civilian infrastructure, environmental damage over a large area such as oil spills).
- Can provide access to harder-to-reach or inaccessible locations such as conflict situations or remote prison camps.
- Before and after photos can show changes to landscape and possibly prove the dates when incidents occurred.

#### **Crowd-sourced information**

- Digital technology can be used for participatory information collection and crowdsourcing – for example by using online platforms (through online and mobile apps) to collect information from people living in conflict/crisis contexts.

#### **Expert assessment/opinion (requested or commissioned)**

- Can identify, confirm or corroborate details. For example, a ballistics/munitions expert can confirm the type of weapons/munitions used (from examining photos of damage, injuries and (certain details of) testimony of an incident). Experts may even be able to identify the perpetrators or source of the weapons based on knowledge of the manufacturers, distributors and users of particular

weapons systems. A doctor/medical expert report could confirm injuries, causes of scarification, cause of death from examination of torture survivors, photos or review key details of an interviewee's testimony.

### *8.1.2 Collecting documentary evidence*

Documentary evidence might be obtained through a wide variety of channels. These could include:

#### **From survivors/victims, witnesses and other sources**

As mentioned in Chapter 7 on interviewing, ask interviewees if they have documents or photographs relevant to the incident(s) they are telling you about, such as court documents or medical reports. Other sources (who might not have testimonial evidence to give) might have relevant documents, reports, photographs, official records or other information. This could include lawyers, community leaders, doctors, hospital staff, officials/government sources, journalists, local organizations.

#### **Commissioning/requesting information**

You might need to commission some documentary evidence. This might include expert witness reports or assessments to confirm/verify some of the information you have collected, identify key details (such as identifying weapons from photographs/testimonial descriptions), or provide relevant contextual information. You might also commission satellite imagery from a commercial provider if the images of the location or the date/time you want to examine are not available on open source mapping sites (such as Google Earth). You might also need to make formal requests for information from official sources, such as freedom of information requests through formal channels, in countries that provide such a right.

#### **From online and digital sources**

Open source material (material accessible to everyone online) and innovative digital tools play an essential role in human rights investigations. This includes material available on websites from official, institutional, organizational, media and other sources (such as reports, statements, databases, statistics) as well as information from mapping websites like Google Earth. It also includes user-generated content – photos and footage, as well as written accounts, which have been uploaded/shared by individual users of websites and social media platforms such as YouTube, Facebook, Twitter, Instagram, and so on. You might also use online applications or other digital tools to crowd-source information. Working with open source material is complex and requires thorough verification practices (see Section 8.4).

Remember that **confidentiality also applies to documentary evidence**. Any reference to, or publication of, documentary evidence in your reporting must be based on careful

consideration of the security of the source and any survivors, victims or others shown in the images who might be put at risk of harm if they are published.

- Informed consent must be obtained for such usage, based on a thorough understanding of the potential risks to those shown in the images. Even with informed consent, it will be necessary to conceal any identifying details of people in the images.
- Informed consent to use images must also be obtained from people who provide images to you (but do not feature in them).
- If photos, videos or other materials are sent directly to your organization, it is important to check that they are genuine. Do you know the sender? Confirm if the sender is also the originator of the content. If you *do know* the sender/it is a trusted contact, you still need to verify the authenticity of the photo/video. If you *do not know* the sender, you will also need to confirm the identity of the originator/owner of the content. Section 8.4 describes these two processes. When you have confirmed the identity of the content owner, you can discuss and agree with them how you will use the content.
- With all images, be very careful about making assumptions. It is important to remember that the contents of photos and video are not always what they appear. A photograph can tell you one aspect of something that took place but might not show key details, which could give a misleading impression of the incident. For example, an image might show a burned house, but does not prove that a human rights violation occurred.

### 8.1.3 *Protecting sources and those featured in photos/footage*

If you are going to use photographs or footage publicly, the core principle of do no harm must be considered in relation to any survivors/victims who appear in the footage. Ensure that any use of photos or footage protects survivors' privacy and does not re-victimize them.

- Who is identifiable in the photo/video, and how are they portrayed? Are they aware they are being filmed? How might their appearance in the footage, if seen by a wider audience, impact them or their community?
- Have any survivors/victims who appear in the images given their consent for the images to be used publicly?
- Does the publication or broadcast of the content identify any personal information that might cause people who are featured in/affected by the violation to be further harmed or otherwise affected?
- Make a professional judgment about whether using footage could violate the consent, privacy or dignity of those filmed.

The mobile app **ObscuraCam** (currently available for Android only) allows users to blur faces in photos and videos. This can enable you to publish or post pictures or videos without revealing the identities of those depicted. YouTube offers a similar tool for blurring faces in videos.

## 8.2 Satellite imagery

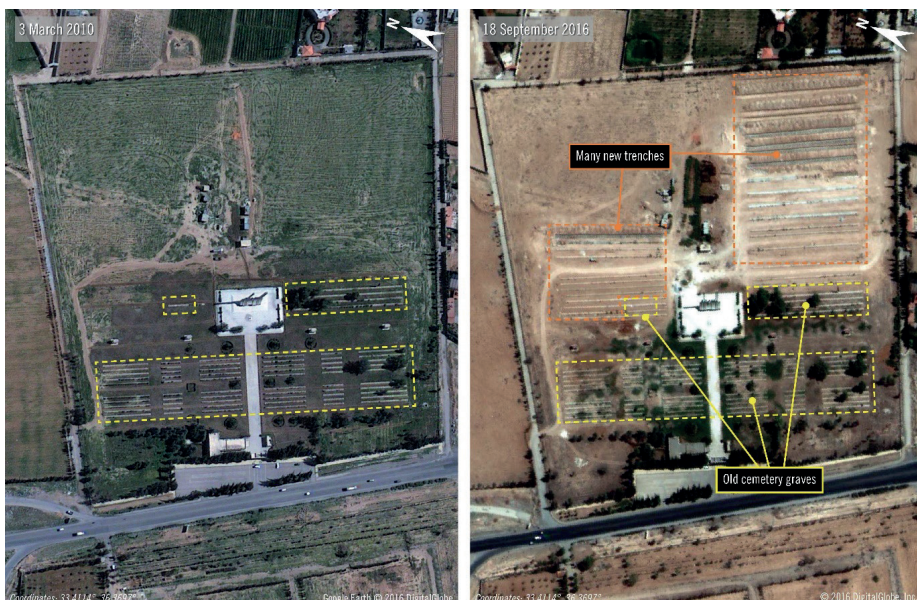
Human rights investigations can employ satellite imagery and geospatial mapping systems in a number of applications.

### Detecting impact on/changes in the landscape that might be evidence of violations

- Satellite images can detect significant changes to buildings, roads, vegetation or other features larger than 2–3m<sup>2</sup>. This might include house demolitions, forced evictions or displacement, bombings (for example, bombing of civilian infrastructure such as hospitals), destruction/burning of villages, mass graves, and certain types of environmental pollution or damage.
- Images taken over a given time period, or “before and after” images, enable you to compare pictures of the same location to detect changes in the landscape or buildings. This sometimes helps investigators establish (and prove) the date when violations occurred.
- Measuring features might be able to establish the approximate extent of the violations/damage.

**Figure 5. Using satellite imagery to document suspected mass graves in Syria and Burundi**

**Example 1:** As part of an investigation into mass enforced disappearances at Saydnaya prison in Syria, Amnesty International analysed satellite imagery to detect significant increases in the number of graves in two cemeteries where victims of enforced disappearance killed at Saydnaya were being buried. This increase was identified by comparing images over a 3-year period.



Left image: Google Earth © 2016 DigitalGlobe. Right image: © 2016 DigitalGlobe, Inc.

A cemetery near Damascus, Syria. Amnesty International used satellite imagery to show how new, 90m-long trenches began to appear in 2013. By 18 September 2016, imagery shows the grave area had more than doubled in size with additional 90m-long trenches. Source: [amnesty.org/download/Documents/MDE2454152017ENGLISH.PDF](https://www.amnesty.org/download/Documents/MDE2454152017ENGLISH.PDF)

**Example 2:** In Burundi in late 2015/early 2016, a number of killings of political protestors were known to have recently taken place. Amnesty International found and documented a suspected mass grave by triangulating the testimony of witnesses on the ground, photos from ground level and satellite imagery. By analysing before and after satellite images around the dates of the killings, Amnesty International could identify the appearance of a newly disturbed area of ground. This correlated with other sources of information that a burial may have taken place in that location. Source: [amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/](https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/)



### **Identifying locations associated with violations**

If you have testimony describing the approximate location of something, you can search satellite imagery of that area for a building or other feature fitting the witness's description. For instance, if an interviewee tells you they were detained in an unofficial detention centre close to landmark x. Often, buildings can be identified in satellite imagery by their shape or proximity to other features. In some cases, shadows cast by a building in images can indicate its height – for example, whether it is taller or shorter than adjacent buildings.

You can also use satellite imagery to verify details of a witness's account, for example if they described a location or landmarks they remember from a journey. You can examine images of these locations on a mapping site (for example, on Google Earth/Google Maps, Yandex Maps, Wikimapia) to verify if the details provided correspond with what you can see of the location.

### **Noting features of a location**

If a violation has been reported in a certain location, you could look on mapping sites such as those mentioned above to examine other features of the area that might be relevant to what occurred. For example, you may be able to determine whether the location isolated or built up, near a military base, and so on.

### **Geo-locating photos and footage, including user-generated content**

This is the process of verifying the location shown in a photo or video footage. For example, in images sent to you or shared on social media and user-generated content sites, to confirm that the photo was taken in the location it claims to show. You can geo-locate images by cross-referencing visible features with other ground-level photos and/or satellite imagery (see Section 8.4).

### **Circumventing access or concealment challenges**

Satellite imagery can be particularly important for observing places that are difficult or impossible for investigators to access such as conflict zones, isolated prison/internment/military camps, and locations to which access is restricted.

### **Extensive data collection and assessment over time and geographic area**

Satellite imagery can enable monitoring/data collection over wider geographic areas and systematic monitoring/data collection over longer time periods. For example, analysis of satellite imagery could provide a comprehensive damage assessment of civilian areas affected by conflict or military operations, or the scale and frequency of housing demolitions and forced evictions.

### Using satellite imagery

- Use geospatial mapping sites such as Google Earth, Google Earth Pro or satellites. pro (which are freely available online or to download – [google.co.uk/earth/download/gep/agree.html](https://google.co.uk/earth/download/gep/agree.html)). These can be very useful tools to conduct some basic imagery research, and can be extremely helpful in uncovering or confirming certain details of your investigation. Note that editable platforms such as WikiMapia or Open Street Map are often more detailed and more frequently updated than closed platforms such as Google Maps and Google Earth.
- You may want or need to commission or buy images from a commercial satellite imagery company. Commissioning enables you to obtain images from exact locations (for example, an area where you believe destruction of villages or environmental damage might have occurred or suspect an internment camp might be). Alternatively, you might need to buy existing images – of a specific location or date. If you do not have the resources to commission satellite imagery, try to partner with a larger/international organization that could assist with funding/commissioning the images.
- The timeline or “history” function of mapping sites such as Google Earth Pro enables you to compare images over a period of time – “before and after” images – to detect basic changes. For example, to explore the extent of housing demolitions. To do this, you need an approximate idea of the dates you wish to compare – roughly when you think the change in the landscape/buildings (linked to a violation) that you are trying to detect may have occurred.
- Take screenshots and record the date and time of the images from satellite imagery/mapping websites.
- Satellite images need to be carefully analysed. Sometimes specialist expertise might be needed to interpret them. If possible, seek the assistance of a specialist in change detection in satellite imagery and GIS. You could partner with larger (international) organizations to access expertise, or try to establish contact with an expert who might assist you pro bono.

**Remember:** Satellite imagery cannot replace thorough on-the-ground investigation and documentation, but can supplement and corroborate other investigation methodologies.

Satellite images can only document violations that leave a clear physical effect, and can only provide limited details about what actually occurred. For example, they might show that a change to the landscape happened, but they do not tell you the identity or the number of perpetrators or victims. They can also only show certain types of violations; other violations may have occurred in the same incidents. For example, in

Darfur, Sudan, satellite images showed villages burned to the ground, but could not show the widespread and systematic rape that occurred.

### 8.3 Handling open source/online information

Open source information is freely available to anyone on the internet. The abundance of information available online means that identifying, collecting and verifying evidence from online sources has become an essential part of many human rights investigations.

- For example, video footage shared through a social media platform may show police firing live ammunition at unarmed protestors, or a statement posted on a ministry website could communicate the government's response to a particular incident.
- Online sources/information can help cross-reference the details of incidents.
  - The insignia seen on the uniform of a perpetrator in a photo of a human rights violation can be checked against websites of military units to identify the unit involved.
  - Satellite imagery can be used to identify a building described in an approximate location by victims/eyewitnesses.
  - Weather information available online can be used to confirm the weather in a particular location on a certain day, which might help confirm the authenticity of a video.
- Online platforms and tools can enable investigators to gather information from a wider range of first-hand witnesses/a wider geographic area, over a longer time period. Tools and free software available online can also provide essential help in verifying online content.

Online information should complement, rather than replace, information collected through interviews and from other sources. **Online content must be used with extreme care. Much material posted or shared online has been altered, edited or fabricated, or is incorrectly labelled** (intentionally and unintentionally). Data can also contain errors, even if it comes from trusted contacts and seemingly reliable sources such as international institutions.

**All information gathered through online sources must be thoroughly verified**, particularly any content shared via social media ("user-generated content", sometimes also known as citizen media).

#### **General rules when working with online content (information openly available online)**

- Develop human sources with whom you can cross-check the validity/accuracy of content.
- Consult multiple, credible sources. The credibility of each online source needs to be verified in **every** case. Some sources are clearly biased but are nevertheless worth consulting as they may contain valuable information.
- Be sceptical and thorough in your investigation of the data.

- Cross-reference new data with the other information you have collected and with what you already know about the situation/context.
- Data that is unsubstantiated by other sources (meaning there are no other reports, photos, tweets about an incident) should be treated as suspicious. Yet there may have been fewer witnesses or limited access to the internet in isolated locations.
- **Beware of fake websites** – some look like legitimate institutions, with very similar URLs (website addresses).
- When using search engines such as Google, try several spelling variations for names and places. Entering search terms in quotation marks will increase accuracy in search results. Names of people and places are frequently spelt in several ways, particularly when languages with different alphabets/scripts are translated or transliterated into the Latin alphabet. When working with Arabic, keep in mind that the pronunciation (and corresponding spelling) of a single word can differ widely among Arabic-speaking countries.
- Remember, even official sources or apparently reliable sources might have gaps or errors in their data sets.
- Chapters 2–5 of the [Verification Handbook](#) provide more details about online search terms/techniques that can enable you to conduct more in-depth searches, including to obtain background information about a person, search for certain types of files, search official (government) databases and investigate companies.
- Communicate/work with experts at verification techniques: many of the methodologies of working with online data sets and verification tools are complicated and require specialist knowledge.

---

**Remember:** The credibility and accuracy of your information is essential. Online content is frequently manipulated, falsified or inaccurate. All online content must be thoroughly verified.

---

Large amounts of false or inaccurate content is shared on the internet, on both websites and social media. Much online information is recycled from other sources and does not always show what it claims to. Misinformation is frequently spread intentionally, which can have severe consequences.

For example, in June 2018, misinformation spread by a Facebook user in Nigeria (images showing violations from different times and even another country) sparked reprisal killings of one ethnic group by another.<sup>1</sup>

The above considerations are particularly essential when working with content shared on social media and other sites and platforms that disseminate user-generated content (see Section 8.4).

