



UNODC

United Nations Office on Drugs and Crime

A TRAINING HANDBOOK FOR CRIMINAL JUSTICE PRACTITIONERS ON CYBERVIOLENCE AGAINST WOMEN AND GIRLS (CVAWG)





UNODC

United Nations Office on Drugs and Crime

ACKNOWLEDGEMENTS

UNODC

Claudia Baroni
Renata Delgado-Schenk
Loya Marin
Linda Naidoo
Bertha Nayelly
Sven Pfeiffer

UNODC gratefully acknowledges the financial support provided by the Austrian Development Agency (ADA) in the development of a Training Handbook for Criminal Justice Practitioners on Cyberviolence against Women and Girls (CVAWG).

OTHER

Wilma Gernandt (Justice College)
Preshan Kissoondoyal (Interpol Regional Bureau)
Susan Kreston (International Consultant)
Simbarashe Manjera (SADC Secretariat)
Phiwayinkhosi Nhlengetfwa (Interpol Regional Bureau)
Karen Steyn (Justice College)
Jakkie Wessels (Regional Court President in Limpopo, South Africa)

United Nations Office on Drugs and Crime, October 2022. All rights reserved.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Information on uniform resource locators and links to Internet sites contained in the present publication are provided for the convenience of the reader and are correct at the time of issue.

The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

Contents

Part One: Introduction to the Training Handbook	5
1.1. Design of the training package	6
1.1.1. Handbook	6
1.1.2. PowerPoint Slides	8
1.1.3. Videos	8
1.1.4. Annexures	8
1.2. Before the workshop	8
1.2.1. Skills development for trainers	8
1.2.2. Developing training interventions	8
1.3. How to facilitate	8
1.3.1. Training guidelines	8
1.3.2. Organising the training intervention	9
1.3.3. Presentation/facilitation skills	10
1.3.4. Different types of presentations	11
1.3.5. Training and instructional aids	11
1.3.6. Dealing with the 'Dirty Dozen'	12
1.4. Alternatives to training - webinars	13
1.5. Conclusion	14
Part Two: Gender-based Violence and CVAWG	15
2.1. Introduction to Gender-based Violence	16
2.2. Prevalence of Gender-based Violence and CVAWG	16
2.3. Myths of Gender-based Violence	22
2.4. Power	26
2.4.1. Expressions of power: over, to, with, and within	26
2.5. International and Regional Legal Frameworks and Standards on GBV	26
2.6. United Nations Human Rights Standards	26
2.6.1. CEDAW	26
2.6.2. Beijing Declaration and Platform for Action (BPfA)	27
2.7. European Union Human Rights Standards	28
2.7.1. The Istanbul Convention	28
2.7.2. The Lanzarote Convention	29
2.8. African Human Rights Standards	30
2.8.1. SADC	30
2.8.2. SADC Gender-Based Violence Model Law 2021	30

2.9. Cybercrime instruments	31
2.9.1. Introduction	31
2.9.2. International, national and regional laws on cybercrime	31
2.9.3. SADC Model Law on computer crime and cybercrime	33
Part Three: Understanding CVAWG	34
3.1. Introduction.....	35
3.2. Forms of CVAWG.....	37
3.2.1. Online exploitation	37
3.2.2. Sextortion	39
3.2.3. Cyberbullying	39
3.2.4. Cyberstalking	40
3.2.4. Online harassment	40
3.2.5 Image-based abuse (IBA)	41
3.2.6 Revenge pornography (Harmful disclosure of an intimate image)	41
3.2.7. Sexting.....	41
3.2.8. Doxxing or doxing	42
3.2.9. Impersonation	42
3.3. Victim impact as a result of gender-based cyberviolence crimes.....	43
3.4. For victims/survivors, the implications of failing to address GBV are profound.....	43
Part Four: Interviewing Survivors	45
4.1. Interviewing and obtaining a statement.....	46
4.1.1. General principles applicable to women and girls (children).....	46
4.1.2. Preparing for the interview	46
4.1.3. Survivor-friendly spaces	46
4.1.4. Key points to consider when interviewing on cyberviolence offences	47
4.1.5. Factors to consider when interviewing girls	48
4.2. Essential Services Package for women and girls subjected to violence	51
4.2.1. Introduction.....	51
4.2.2. Inter-agency Collaboration and Coordination of the Multi-disciplinary Team	51
4.2.3. The Essential Services guidelines framework.....	52
4.2.4. Unique features of the framework specific to essential justice and policing services.....	54
4.2.5. Guidelines for essential justice and policing services.....	55
Part Five: Digital Investigation Proceedings of Electronic and Digital Evidence ...	57
5.1. Introduction.....	58
5.2. What is digital evidence?.....	58
5.3. First Responder	58

5.4. Sources of evidence.....	58
5.5. Search and seizure: Standard Operating Procedures (SOPs) for dealing with electronic evidence.....	59
5.6. Five principles applicable to electronic evidence	59
5.7 Preparation prior to the search and seizure operation.....	60
5.7.1 Planning.....	60
5.7.2 Authorisation.....	60
5.7.3 Personnel.....	61
5.7.4 Equipment	61
5.8 During the search and seizure operation.....	61
5.8.1 Securing the location.....	61
5.8.2 ..Search and seizure.....	62
5.8.4 Transportation of electronic evidence	64
5.8.5 Witness statement of the digital forensic expert.....	65
5.8.6 Preparation for criminal proceedings	65
5.8.7 Consultation with prosecutor.....	65
5.8.8 Non-consensual pornographic and child sexual abuse images.....	65
5.8.9 Criminal proceedings.....	66
5.8.10 Mutual legal assistance	67
Part Six: Annexures	68
RESOURCES.....	86
READING LIST	92

PART ONE

Introduction to the Training Handbook

LEARNING OBJECTIVES

Understanding how criminal justice practitioners can share knowledge on cyberviolence against women and children (CVAWG)



Implementing the factors necessary to plan, develop and present effective training



Applying the guidelines for facilitation



This training handbook is designed to capacitate criminal justice practitioners (e.g. law enforcers, prosecutors and judicial officers) on gender-based violence (GBV) and cyberviolence against women and girls (CVAWG). To effectively combat CVAWG, criminal justice practitioners should have the skills, capacity, and sensitivity to apply the spirit and rule of law comprehensively. It is a priority to address and eliminate online exploitation, abuse and violence against women and girls. Therefore, online or offline harmful gender-based practices should be monitored and perpetrators punished. Evidence shows that the certainty of punishment, rather than its severity, deters crime.¹ Unfortunately in most countries around the world, the key problem is that victims of sexual violence do not have access to justice in the first place – whether due to stigma, fear of reprisals, entrenched gender stereotypes and power imbalances, lack of police and judicial training, laws that condone or excuse certain types of sexual violence or the lack of protection for victims.

Women and girls are disproportionately affected by online violence, which should be seen as a continuation and broadening of offline violence. Women should be active participants in designing measures to prevent and address these crimes, and law enforcement and judicial officials should receive the requisite training in handling such cases.²

1.1. Design of the training package

This training package has been designed to develop and clarify the perspectives of the participants on gender-based violence, specifically in the context of cyberviolence against women and girls. It gives background information on international and regional standards and legislation on GBV and cybercrime, and discusses cybercrime instruments.

The training package shares information on ways to interview survivors and conduct digital investigation proceedings. It introduces the Essential Services Package for women and girls. In addition, it also gives valuable information on how to approach the training and target audience, and effectively use the training material.

Most of the sessions incorporate interactive methods such as brainstorming, case study-based group activity, discussions, problem-solving, etc. to facilitate experiential adult learning for increased participation and practical application of the core issues.

1.1.1. Handbook

The training handbook has been designed for an uninterrupted 5-day training workshop. However, the suggested training agenda could be modified depending on time constraints and the previous experience of the criminal justice practitioners.

Specific areas of focus in this training handbook include:

- Prevalence of GBV and CVAWG
- Key definitions of GBV and CVAWG
- Myths about GBV
- Interviewing survivors
- Understanding trauma
- International conventions and regional protocols
- National legislation on cyberviolence and GBVF
- Digital evidence
- A multi-disciplinary approach
- Guidelines for trainers.

¹ OHCHR: Rape is a monstrous crime, perpetrators must be held accountable – but death penalty and torture are not the answers - Bachelet (15 October 2020). Available online at: <https://www.ohchr.org/en/press-releases/2020/10/rape-monstrous-crime-perpetrators-must-be-held-accountable-death-penalty-and-torture>

² Ibid

To achieve these goals, the handbook consists of **five parts**:

PART 1

INTRODUCTION TO THE TRAINING HANDBOOK

This Part focuses on skills development for trainers regarding identifying the target audience and objectives, organising the training intervention, and presenting the information with the aid of training tools to an adult audience.

PART 2

GENDER-BASED VIOLENCE (GBV) AND CYBERVIOLENCE AGAINST WOMEN AND GIRLS (CVAWG)

This second part introduces gender-based violence (GBV) and cyberviolence against women and girls (CVAWG) and refers to the GBV definition as stated in General Recommendation 19 of the CEDAW committee. It then indicates the prevalence of GBV and CVAWG and points out that the two cannot be conceptualised as two separate phenomena - rather online violence should be seen as a continuation of offline violence. The module addresses various myths about GBV and CVAWG. International and regional standards on GBV are discussed, amongst others, the CEDAW, Beijing Declaration and Platform for Action (BPfA), the Istanbul and Lanzarote Conventions, as well as the SADC Model Law on GBV. It gives an introduction to cybercrime instruments, and finally, international, national and regional laws on cybercrime are presented.

PART 3

UNDERSTANDING CYBERVIOLENCE AGAINST WOMEN AND GIRLS

The third part explores different forms of CVAWG, such as sextortion, cyberbullying and sexting. It also includes a specific focus on the exploitation of children and offenders' commonly indicated methods in this regard. Lastly, it addresses the impact of GBV and cyberviolence on victims/survivors and explores the negative consequences of failing to address GBV.

PART 4

INTERVIEWING SURVIVORS

This part discusses key points of how to interview survivors and witnesses of specifically CVAWG, e.g. the essential information required and protection measures to take into account. It describes factors to consider when interviewing girls, such as helpful questions to ask and questions to avoid, as well as the appropriate duration of an interview. It concludes with the Essential Services Package for women and girls who were subjected to violence.

PART 5

DIGITAL INVESTIGATION PROCEEDINGS OF ELECTRONIC AND DIGITAL EVIDENCE

The last part describes several aspects of digital evidence, including the duties of the First Responder and sources of evidence. It also explains the SOPs for dealing with electronic evidence in the context of Search and Seizure.

1.1.2. PowerPoint Slides

The PP slides are complimentary to the training handbook and reflected in the 5-day training programme. The PowerPoint (PP) slides are provided on a USB.

1.1.3. Videos

The videos are embedded in the PowerPoint slide deck for easy access.

1.1.4. Annexures

Annexure 1: Acronyms

Annexure 2: Glossary

Annexure 3: Example of a training intervention:
draft planning and preparation plan

Annexure 4: Example of a training programme

Annexure 5: Checklist for Gender-based cybercrimes

Annexure 6: Pre- and post-training questionnaire

Annexure 7: Administrative training formats

Annexure 8: Resources and reading list

1.2. Before the workshop

1.2.1. Skills development for trainers

When planning and preparing for any training or awareness-raising initiative, trainers and facilitators should understand the needs of the target audience, the topic to be presented, the objectives of the intervention and the outcomes to be achieved. Trainers, facilitators, and presenters need to continuously improve their skills and ensure that the content of any intervention is up to date.

Some basic principles and guidance will be given in this part for trainers, facilitators, and presenters to consider when developing, planning, preparing for, and presenting training and awareness-raising interventions.

1.2.2. Developing training interventions

When you plan and arrange a training intervention, you must know the identified need, the topic, who will be the target audience, when it will take place, and where and how it will be done. In planning and preparing for your training intervention, you need to:

- Motivate your training intervention, including outcomes
- Identify and state the objectives of the training intervention
- Identify your target audience and the appropriate number of participants
- Consider the training methodology to be used

- Organise the training intervention (including aspects such as time frames, invitations, promoting the intervention, arranging the venue, refreshments, costs involved, proposals for funding if needed, etc.)
- Have a checklist of tools needed, including materials
- Draft a programme for the training intervention and know whether you will facilitate it on your own, have co-facilitators, other presenters, or speakers (the less time available, the fewer speakers/presenters)
- TIP: It is generally useful to have a co-facilitator so you can work in a team, as well as some assistance for the administrative part of arranging any training intervention.

It is important to be organised and to plan and prepare for the training intervention. If you have not previously arranged training interventions, you can use the example of a planning and preparation plan in Annexure 3 to guide you.

1.3. How to facilitate

1.3.1. Training guidelines

The following section outlines some training hints for trainers.

1.3.1.1. Introduction

When you have to present a presentation or facilitate a training session, you should:

- establish the target audience
- establish the needs of your target group
- develop a presentation or training session to fit that need.

When you are preparing and presenting a presentation, you need to take cognisance of the following factors:

- the target audience
- the topic
- the objective of the training session/presentation
- the time available for your training session/presentation

Never underestimate these factors, as this will determine the success of the lecture.

1.3.1.2. Target audience

Typically:

- adults
- matriculated/graduates
- various levels of experience in specific fields

People are shaped differently through:

- physical attributes
- cultural environment
- social environment

The audience differs regarding each individual's personality type. Typical personality types include:

Economical	Practical and concrete
Power	Wants to rule and be served
Social	Focus on human empathy
Theoretical	Intellectualistic (scientists)
Aesthetic	Focus on impression
Religious	Religious values are their priority

People all have different personalities, interests, skills, talents, and capabilities. You should also remember that there are differences regarding:

Intelligence: the capability to execute actions in terms of:	<ul style="list-style-type: none"> • Difficulty • Complexity • Abstraction • Time-saving • Social status • Originality • Perceptions
Frame of reference	<ul style="list-style-type: none"> • Conditioning • Association • Experience
Emotions	<ul style="list-style-type: none"> • Behaviour • Attitudes • Values
Attention	<ul style="list-style-type: none"> • Concentration span • Weariness • Disturbances • Inner emotional capabilities • Vague, uninteresting presentations

In general adult trainees are:

- self-responsible
- concerned with self-respect
- self-appointed
- experienced
- problem focussed - wants to use information/ideas immediately
- not always ready to learn
- tend to have fixed ideas and methods - will change if convinced that training will be to their benefit
- knowledge or information must be of practical use to them.

A trainer is often perceived as a role model and as such s/he is expected to act as one through:

- proper language
- good human relations - respect for others
- well disciplined
- punctuality
- self-respect
- responsibility
- good knowledge of the subject.

1.3.2. Organising the training intervention

When you have to organise a training intervention, make sure that you organise it for a time and place most of your target audience will be available.

Send out invitations/notifications in advance to ensure that participants have time to organise attendance. It is usually a good idea to ask them to let you know whether they will be available/ attach RSVP to invitations to be returned to you by a specific date (usually about 10 days before the training intervention/seminar).

It is often useful to send a reminder with, for example, additional information, the final programme, venue and directions, and/or reading material that will generate interest to the participants to attend.

Please note: If participants have to make their own copies to bring with them, it is imperative to send a reminder a day or two before the date to them in this regard.

If it is a small group, arrangements can be done much easier and more informally, but you still need to ascertain beforehand the number of people attending, as you have to make sure that enough copies are made in time, and that the venue you want to use is suitable and will accommodate all.

You should also have a registration form/attendance register for participants to fill in, as well as an evaluation form that should be completed at the end of the training intervention/ seminar.

Annexure 7 includes examples of these administrative formats.

1.3.3. Presentation/facilitation skills

1.3.3.1. In general

To ensure a successful presentation, you need to be in charge and lay down the ground rules and know the topic and the material you use. You have to plan your presentation - you need to have a framework of how you are going to present it and allocate enough time for each part of the presentation - and adhere to it as far as possible. Always leave time for questions or discussions.

Have a framework in which you break the presentation up, for example:

- Introduction (information about yourself, welcome)
- State the course subject
- State objective/s of a session (what they will get out of the session/learn, etc)
- Presentation (content)
- Summarise
- Questions

Remember to motivate and/or encourage participants - they need to know how they will benefit from the lecture/ presentation.

Always give credit to good answers. When a person asks a question/answer, repeat it for the rest of the group. Formulate questions in advance and ask one question at a time, wait for a response, repeat or rephrase if necessary and always accept responses. It is preferable to tell participants in the beginning, at the time when you lay down ground rules, when they can ask questions - at the end or during the presentation.