---

<sup>1</sup> Yemisi Adegoke, “Like. Share. Kill. Nigerian police say false information on Facebook is killing people,” BBC, 13 November 2018. [bbc.co.uk/news/resources/18-11-18-nigeria\\_fake\\_news](https://www.bbc.co.uk/news/resources/18-11-18-nigeria_fake_news)

## 8.4 Verifying content posted on social media (user-generated content)

User-generated content includes photos, videos, tweets, blogs, and others, that have been posted by the users of a social media or other online platform such as YouTube, Flickr, Facebook, Instagram, Twitter and so on. When the content relates to incidents or events that the user (claims to have) witnessed, it is also sometimes known as eyewitness or citizen media. Content shared online can play a significant role in the investigation of violations of international human rights and humanitarian law.

As with other photos and videos, content shared online can provide evidence that a violation occurred, help establish specific details of a violation, identify or give clues about the identity of perpetrators, and the identity and/or number of victims in an incident. User-generated content can be particularly valuable when posted from places that human rights investigators are not able to access.

**Remember:** Content posted or reposted on social media and other platforms is often manipulated, edited or fabricated. Individual users and websites also frequently take images or footage and post them as their own, without crediting the original source.

Frequently, the same photo or video is reposted repeatedly with different labels – claiming that it shows unconnected incidents in different countries (including in the Nigeria case mentioned above). Audio is frequently added over visual footage that is not from the same recording. It is very easy to fake a tweet and make it look like it is from an authentic source.

It is **essential to properly verify user-generated/social media content before sharing or publicizing it**. Proving the authenticity of the data – that the photo/footage/tweet is genuine, shows what it claims to show, was taken at the time, date and location claimed – is essential before you can consider that its content has any evidentiary value for your human rights investigation. This type of content must also be used and credited in ways that protect the persons who capture and share the material.

Verifying content shared online can be highly technical, and some methods and tools cannot be used without specialist expertise. However, **many digital tools/methodologies are openly available online and usable** without high levels of technical expertise.

### Essential basic rules of using social media content

- Check whether the content (photo/footage) is genuine (shows what it purports to show) and accurate.

- Check whether the content is original (has not been posted before in relation to a different incident).
- Verify the credibility of the originator of the content.

If there is any doubt, do not use it!

If you are investigating a piece of social media content, first **save the file** in case it is removed or deleted before you have finished your investigation. If possible, obtain and save a copy of the original file. Make a note of the URL of the website where it was found (unless it was sent to you directly) and the date and time of the original publication/posting; take a screenshot of the post.

Three main steps must then be taken to **verify the authenticity and accuracy all content shared by users online**.

### 1. Review the metadata

The metadata of a photo or video (sometimes called Exif data) is information embedded in the images that includes what device it was shot on, and – importantly for human rights investigations – when and where the image was created.

- Check if the image has any metadata. If you are taking footage/photos from the internet, many social media sites remove the metadata of images/videos during the upload process, but not all. If you are able to obtain the original files, this will ensure that you can extract the metadata and confirm the time, date and location where the photo/footage was taken. (Note: other ways of confirming the time and location if there is no remaining metadata on the file are discussed below). To uncover the data embedded in a photo/video, use an online Exif /metadata reader, such as [imageforensic.org](http://imageforensic.org) (simply drag/copy an image into the site). Or you can download software that reviews video metadata, like MediaInfo. (Note: these sites give latitude and longitude coordinates where the image was taken. You can enter this information into a site such as [findlatitudeandlongitude.com](http://findlatitudeandlongitude.com), which will tell you the location of those coordinates.)
- Even if you have done this process successfully and the metadata shows a location, you should still cross-reference and confirm this location through the process of geo-locating. Geo-location (explained in more detail below) entails using on-the-ground photos and video footage, and satellite imagery available through online mapping platforms, to try to confirm the details of locations/landscapes. It is necessary to confirm locations beyond what the metadata shows because the metadata location information can be incorrect for several reasons. You may need to use your judgement based on what you can see in the images to assess this.

- If you are looking at online content, you can also check the “public metadata” such as the upload time and location – that is, when the content was posted. Again, this can help to confirm that the content is coming from where the uploader says it is coming from (although it could have been sent to someone else who uploaded it). This tool can help you extract the data from YouTube videos: [citizenevidence.org/2014/07/01/youtube-dataviewer](http://citizenevidence.org/2014/07/01/youtube-dataviewer). Social media location services like Geofeedia and Ban.jo can also help establish where an image was uploaded. Try to work out what the local time would have been in the location where the content was uploaded at the time of the upload using a time zone website such as [timeanddate.com](http://timeanddate.com).
  - Be aware: YouTube, Facebook and Twitter all have different systems for working out the publishing date. For instance, YouTube registers all uploads in the US Pacific Time zone (regardless of where in the world they were posted), which can make some videos look like they were posted *before* the incident occurred (for example, if content was posted immediately after an incident in a part of the world with a time difference significantly ahead of the US west coast). Twitter users can set their own time zone in account settings, while Facebook uses the computer’s settings. Both could cause inaccurate information.
- *Annex 3 contains detailed guidance and tools for verifying online and user-generated content.*

**Remember:** By far the best way to corroborate online content is to find other sources reporting the incident on the same day/location and compare the details (preferably multiple credible sources from varied places).

## 2. Verify the original source and its credibility

Considering the credibility of the source is just as important in verifying photos and videos as it is in other areas of human rights investigations.

- If the images were sent directly to you, ask the sender if it is their original content (namely, whether they took the photo/footage). Content shared online has often been copied from someone else and re-uploaded; many people post other content claiming it as their own. It is best practice to try to find the original source of the content. If it is possible to do so, identify the person who uploaded the content and contact them – through the social media account or email address the image was shared from.
- Ask the person claiming to be the source some basic questions about when and where they took the footage, what they saw and where they were standing when they took the photo/video. This can help to authenticate what they claim to have

witnessed, and might uncover additional important details for your investigation.

- Talking to the uploader of the content will often reveal that they did not take the photo/footage – for instance if they cannot answer these basic questions, or they may admit that they did not take it. Cross-reference the source’s answers about where and when they took the footage with any information from the metadata (as above) and geo-locating (see below) to check whether their information is accurate.

It is **essential to check whether the content has been posted online previously in relation to different contexts**. There are many examples of the same image or footage being reposted multiple times, claiming it is from different contexts/countries showing a range of different things.

- To check if content has been posted before, conduct a reverse image search using Google Images [images.google.com](https://images.google.com) or TinEye [tineye.com](https://tineye.com). If the search produces several links to the same image, click on “view other sizes” to investigate further. Usually, the image with the highest resolution/size will be from the original source.
  - The Chrome browser extension “RevEye Reverse Image Search” allows you to search across five different reverse image search platforms.
  - Amnesty International USA has a tool for conducting a reverse image search on YouTube videos: [citizenevidence.amnestyusa.org](https://citizenevidence.amnestyusa.org). Look for the oldest thumbnail in the search results.
- A reverse image search can be conducted on a cropped section of an image.

You should also try to verify the credibility of the source. Checking all the details available on the profile/account that posted the content can help determine whether the account is real, and whether it is biased or has an agenda.

- Check the user history/activity: is there other content posted by the account holder, such as websites they have linked to, previous pictures and videos posted, previous status updates or tweets; do they have friends or followers, are they following other people?
- These might show whether it is a real account or not: a social media account that has only posted one piece of content (photo/video) is suspicious.
- Review other content from the same account for signs that the uploader comes from the location where the incident occurred. Look at the content, who they are friends with, who they are following and who is following them, what they “like”, retweet or share to see if they display signs of certain affiliations or agendas (political movements, parties to a conflict, and so on).
- Do a reverse image search (as above) on the profile photo of the account. This could lead you to other accounts created by the same individual as part of your verification of the source.



- If the description, tag or comment about a video or photo is in a foreign language, use Google Translate to help you.

### 3. Analyse the content

Careful content analysis is essential in confirming that the images show what they are labelled/claimed to be showing. This includes meticulously scanning an image for details; processes to try to confirm the location, time and date of the content; and cross-referencing with other sources.

Content analysis can provide incredibly important detail, for example about specific units of security forces involved in violations, specific individuals or ranks, weaponry used, identity of victims, and circumstances surrounding the violations. In conflict situations this can help to establish command responsibility for violations.

Content analysis can help to confirm the information extracted from the metadata about the date, time and location where the image/footage was taken. Where there is no metadata, content analysis might be able to provide this information.

If you suspect that pictures, videos or audio have been digitally altered, you need to consult digital forensic experts. Uncovering digital editing or manipulation is a highly technical process and involves specialist software.

#### Small details

- To carry out a thorough content analysis watch videos in slow motion, freezing frame by frame. This can help you to spot vital small details such as a number on a uniform or vehicle, a licence plate, road signs or other details that give clues about locations, perpetrators, and so on. Any (free) video editing software will allow you to watch in slow motion. YouTube videos can be watched in slow motion by changing the playback speed in Settings. This might also show you details that make you suspicious, or outright confirm that the images cannot come from the location or time they claim to be showing.
- Watch the footage again and listen carefully to the audio. Sometimes audio is added to a video that is not from the same recording. If you cannot clearly see the person speaking, ask yourself if you are sure the audio is original to (belongs to) the video. Sounds in footage can also give clues – spoken languages, weapon or artillery fire, traffic noises, sounds from nearby churches or mosques, and so on.

#### Confirming the location shown in a video or photo (geo-locating)

Use geo-locating to confirm the location shown in a photo/footage and specific features such as individual buildings or details of the landscape. This involves comparing the images with other images of the claimed or possible locations taken from ground level, as well as with satellite imagery from geo-spatial mapping sites or other satellite

imagery sites, to see if the details of the location shown in the photo/footage are corroborated by other images of the location where it is claimed the content originates from.

- Look for identifiable features in the image(s), such as street signs/names, identifiable buildings (different shapes/sizes), mosques or churches, school or shop names, landmarks, vegetation and features of the terrain.
- Using the location where it is claimed the footage was taken, or where you suspect it was taken, do an online search for other photos/footage and satellite imagery or street-view imagery available through online mapping platforms or applications such as Google Maps or Google Earth, Wikimapia or Open Street Map.
- A reverse image search (as mentioned above) – use part of the photo or a freeze frame from footage that shows a clear feature of a building or landscape and a reverse image search might reveal other images of that location – may be able to confirm where it is.

**Figure 6. Using satellite imagery to document the abduction of protesters in Sudan**



© BBC News. During an investigation into the abduction of protestors in Sudan in 2018/2019, the BBC compared on-the-ground footage from Khartoum with satellite images and was able to positively identify buildings based on shapes, features and surroundings. In this way the BBC was able to demonstrate multiple aspects of how abductions were being carried out, and by whom. Source: [bbc.com/news/av/world-africa-47216487](https://www.bbc.com/news/av/world-africa-47216487)

- Google Earth and Google Maps also allow you to change your viewpoint to look from street level. This might reveal further details about the location where a violation occurred. The street-view function on Google Maps gives highly detailed pictures of densely populated areas such as cities (click on the small person at the bottom right of the screen).
- Take screenshots of the matched locations on Google Earth or other sites. These can be a record of your verification process and can be used in your reporting to illustrate the match and confirm the location of the content.
- Note: this only works for videos shot outdoors. If a video is taken indoors (meaning you cannot see the weather, landscape or other geographical landmarks) and the metadata has been removed, it can be nearly impossible to verify the location of the footage.

### Confirming the date and time

It is more difficult to confirm the date and time than the location. Without reliable metadata, it can be very difficult to confirm the date and time a piece of footage or a photo was taken (unless the content directly shows this in a reliable way). However, there are some steps you can take to help.

- The weather in the images might give you an approximate indication of the date, and/or can provide information you can use to help verify that images were taken on the day claimed. You can check the weather on a particular date and location at [Wolframalpha.com](https://www.wolframalpha.com). Cross-reference that with the weather conditions you can see in the image to see if they are consistent.
- In some images, you might be able to determine the approximate time of day it was shot by the position of the sun or the shadows cast by the sun. The direction the shadows are falling in the image will tell you the approximate position of the sun. [Suncalc.net](https://www.suncalc.net) enables you to look at the position of the sun in any location at any given time. By cross-referencing this information with what you can see in the images, you can tell what date and time the sun would have been in the position that would have cast the shadows in the direction you can see them in the image. From this, you can tell the approximate time of day the image was taken.
- However, by far the best way to confirm the date is to find other material that corroborates the report of the incident on that date. For example, specific details in images can provide indications of the date and time, such as the fuel prices on a petrol station notice board.

### Identity of perpetrators

- Look out for specific (small) details in images and footage that can help in identifying perpetrators. This includes uniforms, flags, insignia, weapons,

vehicles, inventory or serial numbers (on weapons), munitions, license plates and clothing. These can be compared with publicly available images such as insignia on websites of military, security or police forces, or munitions imagery available on specialized databases and open source content. You may use reverse image searching again to find more information about such insignia.

- Also listen for language, dialect and slang words that might give clues to the identity of the perpetrators.

### Cross-referencing your findings

- Citizen media/user-generated content does not replace traditional forms of human rights investigations. **Information gathered from citizen media or user-generated content must be cross-referenced with first-hand source interviews, field visits and evidence collected through other methods**, both traditional and innovative. Citizen media can sometimes present direct evidence of a violation, but it rarely tells the full story of what happened in the incident(s), and whether it constituted a human rights violation. This is established by collecting and corroborating data using a variety of sources. For example, a video might show clear evidence of a violation, but corroborating sources are needed to establish the time and date of the incident, who were the survivors/victims and multiple other details. Traditional methods of investigating are often necessary to identify or interpret the full detail of what citizen media content shows.
- As with the other aspects of your investigation, all information seen or heard from online and user-generated content should also be cross-referenced with what you already know about the situation/context in which the violation is alleged to have taken place.
- Depending on the content of the image and the nature of the violation, you may want to consult with experts, such as forensic experts, weapons specialists, chemical or medical experts to verify that the content shows what it claims to show. For example, a weapons expert could identify weapons/munitions shown in images, or the type used by the damage shown or the direction they were fired from.

### Bringing it all together

The video in the link below shows an interesting example of how important details can be taken from footage (for example, the vehicle, uniforms identifying the perpetrators), and how taking details from photos, witness testimony, and other sources and cross-referencing them with satellite imagery can help to identify locations where violations have taken place: [bbc.com/news/av/world-africa-47216487](https://www.bbc.com/news/av/world-africa-47216487)

## Seeking permission

If you want to use user-generated content in your reporting, consider whether you need to ask permission from the creator/poster of the content.

When someone uploads a photograph or video to a social network, the copyright remains with the uploader. If you want to use the photo or video elsewhere, you have to seek permission. If you just want to embed the material (for example, include a YouTube video in your online version of a report) legally you do not need to seek permission. Ethically, however, it is good practice to seek permission from the copyright holder of images.

Originators might not want the content to be shared. They may have intended it for a particular community only, for example a Facebook group. They might have been somewhere they should not have been when they captured the footage, or do not want to be associated with allegations of human rights violations against powerful people.

The principles of informed consent, confidentiality and do no harm also apply to using online content: you must ensure you do not put the originator at risk of harm through your use of the footage.

When seeking permission:

- Consider whether the publication or broadcast of the content identifies the originator's location or any personal information that might cause them to be harmed or otherwise affected.
- Be transparent about how you intend to use the photo/footage, including how widely it will be available (for example, if you will put it online, embed it in a report, provide it to media outlets and so on).
- Is the source aware of how they might be affected by sharing this content even if you withhold their identity?
- If the originator gives permission, do they want to be credited (if so, how – name, username?) or remain anonymous? If the latter, be transparent when using the content that your organization does not own the copyright. The photo/footage can be credited to "© Private".
- Get permission in writing, preferably by email. If it is on a social media site, take a screenshot of the messages containing permission as these could subsequently be deleted.
- Ensure you have disguised any identifying traces (such as metadata) of the images before using them.

Asking for permission can also be part of making sure the content is from the original source. It also gives you the opportunity to possibly obtain further information from

that source about what they witnessed. Approach this carefully: the source may be in distress about what they witnessed, or have been directly affected by it.