1.3.3.2. Specific presentation aspects to consider

Enthusiasm	<ul style="list-style-type: none"> • Speak with expressiveness • A variety of tones of voice • Use humorous anecdotes or examples (sparingly and be careful with the jokes) • Gestures with hands, arms, body - don't be 'dead' (but don't overdo) • Eye contact with the audience
Pacing	<ul style="list-style-type: none"> • Slow is better • Key terms on whiteboard/overhead • Summarise periodically • Check for understanding before proceeding to the next point
Clarity	<ul style="list-style-type: none"> • Relates subject matter to interests • Provide real-life examples • Provide multiple examples • Use graphics • Put the outline of the lecture on board/flip chart/PowerPoint slide • Signal transitions
Interaction	<ul style="list-style-type: none"> • Addresses participants by name • Ask questions • Reward and reinforce responses • Communicates with the audience outside of the lecture

1.3.4. Different types of presentations

Training can be done in a variety of different ways, and can also be a combination of different presentations. In deciding how you are going to do your presentation, you again have to keep in mind your target audience, the time available and the time needed to cover the topic, and of course, the topic itself. Certain information can best be disseminated through a demonstration, while other types of topics lend themselves more to work groups or discussion group types of presentations.

The basic ways to disseminate information are:

- a theoretical presentation
- a demonstration
- discussion group
- work groups
- experiential exercises
- a combination of two or more of the above.

In deciding how you are going to do your presentation, you should also take into account the type of venue that will be available to you. For example, for discussion groups, you would preferably have break-away rooms to accommodate the different groups. Alternatively, if it is a very big venue, groups can work in different areas of the venue, or even outside (if the weather permit).

To make the most of training, physical and environmental conditions should be taken into account, and you should try to ensure that participants are as comfortable as possible. To try to disseminate information in any way to participants that are disturbed by outside or physical factors can be a nightmare and can end up as a fruitless exercise.

In planning the training intervention and/or presentation, it is important to make sure that it is done in a manner that will engage participants, answer their questions, and be as practical and work-related as the topic allows.

1.3.5. Training and instructional aids

1.3.5.1. White board

Before the time ensure you have

- correct whiteboard pens (in different colours)
- correct eraser

During presentation

- make sure the writing is clear, readable
- use board economically - don't start in the middle if you are going to write a lot
- do not stand in front of your writing while writing notes
- do not talk while you write, and your back is to the group

After presentation

- clean white board before leaving

1.3.5.2. Video

Before video

- check whether everything is in working order before the time using a laptop and data projector
- with the laptop, check sound and if necessary, use speakers

To the group

- explain the purpose of the video
- explain the content of the video
- emphasise important points that the participants must take note of

During the video presentation

- stop the video for discussion or activities if planned
- do not leave the room while the video is still showing

At the end of the video session

- answer questions
- ask questions
- encourage discussion
- do a predetermined task - a group task rather than an individual task should lead to better discussions

1.3.5.3. Laptop and data projector

Before the presentation

- make sure the data projector is in good order and working, plugged in, knows where to switch on, and connected to the laptop
- placed in the correct position – ensure all can see
- picture in focus and square
- have the PowerPoint presentation opened and ready to start

During the presentation

- do not leave the projector on after the discussion
- do not shift/move the projector when it is switched on
- use a pointer if needed during the discussion
- do not stand in front of the projection screen
- be careful that you are not looking away from the group when you are talking to them
- do not read the PowerPoint slide to the group with your back to them – rather read it from the laptop that faces you facing the participants
- do not stand in front of the screen/block the data projector. It is important to make sure that you do not stand anywhere that might result in you blocking any participant's view of the screen. Check beforehand to determine your 'pacing area' - the area where you can stand and move in without you blocking anybody's view.

1.3.5.4. PowerPoint criteria

- visibility
- simplicity
- clarity
- ensure readable
- not more than 3 ideas/themes on one slide
- not too much typing/information on a slide

- emphasise important points – use another colour/bold, etc.
- When you are printing out the PowerPoint presentations make sure that you print it out with such a number of slides per page that will still ensure readability.

1.3.6. Dealing with the 'Dirty Dozen'

How to handle people who disrupt, side-track, or bog down proceedings

Scannell³ gave the following hints on how to spot problem persons in the audience and how to deal with them.

The Griper

A professional griper with a pet problem. Even if the complaint is legitimate, point out that policy cannot be changed here, and that the object is to operate as best possible under the system. Say that you'll discuss the problem with him after the lecture or by appointment. Depending on the problem, you can also ask a member of the group to respond but be careful as it could turn into a heated debate, side-tracking the whole lecture.

Highly argumentative

The combat personality or professional heckler. They may be normally good-natured but upset by personal or job problems. Keep your temper firmly in check, and do not let the group get excited either. Try to find honest merit in one of this person's points, express your agreement and move on to something else. When such a person makes an obvious mistake, toss it to the group and let them turn it down, rather than yourself. As a last resort, talk to this individual during a recess, or invite the person to discuss the point afterward with you and move on.

The Inarticulate person

A person who cannot put thoughts into proper words. This person may be getting ideas, but cannot convey them. Don't say: 'What you mean is...' Say: 'Let me repeat that ...' and put it into improved language, but don't get impatient and interrupt the person.

Off the subject

The person is not rambling, just off the subject with a question or comment. Take the blame: 'Something I said must have led you off the subject - this is what we should be discussing'. Restate the point or use the whiteboard or overhead projector to refocus the conversation.

3 Newstrom, J.W. & Scannell, E.E. 1997. The Big Book of Presentation Games: Wake-Em-Up Tricks, Icebreakers, and Other Fun Stuff. Available online at: <https://www.amazon.com/Big-Book-Presentation-Games-Icebreakers/dp/0070465010>

The opinion solicitor

Someone is trying to put you on the spot, making you support one view. The person may also simply be looking for your advice.

Generally, avoid solving this person's problem. Point out that your view is relatively unimportant, compared with the view of the entire group - but do not let this become a phobia. There are times when you must and should give a direct answer. Before you do, try to determine the reason for asking your view. Say: 'First, let's get some other opinions', or 'How do you look upon this point?' (Selecting a member of the group to reply).

The overly talkative

The person may be an 'eager beaver' or a show-off. May also be exceptionally well informed and anxious to show it, or just naturally wordy. Do not embarrass this person or be sarcastic - you may want to use the talkative traits later on. Slow him or her down with some difficult questions. Interrupt with: 'That's an interesting point. Now let's see what the group thinks of it'. In general, let the group take care of the situation as much as possible.

Personality clash

When two or more members clash, they sometimes divide the group into factions. Emphasise points of agreement and minimise points of disagreement, if possible. Draw attention to the objectives of the meeting or lecture. Cut across them with a direct question on the topic. Bring an objective member into the discussion. Frankly request that personalities be omitted from the subject at hand.

The quickly helpful

Someone who is trying to help, but actually makes it difficult and keeps others out of the interplay. Tactfully cut off this individual by questioning others. Suggest that 'we put others to work'. Use the eager helper for summarising.

The rambler

One who talks about everything, but the subject often uses farfetched analogies and gets lost. When this person stops for a breath, say thank you, refocus everyone's attention by restating the relevant points, and move on. Grin, say you find the remarks interesting, then point to the white board and in a friendly manner indicate that you're getting a bit off the subject. As a last resort, glance at your watch.

Silent Sam

Someone who just won't talk, who may be bored, indifferent, timid, conceited, or insecure. Your actions will depend upon what is motivating the individual. Ask directly for his or her opinion. Draw out the person next to him or her, then ask the quiet individual for an opinion on the view expressed. If the quiet person is seated near to you, let him or her talk to you, not the group. If he or she is the 'superior' type, indicate your respect for his experience (but don't overdo it or the group will dislike it) and then ask for an opinion or comment on the topic at hand. Toss out a provocative query. If the person is sensitive or timid, however, compliment him or her for joining in - and be sincere.

Stubborn stickler

Someone who won't change his or her mind, who hasn't seen your point. Throw this person's views to the group, and have members counteract. Say that time is short, and you'll be glad to discuss the point later; ask him or her to accept the group viewpoint for the moment.

Talkers on the side

People holding their own conversations, which may be related to the subject or may be personal - but are distracting members of the group and you. Don't embarrass them. Call one by name and ask the person an easy question or call one by name and restate the last remark made by a member of the group, asking for an opinion on it. If during the conference you are in the habit of moving around the room, saunter and stand casually behind members who are talking but don't make your point too obvious.

1.4. Alternatives to training - webinars

With the availability of audio-visual platforms such as Zoom, Google Meet and MS Teams it is often an easy and cost-effective option to do webinars for training and awareness-raising initiatives. As a general rule, it tends to be less interactive and participatory than in-person training, with the potential of connectivity interruptions but can assist to quickly getting information and basic training and awareness to participants on specific topics.

Trainers need to ensure that they are familiar with the audio-visual platform and understand how to use it to increase participation through polls and other tools available on the platform, including how to share PowerPoints, mute and unmute participants, etc.

The invitation and programme can be sent out with the link to join, or the invitation can be sent out with a registration link where after participants receive the link to join the webinar.

With webinars, it is useful to have a moderator to assist the presenters with monitoring questions in the chat or Q&A features as well as raised hands as presenters will often not be able to see that while presenting.

Generally, it is better to keep webinars shorter and focused on a specific topic – preferably 60 to 90 minutes. As webinars can be recorded, the video recording of the presentation and material can further be forwarded to others who could not join the live presentation.

It can also be considered to have a hybrid event by using an audio-visual link for in-person training for participants and speakers who cannot attend in person. Arrangements must then be made for a camera at the event and the other technical requirements.

1.5. Conclusion

With proper planning and preparation, training can be very rewarding and a lot of fun. Good luck with the training you are going to do in the future. Remember that you are only human, and you can expect the unexpected to happen. To be a good trainer, you need not be perfect, or have unlimited knowledge - no person can ever know everything.

Being a trainer can be exhausting, frustrating, and sometimes even demotivating. Look after yourself - physically and mentally and be good to yourself when you are training to avoid becoming frustrated, demotivated or negative.



PART TWO

Gender-based Violence and CVAWG

LEARNING OBJECTIVES

Recognising the prevalence of gender-based violence and cyberviolence against women and girls



Understanding online gender-based violence (GBV)



Identifying the myths about GBV



Knowing about international and regional standards on GBV



Comprehending the SADC Model Law on GBV



Understanding cybercrime instruments



Knowing about national, regional, and international laws on cybercrime



Understanding the SADC Model Law on cybercrime



It is critical for victims/survivors who participate in the criminal justice system to encounter law enforcement and prosecutors who understand and respect both the survivors' rights and their unique vulnerabilities.

2.1. Introduction to Gender-based Violence

To understand online and offline Gender-based Violence (GBV) crimes, particular terminology has been provided in the glossary for reference.

In General Recommendation 19, the CEDAW Committee defines GBV as a form of discrimination. As such, GBV is defined as violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental, or sexual harm or suffering, threats of such acts, coercion, and other deprivations of liberty.

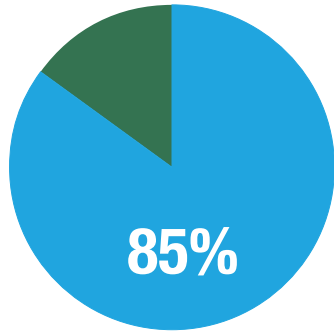
2.2. Prevalence of Gender-based Violence and CVAWG

'... the landscape of gender-based violence has been transformed ... [but] rather than there being a dramatic reduction in violence against women, ... the challenges have become more complex, the resistance to change deeper, the backlash against the empowerment of women more blatant and the methods used to uphold the status quo more sophisticated and insidious'.⁴

⁴ Cyber Violence Against Women And Girls: A World-Wide Wake-Up Call. Report By The UN Broadband Commission For Digital Development Working Group On Broadband And Gender. Available online at: <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>

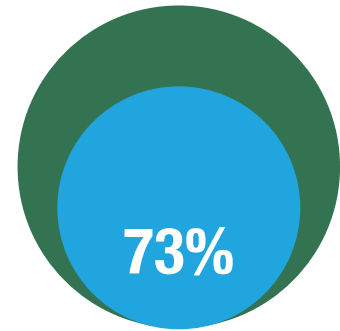
Figure 1: Global prevalence of CVAWG⁵

CVAWG AROUND THE WORLD



Percentage of women who say the internet provides them with more freedom (2013)

Percentage of each gender who use social networking sites



Percentage of women abused online



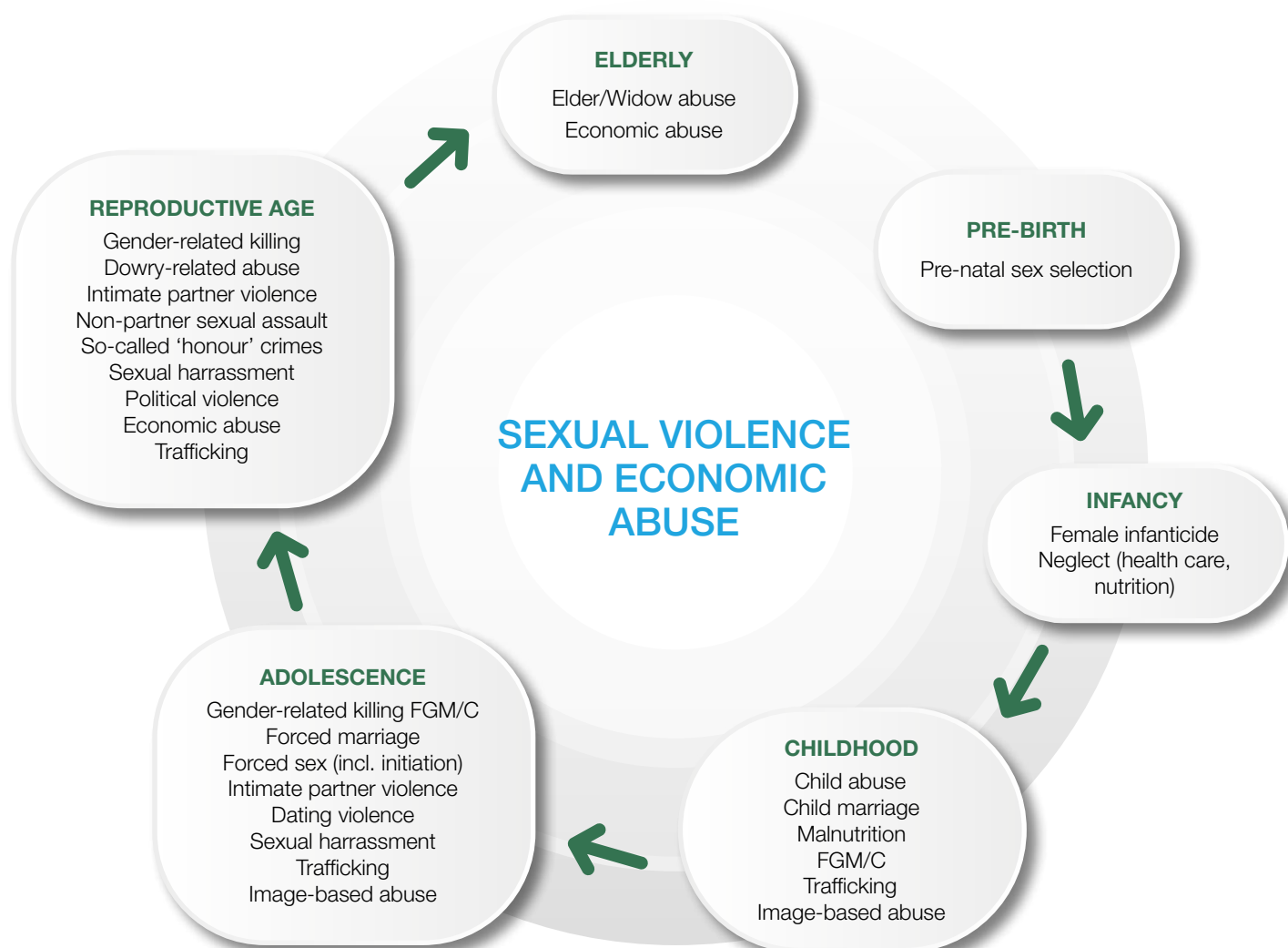
5 Ibid

Gender-based violence and femicide (GBVF) is a universal phenomenon. Globally, one in three women experiences either intimate partner violence or non-partner sexual violence during their lifetime (WHO, 2018). GBV has serious consequences for women's physical health, including their sexual and reproductive health, as well as their mental health. GBV is a fundamental violation of women's human rights and has adverse economic and social consequences for women, men, their children, families and communities. Yet, very few of them seek professional help, preferring to keep their abuse secret due to various barriers, including discrimination and stigma.

Women experience abuse and violence right through their **life cycles**. Some abuses are occurring at a specific stage in a woman's life, but many could reoccur or continue throughout her life.

Violence against women comprises of a wide range of acts – from verbal harassment and other forms of emotional abuse to daily physical or sexual abuse. At the far end of the spectrum is femicide: the murder of a woman. Femicide is generally understood to involve the intentional murder of women because they are women, but broader definitions include any killings of women or girls. Femicide is usually perpetrated by men, but sometimes female family members may be involved.⁷ Most cases of femicide are committed by partners or ex-partners and involve ongoing abuse in the home, threats or intimidation, sexual violence or situations where women have less power or fewer resources than their partner. An ongoing study by WHO shows that more than 35% of all murders of women globally are reported to be committed by an intimate partner. In comparison, the same study estimates that only about 5% of all murders of men are committed by an intimate partner. Evidence also shows

Figure 2: Life cycle of gender-based violence against women and girls⁶



6 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

7 WHO: Understanding and addressing violence against women: Femicide (2012). Available online at https://apps.who.int/iris/bitstream/handle/10665/77421/WHO_RHR_12.38_eng.pdf

that women killing their male intimate partners often act in self-defence following ongoing violence and intimidation⁸.

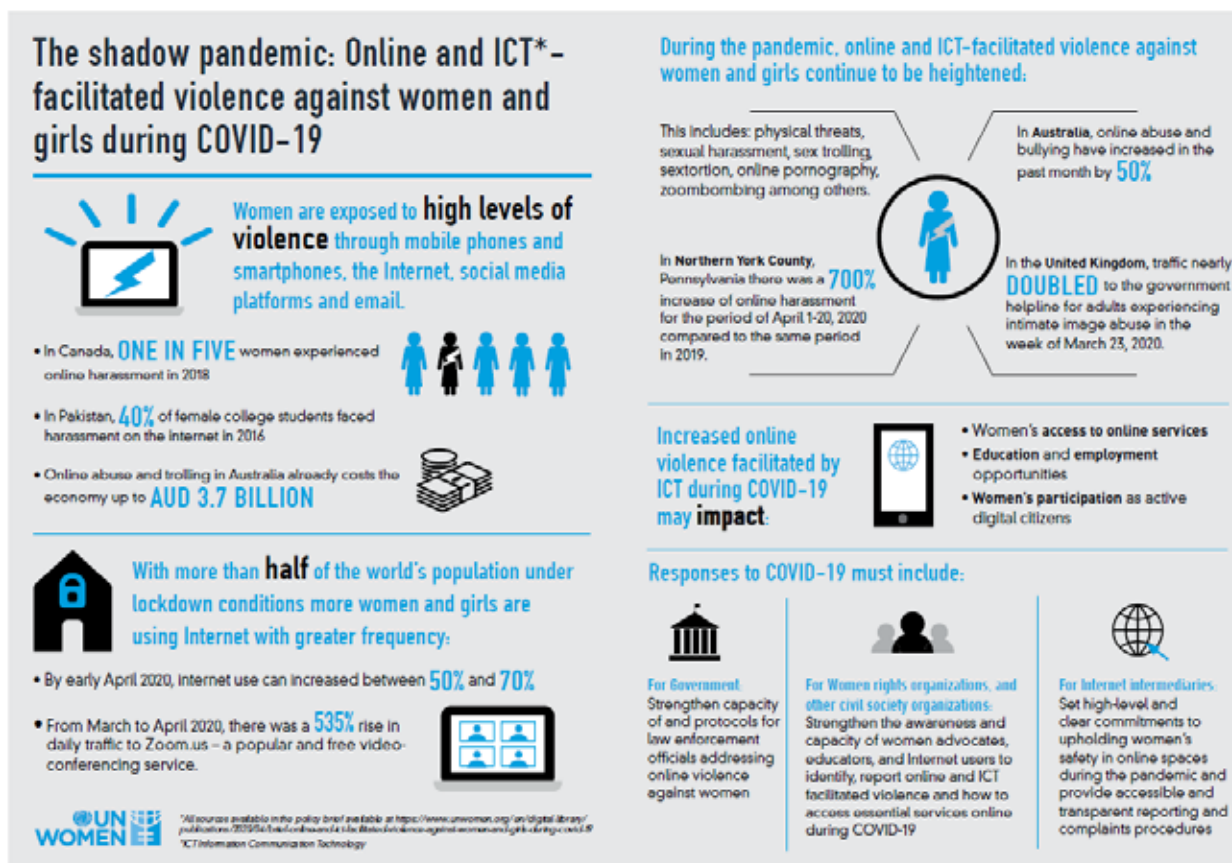
Not only is intimate partner femicide the most extreme consequence of intimate partner violence, but it also has a strong and prolonged impact on women's surroundings. For example, surviving children of women killed by their intimate partners experience long-lasting effects, since they lose one parent to the murder, the other parent to jail, and often have to leave their parental home and adjust to a new environment in which they might be labelled as the child of the murderer.⁹

The **Covid-19** pandemic deepened economic and social stress, enforcing restricted movement and social isolation measures, resulting in increased risks of gender-based violence, particularly in the domestic context. During Covid-19, violence against women manifested in different, extended forms, including domestic violence, and online and ICT-facilitated violence.

Conflict can result in higher levels of gender-based violence against women and girls. **Conflict-related sexual violence (CRSV)** happens both as a result of general lawlessness and as a political or military tactic used frequently and deliberately to target civilians,¹¹ inflicting long-term trauma and humiliation, fracturing families and the social fabric, triggering displacement, and fuelling armed actors' activities. Women and girls continue to be those primarily affected by CRSV, not least due to patterns of gender discrimination and inequality predating the conflict.

The term 'cyber' is used to capture the different ways that the Internet exacerbates, magnifies or broadcasts abuse. The full spectrum of behaviour ranges from online harassment to the desire to inflict physical harm including sexual assaults, murders, fraud, and suicides.¹² The growing reach of the internet, the rapid spread of mobile information and communications technologies (ICTs), and the wide diffusion of social media have presented new opportunities and enabled various efforts to address CVAWG (violence

Figure 3: The shadow pandemic – online and ICT-facilitated violence against women and girls during Covid-19 ¹⁰



8 Daly M. & Wilson M. Evolutionary Social Psychology and Family Homicide. Science. Oct 1988, 242(4874), 519 - 524. Available at: <https://www.science.org/doi/abs/10.1126/science.3175672>

9 Lewandowski L.A., McFarlane, J., Campbell, J.C., Gary, F & Barenski, C. 'He killed my mommy!': murder or attempted murder of a child's mother. Journal of Family Violence, 2004, 19, 211–20. Available online at: <https://link.springer.com/article/10.1023/B:JOFV.0000032631.36582.23>

10 UN Women: Online and ICT facilitated violence against women and girls during Covid-19. Available online at: <https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19> (Infographic)

11 OHCHR: Women's human rights and gender-related concerns in situations of conflict and stability, 1996-2022. Available online at <https://www.ohchr.org/en/women/womens-human-rights-and-gender-related-concerns-situations-conflict-and-instability>

12 The New Yorker: The Story of Amanda Todd by Michelle Dean, 18 October 2012. Available online at: <https://www.google.com/search>

against women and girls).¹³ These types of violence occur on every online platform and internet-connected technological tool available to users. Despite the relatively new and growing phenomenon of internet connectivity, it is estimated that one in ten women has already experienced some form of cyber violence since the age of 15 years.¹⁴ However, ICTs and social media are also being used as tools to inflict harm on women and girls. CVAWG is emerging as a global problem with serious implications for individuals, societies, and economies around the world. The statistics pose risks to the peace and prosperity for all enshrined in the Charter of the United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement.¹⁵

CVAWG cannot be conceptualised as a completely separate phenomenon from ‘real world’ violence, when in fact it is more appropriately seen as a continuum of offline violence. Online and technology-facilitated violence against women is very often the perpetuation of the different forms of violence against women happening offline, such as on the street, in the office, at school and university, at home, and in every course of life. Most of the forms of online and technology-facilitated violence against women already exist offline and are expanded, amplified or generalised, for example in the case of domestic violence, including post-separation abuse and stalking.¹⁶ For example, cyberstalking by a partner or ex-partner follows the same patterns as offline stalking and is therefore intimate partner violence (IPV), simply facilitated by technology. Evidence confirms this continuum: a United Kingdom study of cyberstalking found that over half (54 %) of the cases involved the first encounter in a real-world situation.¹⁷ An inadequate criminal justice response can be attributed in part to the false dichotomy between online and offline CVAWG, which results in police discounting and minimising the harm caused and constructing victims’ experiences as ‘incidents’ rather than patterns of behaviour over time.

While there is still a lack of comprehensive global definitions and data on online and ICT-facilitated violence, research suggests that women are disproportionately targeted and

suffer serious consequences as a result. When women and girls do have access to the Internet, they face online violence more often than men through a continuum of multiple, recurring and interrelated forms of gender-based violence. Gender-based violence against women and girls takes place in a context of widespread systemic gender-based discrimination.

Reports suggest that 73% of women have already been exposed to or have experienced some form of online violence in what must still be considered a relatively new and growing technology.¹⁸

Online and technology-facilitated violence also contains a series of specificities: victimisation is aggravated by the number of perpetrators, the multiplicity of channels engaged, the impossibility to escape, and the difficulty to erase content from the Internet.¹⁹ These characteristics amplify the negative impact of this form of violence on victims. In addition, victims face numerous difficulties on the road to reparation, from the volatility of proof to hardships experienced in finding help and assistance. Prosecution remains difficult as laws are not necessarily keeping up with technological developments and law-enforcement officials may be under-trained, under-resourced, and under-equipped to assist victims.

Changing social attitudes and norms is the first step to shifting the way online abuse is understood as a serious challenge. Violence is not new, but cyberviolence is, and the public needs to recognise this and address it as a priority issue. Hence, sensitisation to CVAWG must include education, capacity development, ensuring safeguards to secure safe online spaces, and putting in place and enforcement of sanctions. Furthermore, an impactful attack on CVAWG also needs to emphatically address ‘victim blaming’. This destructive response needs to be addressed as a primary issue of concern as there is no situation in which a violent act should be accepted or condoned as a result of personal judgement and social behaviour. Therefore, a section on myths has been included in this handbook to address the above.

-
- 13 Europe Institute for Gender Equality (europa.eu): Cyber violence against women and girls (2017). Available online at <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.
 - 14 European Union Agency for Fundamental Rights (2014). Violence against women: an EU-wide survey – Main results. Luxembourg: Publications Office of the European Union, p. 104. Available at: <http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>
 - 15 Broadband Commission: Please see in particular the various reports of the Broadband Commission. Available online at: <http://www.broadbandcommission.org/resources/Pages/default.aspx>
 - 16 Council of Europe: Protecting Women and Girls from Violence in the Digital Age: Adriane van der Wilk, December 2012. Available online at: <https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3>
 - 17 British Journal of Psychiatry: The impact of stalkers on their victims. [Abstract]: Pathé, M. and Mullen, P.E. January 1997, 170(1) 12-17. Available at: <https://www.ncbi.nlm.nih.gov/pubmed/9068768#>
 - 18 UN Women: Facts and figures – Ending violence against women. Available at <http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures>
 - 19 Council of Europe: Protecting Women and Girls from Violence in the Digital Age: Adriane van der Wilk (December 2012). Available online at: <https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3>

As the Internet evolves and social media and networking tools increasingly become an intrinsic part of people's lives around the globe, attitudes and norms that contribute to CVAWG should be addressed. It is vital to expand the description of problems and violations that women encounter online and name them as gender-based violence against women and girls, which includes but is not limited to harassment. Globally, girls and women are subjected to deliberate forms of violence because of their gender. The violence includes dehumanising, aggressive, and harmful acts that are in turn physical, psychological, sexual, and exploitative. These acts take place behind closed doors in the privacy of homes or workplaces, out in the open in public settings, and sometimes amid communities and societies. Violence online and offline, or 'physical' VAWG and 'cyber' VAWG, feed into each other. Abuse may be confined to networked technologies or may be supplemented with offline harassment including vandalism, phone calls and physical assault. Similarly, the viral character of distribution is now explosive. What was once a private affair can now be instantly broadcast to billions of people across the digital world.

In enhancing the fight against ICT-facilitated women and child abuse and exploitation, governments and national authorities should focus on:²⁰

- a women and child protection approach that fully respects human rights
- ensuring that legislation keeps pace with technological innovation
- recruiting, training and maintaining specialised personnel
- gaining access to state-of-the-art technological resources
- developing effective mechanisms for accessing third party data and conducting undercover investigations that are consistent with the rule of law
- developing policy guidance on harmful conduct committed by youth.

The formulation of policies in this area is best based on a multidisciplinary approach that draws on research findings and best practices from social science, legal policy and public policy. Efforts to effectively and comprehensively combat ICT-facilitated child abuse and exploitation

necessitate a multi-stakeholder approach, while actively involving children, families, communities, governments, members of civil society, and the private sector.

As the 'social Internet' continues to grow exponentially, it has become almost impossible to monitor and control illegal and harmful content. To understand the magnitude, some data references are helpful.

In the first quarter of 2022:

- Facebook had 1.62 billion users every day.²¹ This means that just under a quarter of the entire world population are daily active users
- YouTube reported more than 500 hours of video were uploaded every minute and has approximately 122 million users every day²²
- Twitter averaged 237.8 million monthly active users²³
- WhatsApp is the most popular global mobile messenger app worldwide with approximately 2.44 billion monthly active users. In India alone, WhatsApp users reached the 487 million per month mark.²⁴

Women aged 18 to 24 are at a heightened risk of being exposed to every kind of CVAWG. They are 'uniquely likely to experience stalking and sexual harassment, while also not escaping the high rates of other types of harassment common to young people in general', like physical threats.²⁵

As the use of connectivity increases worldwide, so will the reach of violence. Women who are victims of cyberviolence rarely report the crime.²⁶ A report from India, for instance, suggests that 'only 35% of the women have reported about their victimisation, 46.7% have not reported and 18.3% have been unaware of the fact that they have been victimised. Women prefer not to report about their victimisation owing to social issues'.²⁷

While the Internet is a potential engine of equality, it has also often reinforced the power imbalances of offline realities, and escalating CVAWG is one indicator that further cement and magnifies unequal power relations between men and women. The social and structural inequalities contributing to VAWG are well established and recognised within normative frameworks such as CEDAW.

20 UN Women: Safe Digital Spaces: Protection of Women and Girls from Technological Violence – A Background Paper (2019). Available online at: <http://africa.unwomen.org/en/digital-library/publications>

21 Social Shepherd: 30 Essential Facebook Statistics You Need to Know in 2022. Available online at: <https://thesocialshepherd.com/blog/facebook-statistics>

22 Ibid

23 Statista (2022): The Universe of Data – Number of monetizable daily active Twitter users (MDAU) worldwide from 1st quarter 2017 – 2nd quarter 2022. Available online at: <https://www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/>

24 Ibid

25 Hess, A. On the Internet, Men are called Names. Women are Stalked and Sexually Harassed (22 October 2014). Available online at: <https://slate.com/human-interest/2014/10/pew-online-harassment-study-men-are-called-names-women-are-stalked-and-sexually-harassed.html>

26 Inter Press Service News Agency: Cyber Bullies Target Kenya's Women (30 January 2014). Available online at: <http://www.ipsnews.net/2014/01/cyber-bullies-target-kenyas-women/>

27 Halder, D. & Karuppanan, J. Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India (October 2010). Available online at: <https://www.tandfonline.com/doi/abs/10.1080/15564886.2011.607402>

Although gender-based violence is a worldwide problem, it is known to be widespread in the Southern African Development Community (SADC) region and presents a major obstacle to attaining gender equality and equity. Gender-based violence covers a large array of gender-related crimes against women and girls. When referring to gender-based violence SADC recognises that the discussion is not just about the act of violence, but also about education and prevention, as well as victim assistance.

2.3. Myths of Gender-based Violence

People's values, beliefs and attitudes reflect their perceptions of life. They are initially learned from people's families and are, in turn, shaped by culture and society. Over time, and throughout our lifespans, personal experiences cause us to question and sometimes to change our values and beliefs. It's all very well to talk about other people's beliefs about GBV – but what about our own? Do they reflect harmful beliefs and expectations that contribute to fostering sexual violence?

The following so-called 'statements' are in fact myths about gender-based violence that attempt to explain or justify it. Such views lead to a perception that GBV is rare or exceptional and/

or that it is caused by factors outside of men's control. They are used as justifications for violence. These views place the onus on women to ensure that they minimise the chances of their behavior instigating violence. Justifications for violence are frequently based on gender norms.

Gender norms are the socially assigned roles and responsibilities of women and men. Cultural and social norms often socialise men to be aggressive, powerful, unemotional, and controlling. This contributes to a social expectation (by both men and women) that accepts men as dominant. Similarly, expectations of women are that they are passive, nurturing, submissive, and emotional. This reinforces women's roles as weak, powerless, and dependent on men.

The socialisation of both men and women has resulted in an unequal balance of power and unequal power relationships between women and men. In many societies, children learn that men are dominant and that violence is an acceptable means of asserting power and resolving conflict. Women as mothers and mothers-in-law unwittingly perpetuate violence by socialising boys and girls to accept the dominance of men and by acquiescing throughout life to men's demands.