- *See Annex 3 for more details on using this type of content, including ethical guidelines from [Witness.org](https://www.witness.org).*

# Chapter 9

## Verification and analysis

You must verify your information to ensure it is accurate before you make public any claims that human rights violations have occurred. Never publicize any information before you have verified it.

When you have verified your findings, you then need to analyse them. First, compare them against national and international legal frameworks to establish whether one or more human rights violations has taken place. If you are investigating multiple cases or documenting violations over a sustained period of time, you will also need to further analyse your findings to look for patterns and trends.

## 9.1 Verifying information

Verifying your information entails confirming details you can be certain of. Use the **three key criteria** presented below.

### 1. Consistency with other sources

Look at the consistency between the information you have collected from different sources (see Section 3.4) and the consistency of this incident with previous/similar incidents:

- Are details about what happened corroborated by different types of evidence and/or a variety of sources (to avoid bias)?
- Cross-reference the accounts from the first-hand sources you have interviewed. Are they consistent with each other on the details of what happened?
- Are sources that are independent of each other consistent in what they reported/showed? (For instance, they do not originate from connected persons, who may have influenced each other, and are not coordinated by one person – which may intentionally or unintentionally influence the findings.)
- Are the details consistent with other cases you know of or that have been reported by others (for example, have other people from the same political, ethnic, social group been targeted)?
- Are the testimonies of first-hand sources consistent with/supported by the documentary evidence you have collected and the physical evidence you have observed?
- Has expert assessment confirmed technical details in the information or examined the consistency of accounts/photos with what is known on the subject?
- Do not assume that a piece of information is correct just because it comes from a known/trusted source; people can make mistakes or may pass on inaccurate information from another source.
- If you are referencing secondary information, this also needs to be triangulated (checked) with other sources. Remember that even apparently reliable sources,



such as UN reports, get things wrong sometimes. Secondary sources such as media outlets can also be subject to bias.

- Does a source/account contradict other sources? If so, do you need further evidence?

## **2. Credibility of sources**

How credible is/are the source(s) of your information?

- How did the information come to you or how were you introduced to interviewees and other sources? Did these come from trusted contacts?
- Is there sufficient variation in the backgrounds and perspectives of your sources to eliminate the possibility that bias is influencing the findings?
- Is there sufficient gender balance among your sources to ensure that you have obtained information on any gendered differences in who the (alleged) violation affected and how it affected them?
- Is there any reason to suspect that a source has a personal or political agenda in giving you information?
- Remember that people who have suffered traumatic experiences might not be able to remember certain details, or may appear inconsistent. This does not mean they are unreliable.
- Think about where documentary evidence came from: how did your source obtain it? Have you verified the identity of sources who shared content online?
- Is documentary evidence (such as police, court, prison or medical records) consistent/does it look the same as other official documentation? Is it on headed paper, are the format and language similar? Can you cross-check the letterhead with other known official documents from that institution?

## **3. Consistency with the context**

- Is the information/picture of what occurred consistent with what you know about the situation?
- Do not make assumptions! If an alleged incident appears to fit with an existing pattern or what you already know about the context, that does not automatically mean it is true. Every incident needs to be thoroughly verified.
- Similarly, if an incident does not fit with a wider pattern, that does not mean it is not true. An incident may differ from an established pattern for a range of reasons. The divergence may itself be relevant: for example, certain individuals or groups may be subjected to different treatment for discriminatory, gender-based, political or other reasons.
- Are there established facts about places, events on certain dates/times, and so on that can be cross-referenced to check details against? Can you cross-reference

descriptions of locations with photos (online), mapping sites and satellite imagery of that location to confirm the details?

- Is there anything you know/have found out about the context in which an alleged incident took place that makes it unlikely the violation could have happened as described?

Investigations and findings are stronger if they combine a mix of sources (such as testimonial, physical and documentary evidence) that corroborate the incident to a certain level of detail. However, for some violations, only testimonial evidence will be available. Nevertheless, you can still verify information to a level of certainty, provided you have a sufficient number of interviewees, have collected sufficiently detailed accounts from them, the interviewees were independent of each other (that is, there is no possibility that they agreed beforehand on a version of the story), and the information they provided was consistent in specific details.

### **Drawing conclusions about your findings**

- Do a variety of sources and different types of evidence confirm the information to a detailed level?
- Do enough sources corroborate each other and with enough details for you to put together a picture of exactly what happened? (Who did what to whom, when, where, how and why?)
- Are there any gaps in your information, or anything that is inconsistent? Do you need to try to obtain other evidence that could confirm some of the missing details?

In any case, you must reach a preliminary conclusion regarding whether or not the facts of the case are proven or consistent. This allows you to determine whether to consider it for the rest of your work or leave it out of the process.

## **9.2 Analysing your findings**

After verifying the information that you have collected and establishing a picture of what occurred, you then need to analyse your findings. The first stage of analysis is consulting national and international legal frameworks in order to determine whether the incident constitutes a human rights violation.

- Search for all legal texts and instruments applicable to that right.
- You may also want to look at some of the General Comments written by the UN human rights treaty bodies on the main human rights conventions about the realization of that right in practice. These provide more detail on interpreting the treaty in question, for instance the Convention against Torture, and what protection/violation of the right means in practice.

Consider:

1. Aspects of the right affected: Who did what to whom, when, where, how and why? Detailed replies to these questions will point to the type of right affected, and what aspects of that right (content and scope) are most relevant to determine whether it could be a violation.
2. Sources: What are the sources of that right under national/international law (legal instruments and texts, including declarations and General Comments)? Return to point 1 to establish exactly which article(s) and phrase(s) are most likely violated, or what extra information you need to gather to establish if there is a violation. Cite the article(s) and phrase(s) in question.
3. Obligations: Who is the authority (namely government department or service) responsible? Does the authority (for example your government) have obligations under the relevant treaty? Or under national law or standards related to the treaty? What obligations have not been respected – such as the obligation to protect, respect, fulfil? Support your arguments based on concrete findings.
4. For some economic social and cultural rights, where a right is progressive (rather than immediate),<sup>2</sup> you will also need to look at:
  - 4a. Government resources/efforts/constraints: What efforts have the responsible authorities made to address the situation? Could they have done more?

If the incident was an abuse committed by a non-state actor:

  - 4b. Did the government/a government representative know about the abuse(s) and fail to act? Are there grounds to argue that the government should have known the abuse was occurring?
5. **Can you conclude that a human rights violation has occurred, stating what legal obligation has been violated, and by whom?**

National legislation that does not align with international standards:

When conducting your legal analysis, also consider whether any national legislation applied in the case(s) conforms with international laws and standards (such as anti-terrorism legislation, civil society legislation that restricts protected rights). Do you need to call for it to be reviewed/amended?

<sup>2</sup> For more information about (the progressive realization of) economic, social and cultural rights, see Haki Zetu, ESC rights in practice (Amnesty International, 2010): [amnesty.nl/actueel/haki-zetu-esc-rights-in-practice](https://www.amnesty.nl/actueel/haki-zetu-esc-rights-in-practice)

### **Inconclusive information**

In some cases, there will be sufficient evidence to draw firm conclusions. Often, however, it may not be possible to absolutely confirm the details or to draw definite conclusions. Use your judgement and a thorough assessment of the information you have. If there is strong evidence that a violation has taken place but not all the details could be verified, you can still report it, being clear and transparent that some of the information is unconfirmed or the evidence is not conclusive. You can use phrases such as “it appears that...” or “the evidence suggests that...” in your reporting.

### **Calling for further investigation**

Where your information shows strong indications that violations have occurred but it is inconclusive or information is missing, or if you believe that wider violations might be occurring, you can call for further investigations to be carried out by those who have the mandate (and resources) to do so. This would include government bodies, security forces oversight bodies, the national human rights commission or ombudsman’s office, and so on.

Where there is evidence of widespread and serious violations, or where the government has shown itself to be unable or unwilling to conduct thorough, impartial and credible investigations (or any investigations at all), you can call for an independent international investigation.

## **9.3 Storing and categorizing your findings**

Incidents and cases that you have concluded constitute human rights violations could then be entered into a secured database or other storage system (see Chapter 5) that enables you to both adequately search your information for future reference and to efficiently and effectively conduct further analysis of the data – particularly to look for patterns and trends in the occurrence of particular violations.

It is essential to take a systematic approach to recording and storing your information. This means you enter the same information for each case/incident in your record/storage system. This enables you to easily and logically search for information when you need it.

It also allows you to properly analyse large amounts of data (tens or even hundreds of cases) – namely, to review and analyse information across multiple cases according to specific details (variables) looking for patterns and similarities. This is extremely valuable if you are going to write a public report on the violations you have documented.

Take a systematic approach to storing your information. You will need to develop a standardized format in which you can enter the key details of every case/incident. This

might be in the form of a case sheet – a template document (for example in a Word document) with different categories for key pieces of information (see an example in Annex 6) – or directly in a database (for example, an Excel spreadsheet with columns for each category).

A case sheet or database contains a **summary** of information on the case/incident. It cannot contain all of the details or evidence, but will allow you to quickly find and sort information about the cases. If new information emerges or there is a new development in the case, the data record (database entry/case sheet) should be updated.

When preparing a case sheet or a database to file your information, think carefully about the key categories of information you need to include (see Table 3). However, avoid making it too complicated or it will be too difficult and time consuming to maintain the system.

- Adjust the categories accordingly to store information on specific violations.
- Ensure that robust digital security measures are in place, particularly if identifying details of victims/survivors are included.

**Table 3. Sample categories for a case sheet**

Categories	Examples	Remarks
<b>Case or incident identifier</b>	File name or file number	This should correspond to any hard copy or digital files of interview notes, notes from documenting physical evidence, documents, photos/footage collected and any other evidence relating to a case
	Date case information logged or updated	
<b>Details of case or incident</b>	Identity of victim	Age, gender and (if relevant) occupation, ethnicity, political affiliation
	Date and time of incident	Or different parts of incident where relevant
	Year of incident	Separating the year from the date enables easy extraction of all the incidents in one year
	Location of incident	Or different parts of incident

	Deaths/injuries/methods of torture used, alleged perpetrator, authorities' response	If relevant
Evidence collected	Number of interviews	And file numbers
	Types of documentary evidence	And file numbers
	Physical evidence observed/documented – yes/no, brief summary	And file numbers of notes

**Note:** You may also want to store unconfirmed/unverified information while your investigation is ongoing or when you are monitoring over a sustained period, or details about cases/incidents that you were not able to investigate or verify because of limited resources, access or other issues. If so, ensure that you **clearly categorize information that has not been verified**, or keep it in a separate log/database. This could include cases you register from media sources and those that are reported to you by contacts.

You can then state in any report that you write on specific issues that further cases have been reported though they could not be verified.

Some online platforms provide software for organizing your data, and some organizations can help you develop a comprehensive filing and recording system (such as HURIDOCs – [huridocs.org](http://huridocs.org)). Some of the software available from these organizations also allows you to convert your information into graphs and other formats to facilitate the identification – and illustration – of patterns and trends.

**Remember:** Ensuring that you have properly written up the notes of every interview to be a full and accurate summary of what was said is different from filling in a case sheet or database entry. Complete interview notes are essential in order to have an accurate record of what the interviewee said (even if you think you will remember, you won't!). A case record is a useful tool for analysing and reviewing your collective data (though it is not essential).

Storing all your verified data in a standardized format enables you to analyse information across cases and incidents to look for patterns in the details.

## 9.4 Identifying patterns in human rights violations

If you are investigating multiple cases of the same violation, either during a single investigation or when documenting recurrent violations over many years, analysing your findings will involve looking for patterns between cases – where one or more features are repeated across a number of incidents.

You should also watch out for emerging patterns while you are collecting information. Identifying patterns between multiple incidents can help prove that the incidents were human rights violations, rather than common crimes, as explained below. It can also sometimes help understand the “why” question of “who, what, when, where, how and why”.

### Identifying patterns can serve multiple purposes

Patterns in certain aspects of incidents might give you indications of **why the violation(s) happen**. For example, similarities in the profile of the survivors/victims among a number of cases might reveal the motivation for the incidents. In some cases, this could help to distinguish a human rights violation (by (or on behalf of) a state agent) from a common crime. For example, where a series of assaults are politically, rather than criminally, motivated. The absence of a pattern among victims, but a pattern in the perpetrator and/or location, could give another indication, for example, where multiple cases of torture are reported at one police station against victims of a range of profiles, but not at other police stations.

Establishing patterns in the identity of survivors/victims can also show how different **groups are affected differently** by the violation, or **identify discrimination**. For example, you may note that all survivors/victims are from a particular ethnic group, which can reveal a wider pattern of discrimination against that group. It can also help to inform your further investigations – for example, noting patterns in the ways women and girls and men and boys are affected differently by the violation will help to inform the planning and practice of your further investigation of gendered experiences.

Identifying patterns can help you **better explain the circumstances** in which some violations happen – that is, when and where it occurs, and why (for instance, if there is a particular trigger, it occurs in response to particular circumstances). This will help you to better predict and respond to the violation, and may inform your advocacy messages.

Identifying patterns can help **corroborate** information from other sources. New information can be compared with information from other cases to enhance the credibility of your findings.

Identifying patterns promptly can serve as a crucial “early warning” system to help **protect** at-risk individuals and groups. For example, if you establish that a pattern

in victims which shows that union leaders in region X are being specifically targeted (suggesting that a particular group is at risk), you might be able to take urgent action – for example, warn other union leaders or organize protection for them. This can be done by demanding protection from government bodies, informing the media, raising public attention and/or moving potential targets to safe houses.

Identifying patterns is particularly important if they might indicate that **widespread or systematic human rights violations are taking place**, which could amount to crimes against humanity in relation to some violations, in conjunction with the other criteria, as explained in Section 2.1. Examine the cases/incidents that you have verified (and stored in your record system), and look for repetition in the key indicators – that is, location, perpetrator, and so on (Table 4).