MYTHS ON GENDER-BASED VIOLENCE
<p>Myth 1: Domestic violence is a private family matter, in which the state has no right to intervene. How a man treats his partner is a private matter.</p>
<p>Reality: Violence against women is a human rights violation, regardless of whether it occurs in the family or the public sphere.</p>
<p>Myth 2: A man cannot rape his wife.</p>
<p>Reality: Rape is defined by an action and not by the identity of the perpetrator or the survivor. Accordingly, any forced sexual intercourse is rape, irrespective of whether the survivor is married to the perpetrator or not. This statement is also grounded in international human rights law definitions, which encompass all forms of physical, sexual, psychological, or economic violence against women. To stop the scourge of gender-based violence, we need to break the silence. This should not be the responsibility of the victims alone. All of us need to speak up, speak about and speak to the violence.</p>
<p>Myth 3: GBV only includes physical abuse (hitting, punching and pushing).</p>
<p>Reality: Physical abuse is just one form of violence. GBV can also manifest as emotional, verbal and psychological abuse. These forms of abuse can take a variety of forms, such as patterns of degrading or humiliating conduct towards another, including repeated insults, ridicule or name-calling; repeated threats to cause emotional pain; or the repeated exhibition of obsessive possessiveness or jealousy, such that it causes a serious invasion of privacy, integrity or security.</p> <p>Economic abuse is another form of violence. It involves:</p> <ul style="list-style-type: none"> • preventing a victim from acquiring resources (e.g. not being allowed to work) • limiting the number of resources available to him/her • exploiting the victim's economic resources (e.g. keeping or hiding the victim's bank card).

Myth 4: Women allow themselves to be abused. They could leave their partners if they really wanted to.

Reality: No one deserves to be abused. Perpetrators use tactics of control and abuse that make it very difficult for women to escape the violence. It is also important to understand that women who experience violence perpetrated by an intimate partner and seek to leave the relationship to ensure their own and their children's safety, face an increased risk of ongoing and even escalating violence. Research has shown that the time when a woman and/or her children leave an abusive relationship is when they are most likely to be seriously harmed or murdered by their partner. Women are also prevented from leaving violent relationships because of shame and guilt, lack of safe housing, or the stigma of divorce.

Myth 5: Men and women are equally violent to each other.

Reality: The majority of those affected by GBV, particularly intimate partner violence (IPV), are women and girls. Worldwide, almost half (47%) of all female victims of homicide are killed by their intimate partners or family members, compared to less than 6% of male homicide victims. IPV is the most common form of violence experienced by South African women and is the leading cause of death among South African women. On average, a woman dies every eight hours at the hands of an intimate partner in South Africa. More women are killed by their current or former intimate male partner in South Africa than in any other country in the world.

Myth 6: The perpetrators of violence are a minority group of men with mental health issues.

Reality: Violence may be perpetrated by those with mental health problems, but it is by no means a behavior related only to those who are mentally ill. Violence, and GBV in particular, is a common occurrence worldwide. It is a socially and culturally learned behaviour.

Myth 7: Poverty leads to attacks on and abuse of women.

Reality: Poverty may exacerbate levels of violence. Some studies have found this phenomenon to be a risk factor for gender-based violence that cuts across socioeconomic levels. There are many individuals living in poverty who are not violent toward women, and there are many individuals in higher economic quintiles or non-conflict settings that are violent toward women.

Myth 8: Gender-based violence is caused by substance abuse such as alcohol and/or drugs.

Reality: Substance abuse may precipitate violent behavior or make potential victims more susceptible to violence. First, it may lower inhibitions on the side of the perpetrator. For the potential victims, it may impair judgment and cause them to make decisions that put them in situations that increase their risk for abuse or prevent them from defending themselves. It is important to recognise that neither alcohol nor drugs or the victim should be blamed in these situations. Violence against women is unacceptable under all circumstances.

Myth 9: Gender-based violence is an inevitable part of intimate partner relations.

Reality: Disagreements and disputes may be inevitable parts of intimate partner relations. However, violence as a way to resolve those disputes is not. Violence is a learned behavior and can be unlearned.

Myth 10: Violence against women is an inherent part of maleness or a natural expression of male sexual urges.

Reality: Male violence is not genetically based; it is perpetuated by a model of masculinity that permits and even encourages men to be aggressive. It is up to us as individuals, communities, and society to change these gender norms so that violence against women is not accepted or tolerated.

Myth 11: Men who commit rape are mentally ill.

Reality: Perpetrators of rape are generally normal men from all sorts of backgrounds. Most appear to be no different from other men in the community. Research has shown that only 5% of rapists can be classified as mentally ill.

Myth 12: Men abuse girls when their wives are not satisfying them sexually.

Reality: Men who have unsatisfactory sexual relationships with their wives do not usually assault or abuse children.

Myth 13: Some girls are seductive or sexually provocative and cause men to be sexually aroused.

Reality: The victim is not responsible for the perpetrator's actions. This myth takes responsibility for abuse away from the adult and places it on the child. Children are relatively powerless, and adults always retain a choice in how they will respond to a child's behaviour.

Myth 14: Women ‘ask’ to be raped by wearing provocative clothes.

Reality: Rape is a violent and terrifying crime. Nobody wants to be raped or asks to be raped. Appearance and clothing have absolutely nothing to do with who is violated. Victims may be raped regardless of what they are wearing at the time, be it jeans and a T-shirt, a sari, a skirt, or a nun’s habit. Although a man might become aroused when seeing a woman dressed in revealing clothing, most men do not choose to sexually assault her. When one does, the responsibility for the incident lies with the attacker.

Myth 15: Rape is an act of lust or passion.

Reality: Sexual violence is an aggressive act. The underlying factors in many sexually violent acts are power and control, not a sex craving. It is a violent, aggressive and hostile act used to degrade, dominate, humiliate, and control. Sexual violence violates a victim’s sense of privacy, safety and well-being.

MYTHS ON CYBERVIOLENCE

Myth 1: Victims of sexual cybercrime are only those who have been the subject of online threats and bullying to meet someone in person and be sexually abused or assaulted.

Reality: Acts of cyberviolence may involve different forms of harassment, violation of privacy, sexual abuse and sexual exploitation, and bias offences against social groups or communities.²⁸ Cyberviolence may also involve direct threats or physical violence as well as different forms of cybercrime.

Myth 2: Whatever happens on the internet is not real. The victim is not in any actual danger.

Reality: In fact, victims are in greater danger because they may not even know the identity of the perpetrators. The perpetrator can inflict harm with a click of the finger without being physically near the victim. Once uploaded online, harmful comments, images, videos or posts may exist for a long time in the online space and can be shared by others multiple times.

Myth 3: It’s just the internet – victims should not overreact.

Reality: Online abuse can have severe mental health consequences. In fact, 55-67% of women polled in the U.S. and the U.K. said that harassment on social media meant they experienced emotional distress and fear. They were less able to focus on everyday tasks, had experienced stress, anxiety or panic attacks, and had a feeling of apprehension when thinking about social media or receiving social media notifications.²⁹ Women also reported feeling disempowered and wanting to censor themselves online to avoid more harm. (This has the effect of silencing women.) More alarmingly, 41% of these women said that the online abuse made them feel like their physical safety was threatened.

Cybersexual abuse can also impact personal relationships and women’s ability to retain custody of their children. Offenders may use sexually explicit photos in child custody cases to try and portray a mother as an ‘unfit parent,’ send photos to their children or their school or try and portray them as consumers of child pornography.

Myth 4: If the victims switch off their computers/mobile phones, the violence will stop.

Reality: No, the violence does not stop. As the victims have left a ‘digital footprint’ online which is long-lasting, the perpetrators can easily obtain personal information about the victims to continuously harass, intimidate and exploit the victims on the internet in other ways, such as impersonating the victim to commit crimes.

Myth 5: If the perpetrator deletes the comments, images or posts after the incident, then it is not considered online violence because the content is no longer available online.

Reality: Although the perpetrator has deleted the postings, it is still a form of violation or abuse. Deleted comments, images, videos and/or posts can still be found online because they may have been shared or circulated by others on their online platforms.

28 Council of Europe: Types of cyberviolence. Available online at: <https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence>

29 Amnesty International: Violence against Women Online in 2018. Available online at: <https://www.amnesty.org/en/latest/research/2018/12/rights-today-2018-violence-against-women-online/>

Myth 6: Online violence is committed by strangers.

Reality: Online violence can be committed by people that victims know, such as their spouses, colleagues and friends.

Myth 7: Abusers are extremely familiar with the technology.

Reality: Abusing someone online is as easy as setting up a Facebook account,³⁰ or creating fake dating app profiles. More or less, the only thing needed to sign up for a social media platform is an email address. In fact, Facebook estimated in 2018 that there were up to 116 million fake profiles on its platform. If a perpetrator wants to impersonate someone else on a dating app, all they have to do is put in a fake name and some photos. There are applications and software that are readily available and easy to use on the internet that perpetrators can make use of and/or install in their victim's digital devices to hack and monitor phone calls/texts, their GPS location, emails, social media usage, internet browser, etc.

Myth 8: Abusers need money to operate.

Reality: Not true, because most social media platforms and common dating apps are completely free. These companies do not have to ask for a fee because they use **the users to convince advertisers to pay for space to promote their brands**. Advertisers will often pay more to get their posts promoted to reach a larger audience.

Although people do not pay to use social media or dating apps with money, they are paying with something else: their personal information.

Myth 9: Online sexual victimisation only affects women.

Reality: Anyone can be a victim of online abuse and harassment, but it is often gendered and specifically targeted at women and girls. A 2020 report from Plan International, surveying over 14,000 girls from different countries, found that 58% had some experience of online harassment.

Myth 10: The online abuse of children is only carried out by adult men, most of whom are paedophiles or mentally ill, and collect images of child sexual abuse.

Reality: Both men and women participate in child exploitation, although males constitute the majority of perpetrators in child abuse. Certain forms of exploitation including trafficking and cyber-bullying may, however, have a high prevalence of female perpetrators.³¹ A 2018 report by INTERPOL and ECPAT International found that 92% of visible offenders were men, and predominantly from a white or European background.³² Online predators are **internet users who exploit children and teens for sexual and violent purposes**. This may include child grooming, engaging in sexual activities, unwanted exposure of materials and pictures, online harassment, and threats to cause fear or embarrassment.

Myth 11: It only occurs in heterosexual 'romantic' relationships.

Reality: Abuse can occur in any type of relationship, whether you're straight, gay, bisexual, trans, casually dating, married, randomly hooking up, etc. Women, girls and LGBTQIA+ individuals are disproportionately impacted by technology-facilitated GBV. A 2016 study³³ found that internet users who identified as lesbian, gay, or bisexual were significantly more likely to be the target of revenge-porn threats (15% compared to only 3% of all Americans) and were also more likely to have their sexually explicit photos posted online (7% of LBG internet users were victims, while only 2% of all Americans had their photos posted).

Myth 12: It is driven by passion, not violence.

Reality: Abuse always involves control. Abusers might pretend that they just love you so much they can't help themselves. They want to keep you safe, make sure you're being faithful, or keep you where they can see you because they 'just couldn't bear to lose you'. These actions do not come from a place of love. They come from a desire to exert their own power by taking away yours. Online abuse is an act of control and violence.

Offenders create fear through intimidating or threatening messages, isolate their victims by limiting their ability to communicate with friends and family, humiliate them by posting intimate images online, or try to get them fired by sending their nude pictures to employers, etc.

30 Goldberg, C.A. Top 5 Myths about Online Abuse. Available online at: <https://www.cagoldberglaw.com/top-5-myths-about-online-abuse/>

31 UNODC: Facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children, 2014 Available online at: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf

32 INTERPOL and ECPAT: Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018. Available online at: <https://www.iicsa.org.uk/key-documents/3720/view/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf>

33 Center for Innovative Public Health Research: New Report Shows that 4% of U.S. Internet Users Have Been a Victim of "Revenge Porn" (13 December 2016). Available online at: <https://innovativepublichealth.org/press-releases/revenge-porn-report-findings/>

2.4. Power

Power is central to GBV. Violence is both an act of, and abuse of power. Violence involves using power over another. To understand violence, it is necessary to reflect on power, how it is distributed in the community and how it is used over other people, and to reflect on other dimensions of power. Power in itself is not a bad thing. It depends on how it is used. The following information gives an overview of one approach to understanding other expressions of power. When you have read through it, think about the different expressions of power in your own life. How do you exercise power **over** other people? Who do you have power **with**? How can we build power **to**? How might the concept of power **within** be relevant to violence?

2.4.1. Expressions of power: over, to, with, and within

Power over: This is the most commonly recognised form of power. It has many negative associations for people, such as repression, force, coercion, discrimination, corruption and abuse. Power is seen as a win-lose relationship. Having power involves taking it from someone else, and then using it to dominate and prevent others from gaining power. This power perpetuates inequality and injustice. There are three alternative, more collaborative ways of exercising and using power: power to, power with, and power within. These offer positive ways of expressing power that create the possibility of forming more equitable relationships. By affirming people's capacity to act creatively, they provide some basic principles for constructing empowering strategies.

Power to: This kind of power is the unique potential of every person to shape his or her life and world. When based on mutual support and respect, it opens up the possibilities of joint action or 'power with'. It thrives in an atmosphere of trust, empowerment and accountability. It is closely associated with women's, men's, girls' and boys' intimate realms of power. Citizen education or leadership development for advocacy is based on the belief that each individual has the power to make a difference.

Power with: This power depends on finding the common ground among different interests and building collective strength. Based on mutual support, solidarity and collaboration, it multiplies individual talents and knowledge. It can help build bridges across different interests to transform or reduce social conflict and promote equitable relations between women and men. Advocacy groups seek allies and build coalitions drawing on this form of power.

Power within: This form of power relates to a person's sense of self-worth and self-knowledge and it includes the ability to recognise individual differences while respecting others. It is based on self-acceptance and self-respect. It is the capacity to imagine and have hope; it affirms the common human search for dignity and fulfilment. Many grassroots efforts use individual storytelling and reflection to help people affirm their personal worth and recognise their power to and power with. Both these forms of power – 'power with' and 'power within' – are referred to as agency: the ability to act and change the world. 'Power within' is closely related to women's, men's, girls' and boys' intimate realms of power.

2.5. International and Regional Legal Frameworks and Standards on GBV

The international legal framework for GBV is informed by a combination of hard and soft law which has three tiers – an international human rights framework, regional human rights instruments, and the SADC human rights system.

Several human rights Resolutions and Declarations have been adopted by the General Assembly. Although these legal instruments are soft law or not legally binding, they have often been a precursor for binding international treaties such as CEDAW. It also 'receives and discusses reports by the treaty-based bodies and through the Economic and Social Council'. These Resolutions assist in the creation of customary international law. Customary international law can be traced from 'a general and consistent state practice that States follow from a sense of legal obligation'. State practice is exemplified through consenting to treaty-making processes.

2.6. United Nations Human Rights Standards

2.6.1. CEDAW

On 18 December 1979, the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) was adopted by the United Nations General Assembly.³⁴ In 1992, the CEDAW Committee in its General Recommendation No. 19, defines violence against women as a form of discrimination and includes gender-based violence as directed towards a woman because she is a woman, or that affects women disproportionately. The definition comprises acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion, and other deprivations of liberty. In 1993, the Vienna Declaration and Programme of Action recognised that the elimination of violence against women in public and private life is a human rights obligation.

34 United Nations Human Rights - Office of the High Commissioner: General recommendation on the Elimination of Discrimination against Women. Available online at: <https://www.ohchr.org/en/treaty-bodies/cedaw/general-recommendations>

The then Commission on Human Rights condemned gender-based violence for the first time in 1994 and the same year appointed a Special Rapporteur on violence against women, its causes and consequences.

On 14 July 2017, the Committee on the Elimination of Discrimination against Women (CEDAW Committee) adopted General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19. General Recommendation No. 35 elaborates on the gender-based nature of this form of violence, building on the work of the Committee and other international human rights mechanisms, as well as developments at national, regional and international levels.³⁵

Framing gender-based violence against women as a human rights violation implies an important conceptual shift. It means recognising that women are not exposed to violence by accident, or because of an in-born vulnerability. Instead, violence is the result of structural, deep-rooted discrimination, which the State has an obligation to address. Preventing and addressing gender-based violence against women requires legislative, administrative and institutional measures and reforms, including the eradication of gender stereotypes.

The Declaration on the Elimination of Violence Against Women and the CEDAW Committee's General Recommendation No. 35 provide for the concept of due diligence as an obligation of States. Under this obligation, States have to take positive action to prevent and protect women from violence, punish perpetrators of violent acts and compensate victims of violence. The principle of due diligence is crucial as it provides the missing link between human rights obligations and acts of private persons.