**Table 4. Key details of incidents/cases in which you might identify patterns**

Characteristic	Look for patterns
1. Identity of survivors/victims	<p><b>Do the survivors/victims have common characteristics, such as:</b></p> <ul style="list-style-type: none"> <li>• ethnicity, religious background, sexual orientation, gender, age group, professional occupation/activities, political affiliation or activities, refugees or IDPs, known/suspected membership of armed groups, residents of specific areas, class/economic status, disability, suspected criminals, and so on</li> </ul>
2. Identity of perpetrator(s)	<p><b>Do the perpetrators have common characteristics, such as:</b></p> <ul style="list-style-type: none"> <li>• same uniforms/fatigues/civilian clothing, headbands, tattoos, carrying same weapons, using same vehicles, speaking a certain language/dialect</li> <li>• belong to a specific branch/unit of security forces, from a particular police station, prison guards, militia, paramilitary or insurgent group (if you are able to identify the specific unit/entity)</li> <li>• specific rank(s), specific commanders in charge</li> <li>• chain of command: who gave the orders – at the scene or in advance? (This could include oral or written orders from superior officers within the security forces or from political or religious leaders.)</li> </ul>



<b>3. Methods used in committing violation(s)</b>	<p><b>Are the same methods used in committing violations, such as:</b></p> <ul style="list-style-type: none"> <li>• methods/instruments of killings or torture: type of weapon used, specific instrument or method used to kill, methods/instruments of torture, specific restraining techniques, forms of sexual violence, mutilation, same part of the body targeted (such as gunshot to the head, hands cut off), use of heavy weaponry, drone attacks</li> <li>• timing of incidents, such as abduction during the night; methods during incidents, such as violence used during arrests, intimidation and/or death threats received; number of perpetrators involved/roles taken</li> </ul>
<b>4. Location</b>	<p><b>Are the violations taking place in specific areas, such as:</b></p> <ul style="list-style-type: none"> <li>• specific regions, cities, neighbourhoods, localities, detention centres, informal settlements, IDP/refugee camps, checkpoints or border crossings</li> <li>• areas predominantly inhabited by a specific ethnic, religious, political or other group; areas where government bodies are under/overrepresented, and so on</li> </ul>
<b>5. Reasons given/indicated</b>	<p><b>Did the perpetrators give similar reasons for the violation?</b></p> <ul style="list-style-type: none"> <li>• similar statements made at the time of the violation (for example, during arrest, torture, evictions), certain language used (could show common orders, common motivation of the violation/its intended purpose or impact, and so on)</li> <li>• same warnings/threats made (for example, refraining from political activity)</li> </ul> <p>Note: patterns in the identity of the victims/ those targeted are often key indications of why a violation took place (the motivation). Patterns in the reasons indicated should align with those related to the victims' identity.</p>

6. Specific context	<p><b>Are there similarities in the specific context surrounding the violations, including circumstances preceding or following violations?</b></p> <ul style="list-style-type: none"> <li>• for example, before or after elections, demonstrations/protests, introduction of new legislation, declaration of a state of emergency, internal/international armed conflict, military operations/reprisals, counter-terrorism operations, curfew in place, in long-term detention, in incommunicado detention</li> </ul>
7. Reactions of government authorities	<p><b>Are there similarities in the way the government/armed group responds to allegations of violations, such as:</b></p> <ul style="list-style-type: none"> <li>• similarities in statements made in response to allegations of violations occurring/treatment of victims making complaints</li> <li>• official investigations or lack thereof, similarities in investigations (who carries it out, how thorough, failure to respond to requests about victim's whereabouts, denial, evasions, justifications given, absence of prosecutions or the conformity of prosecutions with international standards (such as intimidation of witnesses), courts responsible for prosecution (military/civilian), absence or nature of the verdict, and so on)</li> </ul>

When reviewing your data from a number of cases and/or a number of months or years, **look out for exceptions to patterns**. For example, reviewing your database of cases involving extrajudicial killings during military operations in the country over the last 5 years may show that there has been an overall decrease in the number of incidents. However, during the same period, the rate of extrajudicial killings during military operations may have increased in one particular region, and decreased in all other regions.

**Do not assume a violation is part of a pattern without confirming the details.** For example, if someone has been killed in an area where a number of extrajudicial killings have taken place, do not assume this death belongs to the same pattern. Investigate the method of killing, the identity of the victim, the circumstances in which the killing took place, and so on, as you would when investigating all other violations. Do the details fit

with what you know already of the pattern? Just as importantly, consider whether there are any details that do not fit with the pattern and indicate that something different took place here.

Do not extrapolate wider patterns than the data show. Remember that the data might relate to a very specific set of circumstances and targets within a given context.

#### Box 18. Patterns that data does and does not show you – example

You have interviewed X number of former detainees about their treatment in detention in a particular detention centre. All the interviewees (who were arrested in relation to the same incident – a peaceful protest) reported that they were tortured using the same methods. They all said that this occurred in the morning, every day during the first week of detention while they were interrogated but ceased after that.

The consistency of the details is important in establishing the reliability of the individual accounts. The consistency across a number of cases also shows a pattern of the use of torture. The pattern indicates that the torture was motivated by a desire to silence protest.

Other prisoners may not be tortured – that is, the pattern **does not show** a) whether or not torture is used against all prisoners in that detention centre/more widely, or b) whether torture is used in *all politically motivated detention cases* in that detention centre/more widely.

The government or security forces may have been acting against that particular protest movement. Torture may have been used against those detainees in order to intimidate, interrogate or obtain additional names, but may not be used against detainees or prisoners arrested or convicted of a (common) crime. You can develop theories from your data, but these need to be tested to see if they are proven or not.

If you want to investigate whether torture is used more widely against political prisoners/during politically motivated detentions (in other cases and in other detention centres), then you will need to identify and interview people formerly detained for political reasons in the same and in other detention centres. (Or those currently detained, if you can get access to detention centres.)

If you want to look at the possibility that torture is used more widely/systematically in that particular detention centre, you will need to identify and interview former detainees who were detained/imprisoned for a range of alleged or actual offences. (Or again, current detainees if you can get access to the detention centre.)

Interviewing former detainees and prisoners held over a wider time period (political prisoners and prisoners convicted of criminal offences) could also help to establish whether there were any trends in the frequency of torture use (and why). For example, there may have been an increase in the use of torture, which coincided with the arrival of a new commander at a particular detention centre.

### Identifying trends

Continuously monitoring the human rights situation in a region/country, and systematically storing information and reviewing the data over extended periods of time, might help you identify long-term patterns or **detect changes in violations and patterns of violations (namely, trends)**. For example, you may identify trends in the frequency/location of a violation (where a violation that was recurrent in one region ceases there, but may increase in another region) or trends in types of violations (for example, a decrease in the occurrence of a particular violation over a certain time period).

**Analysing the overall situation and identifying trends:** Establishing a pattern in a type of violation will increase your awareness of changes in the pattern – for example when incidents change or increase/decrease in frequency.

Monitoring and documenting information on a certain violation over a period of time can reveal important trends in frequency – for example, you might note that the number of incidents per week or per month has increased or decreased over a certain period. More widely, if you are monitoring the country's general human rights situation over a sustained period, you might see trends in the type of violations reported.

**Do not make assumptions about the reason for a trend without verifying the cause.** For example, if the number of reported incidents of sexual violence by the military has decreased, that does not necessarily mean the actual number of incidents has decreased. Reporting rates could have gone down because reprisals for reporting have increased, and so on.

When a trend has been identified, you might want to **look at contextual information to see if additional dynamics have contributed to the change**. For example, a drop or rise in extrajudicial executions might come shortly after a political change, or an increase in military operations targeting civilians in region X may follow a change in the commander of the military stationed in that region.

# Chapter 10

## Report writing

Human rights reports are used to present the findings of investigations to external audiences of specific stakeholders, such as governments, international bodies and/or the wider public. Reports can also be for internal use. The purpose of reporting is to provide and expose detailed information on human rights violations in order to inform the various audiences of what is occurring and advocate changes in policies or practice.

Some external reports might be confidential, such as those that will only be shared with specific UN offices or certain governments.

A report might cover a single incident involving one or more cases of a violation – for example, an individual case of arbitrary detention or enforced disappearance, or a forced eviction involving many families. Reports may also cover multiple violations occurring in one context – for example, the use of torture and the detention conditions in one prison, or multiple cases of a certain violation in a pattern, such as sexual violence against civilians during an armed conflict.

### 10.1 Guiding principles

There are **two fundamental principles of any report-writing process – accuracy and confidentiality.**

**Accuracy** is vital to the credibility of your report and your reputation. As discussed in Chapters 1 and 9, the accuracy of your report depends on robust verification and analysis of your findings. Thus you must invest time to verify and corroborate information across multiple sources. This may mean:

- Interviewing and re-interviewing the same or other sources: accuracy must never be sacrificed for speed of reporting.
- Being able to reference specific provisions of national or international law to show what right has been violated.

Accuracy also requires you to:

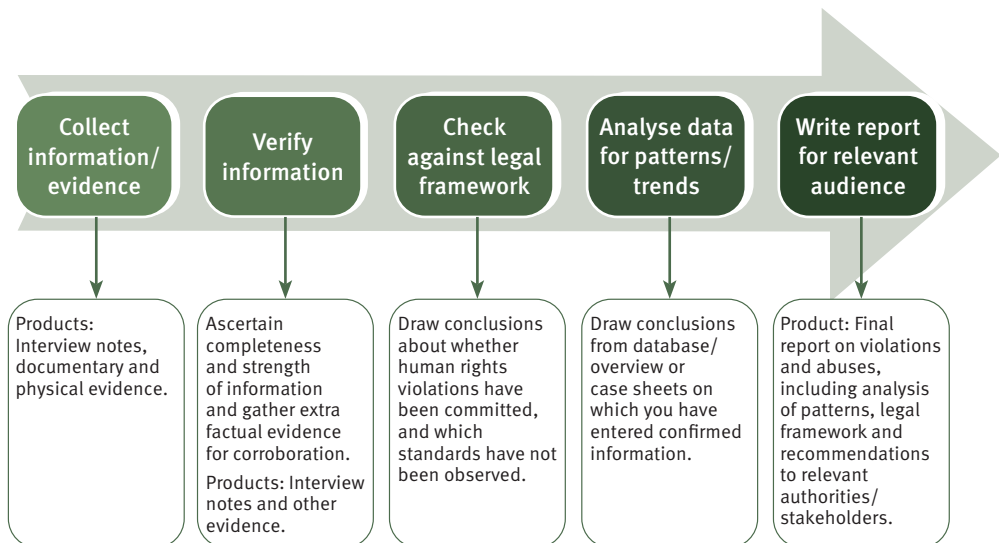
- Use language cautiously in cases of uncertainty. For example, you can use words such as “allegedly” or “reportedly” to qualify a statement without presenting it as fact – such as “two detainees have allegedly been tortured”. This signals that the torture of two detainees “allegedly” happened but could (yet) not be corroborated. You can also use a phrase such as “it has not possible to verify this information”. Note that the cautious use of language is never a substitute for pursuing the facts, obtaining first-hand information and double-checking that information with different, unrelated sources.
- Use technical terminology carefully. For example, “enforced disappearances”, not “forced disappearances”. Ensure all dates, locations and numbers are correct.

The **confidentiality** of your sources is paramount and must be securely protected. Breaching confidentiality, as discussed in Chapter 1, can put your sources at serious risk of harm, and will undermine people’s confidence in your work and other human rights work in the future.

- Do not use your interviewees’/sources’ personal details including, names, address, age, date of birth and profession.
- If sources have specified that certain details of their testimony may not be used publicly, you must respect that. This information can be used to inform your findings and conclusions without being included directly.
- When providing a citation for testimonial sources in the report or in footnotes (for example, “Interview with... (insert pseudonym/or gender of interviewee), ... (age), ... (location of interview), ... (date of interview)”, it might be necessary to withhold some of those details if it would make it possible to identify the source – for example if specifying the interview location would risk revealing the source. You can state, for example, “location of interview withheld for security reasons”.

## 10.2 Report content

### What to report



After analysing your findings as explained in Chapter 9, you should have a clear picture of what human rights violations have occurred (if any), and if there is a pattern across multiple violations in relation to one or more aspects. Writing up the key details of each case/incident on a case sheet or database entry should have given you a good summary of the case, including what evidence contributes to that picture.

To begin the process of writing a report on your findings:

- Draft an outline of your findings as the starting point for a report (public or non-public). What violation(s) do you want to report? What are the different aspects that you need to explain or describe in the report?
  - Write a list of headings that reference the different violations that have been committed, various aspects of the violations/circumstances, or different phases in a specific crisis situation to help to give the reader a clear picture of what happened, and in what circumstances.
  - If you have reviewed case sheets or database entries for patterns, write a summary of the pattern. What is the pattern (between what aspect of incidents – perpetrator, location, methods, and so on)? How many cases have you investigated that demonstrate features of the pattern? Do some cases exhibit some aspects of the pattern but differ in other respects?
- To help you organize your findings and your information before starting to write your report, you might want to write a summary in two columns detailing each violation/aspect of the violation you need to cover in your report and the evidence to refer to, and possibly cite, in writing about each section:

For example:

<b>Detention</b>	<ul style="list-style-type: none"> <li>• 19 interviews (Interview/file numbers x, x, x...)</li> <li>• Photos of outside of detention centre x</li> <li>• Screenshots from Google Earth</li> </ul>
<b>Torture</b>	<ul style="list-style-type: none"> <li>• 11 interviews (Interview/file numbers x, x, x...)</li> <li>• Photos of interviewees (Interview/file numbers x, x, x...)</li> <li>• Expert testimony from Dr X...</li> </ul>
<b>Death in custody</b>	<ul style="list-style-type: none"> <li>• 3 interviews (Interview/file numbers x, x, x...)</li> </ul>

### Presenting your findings

- Present your findings clearly, laying out what happened and clearly stating what human rights violations or abuses were committed.
- As much as possible, your report should cover the central questions: who did what to whom, when, where, how and why, though it might not always be possible to answer all of these questions. The “why” in particular might not be clear.
- As above, always include the specific details of your legal analysis:
  - State exactly what human rights violation(s) has been committed by whom, in



violation of which national or international legal instrument. At the beginning or end of each section or chapter addressing a different violation or aspect of the violation, specify the relevant provisions of international, regional or national law that it violates. You might also want to include a general legal section at the front of the report that lays out all the relevant provisions of national and international law.

- If national-level legislation applied in the case(s) does not conform with international human rights obligations (for example if it restricts internationally guaranteed rights), note the specific provisions of national law and the relevant provisions of international law that they infringe upon.
- How you present the findings might depend on what you are reporting. Generally, it works well to present the findings thematically.
- Before presenting your detailed findings and analysis, provide an overview of the incident(s) or the context in which the violations occurred. Provide sufficient background information or detail of the wider context that it can be understood by a reader with no prior knowledge of the situation.
- If you are writing about more than one violation, separate them into different headings or chapters.
- Make sure you explain the context in which violations occurred – for example, if reporting on torture, contextual information (the circumstances leading up to the incident) is very important to understanding the circumstances in which the violation took place.
  - If you are writing about torture and conditions in a detention centre, you might organize your findings under headings covering: general details of the detention centre (location, size, layout, number of prisoners, and so on), circumstances of torture (for example, during interrogation, patterns in usage), methods of torture, conditions (cells, sleeping conditions, food, sanitation conditions, and so on), other issues (for example, access to healthcare).
  - Write about the main concern first (for example, torture), and then related concerns or violations.
  - For a complex violation such as enforced disappearances involving a number of different components, it might be helpful to organize your findings according to different stages of the violation: abductions, detention, torture, killings, releases, and so on, in the order in which they occurred (chronologically).
- If your report covers multiple cases and includes a range of violations and details, specify in how many cases each aspect was reported.
  - For example, in writing a report about torture, state at the beginning of the chapter/report that several different methods were reported in one or more detention centre (or other location). When you name the different methods,

specify how many people reported each, for example, “Eight former detainees said they were subjected to mock drowning during interrogation...” or “Twenty-seven former detainees reported that they were beaten on the soles of their feet”.

- If you are reporting on forced evictions, write how many people/families were affected; of those, how many lost livelihoods as well as homes in the evictions; how many people reported violence, and so on.
- Provide examples from the cases you have documented, but conceal any identifying details of the victim. For example, “In one case documented by our organization...” or “A 48-year-old woman reported...”
- Findings can also be organized by survivor/victim group, by alleged perpetrator, by geographic region/area, or by time period, depending on the information.
- Add testimonies as direct quote in the report: it is important to highlight (strong) testimonies or to bring in some quotes. This gives a human face to the report and to the work as a whole.

### Language, tone and style

- Use impartial and neutral language; avoid emotive or dramatic language, an angry tone or judgement when describing events and persons involved, which would affect the report’s credibility and may show a lack of impartiality.
- Write a neutral account describing the specific incidents and details of exactly what happened.
- Do not write “he was very brutally tortured”, which is emotive but also unclear on what actually happened. Instead write, for example, “X said that during three hours of interrogation, he was subjected to multiple different methods of torture, including being beaten repeatedly on the soles of his feet, burnt with cigarette butts, and had electric shocks applied to several parts of his body including his genitals.”
- Use language that is suitable for your target audience, clear and easy to read. Avoid overly technical language or academic style language if you are writing for a general public audience, but do not use informal language. This can make your report and findings seem less credible.
- Think about what spoken language your key target audiences speak. A country’s first language is generally spoken by the middle and upper class, while local languages are often spoken by most of the population, including communities in rural areas. Publishing reports in languages not spoken by affected communities can exclude them. If possible, translate reports into the most relevant languages for the different stakeholder groups.
- Be consistent in how you present and/or spell the names of locations and

persons, terminology and analysis throughout the report. If certain terms are used inconsistently, or spellings are inconsistent, the report may be perceived as sloppy or inaccurate.