Because GBV affects women throughout their life cycle, the focus should be on women and girls. The CEDAW Committee recognises that traditional attitudes by which women are regarded as subordinate to men or as having stereotyped roles perpetuate widespread practices involving violence or coercion, such as family violence and abuse, forced marriage, dowry deaths, acid attacks and female circumcision. Such prejudices and practices may justify gender-based violence as a form of protection or control of women. The effect of such violence on the physical and mental integrity of women is to deprive them of equal enjoyment, exercise and knowledge of human rights and fundamental freedoms. While this comment addresses mainly actual or threatened violence the underlying consequences of these forms of gender-based violence help to maintain women in subordinate roles and contribute to their low level of political participation and their lower level of education, skills and work opportunities.

These attitudes also contribute to the propagation of pornography and the depiction and other commercial exploitation of women as sexual objects, rather than as individuals. This in turn contributes to gender-based violence.

In 2017, the CEDAW Committee, marked the 25th anniversary of its General Recommendation No. 19, by further elaborating the international standards on gender-based violence against women. As of December 2021, the Committee has adopted 38 general recommendations. It is instructive to note that the CEDAW Committee brought 'violence against women within the jurisdiction of international law and in many ways, it has transformed the CEDAW from an anti-discrimination treaty into a gender-based violence treaty'. It recognises the 'close connection between discrimination against women, gender-based violence, and violations of human rights and fundamental freedoms'.

In General Recommendation No. 35, the CEDAW Committee recognised that the prohibition of gender-based violence against women has evolved into a principle of customary international law, binding all States.

2.6.2. Beijing Declaration and Platform for Action (BPfA)

In 1995, the Fourth World Conference on Women in the Chinese capital, resulted in the Beijing Declaration and Platform for Action (BPfA), seen as a landmark document for advancing women's rights and gender equality worldwide. It is an agenda for change across 12 critical areas to realise the human rights of women and girls: (1) women and poverty; (2) education and training of women; (3) women and health; (4) violence against women; (5) women and armed conflict; (6) women and the economy; (7) women in power and decision-making; (8) institutional mechanisms; (9) human rights of women; (10) women and media; (11) women and the environment; (12) the girl child. The BPfA affirmed the principles that would govern future actions and strategies for women, and firmly set in place an agenda for empowering women by integrating their concerns into national plans and policies. Governments and the UN agreed to promote gender mainstreaming as a strategy to ensure that a gender perspective is reflected in all policies and programs at the national, regional and international levels.³⁶

35 Council of Europe. Newsroom: CEDAW launches General Recommendation No.35 on general-based violence against women, 2017. Available online at: <https://www.coe.int/en/web/istanbul-convention/-/cedaw-launches-general-recommendation-35-on-gender-based-violence-against-women>

36 Republic of the Philippines – Philippine Commission on Women: Beijing Platform for Action. Available online at: <https://pcw.gov.ph/beijing-platform-for-action>

Now, more than 25 years later, despite some progress, no country has fully delivered on the commitments of the Platform, according to a 2020 UN Women report.³⁷ This report is based on the UN Secretary-General's Report, which is the most comprehensive and participatory stock-taking exercise on women's rights ever undertaken, with contributions from 170 Member States.

The report finds that progress toward gender equality is faltering, and hard-won advances are being reversed.³⁸ Rampant inequality, the climate emergency, conflict and the alarming rise of exclusionary politics all threaten future progress towards gender equality. The report flags the lack of effective action to boost women's representation at the tables of power and warns that the vision of the Beijing Platform for Action will never be realised if the most excluded, women and girls, are not acknowledged and prioritised.

Furthermore, research shows the far-reaching social and economic impacts of the Covid-19 pandemic exacerbated pre-existing inequalities and threatened to halt or reverse the gains of decades of collective effort. For example, it is estimated that the pandemic pushed 47 million more women and girls below the poverty line.

Despite unprecedented global challenges, the report also proves that positive change is possible, as shown by the success of women's collective action to obtain accountability for crimes against them and the flourishing of feminist movements across the world. The report showcases successful initiatives in scaling up public services to meet women's rights, from increasing access to contraception and childcare, to reducing domestic violence and increasing women's participation in politics and peacebuilding.

The United Nations Declaration on the Elimination of Violence against Women, which stresses that States have the duty to exercise due diligence to prevent, investigate and, in accordance with national legislation, punish acts of violence against women, whether those acts are perpetrated by the State or by private persons.

The UN updated Model Strategy and Practical Measures on the Elimination of Violence against Women in the Field of Crime Prevention and Criminal Justice sets out guiding principles for all criminal justice responses (human rights-

based; victim-centred; ensuring perpetrator accountability) and calls on States to criminalise and prohibit all forms of violence against women.³⁹ They call for crime prevention and criminal justice responses to the production, possession and dissemination of games, images and all other materials that depict or glorify acts of violence against women and children, and their impact on the general public's attitude towards women and children, as well as the mental and emotional development of children, particularly through new information technologies, including the Internet.

2.7. European Union Human Rights Standards

2.7.1. The Istanbul Convention

The Istanbul Convention⁴⁰ and its explanatory report were adopted by the Committee of Ministers of the Council of Europe on 7 April 2011. It was opened for signature on 11 May 2011 on the occasion of the 121st Session of the Committee of Ministers in Istanbul. It entered into force on 1 August 2014 and as of October 2021, thirty-four States are parties to the convention. The convention is open for accession by any country prepared to implement its provisions.

As a landmark treaty for women's rights, the Istanbul Convention offers the most comprehensive set of measures for governments to prevent and combat all forms of violence against women and domestic violence. It positions such violence as a human rights violation and a form of discrimination against women and links its eradication firmly with the achievement of women's equality with men. In its preamble (Council of Europe 2011a), the convention recalls the European Convention for the Protection of Human Rights and Fundamental Freedoms, the European Social Charter, and the Council of Europe Convention on Action against Trafficking in Human Beings as well as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The Istanbul Convention also recalls the United Nations Convention on the Elimination of all Forms of Discrimination against Women (CEDAW) and its subsequent general recommendations, the United Nations Convention on the Rights of the Child, and the United Nations Convention on the Rights of Persons with Disabilities.

37 UN Women: Gender equality: Women's Rights in Review 25 years after Beijing (2020). Available online at: <https://www.unwomen.org/en/digital-library/publications/2020/03/womens-rights-in-review>

UN Women: Press Release: Ahead of International Women's Day, new UN Women report warns that progress towards gender equality is lagging and hard-fought gains are under threat (5 March 2020). Available online at: <https://www.unwomen.org/en/news/stories/2020/3/press-release-ahead-of-international-womens-day-report-warns-that-progress-is-lagging>

38 UN Women: Press Release: Ahead of International Women's Day, new UN Women report warns that progress towards gender equality is lagging and hard-fought gains are under threat (5 March 2020). Available online at: <https://www.unwomen.org/en/news/stories/2020/3/press-release-ahead-of-international-womens-day-report-warns-that-progress-is-lagging>

39 UNODC: Strengthening Crime Prevention and Criminal Justice Responses to Violence Against Women, 2014 Available online at: https://evaw-un.inventory.unwomen.org/en/agencies/unodc?pageNumber=2&un_inventory_period

40 Council of Europe: Istanbul Convention: Action against violence against women and domestic violence (2011). Available online at: www.coe.int/en/web/istanbul-convention/country-monitoring-work

The text reaffirms the structural and gendered nature of violence against women and presents a comprehensive framework to end violence against women and domestic violence. The convention is structured around the '4 Ps': prevention, protection and support of victims, prosecution of offenders, and coordinated policies (Council of Europe 2020c).

Regarding its scope (Article 2) (Council of Europe 2011a), the Istanbul Convention 'apply(s) to all forms of violence against women, including domestic violence' and 'shall apply in times of peace and situations of armed conflict', covering every situation in which women are targeted by violence.

The convention sets out several definitions and concepts and defines violence against women as 'a violation of human rights and a form of discrimination against women' and a form of gender-based violence that results in 'physical, sexual, psychological or economic harm or suffering to women' (Article 3a), thus targeting women because of their gender, and gendered 'socially constructed roles, behaviours, activities and attributes' (Article 3c).

In addition, Article 3a also states that 'threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life' are considered gender-based violence against women. Girls under the age of 18 are included in the category 'women' (Article 3f).

In Article 4, the convention reminds parties that they 'shall take the necessary legislative and other measures to promote and protect the right for everyone, particularly women, to live free from violence in both the public and the private sphere.' In Article 5, the convention integrates the due diligence standards required from parties: 'Parties shall take the necessary legislative and other measures to exercise due diligence to prevent, investigate, punish and provide reparation for acts of violence covered by the scope of this Convention that is perpetrated by non-State actors, thus reminding parties to the convention that they have the obligation to develop integrated policies to prevent, protect from and prosecute all forms of violence affecting women and girls, both in public and private life.

With detailed obligations to take steps towards the prevention of all forms of violence against women through awareness raising and education, including the training of professionals and work with perpetrators, it seeks to curb attitudes that condone or help perpetuate violence against women and girls. Protection and support to victims and those at risk must be provided in a victim-centred, empowering manner and be accessible to all. Investigations and criminal proceedings must be pursued to bring perpetrators to justice and ensure accountability.

All of the above need to form part of a holistic response to the different forms of violence against women – a feature rendering this important legal treaty unique.

While the Istanbul Convention does not contain an explicit reference to the digital dimension of violence against women, its scope as defined in Article 2 extends to violence committed in the digital space, as intended by its drafters. Indeed, several articles of the Istanbul Convention are applicable in the digital context. For example, Article 40 applies to online and technology-facilitated sexual harassment as per its definition: 'any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment'.

The convention's provision on stalking (Article 34) also applies to online and technology-facilitated stalking, as stalking is herein defined as 'the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety'. The extension of Article 34's scope to the digital sphere has been affirmed in the explanatory report to the convention which explicitly classifies 'the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICTs' as unwanted contact within the meaning of the said provision. Given the serious psychological consequences that many forms of online and technology-facilitated violence can have on women and girls, the Istanbul Convention's requirement to criminalise psychological violence (Article 33) takes on important meaning.

The Istanbul Convention can be a particularly relevant instrument for addressing online and technology-facilitated violence against women, being the most far-reaching legally binding human rights treaty covering all forms of violence against women and domestic violence⁴¹.

2.7.2. The Lanzarote Convention

Sexual exploitation and sexual abuse are among the worst forms of violence against children. To protect them against these, the Council of Europe has adopted the most comprehensive legal instrument in this field, the Lanzarote Convention. Since sexual violence against children is a global concern, any country across the globe may accede to the Convention.

The Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, also

41 Council of Europe: Protecting Women and Girls from Violence in the Digital Age: Adriane van der Wilk (December 2012). Available online at: <https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3>

known as ‘the Lanzarote Convention’, is a human rights treaty dedicated specifically to prevent and respond to all forms of sexual violence against children.⁴² By putting children’s rights at its heart, it adopts a victim-centred approach with far-reaching provisions that improve systems and services, therefore, helping States to fight against all forms of violence against children. The Lanzarote Convention requires criminalisation of all kinds of sexual offences against children. It sets out that States in Europe and beyond shall adopt specific legislation and take measures to prevent sexual violence, protect child victims and prosecute perpetrators.

The Council of Europe Strategy for the Rights of the Child, states that children:⁴³ ‘...have the right to learn, play and communicate online – and to be protected from bullying, hate speech, radicalisation, sexual abuse, and other risks of the ‘dark net’. Guaranteeing the rights of the child in the digital environment is a key challenge all members of the Council of Europe face, and the Strategy will help them provide children with practical knowledge of how to be online and stay safe.’

Given the complexity of this phenomenon, countries need to have a multidisciplinary approach by joining forces of the different stakeholders to have successful prevention, awareness raising, and criminal justice measures.

2.8. African Human Rights Standards

2.8.1. SADC

The Maputo Protocol requires States parties to enact and enforce laws to prohibit all forms of violence against women (article 4(2)); and to adopt legislative, administrative, social and economic measures to ensure the prevention, punishment, and eradication of all forms of violence against women (Article 4(2)).

The Revised Southern African Development Community (SADC) Protocol on Gender and Development (2018) defines GBV as follows: ‘all acts perpetrated against women, men, girls, and boys based on their sex which causes or could cause them physical, sexual, psychological, emotional or economic harm, including the threat to take such acts or to undertake the imposition of arbitrary restrictions on or deprivation of fundamental freedoms in private or public life in peacetime and during situations of armed or other forms of conflict.’ (Article 1:2).

The SADC Protocol on Gender and Development has set targets, and aims to eliminate gender-based violence at every level:

- Enact and enforce legislation prohibiting all forms of gender-based violence

- Ensure that the laws on gender-based violence provide for the comprehensive testing, treatment and care of survivors of sexual assault
- Review and reform their criminal laws and procedures applicable to cases of sexual offences and gender-based violence
- Enact and adopt specific legislative provisions to prevent human trafficking and provide holistic services to the victims, with the aim of re-integrating them into society
- Enact legislative provisions, and adopt and implement policies, strategies, and programmes which define and prohibit sexual harassment in all spheres, and provide deterrent sanctions for perpetrators of sexual harassment
- Adopt integrated approaches, including institutional cross-sector structures, to reduce current levels of gender-based violence by 2015.

The SADC Gender Protocol Barometer is updated annually by the Southern Africa Gender Protocol Alliance and measures the success of these commitments at the Member State level.

2.8.2. SADC Gender-Based Violence Model Law 2021

During the SADC-PF, 44th Plenary Assembly Session, the SADC-PF Regional Women’s Parliamentary Caucus (RWPC), sponsored a motion to develop a model law on GBV that will be used by SADC Member States to prevent, address, and combat all forms of GBV which is on the increase by 2030.

The SADC GBV Model provides comprehensive guidance on how to eradicate GBV, from both a normative and operational perspective, and respond to GBV, succinctly. The model law on Gender-Based Violence in the SADC region is a response to the prevailing shortfalls in legislation on Gender-Based Violence and the chronic implementation gap across the region. A model law can guide these initiatives and interventions and ensure that they adhere to regional and international human rights frameworks and consider the increased vulnerability due to statelessness, unequal nationality rights, and forced displacement.

A Model Law on eradicating GBV and protecting vulnerable persons can be useful to national legislatures, drafters, and other stakeholders seeking to eradicate and prevent GBV through legislative means, in respective SMSs, for the following reasons:

- It can guide national legislators on what law on GBV should cover and how;
- It can serve as a yardstick to national legislators;
- It can reinforce a commonality of approach;
- It can affirm the need for appropriate legislative action;

42 Council of Europe: Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse: Lanzarote Convention (2007). Available online at: <https://www.coe.int/en/web/children/convention>

43 Council of Europe: Cyberviolence against children. Available online at: <https://www.coe.int/en/web/cyberviolence/cyberviolence-against-children>

- It can be a stimulus for debate and advocacy;
- It can provide a legal framework in conformity with international and regional law;
- It can stimulate the adoption of national legislation; and
- It can help develop a uniform legal regime for GBV victims and vulnerable persons.

2.9. Cybercrime instruments

2.9.1. Introduction

The internet and digital technologies, including social media platforms have created a space for the widespread and ‘unrestricted’ exercise of rights such as freedom of expression, freedom of assembly and access to information. It facilitates the conducting of online transactions, e-learning, remote working, video conferencing and many other political, economic, cultural and social activities. The use of technology, the Internet and social media have become a part of our daily lives. It also created opportunities for criminals for easy access to unlimited numbers of potential victims anywhere in the world, getting access to personal data as well as bringing about the advent of dark forms of online participation such as the spread of misinformation, disinformation, cyberbullying, cyberharassment and revenge porn.

The right to privacy is guaranteed in international and regional human rights instruments. It is enshrined in Article 12 of the UDHR, article 17 of the ICCPR, Article 16 of the Convention of the Rights of the Child (CRC), and Article 10 of the African Charter on the Rights and Welfare of the Child (AFDEC, 2020). Though the African Charter does not have a provision for the right to privacy, this right has been acknowledged under the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) (the Declaration).

‘Cybercrime is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organised crime groups. Perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response’.⁴⁴

Cyber offences generally cluster around the following categories:

- offences against the confidentiality, integrity and availability of computer data and systems
- computer-related offences
- content-related offences
- offences related to infringements of copyright and related rights.

Cybercrime can be described as:

- **Cyber-dependent crime** - requires an ICT infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).
- **Cyber-enabled crime** - can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online, and online money laundering.
- **Sexual exploitation and abuse** - includes abuse on the clear internet, darknet forums, and increasingly, the exploitation of self-created imagery via extortion, known as ‘sextortion’.⁴⁵

2.9.2. International, national and regional laws on cybercrime

The existence of national, regional, and international laws on cybercrime, and the harmonisation of laws across states facilitate international cooperation. The harmonisation and enforcement of national, regional, and international laws also eliminate cybercrime safe-havens. Cybercrime safe-havens are created in countries that do not have cybercrime laws because a person cannot be prosecuted for a cybercrime unless it is considered an illicit activity punishable by law. These cybercrime safe-havens can also be created if cybercrime laws are not adequately enforced and/or there is a divergence between national cybercrime laws.