- Cite information or quotes from testimonies and sources in footnotes or end notes to bolster the credibility of your findings. But do not use the source's name unless it would not put them at any risk. Use initials or pseudonyms, or "name withheld for security reasons" depending on confidentiality and security considerations. If the information came from an interview, include the date and location of the interview unless it is necessary to withhold that information for security reasons.

### Use of quotes

Testimonies of survivors, victims and witnesses can be used to illustrate the issues covered in the report and provide personal, first-hand accounts of the experience and impact of the violations discussed. First-hand descriptions can be a very powerful way of communicating the issues, and will often make the report more interesting for the reader.

- Make sure you quote exactly what the interviewee said. If you need to insert a word to clarify the meaning of a sentence, use square brackets [...] to indicate that this is your insertion. For example, the interviewee was talking about a police raid on her house and had mentioned the police earlier in the interview and said "They came to the house first thing in the morning, when I was making breakfast for my children." If necessary for clarity in your report, you can write "They [the police] came to the house first thing in the morning..."
- A quote must repeat exactly what the interviewee said, so record quotes properly during your interviews. For example, when an interviewee says an interesting sentence you think might make a good quote to illustrate a point/issue, make sure you write it down accurately; you might want to mark it in your notes (for example, with a "Q" in the margin) to find it easily later. If you made an audio recording of the interview, it will be easier to write exact quotes.
- You can use an ellipsis (...) to connect two parts of a quote while missing out a section of speech in the middle. An ellipsis indicates that a section has been removed.

### Use of photos/pictures

Photos can help give the reader a further picture or understanding of issues referenced in the report, including damage to bodies, homes, landscapes, types of weapons and even images of violations taking place.

- As covered in Chapter 8, **before and after** photos (including satellite photos) might constitute a key piece of evidence – for example, showing the destruction

of homes, villages or crops. They can also demonstrate the approximate or exact date the destruction happened as well as the scale of the destruction.

- Confidentiality protections and the informed consent of persons shown in the photos are essential. You must ensure that survivors, victims, witnesses and sources cannot be recognized in any photos you use publicly. You may be able to obscure faces using an edit function if it is a digital photo. If so, ensure there is nothing else identifiable in the image (such as ID cards, car registration numbers, uniforms).
- Do not show anyone's face unless the case is already highly publicized (for example, a journalist has been arrested and many new reports have already covered the case including photographs of them).
- Similarly, do not use images that show details that could identify the source/people related to the image, such as people's homes or workplaces.
- Images of body parts can be used where the person's face and any identifiable features are obscured. For example, images of parts of a victim's body showing scarring from torture methods, from which it would not be possible to identify the individual.
- You must have the permission of the person in question to use the image publicly. This should have been obtained through informed consent when you took the photo, with explicit agreement on the part of the individual about how the image can be used.
- It may also be possible to use a photo showing victims or others from behind, which may still be interesting to include.

When using photos from other sources (such as images you did not take yourself or receive from an interviewee/source), be careful about the copyright of images. Make sure you have the correct permissions from the owner/originator of an image before you use it in a public report, or you may be subject to legal action.

### General points

- Never publicize an image if you have not verified the content (as explained in Chapter 9). Be certain that the image shows what you are reporting it shows and was taken on the date/at the location you are reporting.
- Include a brief description of what each image shows (in a caption below the image).
- Include a copyright reference for each image: this states who owns the rights to the image, including whether it is you or your organization. Use © Private if the confidentiality of the source needs to be protected.
- With images of dead bodies, consider the dignity of the deceased person before deciding whether to publish.

- Be cautious about using graphic or disturbing images, such as executions, injured people or dead bodies. These might be important evidence and illustrate the extent of the violations, but some people might consider them inappropriate and they may deter some readers from continuing to read the report.

### **Drafting recommendations**

Reports will usually include recommendations for state(s) or non-state actors implicated in the findings, and for other relevant stakeholders.

- Recommendations need to be specific, actionable and targeted: be clear about what you are asking to be done, by whom and in what time frame.
- Draw on what the legal framework (national and international) says about the right in question and reference the legal obligations of the alleged perpetrators.
- Be realistic about what is achievable.
- Recommendations should include short- and medium-term actions, namely specific actions that are possible to implement in the short and medium term that will work towards the necessary long-term change (for example, an end to the violation, better protection and respect for the right in question).
- Think about the different actors who are relevant to achieving that change – all those who have a mandate relevant to the right in question, national bodies and the international community.
- Wherever possible, be clear about (and name) the part of the government that has the authority/responsibility over the issues in question, rather than directing your recommendations to “the Government”.
- Group recommendations to different targets separately. For example, “To the Minister of Justice... (recommendations a, b, c); To the Director General of the Police Service... (recommendations a, b, c); “To the international community...”
- Limit the number of recommendations to the most important priorities. With bigger, long-term goals, focus on specific short- and medium-term steps that should be taken. (You can also reference the long-term change that is the objective of those more immediate steps.)

### **Structure of reports**

The structure and content of each human rights report might vary depending on the target audience, the issues discussed, the objective or other factors. Table 5 presents an example of a possible structure and the purpose of each section.

**Table 5. Outline of a human rights report**

<b>Title page</b>	<ul style="list-style-type: none"> <li>• Title of the report (quotes can be attractive titles that grab the attention of the target audience and preview the report's content).</li> <li>• The name of the organization/authors (if including), date of publication, and so on.</li> </ul>
<b>Table of contents</b>	Provides an overview of the structure of the report.
<b>Executive summary</b>	An executive summary can be very useful, especially as a standalone document, for example for advocacy purposes. At a minimum, it should contain a brief overview of the key findings and the main recommendations. It can also include a limited number of sub-headings reflecting the key areas of the contents.
<b>Introduction (optional)</b>	Introduces the objective of the report and the main human rights issues. It may also describe the organization and recognize/acknowledge the authors and other contributors to the report such as survivors, victims and witnesses for sharing their stories (while bearing in mind the “do no harm” principle). Some reports will not have an introduction, but a background section only.
<b>Methodology</b>	<p>Describing your methodology enhances the report's credibility. It explains how you collected and analysed your information and reached your findings (from what types of sources, information collection methods used, when and where).</p> <ul style="list-style-type: none"> <li>• Dates the research took place.</li> <li>• Location(s)/areas visited to conduct interviews and examine physical evidence. Do not specify what was done in each place if revealing this information may pose a risk to sources.</li> <li>• Number of investigators involved.</li> <li>• Selection of interviewees.</li> <li>• Number of interviews, and breakdown of demographic details: age, sex/gender, nationality/ethnicity (if relevant), format (online or face to face).</li> </ul>

	<ul style="list-style-type: none"> <li>• Languages used for interviews and use of interpreter (if so, how many).</li> <li>• Other methods of information collection: for example, focus group discussions (how many, demographic details of participants); commissioned satellite images, commissioned expert reports; online research; desk research (list types of sources such as government reports, academic sources).</li> <li>• Use of pseudonyms for security reasons.</li> <li>• Interviews with other stakeholders (government official, NGO staff, and so on).</li> <li>• Efforts to interview/request response from the authorities in question (right to respond).</li> <li>• Challenges or limitations encountered during the research (for example, denial of access to certain research locations).</li> </ul>
<b>Context/background (optional)</b>	A description of the relevant political, historical, cultural, or economic context and circumstances in the country and/or region.
<b>Legal framework</b>	A brief overview of what the relevant provisions of national, regional and international legal frameworks say in relation to the human rights issues covered in the report and the legal obligations of the relevant duty bearers.
<b>Findings</b>	<ul style="list-style-type: none"> <li>• Detailed account of what happened in an incident or series of incidents that constitute human rights violations. The more detailed the account (providing they have been properly verified), the more credible the findings are.</li> <li>• Findings cover the central questions of who did what to whom, when, where, how and why.</li> <li>• They will usually be organized under thematic chapters or sub-headings to explain the different violations that occurred within the context, or the different stages of the violation, and/or other details of the context that are relevant to how and why the violations occurred.</li> <li>• Findings will specifically identify the different areas of national, regional and international</li> </ul>

	<p>law that have been violated, and how they have been violated, specifying the responsibilities of various actors.</p> <ul style="list-style-type: none"> <li>• Findings might also show patterns in violations.</li> </ul>
<b>Measures taken by the government or other relevant stakeholders</b>	<ul style="list-style-type: none"> <li>• Outline of the (positive and negative) steps that have been taken by the government or other relevant stakeholders to address the human rights issues mentioned in the report, when applicable.</li> <li>• For example, if an investigation was conducted, describe when, where, by whom, findings/ outcomes and concerns/shortcomings.</li> <li>• If a response was sought/received from the government, provide details.</li> </ul>
<b>Recommendation(s)</b>	<p>Clear, specific and targeted recommendations of actions that need to be taken by duty bearers and other parties that have influence over the situation.</p> <p>Recommendations name the different parties addressed and make clear what needs to be done by whom (having confirmed that party has the responsibility/mandate to take the needed action).</p> <p>Recommendations are action oriented, limited in number, have a short- or medium-term focus, and should be achievable.</p>
<b>Conclusion(s) (optional)</b>	<p>Conclusions drawn based on the analysis of the findings. Do not include new information in this section.</p> <p>Depending on how you have presented the information, a conclusion might not be necessary.</p>
<b>Annexes</b>	<p>If relevant, may include photographs, tables with statistical data, maps, sketches of incident sites, chronology of events, official government response to the findings.</p>



### 10.3 When to publish your report, and seeking a government response

- The timing of going public with the report should be considered carefully, as much in advance as possible. The timing of publication can influence how much attention, media coverage and/or impact your report has, including in gaining access to discuss your findings with key decision makers.
- If it is safe to do so, you might want to present the government with a summary of the report's findings – possibly the Executive Summary – before you publish it, and give them sufficient time to respond. (Do not do this if you believe it would put you or your organization at risk.) Send the summary with an official letter welcoming a response and any additional or counter data the government might want to provide.
- Be sure the situation has not changed since your investigation. Before publishing, check the information is still relevant.
- If something relevant occurs shortly before publication, for example the government releases the findings of an investigation into the issues, you could use an addendum to acknowledge this and add an analysis of the outcome without having to change the main findings of the report.
- If a situation is urgent, never go public at the expense of the report's or statement's accuracy and quality.
- When less urgent, going public might be most impactful when the release of the report coincides with relevant national or international events – for example, at a time relevant to an ongoing debate about a change to policy or legislation, or to coincide with a conference related to the issue(s) addressed in the report.
- Certain dates can make good hooks to gain increased media attention for your report – for example, the International Day of the Disappeared if you are writing about enforced disappearances. Conversely, if big unrelated events are happening on or around the publication date, this can significantly detract from the attention given to your report. This may be unavoidable: sudden national or international news unrelated to the report's focus may make headlines around the same time as its publication.

# Chapter 11

**Stress, trauma and burnout:  
managing the well-being of  
human rights investigators**

Human rights investigators frequently operate in difficult, insecure and volatile environments. Conducting investigations regularly involves witnessing or listening to accounts of human rights violations. Investigators are also often exposed to the mental, emotional or physical distress of other people. Further, the recent increase of citizen media means that human rights investigators are witnessing violations even more frequently through footage and photographs shared online.

Investigators frequently feel responsible for those affected by the violations they are documenting. This can be exacerbated by feelings of an inability to help or make a difference, or frustration with the seeming inactivity or apathy of those in a position to help or have a positive impact on the issue.

Investigators may also be the victims of violations themselves, or have to take constant precautions because their life, and/or the lives of family members or friends, are at risk. They may experience suspicion, surveillance or harassment from authorities. Many work in high-risk situations such as conflict-affected areas.

Long-term exposure to human rights violations, traumatic situations and distressed people, along with high levels of work pressure, can severely affect your mental health and well-being. Human rights investigators are often affected by conditions such as vicarious trauma, chronic stress, burnout and depression.

Negative impacts of these conditions can affect investigators professionally and personally. They can have a serious impact on the way you feel, think, behave and on your physical health, and can also have a significant impact on your family. They can result in diminished empathy, interest or even lead to irritation with survivors and victims, and an inability to use judgement and make sensible, informed decisions. This can affect your (and other people's) security and the credibility of your data collection.

You must be aware of the effect the work can have on your mental health and well-being and on that of your colleagues, and the effect that the symptoms of stress and trauma-related conditions can have on your work. It is also essential that organizations and managers take responsibility for the mental and emotional well-being of their staff.

**Mental health and well-being risks and symptoms must be anticipated, managed and responded to in the same way as all other risks to the safety and security of human rights investigators** (as covered in *Chapter 4: Security planning*). Steps should be taken to reduce the likelihood that the risk will materialize, and to minimize the impact if it does occur, and measures should be put in place in advance to respond to such risks if they do arise.

These conditions, especially the most severe ones, need to be properly diagnosed and treated by professionals. However, it is important to understand how they can affect you and your colleagues, how to reduce their likelihood/impact, and how to respond to them appropriately if they do occur. As a first step, investigators should be able to recognize the symptoms of stress, burnout, depression, trauma, vicarious trauma and post-traumatic stress disorder (PTSD).

### 11.1 Identifying conditions and recognizing symptoms

#### Severe or chronic stress

Chronic stress can be caused by work or emotional pressure experienced over a prolonged period of time. In human rights work this can result from dealing with persistently demanding workloads, working long hours, emotional pressures of the work, and feelings of responsibility towards survivors, victims and their families. An individual's level of stress depends on the pressure (perceived or actual) they experience and their ability to cope with it.

Stress-related symptoms generally fall into the following categories:

- Cognitive: memory or concentration problems, constantly worrying about the workload.
- Psychological (or emotional): including depression, anger, anxiety, panic attacks, guilt, feeling overwhelmed / unable to cope.
- Physical: such as tension or pain in parts of the body (shoulders or stomach are common), nausea, diarrhoea or constipation, indigestion or headaches.
- Behavioural: such as insomnia, passive, withdrawn or aggressive behaviour, conflictive relationships with colleagues, irritability or outbursts of violence directed at family members, alcohol or drug abuse.

#### Burnout

When a high level of stress is sustained over a prolonged period, and is accompanied by a perceived inability to cope with certain pressures, this can lead to burnout – a condition of emotional, mental and physical exhaustion. Burnout is often experienced by people who work long hours in a highly stressful environment, have an overwhelming workload, experience prolonged frustration, work in situations where their safety is regularly at risk, and whose work is emotionally demanding. It can also result from, or be exacerbated by, having inadequate support and supervision in the work.

Burnout develops over time and is cumulative. It can result in:

- Severe reduction in professional motivation, in seeing any point in continuing with the work you are doing, and a decline in productivity and in your interest in discussing and collaborating with colleagues.

- Negative attitudes about the people you work with (survivors, victims and their families), such as a loss of concern or empathy, or feeling unable to give as much emotionally.
- A reduction in self-esteem, feeling you are being ineffective, overwhelmed by the stress of the job, or other negative self-perception.

## Depression

Depression is a mood disorder that can result from (long-term) exposure to stress or stressful situations, or because of a traumatic or emotional experience. It is generally characterized by feelings of sadness, dejection or hopelessness, social isolation, diminished motivation in work, concentration issues, decreased enjoyment in things, inactivity, chronic tiredness, increased irritability and a general feeling of being unwell, among other symptoms.

## Trauma

Trauma is longer-term psychological distress resulting from experiencing or witnessing extreme fear, horror, distress or physical pain. Traumatic events are often accompanied by a sense of powerlessness and loss of control. When people experience trauma, their capacity to process and cope with what they saw or experienced may be overwhelmed and their ability to manage daily life activities may be compromised.