The United Nations General Assembly adopted, since 2000, formal resolutions on *Combating the Criminal Misuse of Information Technologies*. The first one was the Resolution adopted by the General Assembly 55/63, on combating the criminal misuse of information technologies, (adopted by the 81st Plenary Meeting, on 4 December 2000).

The **Resolutions on Combating the Criminal Misuse of Information Technologies** (Resolutions 55/63 and 56/121) include the following:

- the need to ensure that each State adopts a proper law on cybercrime – **to eliminate safe havens**
- the need for the exchange of information, cooperation and coordination **among all the States related to some concrete criminal investigation on**

⁴⁴ UNODC: Cybercrime. Available online at: <https://www.unodc.org/unodc/en/cybercrime/index.html>

⁴⁵ UNODC: Cybercrime. Available online at: <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>

international cases of criminal misuse of information technologies.

The African Union adopted the African Union's Convention on Cyber Security and Personal Data Protection in July 2014. The Convention aims to harmonise the laws of African States on electronic commerce, data protection, cyber security promotion and cybercrime control. The objective of this Convention was to propose the adoption at the level of the African Union, a Convention establishing a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance, and combating cybercrime.

The AU Convention covers:

Chapter I – Electronic transactions

Chapter II – Personal data protection

Chapter III – Cyber security and cybercrime.

The AU Convention unites different aspects related to information technology law and includes some non-digital and non-criminal justice issues. It recognises that cybercrime 'constitutes a real threat to the security of computer networks and the development of the Information Society in Africa'. It imposes obligations on the Member States to establish national legal, policy and institutional governance mechanisms on cyber security. According to Article 28 of the Convention, there is a need for the Member States to facilitate

international cooperation on cyber security. It also requires the AU Member States to make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) to promote cyber security and tackle cyber threats.

Article 28:1 of the Convention posits that: 'State parties shall ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonisation of these measures and respect the principle of double criminal liability'.

The Convention defines some key terms such as child pornography, computer system, cryptology, cryptology tools, cryptology service provider, data controller, data subject, double criminality, electronic communication, electronic mail, electronic signature, encryption, personal data, racism and xenophobia in information and telecommunication, sensitive data, and third party.

Article 25 of the Convention empowers member states 'to adopt legislative and/or regulatory measures as it deems necessary to confer specific responsibilities on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, intending to confer on them a statutory and legal capacity to act in all aspects of cyber security application'. There is a caveat to this provision namely that, 'each State Party shall ensure that measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws,



and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others'.

In a comprehensive study by the UNODC in 2013 on cybercrime and responses to it by the Member States, the international community and the private sector, it was found that the Council of Europe Convention on Cybercrime (Budapest Convention, 2001) is the most used multilateral instrument for the development of cybercrime legislation.⁴⁶ Some SADC countries have used the Budapest Convention as a model for developing their domestic legislation on cybercrime, such as Mauritius, Botswana, Tanzania, and South Africa. Both the SADC Model Law on Computer Crime and Cyber Crime and the Commonwealth Group of Nations cybercrime model law are also modeled on the Budapest Convention.

2.9.3. SADC Model Law on computer crime and cybercrime

An initiative called 'Support for the Harmonisation of the ICT Policies in Sub-Saharan Africa project (HIPSSA)' was launched in Addis Ababa in 2008. The Project is jointly funded by the ITU and European Commission (EC) and executed by the ITU. Cybersecurity is one of the priorities of the Project. As its regional outcome, the SADC Model Law on Computer Crime and Cybercrime⁴⁷, the SADC Model Law on Data Protection and the SADC Model Law on Electronic Transactions and Electronic Commerce

were adopted by the SADC Ministers in charge of ICT and telecommunications in 2012.⁴⁸

The aim of the Model Law on Computer Crime and Cybercrime is to offer guidance on how cybercrime and cybersecurity can be regulated by the SADC member states and identifies offences that can be incorporated into national laws for the combating of cybercrime. These offences include illegal access, interception, data interference, espionage, forgery, fraud, pornography, xenophobic material and disclosure of details of an investigation.⁴⁹ As it is a model law, it does not pose any legal cooperation obligations on states.

The states that have and/or create cybercrime laws can utilize the SADC Protocol on Mutual Legal Assistance in Criminal Matters⁵⁰ and the SADC Protocol on Extradition⁵¹ to facilitate cooperation and coordination in international cybercrime investigations.

A useful guidance document is the UNODC Data Disclosure Framework (DDF)⁵² which contains general practices developed by international service providers in responding to overseas government requests for data. The Data Disclosure Framework was developed to improve communication and cooperation between the public and private sectors in their handling of electronic evidence, in line with international human rights laws and the principles of necessity and proportionality.

46 UNODC: Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector (23 January 2013). Available online at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf

47 HIPSSA (Harmonization of ICT Policies in Sub-Saharan Africa): Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law (2013). Available online at: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf>

48 SADC (Southern Africa Development Community): The NATO Cooperative Cyber Defence Centre of Excellence. Available online at: <https://ccdcoe.org/organisations/sadc/>

49 MISA-Zimbabwe in partnership with Konrad Adenauer Stiftung: Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights (2021). Available online at: <https://www.ictworks.org/wp-content/uploads/2021/11/Cybersecurity-Laws-SADC-Region-Human-Rights.pdf>

50 SADC Protocol on Mutual Legal Assistance in Criminal Matters (2002). Available online at: https://www.sadc.int/sites/default/files/2021-08/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf

51 SADC Protocol on Extradition (2002). Available online at: <https://www.sadc.int/document/protocol-extradition-2002-0#:~:text=The%20SADC%20Protocol%20on%20Extradition,in%20the%20requesting%20Member%20State>

52 UNODC Data Disclosure Framework (DDF) (August 2021). Available online at: [https://sherloc.unodc.org/cld/en/st/evidence/ddf.html#:~:text=The%20Data%20Disclosure%20Framework%20\(DDF,respecting%20the%20right%20to%20privacy](https://sherloc.unodc.org/cld/en/st/evidence/ddf.html#:~:text=The%20Data%20Disclosure%20Framework%20(DDF,respecting%20the%20right%20to%20privacy)

PART THREE

Understanding CVAWG

LEARNING OBJECTIVES

Understanding forms of cyberviolence against women and girls (CVAWG)

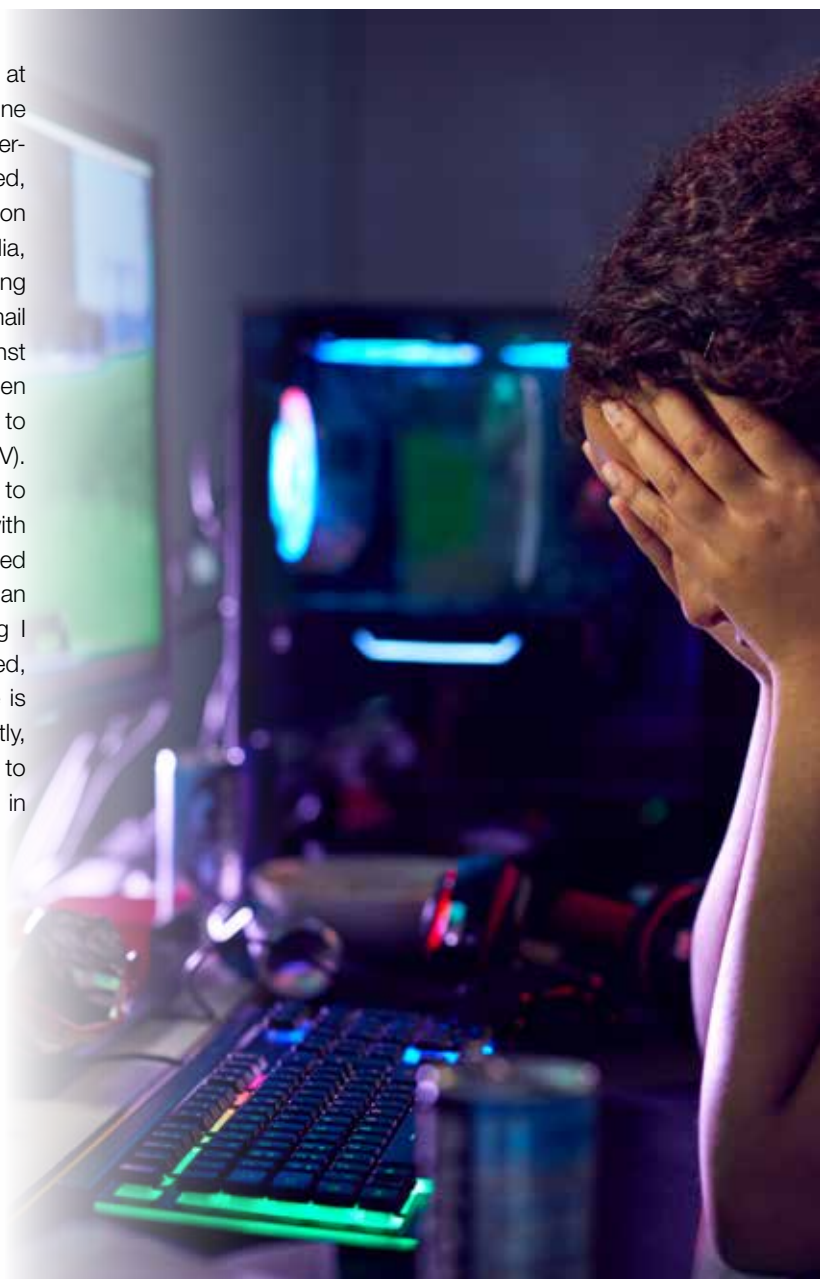


Understanding the impact of cyberviolence on victims/survivors



3.1. Introduction

Cyberviolence takes different forms, which is increasing at a rapid rate, as new technologies are developed. Online violence against women extends to any act of gender-based violence against women that is committed, assisted, or aggravated in part or fully by the use of information and communication technologies (ICT) or digital media, such as mobile phones and smartphones, GPS, tracking devices, drones, the Internet, social media platforms, email or non-internet connected recording devices⁵³ against a woman because she is a woman, or affects women disproportionately. Online violence can also be referred to as Technology-facilitated Gender-based Violence (TFGBV). The anonymity that the Web affords allows perpetrators to violate laws prohibiting sexual exploitation and violence with impunity. In an online survey, 23.3% of women reported being blamed for the violence done to them. One woman writes, 'most people blamed me for the abuse saying I deserved it, while others ignored it'. Another responded, 'No help no support at all. I was told that being online is a risk and if I'm being harassed it's my fault'.⁵⁴ Currently, mobile phones are the most commonly used tool to perpetuate cyberviolence against women, especially in emerging regions like Africa.



53 UNFPA-Technology-Facilitated GBV-Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

54 West, Jessica. Cyber-Violence Against Women (2014). Available online at: <http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf>

Cyberviolence has distinct characteristics related to its digital nature as depicted in figure 4 below.

Figure 4: Distinct characteristics of cyberviolence⁵⁵

digital nature

- Anonymity**
The perpetrator or abuser can remain anonymous.
- Action at a distance**
It can be perpetrated at a distance, from anywhere in the world and without personal or physical contact with the survivor.
- Accessibility and affordability**
It is accessible and affordable to perpetrators, since information and communications technology have reduced the cost and difficulty of producing and distributing information at scale.
- Propagation**
It is constant and easily propagated through the Internet, retraumatizing survivors. The ease, efficiency and affordability of automating and multiplying instances of abuse against a particular group or individual means that it is an effective form of violence in wielding harm.
- Impunity**
It is often perpetrated with impunity. Given that TFGBV can be committed anonymously and from a distance, there are difficulties in law enforcement across countries and jurisdictions that limit judicial systems' ability to hold abusers accountable for their actions.
- Automation**
It can be automatic and easy to perpetrate, and allows perpetrators to control women's movements, monitor their online activity and distribute images or information, among other harmful abusive actions, with limited time and effort.
- Collectivity**
It can be collectively organized and perpetrated by a large number of individuals.
- Normalization of violence**
TFGBV contributes to the normalization of violence against women and girls. Physical violence against women is often normalized and justified, particularly by women themselves. In fact, across 49 low- and middle-income countries, 41 per cent of women and 32 per cent of men justify domestic physical violence in at least one circumstance.¹⁵ It is likely that this normalization of violence is exacerbated in the digital space, and that TFGBV is perceived as less serious, harmful or dangerous to survivors.
- Perpetuity**
It can be committed in perpetuity, as images and digital materials used to perpetrate abuse are likely to exist indefinitely or for long periods of time.

Technology also has the potential to facilitate the prosecution of crimes in cases of gender-based violence.

55 UNFPA-Technology-Facilitated GBV-Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

3.2. Forms of CVAWG

3.2.1. Online exploitation

The notion of online violence should include exploitation that may cause any form of harm to women and children.

3.2.1.1. Women

Online exploitation against women may take on various forms, such as cyber fraud via online dating sites known as catfishing.⁵⁶ It is a deceptive activity where a person creates a fictional persona or fake identity on a social networking service, usually targeting a specific victim. The scammer wants to steal personal information, money, or both.

Scammers in **catfishing** use and post fake pictures and fabricate stories to send encouraging messages to entice inexperienced people into a relationship. They create fake profiles on legitimate dating websites and use these profiles to try to enter into a relationship with the victim so they can obtain money from the victim or their personal details.

The scammer will develop a strong rapport with the victim and then ask for money to help cover costs associated with illness, injury, travel or a family crisis. Scammers seek to exploit the victim's emotions as a result of the online bond between the victim and the scammer. This trust can be built over months.

Domestic violence and online romance scams use similar psychological deceptions⁵⁷ such as:

- **Isolation** - Isolation occurs when offenders interrupt the support networks of their victims. Romance fraud offenders were quick to move communication with victims from the dating and social media platforms onto private email or messaging.
- **Monopolisation** - Monopolisation refers to offenders' efforts to consume the attention of their victims throughout the day.
- **Degradation** - Degradation is behaviour that makes others feel less worthy. This includes verbal abuse such as name-calling, insults, and questioning the competency of victims.
- **Emotional or interpersonal withdrawal** - While the above techniques are active, psychological abuse also involves passive tactics. Romance fraud offenders periodically cut off communication. This resulted in victims becoming anxious about the status of their relationship or the well-being of the offender.

Research on non-physical abuse in the context of domestic violence has documented severe consequences for victims, including ongoing symptoms of trauma physical health, depression, breakdown of their supportive relationships, unemployment, homelessness, and even contemplation of suicide.

The common denominator of online exploitation is causing harm in various forms.⁵⁸

3.2.1.2. Children

Sexual Exploitation of Children is regarded as any form of sexual abuse of children which has a link to the online environment. Online sexual abuse may include abuse, harassment, cyberbullying, sexting, grooming, and the disclosure of harmful intimate images through social media or other online channels. The majority of reported child victims in online exploitation cases were girls.

Although one primary victim was identified per online exploitation report, almost 1 in 4 reports (23%) indicated that the offender had additional child victims. However, this estimate is likely an under-representation, given that there was often not enough information about additional children victimised by the same offender.

Of the reports in which it could be determined, 9% of reports indicated that the child victims had certain vulnerabilities before, or at the time of the online enticement situation being reported. These vulnerabilities included mental health histories, developmental disorders, a history of talking to adults online and/or trading sexually explicit content online, a history of running away, and/or some type of family abuse history.

Of the 5,917 offenders named in the reports, the majority were male (82%) while only 9% were female (for 9% of offenders, gender could not be determined). While an overall offender age range and average age could not be calculated, some reported offenders were indicated to be as young as early teens and others as old as late adulthood, even into their late seventies.

Of the total reported offenders, 98% were individuals seemingly unknown to the children in real life while only 2% were likely known. Of these likely known offenders, more than half (53%) were indicated as family members, and over half were identified as male (56%). Over one-third were identified as female (38%) and the gender was unknown for 6%. The most common reported familial offenders were

56 Cross, C. and Dragiewicz, M. Domestic violence and online romance scams use similar psychological tricks (1 April 2018). Available online at: <https://www.abc.net.au/news/2018-04-05/online-romance-scams/9622066>

57 Ibid

58 United Nations Human Rights Council. Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective (2018). Available online at: <https://digitallibrary.un.org/record/1641160?ln=en>

identified as parents/step-parents (57%) or siblings (37%) while more distant familial relationships were rare (e.g. aunts, uncles, cousins). Likely known non-familial offenders also ranged in closeness to the child, from those with greater physical access to the child (e.g. family friends, ex-intimate partners, etc.) to those with less physical access to the child (e.g. acquaintances in the community).