Human rights investigators might experience or witness traumatic events directly and experience (direct) trauma as a result. They might also be affected by vicarious trauma as a result of their work.

## Vicarious trauma

Vicarious trauma can result from cumulative exposure to the pain of others. This means that you **can develop symptoms of trauma even if you do not directly witness or experience a traumatic event yourself**. This results from continuous exposure to situations of violations and violence, listening to the stories of survivors and victims, watching footage or looking at photos of violations, reading medical reports of torture, responding to the aftermath of violence and deaths, and similar activities.

People affected by vicarious trauma often experience a change in their world view, which can lead them to become either more cynical or fearful, or more appreciative of what they have.

Symptoms of vicarious trauma can include:

- Avoidance: of memories, feelings, people, places, conversations, work, interactions with survivors, victims;
- Social isolation, relationship problems: withdrawing from friends and family, increased interpersonal conflicts, avoiding intimacy, decreased participation in

activities that used to be enjoyable;

- Cognitions/moods: negative beliefs/thoughts/moods, blame, inability to feel pleasure in normally pleasurable activities, detachment, loss of sense of meaning in life, hopelessness about the future;
- Anxiety: feeling vulnerable, excessive worrying about potential dangers and loved ones' safety;
- Emotional reactions: difficulty managing emotions, irritability, anger, aggression, explosive or violent outbursts and behaviour, concentration/memory issues, sleep problems, emotional numbness/isolation;
- Physical problems: aches, pain, decreased resistance to illness, chronic fatigue, emotional exhaustion;
- Destructive coping or addictive behaviours (for example, over/under-eating, substance abuse, gambling, taking undue risks in sports or driving).

**Note:** “Vicarious trauma” is sometimes used interchangeably with “secondary trauma”. Some experts define secondary trauma as resulting from someone such as a human rights interviewer (or therapist or other service provider) taking on the trauma of a particular victim/client they are working with. They may suddenly begin to experience similar symptoms as that person, even within one session. Vicarious trauma, however, is cumulative, and results from repeated exposure to multiple people’s trauma.

### Post-traumatic stress disorder

PTSD is a clinical disorder that can develop after experiencing or witnessing a traumatic event, or after a prolonged traumatic experience. It can develop immediately after a disturbing event or weeks, months or even years later. The most common symptom of PTSD is “re-experiencing”, where the sufferer keeps involuntarily and vividly reliving the traumatic event – in the form of nightmares, flashbacks, repetitive and distressing images or sensations, and physical sensations such as pain, sweating, nausea or shaking. Re-experiencing can be triggered by particular sounds, someone touching a certain part of their body, and so on.

Other symptoms of PTSD include:

- Avoidance: of reminders of the event – avoiding certain people or places, not talking about the event;
- Negative feelings about self or others: guilt or shame, constantly questioning oneself, including whether one could have done anything to stop the event;
- “Emotional numbing” – trying to manage feelings by not feeling anything, causing social isolation;

- Hyperarousal: being constantly on edge, unable to relax; this can cause irritability, anger, sleep and concentration problems.

Symptoms of PTSD are sustained over a prolonged period and can significantly impair a sufferer's daily functioning. It can lead to depression and anxiety, destructive behaviour such as drug or alcohol misuse, physical symptoms, headaches and chest pain.

### **Relation between stress, safety and security**

As well as damaging your health, relationships and ability to work, long periods of severe stress may directly affect your personal safety and security, and can impact the safety and security of others:

- People under severe stress can become less aware, less cautious, or even careless of dangers or risks. As a result, investigators not only put themselves at risk, but possibly also their contacts (survivors, victims, witnesses and other sources) and colleagues.
- Taking decisions (and taking the right decisions) can become more difficult for people under severe stress. This can have a direct impact on their safety and wellbeing, and on the safety and wellbeing of those around them.
- Severe stress often reduces levels of concentration and, in turn, accuracy, both of which are required to deal carefully with sensitive information.
- People under severe stress are likely to demonstrate angry, agitated or moody behaviour. This can lead to losing valuable contacts or support. It can also lead to dangerous behaviour/being unable to control anger in sensitive situations such as at military checkpoints, increasing the likelihood of harm.
- To relieve stress, people may resort to drinking more alcohol or taking drugs. Substance abuse is not only harmful to a person's health and wellbeing, it may also lead to poor judgement, poor decisions, confrontational behaviour, and in other ways put people and anyone they engage with at risk.

## **11.2 Good practices for managing the impact of stress and trauma**

Adequate stress management can significantly reduce risk of stress, vicarious trauma and burnout.

In order to reduce the risk of stress and trauma, and to minimize their impact on you or your colleagues if you are experiencing or exposed to them:

- Acknowledge that your own, your colleagues' and your employees' mental health and well-being are likely to be affected by conducting human rights investigations.
- Be aware of the symptoms of stress, burnout, depression and vicarious trauma and learn how to recognize them in yourself, your colleagues and the staff you manage.

- Do not feel guilty or ashamed if you display symptoms of stress or trauma. Recognize that these are normal reactions to experiencing, witnessing or listening to accounts of traumatic incidents, and of high-pressure work, often undertaken in high-risk environments.

Develop practices that help you manage stress: do these yourself and encourage colleagues to do the same. Build them into your work routines:

- Take time for yourself and look after yourself – exercise, eat healthily and regularly, sleep; allow time for leisure.
- Identify activities that relax you when stressed (sometimes known as “grounding techniques”) – playing sport, having a massage, going for a walk, listening to music, watching/listening to a comedy show/podcast, calling a sibling/friend – and make time for that in your routine.
- Take time to sustain relationships with family, friends and colleagues; make time to talk to people about topics other than work. It can be helpful to have a regular phone call with someone you find entertaining/relaxing /supportive, for example, once a week or however frequently feels useful for you. It can be grounding to talk to people you are close to, who are unconnected to your work.
- Set boundaries between work and private life, identify a “transition activity” when you disconnect from work at the end of the day; make sure you take breaks and holidays.
- Recognize that your work and the related stress can impact your family members. Talk to your family about your work, including talking to children in an age-appropriate manner.

At work:

- If you find certain issues particularly stressful, let your colleagues or your manager know.
- If viewing potentially traumatic footage or images, minimize the sound and take regular breaks from the footage; do not share distressing footage or images with colleagues without warning them. Unexpectedly viewing disturbing images can cause additional distress and trauma.
- Robust safety and security practices can help reduce feelings of stress. Make sure you feel confident about your security planning and risk mitigation plan before you travel to a high-risk location. Have clear security procedures: know who you will call in the event of an incident, establish daily check-ins and have a clear agreement to abort the trip if the risks become too high. These measures will minimize the stress of travel in high-risk locations.
- Identify a support system: who will you talk to if you recognize symptoms of stress or trauma in yourself?



- Breathing techniques can be very helpful in managing feelings of stress. Take short breaks in your work to practice breathing techniques if you are feeling stressed. Keeping a stress journal can also help you to control stress by noting what responses are effective for you and helping you monitor increases in your stress levels.

Managers/organizations should also:

- Make all staff and management aware of symptoms of severe stress, burnout and depression so they can more easily recognize the signs in their colleagues or themselves.
- Encourage investigators and management to communicate with each other about work-related concerns, however big or small, and to strategize together when staff are overworked.
- Ensure staff maintain a healthy work/life balance, take breaks and holidays.
- Ensure an effective peer support system or other process is in place to discuss traumatic content of the work and create a supportive working environment for investigators to talk about how they are feeling. This can help staff avoid feeling isolated and ignoring the symptoms of stress for prolonged periods.
- Organize regular debriefing sessions: for colleagues to debrief each other after difficult experiences, witnessing violations, difficult field trips or distressing interviews, to discuss the events and the feelings of the investigators. Note: this **does not** replace facilitating professional counselling for staff as required after stressful incidents.

### **Ignoring the symptoms**

If you ignore the symptoms of these conditions when they start to develop, it can make you less able to deal with other traumatic events you may witness or investigate, and less able to be empathetic or considerate to survivors and victims. It can also make you less able to concentrate and can lead to errors in your work, and make you less effective in your work.

Stress can also make you physically and mentally ill, cause depression and anxiety, affect your relationships and cause conflict with your colleagues and your family. It can affect your behaviour, and even lead to violence. It may also make you less able to deal with other issues in your life, including things that would not normally affect you.

### **11.3 Responding to symptoms**

**If you are displaying symptoms of stress, depression, burnout or (vicarious) trauma:**

- Acknowledge that you are stressed and suffering from a form of trauma or burnout. This is the first step towards addressing the problem before the effects become chronic, damaging or even dangerous.

- Never feel ashamed, or believe that it means you are not good at your job. Do not feel that you have to hide these symptoms or deal with them alone. Remember they are a normal reaction to the work you do, and should be managed effectively.
- Talk to someone you trust about how you feel – a family member, friend, colleague, manager or mental health professional. Never isolate yourself or hesitate to express how you feel.
- With your manager, identify steps you need to take to deal with your symptoms, including taking some time off, reducing your workload, seeking professional help (with the organization's assistance), seeking additional training in certain areas.
- Seek therapeutic/professional assistance: mental health professionals (such as counsellors), doctors and victims' support NGOs can you help to manage severe stress, burnout, depression, vicarious trauma and PTSD. Do not feel ashamed about seeking professional help: it is a sign that you are proactively managing the challenges of your work, and will make you better at your job.
- If your family is suffering because of your stress, seek assistance and talk about it with family members. Do not let it continue without taking steps to address it. Neglecting your family and outbursts of anger can damage your family life and your reputation; stress can also lead to domestic violence, which is a form of human rights abuse and a crime.

**If you believe a colleague might be experiencing stress or trauma-related symptoms,** approach them and try talking to them one on one about the impact of the work. Encourage and support them to follow the steps above.

**For managers of human rights investigators,** remain alert to symptoms of stress or trauma manifesting in staff you supervise. If they do, address them immediately. Discuss steps that can be put in place immediately and in the longer term to manage their well-being, including reducing their workload, taking time off, support mechanisms and professional assistance.

# Glossary

Most of these definitions are taken and/or adapted from two Amnesty International publications: *Fair Trial Manual* (2nd edition, 2014) and *Monitoring, Documenting and Reporting: A Trainer's Manual on Taking Action Against Human Rights Violations in the Middle East and North Africa Region* (unpublished).

## **Abuses (human rights abuses) – see also human rights violations**

Acts by non-state actors. It is sometimes used generally to refer to acts by both state and non-state actors.

## **Amparo**

In many Latin American countries, a writ of amparo is a prompt, procedural remedy designed to give any individual or group recourse to a competent court for protection against acts by officials (legislators, executive officials, judges) that violate the individual's or group's fundamental rights. It is used as an emergency procedure to protect a detained person's rights to liberty and security.

## **Arbitrary detention**

The UN Working Group on Arbitrary Detention uses the term arbitrary detention to describe any of the following three situations:

1. Where there is no legal basis for detention. This includes people held without charge or trial or despite a judicial order for their release, or those still in prison after their sentence has expired.
2. An arrest or detention that is legal under national law but arbitrary under international standards, for example if the relevant national law is vague, excessively broad or violates human rights such as the right to freedom of expression.
3. When there has been a grave violation of the detainee's right to a fair trial.

## **Armed groups**

Organized, non-governmental groups that use armed force for political, religious, ideological or similar reasons. Armed groups are distinct from other armed non-state actors, such as private military and security contractors, vigilante groups or criminal groups, and from pro-government militia and paramilitary groups, whose violations are directly attributable to the state.

## **Biological sex**

The physical, genetic and chromosomal characteristics that make a person physically male, female or intersex.

**Child**

An individual under the age of 18. The Convention on the Rights of the Child defines a child as “every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier”. Some national legal systems define the age of majority at a younger age.

**Crimes against humanity**

Acts that have been “committed as part of a widespread or systematic attack”, “directed against a civilian population” and committed according to “a state or organizational policy”. The Rome Statute of the International Criminal Court defines 11 types of acts as being capable of amounting to crimes against humanity under these circumstances, including murder, extermination, enslavement, deportation or forcible transfer of population, torture, rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity, persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender, or other grounds that are universally recognized as impermissible under international law and enforced disappearances.

**Customary international law**

Unwritten law that is binding on states and adhered to out of custom. When enough states behave as though something is law, it becomes law “by use” – a general practice accepted as law. Customary international law is a primary source of international legal obligations that are binding on all states, independent of their treaty obligations.

**Discrimination**

The systematic denial of certain peoples’ or groups’ full human rights because of who they are or what they believe.

**Documenting**

The process of investigating and recording information about human rights violations. Documenting involves investigating individual or multiple allegations of a specific violation, or a wider human rights situation; recording and securely storing information; identifying trends; and processing information in a report.

**Due process**

The right to a fair hearing in criminal trials is underpinned by a number of specific rights set out in international standards, sometimes referred to as “due process rights”, which apply to any person arrested and/or charged with a criminal offence. These include the rights to be presumed innocent, to adequate time and facilities to prepare a defence, to be tried without undue delay, to defend oneself in person or through counsel, to call and examine witnesses, not to incriminate oneself, to appeal and the right to protection from retroactive criminal laws.

**Extrajudicial executions**

Deliberate and unlawful killings carried out on the order of a government or with its complicity or acquiescence, or by an official or state agent acting without orders. These can be carried out by regular military or police forces, special units created to function without normal supervision, or civilian agents working with government forces (or with their complicity). Extrajudicial executions are sometimes carried out across international borders. Where an intent to kill cannot be established, it may nevertheless be an unlawful killing.

**Fact finding**

Fact finding or evidence gathering is another name for the process of investigating allegations of one or more human rights violations – namely, collecting or finding a set of facts that proves or disproves if a violation occurred and how it occurred.

**Fair trial standards**

International standards relating to the rights of a person accused of a crime to have a fair hearing in a criminal trial. International law sets out multiple specific rights pertaining to anyone accused of a crime. These include: to be informed promptly of the allegations against them; the assistance of independent legal counsel of their own choosing, including through confidential communications; to be present at their trial; and not to be compelled to testify against themselves or to confess their guilt (see Amnesty International, *Fair Trial Manual* [2nd Edition, 2014] for detailed guidance on fair trial standards).

**Gender**

The socially constructed roles, behaviours, activities and attributes that a given society considers appropriate for women and men.

**Gender-based violence**

Violence directed at an individual because of their gender, the way they express their gender or their gender identity. While most such violence targets women because they are women, people of other genders can suffer from it as well. For example, men who are attacked because they do not conform to socially approved views of masculinity and violence directed against transgender individuals because of their gender identity are also examples of gender-based violence. Most such violence is committed by men, and is directed towards women and girls, but it can be perpetrated by anyone. It is frequently linked to gender inequality, stigma and discrimination.

**Incommunicado**

Detention without contact with the outside world – that is, no contact or communication with a legal representative, family members or others. Incommunicado detention facilitates torture and other ill-treatment and human rights violations. In some

circumstances, it can itself constitute torture or other cruel, inhuman or degrading treatment.

### **Informed consent**

The process of ensuring that every person involved in a human rights investigation (for example, are interviewed, provide information, testimony, photographs or participate in other ways) gives their full consent to do so, based on a clear understanding of the purpose of the work, how their information will be used, what the possible consequences may be (including security consequences), what principles of confidentiality apply, and the limits of that confidentiality.

### **International criminal law**

ICL establishes individual criminal responsibility for the most serious violations and abuses of international human rights and international humanitarian law. The central instrument of ICL is the Rome Statute of the International Criminal Court which covers genocide, war crimes, crimes against humanity and crimes of aggression.

### **International human rights instruments**

Documents agreed to by states or regional or international bodies for the promotion and protection of human rights. Instruments may be legally binding – such as treaties, which are also sometimes called covenants and conventions, pacts or protocols. Other instruments are not legally binding but are considered authoritative because they have been adopted by intergovernmental bodies such as the UN. These include declarations, codes of conduct, principles, guidelines and UN resolutions.