Of the reported offenders for whom it could be evaluated (n=3,592), a variety of apparent goals emerged (for 3% of offenders, more than one goal was indicated). Most commonly, offenders seemed to want sexually explicit images of children (60%); to meet and have sexual contact with children (32%); to engage in sexual conversation/role-play with children online (8%), and to acquire some type of financial goal (2%).

In addition, there were other, less common and/or more difficult goals to determine, including trying to use children for sex trafficking purposes, whether in person or online; wanting revenge on children, by distributing their content to others; having some form of exhibitionist goals and for children to offend upon other children.

COMMONLY INDICATED OFFENDERS' METHODS AGAINST CHILDREN

- Engaging the child in sexual conversation/ role-play as a grooming method, rather than a goal (34%).
- Asking the child for sexually explicit images of themselves (33%).
- Developing a positive rapport with the child, often through compliments, praise, discussing "shared" interests or acting caring/empathic, 'liking'/commenting on children's online posts, etc. (29%).
- Sending unprompted sexually explicit images of themselves (23%).
- Pretending to be younger (20%), often by lying to the children but, sometimes, just when registering for their online account to circumvent the system and communicate with minors (22% of 'younger' reports).
- Offering sexually explicit images of themselves to children (10%).
- Asking children to reciprocally/mutually exchange images (9%), often initiated by the offender, but sometimes as a compromise or 'self-protection' measure by the child if the offender first 'asked' for images.
- Offering something (other than images) in exchange for fulfilling their goal (8%), such as some type of financial incentive (e.g. money, gift card, etc.); promises to buy them goods/gifts; substances (e.g. alcohol, drugs, cigarettes) and; other necessities, such as lodging, transportation or food.
- In addition, offenders used a variety of less commonly indicated methods (less than 5%) such as pretending to be female, or a modeling agent/photographer; or asking the child to rate/evaluate a picture of them (often explicit).

Children sometimes engage in behaviors that made them more vulnerable to exploitation, such as lying about being older when creating online accounts; initiating online communication with offenders, and offering offenders an exchange for sex or explicit images, such as financial compensation, alcohol or drugs, lodging, transportation, or goods/gifts.

In conclusion, online exploitation appears to be a very different experience based on child and offender factors and should not be viewed as a one-size-fits-all type of victimisation.



3.2.2. Sextortion⁵⁹

Sextortion is defined as: ‘the abuse of power to obtain a sexual benefit or advantage’.⁶⁰ Online predators use fake profiles as their identity to chat and lure victims on social networking sites. After gaining the trust and confidence of victims, they convince them to engage in video calls or to send private intimate images. These videos and images are captured and recorded by online predators and are used to harass and or extort them morally as well as for monetary gains. In some cases, when victims refuse to act in favour of online predators, their pictures are posted on their social networking profiles or even sent to the victim’s friends.⁶¹

Statistics reflect that children also fall prey to this online violence offence:

- 78% of the reports involved female children and 15% involved male children (In 8% of reports, child gender could not be determined)
- Male and female children each ranged in age from 8-17 years old and had an average age of fifteen years old; however, compared to female children, it was less common for male children to be on the younger end of the spectrum
- In 24% of the reports, reporters mentioned that they suspected or knew that additional children were targeted by the same offender.

There are important child gender and age differences. While male children were significantly more likely than female children to self-report, female children were significantly more likely than male children to have Internet companies and peers report on their behalf. Parents/guardians and other authority figures were equally likely to report for male and female children. While self- and Internet company reports were more likely among older children, parent/guardian-, authority figure- and online stranger reports were more likely among younger children. Peers were equally likely to report for older and younger children.

Sextortion most commonly occur via phone/tablet messaging apps, social networking sites and video chats. Of the reports in which an online location was mentioned, the total number of platforms that offenders used to communicate with children ranged widely from one platform

to as many as seven platforms. While over half of the reports (56%) indicated that only one platform was involved, the use of multiple platforms was indicated in 42% of the reports.

3.2.3. Cyberbullying⁶²

Cyberbullying can take place through digital devices like cell phones, computers, and tablets. It can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Victims may also be tricked into giving out personal information. Cyberbullies may also send threatening or cruel messages or impersonate somebody else to send mean or embarrassing messages. An online bully is also called an internet troll, someone who deliberately tries to offend, cause trouble or directly attack people.⁶³ This differs considerably from a healthy and respectful difference of opinion between people – which can be invaluable on forums and other social media.

Cyberbullying is normally thought of as occurring between or targeting a minor (someone under 18 years of age). Cyberbullying provides the perpetrator with a feeling of anonymity that the Internet gives them. Cyberbullies do real damage. Victims can suffer from low self-esteem, fall behind in school work, or become anxious, depressed, and even suicidal. This is compounded by the reality that minors are often reluctant to tell an adult if they are being bullied online.⁶⁴

The most common places where cyberbullying occurs are on social media, including Facebook, Instagram, Snapchat, and TikTok. It can take place using any number of methods, including the following:

- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards
- Email
- Online gaming communities.

59 National Center for Missing & Exploited Children: Trends identified in CyberTipline sextortion reports (2016). Available online at: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf>

60 International Association of Women Judges (IAWJ): Naming, Shaming, and Ending Sextortion – A Toolkit (2012). Available online at: https://www.unodc.org/res/jji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf

61 MAUCORS (The Mauritian Cybercrime Online Reporting System): Sextortion. Available online at: https://maucors.govmu.org/maucors/?page_id=1073

62 Stopbullying.gov - A federal government website managed by the U.S. Department of Health and Human Services: What Is Cyberbullying. Available online at: <https://www.stopbullying.gov/cyberbullying/what-is-it>

63 Internet trolling: A definition. Available online at: <https://www.endsleigh.co.uk/blog/post/what-is-internet-trolling/>

64 Cyberbullying.org.za: Cyberbullying Definition – Safety & Security guide (South African portal for resources and information on Cybercrime. Available online at: <https://cybercrime.org.za/>

With the prevalence of social media and digital forums, comments, photos, posts, and content shared by individuals can often be viewed by strangers as well as acquaintances. The content an individual shares online – both their personal content as well as any negative, mean, or hurtful content – creates a permanent public record of their views, activities, and behavior. This public record can be thought of as an online reputation, which may be accessible to schools, employers, colleges, clubs, and others who may be researching an individual now or in the future. Cyberbullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it.

- **Persistent** – Digital devices offer an ability to immediately and continuously communicate 24 hours a day, so it can be difficult for children experiencing cyberbullying to find relief
- **Permanent** – Most information communicated electronically is permanent and public, if not reported and removed. A negative online reputation, including those who bully, can impact college admissions, employment, and other areas of life
- **Hard to Notice** – Because teachers and parents may not overhear or see cyberbullying taking place, it is harder to recognise.

3.2.4. Cyberstalking

A related concept is cyberstalking, though this is more often used in relation to adults than minors. However, a victim of any age may be cyberstalked. Cyberstalking can be defined as using the Internet to threaten or make unwanted advances toward someone else. Cyberstalking can also be described as 'the use of technology to stalk and monitor someone's activities and behaviours in real-time or historically'.⁶⁵ Cyberstalking is usually seen as an extension of offline stalking, using technological tools, and it involves a set of unwanted, repetitive, intrusive, threatening, and harassing behaviours which in some instances are seen as a relatively normal relational or dating practice. Some scholars use the term 'cyberobsessional pursuit' to refer to the 'unwanted pursuit of intimacy through a repeated invasion of a person's sense of physical or symbolic intimacy,

using digital or online means', and consider cyberstalking a severe form of cyberobsessional pursuit and surveillance, which may be motivated by relational control or destruction and cause the survivor to feel fear. Cyberstalking involves, for example, monitoring or tracking a person's location and/or activities using GPS trackers, spyware,⁶⁶ cameras and microphones, and location-based dating apps, checking email, call or message histories, as well as monitoring a person's social media profiles.

It shares much of its psychological profile with cyberbullying in terms of hiding behind the perceived anonymity of the Internet, taking pleasure in the fear or humiliation of another, etc.

While the phenomenon of *stalking* has been around for decades and has generated pieces of legislation in some jurisdictions to specifically address it, cyberstalking occurs more readily given the use of already ubiquitous Internet-based platforms and resources to help accomplish victimisation. The explosion of social media, 24/7 connectivity, and the reality that stalkers would naturally extend their reach through online means all give rise to the creation and increased numbers of cyberstalking.

3.2.4. Online harassment

Cyberstalking is closely related to online harassment or 'cyberharassment' and has also been referred to as 'interpersonal terrorism'.⁶⁷ This sort of stalking and harassment can cause physical, emotional, and psychological damage to the victim.⁶⁸ Online harassment is the use of technology to repeatedly contact, annoy, threaten or scare another person.⁶⁹ Online harassment is an ongoing behaviour over time rather than an isolated incident. Online harassment can be perpetrated by a single individual or mobs of individuals (*mobbing*), usually networks of male perpetrators who target women and minorities.⁷⁰ Online sexual harassment is a specific form of harassment that may involve unwanted sexual attention and sexual coercion.⁷¹ It has also been defined as 'any unwanted sexual behaviour via electronic means and can include unwanted sexual solicitation; unwanted requests to talk about sex; unwanted requests to do something sexual online or in person; receiving unwanted sexual messages and images; having sexual messages and images shared

65 UNFPA-Technology-Facilitated GBV (TFGBV) -Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

66 Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C. & Deibert, R. (2019). The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. The Citizen Lab. Available online at: <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/>

67 Spitzberg, B.H. and G. Hoobler. Cyberstalking and the technologies of interpersonal terrorism. *New media & society*, 2002. 4(1): p. 71-92. Available online at: <https://doi.org/10.1177/14614440222226271>

68 Cyberbullying.org.za: Cyberbullying Definition – Safety & Security guide (South African portal for resources and information on Cybercrime. Available online at: <https://cybercrime.org.za/>

69 UNFPA-Technology-Facilitated GBV-Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

70 VAW Learning Network (2013). Technology-related Violence Against Women. Available online at http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

without permission; and revealing identifying and personal information about a person online'.⁷²

3.2.5 Image-based abuse (IBA)

IBA consists of 'using images to coerce, threaten, harass, objectify or abuse'. One form of IBA is image-based sexual abuse (IBSA),⁷³ which involves at least one of three behaviours: taking, sharing or threatening to share sexually explicit images without consent. Some scholars have argued for the inclusion of other forms of gendered and sexualised abuse, perpetrated using technological tools, such as *upskirting*, or non-consensually taking an image up a person's skirt or dress; *deepfakes*, or non-consensually created sexual imagery that sexually depict the victim, usually developed using AI tools; and *cyberflashing*, or sending unsolicited images of their own genitals to another person.⁷⁴ Other examples include photographing or filming someone without their consent or knowledge, or coercing someone to engage in unwanted sexual behaviour online.⁷⁵

3.2.6 Revenge pornography (Harmful disclosure of an intimate image)

Revenge pornography or harmful disclosure of an intimate image is an offence where the perpetrator targets the integrity of the specific victim. The disclosure of an intimate image does not only affect adults but children as well.

It can be defined as: '*the dissemination or posting of sexually explicit media, without the consent of the individual in the media, particularly where the intent is to shame, humiliate or frighten the person or otherwise cause them harm*'.⁷⁶

The images can be distributed via social media, text messages, e-mails or even uploaded onto pornographic websites. Initially, the intention was to humiliate the individual, or profit from intimate multimedia sent by an ex or a former partner – thus the term 'revenge porn'. However, research has shown not all perpetrators disclose for revenge purposes. It may also be for sexual gratification, extortion or financial gain.⁷⁷

Revenge pornography can also be seen as a form of cyberbullying that involves the use of information that enforces hostile behaviour by the individual.⁷⁸

The term 'distribution' or 'dissemination' refers to disclosure using an electronic system. A form of disclosure should include the sending or storing of the image on an electronic communications network, where the image can be viewed, copied or downloaded. The image can otherwise be made available to a person, by sending a link to the image that has been stored on an electronic communication network, where the image can be viewed, copied or downloaded.⁷⁹

The person might have consented to the original creation of such a photograph or film. This does not entail that the victim consented to the disclosure of the image. The absence of the victim's consent is the ground for the unlawfulness of revenge pornography as well as the infringement of the right of protecting the privacy and the integrity of the victim.⁸⁰

3.2.7 Sexting

Sexting is a combination of the words 'sex' and 'text'. It can be defined as sending and receiving explicit sexual messages, nude or semi-nude images of oneself via a cellphone or the Internet using social media platforms such as instant messaging on Facebook, Twitter and email.⁸¹ Sharing of messages and intimate images between consenting adults might not be regarded as illegal depending on the specific countries' legislation. It can be seen as the modern day of sexual expression and intimate relationships. The evidence shows that sexting occurs in committed relationships.

Studies also have shown that 'sexting' is more popular with younger generations but is not only exclusive to younger people.⁸²

The non-consensual disclosure and disclosure of sexual images of children are unlawful. This will be viewed as the creation, possession or distribution of sexual abuse

71 Flynn, A., Powell, A. & Hinds, S. 2022. Technology-facilitated abuse: Interviews with victims and survivors and perpetrators. Available online at: <https://apo.org.au/node/309987>

72 UNFPA-Technology-Facilitated GBV-Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

73 McGlynn, C. & Rackley, E. 'Image-Based Sexual Abuse', *Oxford Journal of Legal Studies*, vol. 37, No. 3, (2017), pp. 534–561. Available online at: <https://doi.org/10.1093/ojls/gqw033>

74 Ibid 68

75 Henry, N., Flynn, A. & Powell, A. 'Technology-facilitated domestic and sexual violence: a review', *Violence Against Women*, vol. 26, No. 15–16, (2020), pp. 1828–1854. Available online at: <https://doi.org/10.1177/1077801219875821>

76 Lornard, T., Martland, T. & White, D. A Legal Examination of Revenge Pornography and Cyber Harassment (2016). *Journal of Digital Forensic Security and Law* Volume 11(3) 79 – 92. Available online at: <https://commons.erau.edu/jdfs/>

77 Sepec, Miha: Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence (2019). *International Journal of Cyber Criminology: Volume 11, Issue 2, July to December*, p418-438. 21p.

78 Ibid

79 Cybercrimes Act 19 of 2020, South African Government. Section 13: Definitions. Available online at: <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000>

80 Ibid : 18

81 Ngo, F., Jaishankar, K., Agustina, J.R. Special Issue on Sexting: Current Research Gaps and Legislative Issues. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>



material.⁸³ An important question to consider is: why the image or messages were disclosed? Was the motivation to impress other peers or was it done out of malicious intent to cause harm in any form?⁸⁴

The second question that arises is whether sexting between two children falls in the same category as exploitation and distribution of sexual abuse images (child pornography) that are usually calculative and habitual.⁸⁵ The potential risk of harm will be when sexting results in the distribution of child abuse images, revenge pornography and or cyberbullying.⁸⁶

3.2.8. Doxing or doxing

Doxing is the non-consensual disclosure of personal information. It involves the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend.⁸⁷ Doxing is a form of online harassment that rarely occurs in isolation, rather it is accompanied with other forms of harassment such as IBA.⁸⁸ Women, especially from minority groups, are more

likely to be subjected to doxing, which disproportionately impacts women of colour and LGBTQIA+ communities.⁸⁹ According to Douglas, there are three types of doxing: de-anonymising, or revealing someone's identity; targeting, or revealing someone's personal and private information that allows her to be physically located, the consequences of which are gendered and may pose serious security implications for most women; and de-legitimising, releasing private information in order to undermine someone's credibility or reputation and to shame and humiliate them.⁹⁰ Doxing often leads to further online and physical harassment, such as receiving large amounts of abusive messages and threats by email, phone or post.

3.2.9. Impersonation

Impersonation is the process of stealing someone's identity to threaten or intimidate, as well as to discredit or damage a user's reputation.⁹¹ Perpetrators may take over or create fake online accounts and websites of women to spread false information and damage their reputation, to ruin their personal and/or professional relationships,⁹² to call for violence against them through sex work advertisements or dating apps or to obtain information about the survivor.



82 Marganski, A. Special Issue on Sexting: Sexting in Poland and the United States: A Comparison Study of Personal and Social-Situational Factors. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>.

83 Hasinoff, A. A. Sexting and Privacy Violations: A case study on sympathy and blame. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>.