### **International human rights law**

IHRL is the primary source of international legal protections of human rights. It is legally binding on states that have ratified the relevant treaties, as well as their armed forces and all other state agents. Some IHRL provisions are considered to amount to norms of customary international law, meaning they are binding on states irrespective of whether they have ratified the relevant treaty. This body of law applies in both peacetime and during armed conflict. As well as guaranteeing the rights of all persons, it also establishes the right of victims of human rights violations to remedy, including justice, truth and reparations.

### **International human rights mechanisms**

Mechanisms under the UN system mandated to monitor human rights observation by member states. These include the bodies established by international human rights treaties to monitor the implementation of the treaty by states parties, as well as special procedures, which include working groups, independent experts, and special representatives or special rapporteurs who monitor and report on thematic human rights issues or situations of concern.

**International human rights standards**

Standards set out in international human rights treaties. The term is also used to refer to standards laid out in non-binding international instruments such as declarations, guidelines and bodies of principles.

**International humanitarian law**

IHL – also known as the laws of war – refers to the rules and principles regulating the protection of people and the conduct of hostilities during armed conflict. It seeks to limit, to the extent feasible, human suffering in times of armed conflict. IHL protects people who are not participating in hostilities (civilians and civilian objects including schools and hospitals) and contains protections for certain combatants, including those who are no longer participating in hostilities because they have been wounded or captured. IHL also sets out standards of humane conduct, treatment of prisoners of war, and limits the means and methods of conducting military operations.

**Monitoring**

The long-term observation and analysis of the human rights situation in a country or region.

**Non-state actors**

Private individuals or groups that are not acting as representatives of a government or armed group, including groups that exert informal authority within a community, such as religious groups and criminal gangs, as well as organizations including businesses.

**Sexual violence**

Includes physical and psychological attacks directed at a person's sexual characteristics. It is not limited to a physical invasion of the person's body and may include acts that do not involve penetration or physical contact. Sexual violence includes crimes such as sexual harassment, sexual assault, incest and rape. The perpetrator of sexual violence may be a stranger, acquaintance, friend, family member or intimate partner. All forms of sexual violence harm the person and constitute human rights violations.

**Soft law**

Non-binding documents such as declarations, guidelines, bodies of principles and codes of conduct that are nevertheless considered authoritative as they have been adopted by governments or regional or international intergovernmental organizations. These instruments contribute to the understanding, implementation and development of human rights law.

**State party**

A state that has ratified or acceded to a treaty and is legally bound to follow its provisions. Governments do not ratify treaties; only states do.

### Surveillance

Observation or monitoring of activities or information. This includes in-person observation of offices or individuals by members of security or intelligence services, informers or other persons, tapping of phones or rooms/buildings in order to monitor conversations/communications; and digital surveillance – interception of emails and other internet-based correspondence, installation of spyware on electronic devices in order to track activities – communications, internet activity, and so on.

### Torture

The UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment defines torture as “any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.” The term is applied to forms of ill-treatment that are particularly severe and deliberate. The convention prohibits torture as an independent crime, as a war crime and as a crime against humanity, absolutely and in all circumstances. Every act of torture is a crime under international law.

### Vicarious trauma

Sometimes used interchangeably with “secondary trauma”, it refers to trauma that can result from cumulative exposure to the pain of others. An individual **can develop symptoms of trauma even if they do not directly witness or experience a traumatic event**. It can be caused by listening to the stories of survivors and victims, watching footage or looking at photos of violations, reading medical reports of torture, and responding to the aftermath of violence and deaths.

### Violations (human rights violations) – see also human rights abuses

Acts by state agents that violate the state’s obligations under IHRL. Armed groups, which have direct obligations under IHL during armed conflict, also commit violations of IHL.

### War crimes

Serious violations of IHL and customary international law. War crimes include “grave breaches” during international armed conflict listed in the Geneva Conventions and Additional Protocol I, conduct in international and non-international armed conflict described in the Rome Statute, and some conduct considered prohibited under customary international law.



# **Annex 1**

**Reference materials, resources  
and tools – security of human  
rights investigators**

- Barcia, I. (2014). *Our Right to Safety: Women Human Rights Defenders' Holistic Approach to Protection*. Toronto, Mexico City, Cape Town: Association for Women's Rights in Development.  
[awid.org/sites/default/files/atoms/files/Our%20Right%20To%20Safety\\_FINAL.pdf](http://awid.org/sites/default/files/atoms/files/Our%20Right%20To%20Safety_FINAL.pdf)
  - *This publication addresses several aspects of the security and protection of women human rights defenders. It analyses the risks and threats, the wide range of protection mechanisms and states' responsibility to protect women human rights investigators.*
- Barry, J. and Nainar, V. (2008). *Women Human Rights Defenders' Security Strategies: Insiste, Resiste, Persiste, Existe*. Canada: Urgent Action Fund for Women's Human Rights, the Kvinna till Kvinna Foundation, Front Line.  
[kvinna.tillkvinna.org/wp-content/uploads/2018/10/23-Insiste-Persiste-Resiste-Existe\\_ENG.pdf](http://kvinna.tillkvinna.org/wp-content/uploads/2018/10/23-Insiste-Persiste-Resiste-Existe_ENG.pdf)
  - *This book is primarily produced for women human rights investigators, providing them with information about the threats they may face and a range of useful ideas about security strategies.*
- DefendDefenders – East and Horn of Africa Human Rights Defenders Project (EHAHRDP) (2012). "Human Rights Defenders Under Threat: A Field Security Approach to their Work". In: *Defending Human Rights: A Resource Book for Human Rights Defenders*. Kampala: EHAHRDP, pp. 11–17.  
[defenddefenders.org/wp-content/uploads/2011/07/EHAHRPD\\_Resource\\_book\\_ENG.pdf](http://defenddefenders.org/wp-content/uploads/2011/07/EHAHRPD_Resource_book_ENG.pdf)
  - *This resource provides human rights investigators with additional information on safety and security, risk assessments and ways to help human rights investigators better undertake strategies for coping with the increasing security challenges of human rights work.*
- Eguren, E. and Caraj, M. (2009). *New Protection Manual for Human Rights Defenders*. Brussels: Protection International.  
[protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf](http://protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf)
  - *This manual provides human rights investigators with additional knowledge and tools that may be useful for improving their understanding of security and protection. It supports training on security and protection and helps investigators carry out their own risk assessments and develop security rules and procedures to suit each situation.*
- Front Line Defenders (2016). *Workbook on Security: Practical Steps for Human Rights Defenders at Risk*. Dublin: Front Line.  
[frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk](http://frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk)

- *This workbook takes the human rights monitor through the steps to producing a security plan – for themselves and for their human rights organization (if applicable). It follows a systematic approach to assessing one’s security situation and developing risk and vulnerability reduction strategies and tactics.*
- Office of the High Commissioner for Human Rights (OHCHR) (2001). “Security”. In: *Training Manual on Human Rights Monitoring*. Geneva: OHCHR, pp. 469–480.  
[hrlibrary.umn.edu/monitoring/chapter24.html](http://hrlibrary.umn.edu/monitoring/chapter24.html)
  - *This manual is meant for human rights investigators working for UN organizations but is also very useful for other human rights investigators. This chapter contains useful and detailed information on security risks for investigators, security guidelines and other ways to reduce security risks.*

### Relevant organizations and security training

- The **Women Human Rights Defenders International Coalition** is a network that supports and protects women human rights defenders worldwide in their defence of human rights. It has several resources on issues relating to women human rights defenders.  
[whrdic.org](http://whrdic.org)
- **Protection International** provides tools and strategies to help people who defend human rights protect themselves. It supports individuals, organizations, networks and communities whose right to defend human rights is being violated through threats, judicial harassment, stigmatization or other forms of repression. It offers trainings and e-learning courses on security management and protection for human rights activists and organizations.  
[protectioninternational.org](http://protectioninternational.org)  
 Email: [pi@protectioninternational.org](mailto:pi@protectioninternational.org)
- **Front Line Defenders** is the International Foundation for the Protection of Human Rights Defenders. It aims to protect human rights defenders at risk, people who work, non-violently, for any or all the rights enshrined in the Universal Declaration of Human Rights. Front Line Defenders addresses the protection needs identified by defenders themselves. It offers training on security and protection for human rights defenders including risk assessment, threat analysis, reaction to security incidents, dealing with stress, basic digital security, and development of individual and organizational practical security plans.  
[frontlinedefenders.org](http://frontlinedefenders.org)  
 Email: [protectiontraining@frontlinedefenders.org](mailto:protectiontraining@frontlinedefenders.org)
- **DefendDefenders** (East and Horn of Africa Human Rights Defenders Project) seeks to strengthen the work of human rights defenders throughout the region

by reducing their vulnerability to the risks of persecution and enhancing their capacity to effectively defend human rights. DefendDefenders works in Burundi, Djibouti, Eritrea, Ethiopia, Kenya, Rwanda, Somalia (and Somaliland), South Sudan, Sudan, Tanzania and Uganda. It offers capacity building for human rights defenders and their organizations on protection mechanisms and security management, among other things.

[defenddefenders.org](https://defenddefenders.org)

Email: [info@defenddefenders.org](mailto:info@defenddefenders.org)

# **Annex 2**

**Reference materials, resources  
and tools – digital security**

- DefendDefenders – East and Horn of Africa Human Rights Defenders Project (EHAHRDP) (2017). *Stand Up! Security Guide for Human Rights Defenders in Africa*. [defenddefenders.org/wp-content/uploads/2017/04/StandUp.pdf](https://defenddefenders.org/wp-content/uploads/2017/04/StandUp.pdf)  
 ➤ *A small toolkit that helps human rights defenders reduce their vulnerability and enhance their security awareness. Addresses physical and digital security.*
- Eguren, E. and Caraj, M. (2013). *New Protection Manual for Human Rights Defenders*. Brussels: Protection International. [protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf](https://protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf)
- O'Brien, D. (2012). "Information Security". In: *Journalist Security Guide*. New York: Committee to Protect Journalists pp. 16–23. [en.arij.net/wp-content/uploads/sites/3/2015/02/Journalist-Security-guide.pdf](https://en.arij.net/wp-content/uploads/sites/3/2015/02/Journalist-Security-guide.pdf)
- Vitaliev, D. and Frontline Defenders (2007). *Digital Security and Privacy for Human Rights Defenders*. Dublin: Frontline Defenders. [unapcict.org/sites/default/files/2019-01/Digital%20Security%20-%20Privacy%20for%20Human%20Rights%20Defenders.pdf](https://unapcict.org/sites/default/files/2019-01/Digital%20Security%20-%20Privacy%20for%20Human%20Rights%20Defenders.pdf)

### Digital security toolkits

- **Security in-a-box** – created by Tactical Technology Collective and Front Line Defenders. [securityinabox.org](https://securityinabox.org)  
 ➤ *This toolkit is designed to meet the digital security and privacy needs of advocates and human rights investigators.*
- **Digital Security First-Aid Kit for Human Rights Defenders** – Association for Progressive Communications. [apc.org/en/irhr/digital-security-first-aid-kit](https://apc.org/en/irhr/digital-security-first-aid-kit)  
 ➤ *This toolkit provides short guides for human rights investigators who are confronted with emergencies related to communication and digital security.*
- **Witness** – Best Practices: Capturing, Storing & Sharing Video Evidence. [vae.witness.org/video-as-evidence-field-guide](https://vae.witness.org/video-as-evidence-field-guide)  
 ➤ *This guide contains information on how human rights investigators can protect their media and store videos safely, so they can be used as evidence.*
- **Level Up** - Resources for the global digital safety training community. [level-up.cc](https://level-up.cc)  
 ➤ *Level Up provides support to and enables the creation of resources and sharing of knowledge within a growing network of individuals, providing needed digital safety training and education to technology users worldwide.*

- **Surveillance Self-Defence** – Tips, Tools and How-Tos for Safer Online Communications, Electronic Frontier Foundation (EFF).

[ssd.eff.org](https://ssd.eff.org)

- *This is a guide on protection from electronic surveillance. It includes step-by-step tutorials for installing and using a variety of privacy and security tools. It also aims to teach people how to think about online privacy and security in a sophisticated way that empowers them to choose appropriate tools and practices even as the tools and adversaries change around them.*

### **Organizations providing digital security support**

Access Now Digital Security Helpline ([accessnow.org/help](https://accessnow.org/help))

DefendDefenders ([defenddefenders.org](https://defenddefenders.org))

Digital Defenders ([digitaldefenders.org](https://digitaldefenders.org))

Front Line Defenders ([frontlinedefenders.org](https://frontlinedefenders.org))

Protection International ([protectioninternational.org](https://protectioninternational.org))

Tactical Tech ([tacticaltech.org](https://tacticaltech.org))

# **Annex 3**

**Tools for verifying open source material, photos and videos**



For much more detail on tools and techniques for gathering, verifying and using open source material see:

### **Amnesty International, Citizen Evidence Lab**

[citizenevidence.org](http://citizenevidence.org)

- *This website contains information and tools for human rights investigators to work with open source information.*

**Verification Handbooks 1 and 2:** *Verification Handbook for Investigative Reporting: A Guide to Online Search and Research Techniques for using UGC and Open Source Information in Investigations.*

[verificationhandbook.com](http://verificationhandbook.com)

[verificationhandbook.com/book2](http://verificationhandbook.com/book2)

- *A definitive guide to verifying digital content for emergency coverage. These handbooks provide detailed and user-friendly explanations of tools, techniques and step-by-step guidelines for how to deal with user-generated content.*

### **Research Clinic**

[researchclinic.net](http://researchclinic.net)

- *Websites and tools supporting open source investigations.*

### **Witness.org**

- A new guide on the ethics of sharing videos: [library.witness.org/product/video-as-evidence-ethical-guidelines](http://library.witness.org/product/video-as-evidence-ethical-guidelines)
- A guide to archiving video footage in Arabic: [ar.witness.org/resources](http://ar.witness.org/resources)
  - *See in particular sections on organizing and cataloguing*
- Deconstructing digital video: [youtube.com/watch?v=Rm4Oow31uUY](https://youtube.com/watch?v=Rm4Oow31uUY)
- What is video metadata: [youtube.com/watch?v=Aog8JnuwiX8](https://youtube.com/watch?v=Aog8JnuwiX8)
- Planning to preserve video for human rights: [youtube.com/watch?v=g13Pog1BkM](https://youtube.com/watch?v=g13Pog1BkM)

### **Witness.org**

*Ethical Guidelines for Using Eye Witness Footage*

[witness.org/portfolio\\_page/ethical-guidelines-for-using-videos-in-human-rights-reporting-and-advocacy](http://witness.org/portfolio_page/ethical-guidelines-for-using-videos-in-human-rights-reporting-and-advocacy)

- *Human rights organizations, journalists and others are still working through the most appropriate ways to use this kind of content, in consideration of do no harm principles as well as the importance of this content for exposing human rights violations. These guidelines have been put together by the organization Witness to give guidance on ethical considerations.*

The **OSINT** (Open Source Intelligence) framework contains links to numerous online databases for open source investigation: [osintframework.com](http://osintframework.com)

# **Annex 4**

## **Types of interview questions**

There are different types of questions that you can use in an interview, and some to avoid. Using the right type of questions appropriately is important to get the most out of an interview, to minimize biases and avoid misinformation. The table below describes the types of questions and how they are used.

**Table 6. Interview questions**

Type of question	Sample question
<p><b>1. Open (or open-ended) questions</b></p> <p>These questions invite the interviewee to respond freely. They are a good way to begin an interview. They usually begin with or contain words like “who”, “what”, “when”, “where”, “how” and “why”.</p> <p>Open questions can be very broad, such as “what happened to your brother?”</p> <p>They can also be used to gather subsequent details of the story, on more specific aspects, for example: “Who arrested your brother?”</p> <p>Open questions are used a lot in interviews but may be interspersed with most of the other types of questions below.</p> <p>Open questions are also useful when you want to cross-check the consistency of information. You can ask the same open question to two witnesses to check for inconsistencies or biases.</p>	<ul style="list-style-type: none"> <li>• Can you tell me what happened to your brother?</li> <li>• Could you describe what the facility looked like where the agents took you?</li> <li>• Where did you see that military vehicle?</li> <li>• How did you manage to get out of that building?</li> </ul>
<p><b>2. Hypothetical questions</b></p> <p>These types of questions help people to imagine situations and stimulate their thinking.</p> <p><i>Hypothetical questions are open-ended questions.</i></p>	<ul style="list-style-type: none"> <li>• What would you do if...?</li> </ul>
<p><b>3. Supporting questions</b></p> <p>Supporting questions encourage people to feel comfortable to give further details. They are intended to further draw out people’s experiences and views.</p> <p><i>Supporting questions are open-ended questions.</i></p>	<ul style="list-style-type: none"> <li>• That’s interesting, what happened next?</li> <li>• I understand that was difficult, what did you do?</li> </ul>

<p><b>4. Probing questions</b></p> <p>These are follow-up questions. These are not to challenge the interviewee, but to help them think more deeply and justify/analyse their opinions. This could reveal another important detail which is the foundation of the interviewee's opinion/relevant to the context in which the violations took place. Interviewees' perceptions can signpost underlying issues.</p> <p><i>Probing questions are open-ended questions.</i></p>	<ul style="list-style-type: none"> <li>• What makes you believe this?</li> <li>• Why do you think...?</li> </ul>
<p><b>5. Clarifying questions</b></p> <p>These summarize what a person said to make sure that you have understood correctly.</p> <p><i>Clarifying questions are closed questions (they can be answered with a simple "yes" or "no") but aim for further explanation/detail.</i></p>	<ul style="list-style-type: none"> <li>• Am I right to say that you think...?</li> <li>• Is this what you said...</li> <li>• Did I hear you correctly when you said...?</li> </ul>
<p><b>6. Concluding questions</b></p> <p>These types of questions can provoke discussion or can come at the end, when you can agree to move to the next topic.</p> <p><i>Concluding questions are closed questions (can be answered with a simple "yes" or "no") but aim to confirm and continue.</i></p>	<ul style="list-style-type: none"> <li>• Is there anything else to add to that part...?</li> <li>• Do we agree that...?</li> <li>• Do we both understand that...?</li> </ul>
<p><b>7. Leading questions</b></p> <p>In a leading question the way the question is phrased influences the interviewee to give or agree to a certain (expected) answer.</p> <p><b>Leading questions should be avoided!</b></p> <p><i>By using leading questions, the interviewer "leads" the interviewee to say something they otherwise might not have said or might have said differently.</i></p>	<ul style="list-style-type: none"> <li>• Were those who arrested you army soldiers? (Ask instead: Who arrested you?)</li> <li>• How badly were you beaten in prison? (Ask instead: How were you treated in prison?)</li> </ul>
<p><b>8. Closed questions</b></p> <p>Closed questions aim to get a brief answer and not an elaborate response. They can often be answered with a "yes" or "no" and can be leading.</p> <p><i>Closed questions are useful to get specific information.</i></p>	<ul style="list-style-type: none"> <li>• Is your mother still alive?</li> <li>• Were they armed? (yes/no)</li> <li>• Were the demonstrators taken to prison? (yes/no)</li> <li>• Did the police officer do that to you? (yes/no)</li> </ul>

# **Annex 5**

## **Sample interview guide**

Below is an example of the structure and content of an interview. You can use this as a reference while you are building confidence and becoming more familiar with the interview process. The who, what, when, where, how and why questions can be adapted to the case or issue you are investigating.

It is a good idea to read through this guide before every interview to help you design your own checklist of what not to forget. As discussed in the handbook, always avoid having a long guide like this on the table during interviews, as it can disrupt the flow of the interview, influence your body language and make you less open to other information that may emerge. If you think it will be helpful, use this guide to make a very short bullet list of things you need to remember to say or ask about.

When you become more familiar and confident in the interviewing process, you will find that you may not need to consult this guide before you go into an interview.

INTERVIEW CHECKLIST	CONFIDENTIAL
<ol style="list-style-type: none"> <li>1. Interviewer name</li> <li>2. Date of interview (DD/MM/YY)</li> <li>3. Number of the interview (for that day)</li> <li>4. Location of interview</li> <li>5. Name of interpreter (if any)</li> <li>6. Other person/s present at the interview (if any)</li> <li>7. Language of interview</li> </ol>	
<p><b>Introduction</b></p> <p>My name is ....., I work with ..... (organization); the organization works on .....</p> <p>Reasons for conducting the interview..... (for example, investigating incident/ issue X, and trying to collect information to establish what happened)</p> <p>Intended actions with information..... (write report, do advocacy/media work with objective of effecting X change)</p> <p>Realistic possible outcomes....</p>	
<p><b>Informed consent</b></p> <p>Obtain consent to conduct the interview <b>and</b> consent to use the information in future reports. Ensure that interviewees fully understand the purpose of the interview. Assure victims and witnesses that you will not include their names in reporting, for example:</p> <p>“We intend to use the information to compile a report about torture. We will use the report to conduct advocacy for those who have used torture to be brought to justice, and to push to end torture and any other ill-treatment in detention facilities</p>	

in [this country]. We will not use your name in the report or any details that could be used to identify you. If you agree, we will share your testimony with two colleagues working with us on the issue. We will not share your identity or your testimony with anyone outside the organization unless you give us specific permission.”

Please confirm:

1. Can I proceed to interview you?
2. Can I use the information you provide in our report, while concealing your name and identity?
3. Can we share your name, contact information, and information you have provided us with independent investigative and judicial bodies? (Give examples that this could be UN investigative missions/commissions of inquiries, investigations by the International Criminal Court, and so on.)

Tell the interviewee: You do not have to answer questions if you do not want to. I may need to ask questions that can be difficult for you. We can take breaks any time you need to and you can stop the interview at any time.

### **Interviewee identification**

1. Name
2. Sex
3. Age (or date of birth)

Other biographical information you may want to note during the course of the interview, where relevant to the violation in question (do not ask a long list of personal details at the start):

4. Place of birth (county, state)
5. Nationality
6. Ethnic group
7. Religion
8. Occupation
9. Level of education
10. Marital status (single/engaged/married/divorced/separated/widowed)
11. Occupation of husband/wife (if any)
12. Number of children (if any)
13. Members of household
14. Language(s) spoken and understood
15. Suggested pseudonym

**Contact details**

1. Current address
2. Permanent address
3. How can I contact you in the future? (Telephone number?)

**Introduction**

Start with non-sensitive questions about the person's current situation, how s/he feels, makes a living, and so on. Try to gain trust and to make the victim/witness feel comfortable.

**The incident(s)**

Then ask the interviewee to tell what happened, everything he or she knows about the event(s). Do not intervene too much, but if the victim/witness seems to have difficulty telling his or her story or if he or she is omitting important details, ask open-ended questions such as: Who? What? Where? When? How? Why?

To make sure you have all the important details, use the points below.

Additional guidance:

1. When the victim/witness gives specific information, establish how he or she knows this to distinguish direct evidence from hypothesis and hearsay.
2. Note any inconsistencies, contradictions, exaggerations or confusion: try to clarify them, but if that does not work, check these with other victims or witnesses.
3. Ask short questions and only one question at a time.
4. If you are repeating questions, explain why you are doing it: do not let the victim think they have done something wrong.
5. If you do not get an answer, try rephrasing the question or taking a different approach.
6. If a victim/witness is visibly upset, change the tenor of the questions or suggest a break.

**WHERE?**

- Detailed questions on where the incident(s) took place; if multiple locations, note in chronological order (such as when survivor/victim/witness was moved to different places, facilities).
- If unknown to survivor/victim/witness, obtain details of the environment (bush, rural, urban, distinguishing features of the landscapes, recognizable buildings around, and so on); if they were in a building but do not know which building/what type of building it was – can they describe the building/the rooms they were in?



### WHAT AND HOW?

- What was done? Detailed questions/descriptions of the incident(s)/act(s), including time, duration, circumstances, chronology.
- Injuries sustained? (Where – body parts (details), saw a doctor, obtained a medical report?)
- Any other damage – homes, property, and so on.
- Tools/instruments/arms used.
- What was said by perpetrators during act(s)/incident(s).
- Specific questions asked or comments made (motivations for act(s)).

### WHO?

- Who were the survivors/victims (distinguishing features, reasons for targeting – such as ethnic group, political affiliation/opinion, actions (for example, demonstrating), students).
- Who were the perpetrators – who was present and who did what (names, ranks, different roles, languages spoken)? If the perpetrator(s) unknown – any distinguishing features? (Such as a uniform (colour, insignia on uniform), vehicle used (brand, colour, number plate).)
- Language(s) used by perpetrator(s).
- Details of other (possible) victims present.
- Any witnesses to the incident(s) (collect details if possible – names and contact information).

### WHEN?

- Details on when act(s)/incident(s) took place, in chronological order (date, day, time).
- How long act(s)/incident(s) lasted.
- Change of act(s)/incident(s)/perpetrators over time.
- Change in type of demands, behaviour, perpetrators over time.

### WHY?

- Why survivor/victim/witness thinks this was done to them (for motivations of ethnicity, religion, political affiliation, sexual orientation, human rights work, and so on).
- What was said by perpetrators, motivations mentioned?
- If interrogated (for example in detention) were particular questions/details asked or focused on?
- Any indication in advance that the violation might happen – warning, threat, harassment? (First time the interviewee has experienced or concerns about such issues?) Previous history of problems (individual/community)?

**IMPACT?**

- Detailed questions about the impact (physical, psychosocial, economic, other).
- Impact on daily life and relationships.
- Questions about medical care/counselling received/still receiving.
- Details about visible and non-visible injuries, scars and symptoms (pictures when agreed).

**RESPONSE BY AUTHORITIES?**

- Details on any authority/government response (investigations, arrests, and so on).
- Any reporting done to police/authorities (pictures when agreed).
- Details of who/which NGO/other the victim/witness has already spoken to.
- Any support provided/needed.

**RECOMMENDATIONS?**

- Get witness/victim's views on what justice they want; what kind of support/assistance they and other witnesses/victims need.

[Note: this may not be appropriate in all cases; be careful about managing expectations.]

**CLOSING**

- Check whether there are any other details you have not discussed, or whether they want to share anything else, whether they have any questions for you; how they felt about this interview.

**SUPPORTING EVIDENCE**

- ☐ Photos of injuries
- ☐ Footage of injuries
- ☐ Official charges/warrants
- ☐ Medical reports of medical personnel prior to incident
- ☐ Medical reports of medical personnel after incident
- ☐ Statements from lawyers, human rights groups
- ☐ Witness statements corroborating victim's testimony
- ☐ Other

**Concluding observations /other details**

Description of victim/witness demeanour

# Annex 6

## Incident report form

An incident report form or case sheet can help record and keep track of an incident/case in which violations/abuses may have taken place. Such a form needs to refer to all the interview notes/reports and other documentary and physical evidence that you have gathered on a single event or incident. Each violation or abuse must be substantiated by information from several sources.

Such forms are particularly useful when you collect a large amount of information on incidents and violations over a number of months or years. It allows you to synthesize and provide easier access to supporting documentation. It could also be used as a basis to enter information on cases (of violations/abuses) in a database.

This form could be used as a model to guide you in the development of your own incident report form or case sheet, suitable to your particular case, context and circumstances.

INCIDENT REPORT FORM – ALLEGED HUMAN RIGHTS ABUSE/VIOLATION						
Code number:				MM/DD/YY of registration:		
Visit to the scene:		<input type="checkbox"/> Yes <input type="checkbox"/> No		MM/DD/YY:		
List of persons interviewed						
Name	Sex	Age/ Date of birth	Profession/ Occupation	Contact number	Victim/ witness/ relative	File name/code (to retrieve the interview notes)
Time and location of incident						
Date and (approximate) time of the incident:						

Region (province, district):		City/village (or nearest):	
Place of incident (description/geo-location):			
<b>Nature of incident(s) / alleged human rights abuse / violation</b>			
Alleged nature of incident (tick all that apply):	<input type="checkbox"/> Attack on civilians <input type="checkbox"/> Displacement of population <input type="checkbox"/> Unlawful killing(s) <input type="checkbox"/> Excessive use of force <input type="checkbox"/> Arbitrary arrest & detention	<input type="checkbox"/> Enforced disappearance/abduction <input type="checkbox"/> Sexual violence <input type="checkbox"/> Unfair trial <input type="checkbox"/> Torture & ill-treatment <input type="checkbox"/> Burning, looting, destruction of property	<input type="checkbox"/> Child soldier recruitment <input type="checkbox"/> Assault to freedom of expression <input type="checkbox"/> Assault to freedom of assembly <input type="checkbox"/> Other:
<b>Description of the incident and its impact</b> Briefly describe the motivations and circumstances in which the violation(s) took place. Briefly describe the events immediately preceding the incident (such as new legislation, military attacks, demonstrations, other).			
Number of victims (how many men, women, boys, girls, elderly):			
How have male and female victims been affected differently?			
<b>Alleged perpetrators</b> (such as police forces, armed forces, armed groups, civilians) Provide details on weaponry used, clothing worn, other details to identify specific groups.			

### Other evidence (documentary and physical)

Medical and/or forensic evidence present? What does it say?  
(Attach copy of original, if possible)

Court or police record present? What does it say?  
(Attach copy of original, if possible)

Photo/video taken? Number/describe

Other

### Governmental responses, if any

Complaint lodged

When?

Where?  
Which  
government  
body?

Public statements  
(give details)

Official investigation  
(give details)

Judgement

### Response of traditional institution or armed group, if any

Institution

Response

### Action taken

Was any action taken by the monitor  
(for example, referral to police/  
hospital/safehouse/NGO)?  
(give details)

# UKWELI

## Investigating human rights violations

### Main Book

Every day, human rights activists and organizations across the globe are investigating human rights violations being committed in the context of conflict, shrinking civic space, or for instance, counter-terrorism policies. It is essential that such investigations are conducted accurately and consistently. The findings of high-quality and credible investigations can influence policy and practice; provide reasonable grounds to start judicial investigations; help campaign and advocate for justice, remedy and assistance for survivors and victims of violations and accountability by perpetrators. It can also generate pressure on duty bearers. Moreover, reliable investigations are crucial for building and maintaining the legitimacy and reputation of human rights organizations and activists, locally, nationally and internationally.

This main book provides detailed guidance to human rights activists and organizations on conducting accurate and high-quality investigations into possible human rights violations, verifying findings and writing reports. It discusses principles of research, provides guidelines for contact building, monitoring, fact-finding, interviewing, documenting, and suggests strategies for tackling problems and challenges. In light of the shrinking space worldwide for human rights defenders and the increasing risk of repercussions against their sources, the guide emphasizes safety and security planning for investigators, sources and the work itself, including secure digital, information and communications practices. It also covers the critical aspect of managing the well-being of human rights investigators. *Ukweli Abridged* revisits the main book to offer an abridged read, focusing on its practicality.

This main book is accompanied by – and can be read in conjunction with – thematic handbooks that provide detailed information and guidance relevant to investigating specific violations. These include handbooks on investigating enforced disappearances and on investigating torture and cruel, inhuman or degrading treatment or punishment, as well as a number of other thematic issues.

The Human Rights Capacity-Building Programme (HURICAP) of Amnesty International Netherlands has worked with African civil society organizations in building human rights capacity for 30 years. Following the successes of working with African civil society, HURICAP started operating in the Middle East in 2016. A key part of this work has been in strengthening the knowledge and skills of local human rights organizations and activists to monitor, document, and report on human rights violations and abuses. This book draws on this experience.