84 O'Connor, K., Drouin, M., Yergens, N. and Newsham, G. Sexting Legislation in the United States and Abroad: A Call for Uniformity. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>

85 Ibid: 19

86 Ibid: 19

87 UNFPA-Technology-Facilitated GBV-Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf

88 MacAllister, J.M. The doxing dilemma: seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, vol. 85, (2017), pp. 2451–2383. Available online at: <https://ir.lawnet.fordham.edu/flr/vol85/iss5/21/>

89 Eckert, S and Metzger-Riftkin, J. (2020). Doxing. *The International Encyclopedia of Gender, Media, and Communication*. Available online at <https://doi.org/10.1002/9781119429128.iegmc009>

90 Douglas, D. 'Doxing: a conceptual analysis', *Ethics and Information Technology*, vol. 18, (2016), pp. 199–210. Available at: <https://www.studocu.com/row/document/mekelle-university/international-criminal-law/doxing-a-conceptual-analysis/10452762>

91 European Parliament, Directorate-General for Internal Policies of the Union, Wilk, A. Cyber violence and hate speech online against women, European Parliament, 2018. Available online at: <https://data.europa.eu/doi/10.2861/738618>

92 Freed, D, Palmer, J Minchala, D.E, Levy, K Ristenpart, T and Dell, N. 'Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders', *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, (2017), pp. 1–22. Available at <https://doi.org/10.1145/3134681>

3.3. Victim impact as a result of gender-based cyberviolence crimes⁹³

Cyberviolence is an increasing problem worldwide and is often gender-based and targeting women and girls. Predominantly, the root cause of violence against women and girls is gender inequality (discrimination, gender stereotypes, sexism). Moreover, women who have more than one commonly-targeted characteristic – for example, women of color, members of minority religions, or people who identify as LGBTQIA+ – may be attacked more frequently.

- The impact of online GBV is profound. Once the victim has endured this form of violation the consequences can be life changing. These factors
- Violation of privacy.
- Restriction of movement.

should be considered as aggravating factors that could be taken into account for sentencing purposes.

- Causing the victim emotional stress.
- Feelings of fear and of being under threat.
- Feelings of helplessness, anxiety, guilt, shame and powerlessness.
- Can lead to depression and post-traumatic stress disorder.
- Sociological consequences:
 - alter their lifestyles in terms of interpersonal, professional and general social functioning.
 - change personal information.
 - avoidance of certain locations.
 - the installation of extra security measures and restriction of social interactions.



3.4. For victims/survivors, the implications of failing to address GBV are profound.

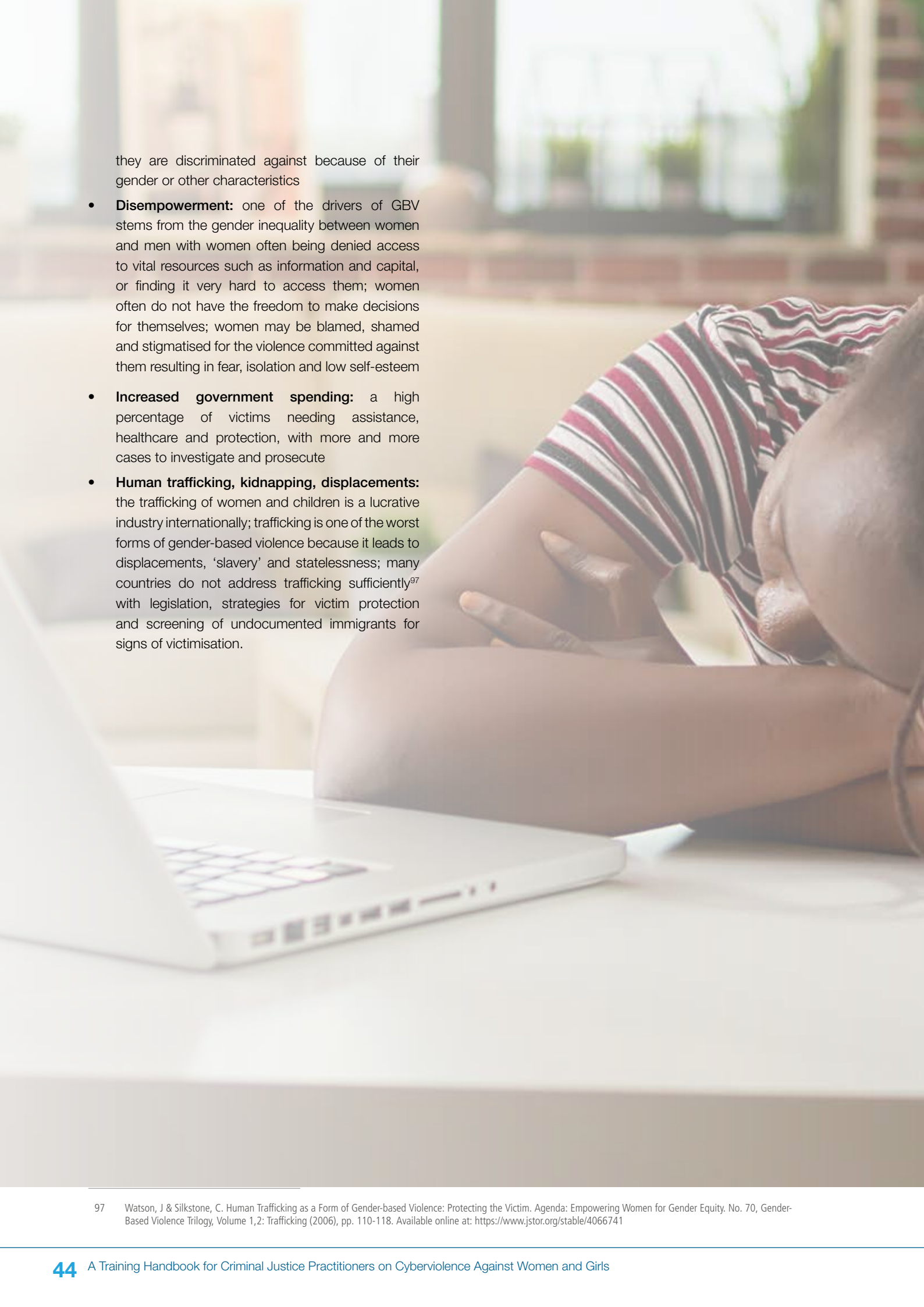
- **Injustice:** high number of violent cases going unreported and unprosecuted (poorly collected DNA samples, backlogs of cases, untraceable perpetrators) create a lack of confidence and trust in the criminal justice institutions and processes
- **Emotional reactions:** fear, distrust, sadness, vulnerability, isolation, and anxiety
- **Physical reactions:** changes in eating or sleeping patterns, increased startled response, concerns about physical safety, lack of control anger, numbness, confusion, denial, eating disorders, substance use or abuse, phobias, low self-esteem, physical injury, and concerns about pregnancy⁹⁴ or contracting an STI or HIV
- **Mental reactions:** depression, drug and alcohol abuse, self-harming behaviour⁹⁵
- **Desperation:** if the victim realises there is little chance of redress and justice she could attempt suicide; as a way to survive she could be forced to steal, ‘kidnap’ her children (if the perpetrator is the father), and flee
- **High probability of repeated abuse:** if the perpetrator believes there is little chance of him being arrested and sentenced he could continue with his abuse which could lead to femicide or the murder of those close to his victim (e.g. her children, siblings, parents)
- **Psychological consequences of sexual abuse:** nightmares, flashbacks, depression, difficulty concentrating and Post-traumatic Stress Disorder (PTSD)⁹⁶
- **Femicide:** increase in these cases as violence escalates
- **Dominance:** perpetrator ‘triumphs’ because out of fear the survivor does not report him, or the household members or community protects him, or he ‘pays’ corrupt law enforcers to get him off the hook, or the judicial system is ineffective – this leads to a strengthened belief in his superiority and sense of being untouchable
- **Scared society:** an uncaring, wounded society without values or compassion
- **Lack of democracy and equality:** false democracy where certain groups of the population (e.g. women and other vulnerable groups) do not effectively participate in the political or civil processes of that country because

93 CSVR Gender – Based Violence: A Brief Overview (April 2016 p15). Available online at: <https://www.csvr.org.za/pdf/Gender%20Based%20Violence%20in%20South%20Africa%20-%20A%20Brief%20Review.pdf>

94 WHO Departmental news. Gender-based violence is a public health issue: using a health systems approach, 2021. Available online at: <https://www.who.int/news/item/25-11-2021-gender-based-violence-is-a-public-health-issue-using-a-health-systems-approach>

95 Council of Europe. Why is gender-based violence a problem? Available online at: <https://www.coe.int/en/web/gender-matters/why-is-gender-based-violence-a-problem>

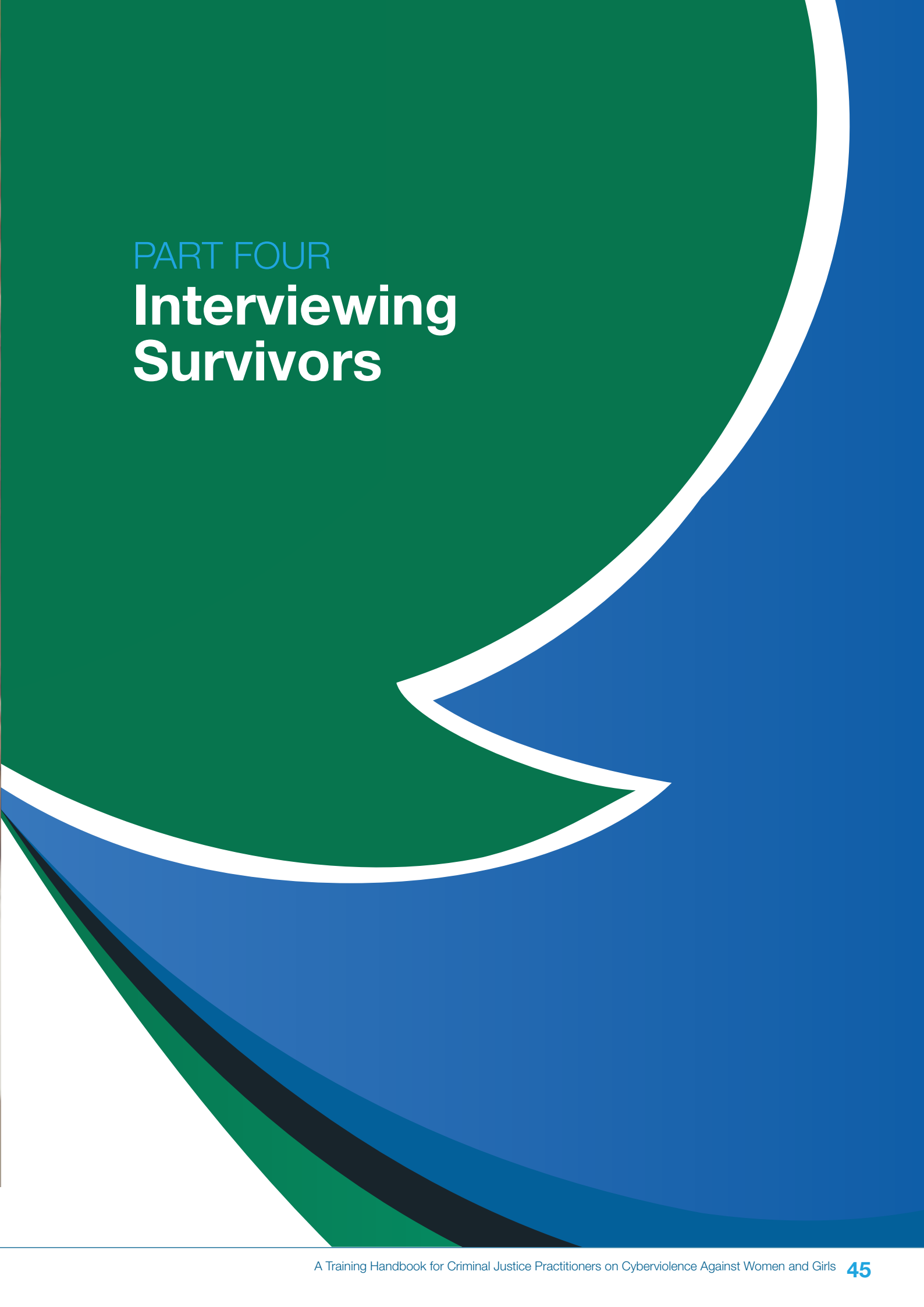
96 European Institute for Gender Equality. EIGE-2021 Gender Equality Index 2021 Report: Health. Available online at: <https://eige.europa.eu/publications/gender-equality-index-2021-report/gender-based-violence>

A photograph of a woman with her head resting on her hand, looking down at a laptop. She is wearing a red, white, and black striped shirt. The background is a blurred indoor setting with a window.

they are discriminated against because of their gender or other characteristics

- **Disempowerment:** one of the drivers of GBV stems from the gender inequality between women and men with women often being denied access to vital resources such as information and capital, or finding it very hard to access them; women often do not have the freedom to make decisions for themselves; women may be blamed, shamed and stigmatised for the violence committed against them resulting in fear, isolation and low self-esteem
- **Increased government spending:** a high percentage of victims needing assistance, healthcare and protection, with more and more cases to investigate and prosecute
- **Human trafficking, kidnapping, displacements:** the trafficking of women and children is a lucrative industry internationally; trafficking is one of the worst forms of gender-based violence because it leads to displacements, 'slavery' and statelessness; many countries do not address trafficking sufficiently⁹⁷ with legislation, strategies for victim protection and screening of undocumented immigrants for signs of victimisation.

97 Watson, J & Silkstone, C. Human Trafficking as a Form of Gender-based Violence: Protecting the Victim. Agenda: Empowering Women for Gender Equity. No. 70, Gender-Based Violence Trilogy, Volume 1,2: Trafficking (2006), pp. 110-118. Available online at: <https://www.jstor.org/stable/4066741>



PART FOUR
**Interviewing
Survivors**

LEARNING OBJECTIVES

Understanding how to interview victims and witnesses of CVAWG



Applying a collaborative approach to investigate and prosecute CVAWG



Understanding the Essential Services Package



4.1. Interviewing and obtaining a statement

4.1.1. General principles applicable to women and girls (children)⁹⁸

Interviewers should be mindful of the following considerations:

- the dynamics and nature of violence, abuse and exploitation
- the impact and consequences, including negative physical and psychological effects, of these crimes, including the role trauma can play in memory and language difficulties, as well as impacting on the victim's ability to form trusting relationships
- special measures and techniques to assist victims, such as the use of body diagrams, asking questions in a language the victim can easily understand, and to consider preferred time limits in interviewing
- using interview techniques that minimise distress or trauma to victims while maximising the quality of information received from them, always treating victims in a sensitive, understanding, constructive and reassuring manner
- the child's developmental stage, as well as cultural and age-related linguistic issues
- the power dynamics of working with children and women from marginalised or disadvantaged groups.

4.1.2. Preparing for the interview

When conducting the interviews, ensure that interviewing protocols are survivor-friendly, while also being able to adapt general protocols to the specific needs of the individual victim.⁹⁹ Any information already available concerning the case should be shared with the interviewer, to allow for optimal preparation in terms of being aware of the type of abuse alleged, the dynamics that may be present, and the age and developmental level of the child. Protocols for interviewing are not a script from which the interviewer merely reads. Rather they are a guide to a phased, systemic approach to interviewing, that ensures consistency in question areas while allowing for adaptation to reflect the fact that every child is an individual and every case is unique.

4.1.3. Survivor-friendly spaces

Optimally, interviewing survivors should take place in a neutral, non-intimidating, environment that is private, informal and free from unnecessary distractions. An informal setting might include furniture that is size appropriate for both children and adults and having the person conducting the interview dressed casually. Ensuring no unnecessary distractions may be accomplished by simply putting a 'Do Not Disturb' sign on the door. The privacy should ensure no one can hear or see the survivor as they give their statement. This may be accomplished by conducting the interview in a separate location, such as a specially designated interview facility, or scheduling interviews so that offenders and survivors do not overlap. Multiple interviews should be

98 Child Welfare Information Gateway. Forensic Interviewing: A Primer for Child Welfare Professionals (2017). Children's Bureau. U.S Department of Health and Human Services. Available online at: <https://www.childwelfare.gov/pubs/factsheets/forensicinterviewing/>

99 United Nations Human Rights - Office of the High Commissioner: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (25 May 2000) – Human Rights Instrument. Available online at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>

avoided, if possible, and relevant agencies should jointly use the results of the interview, to avoid additional interviews. Specialised interview rooms are advantageous because they are generally friendly, and allow for observation without being in the same room with the survivor, as well as having audio and video recording resources.

Just as survivors must be safe when they give their initial statements, it is critical to keep vulnerable witnesses safe in court. This may be achieved by providing an opportunity for survivors to be allowed to testify via closed-circuit television

(CCTV) or remote audio-visual link or, if this is not available, either in camera or from behind a screen, to preclude the defendant from visually intimidating the witness. While waiting to testify, there should be victim-friendly spaces where the defendant and the witnesses cannot see, hear, or otherwise have contact with each other. These areas can be pointed out to the survivors during court preparation, which will acquaint the survivor with how courts work and also what they can expect as they testify. By 'demystifying' the court process, witnesses will be better able to answer questions asked of them either in open court or through CCTV.

4.1.4. Key points to consider when interviewing on cyberviolence offences ¹⁰⁰

4.1.4.1. Interviewing the complainant

- Introduce yourself and explain the purpose of the interview.
- Establish the necessity to obtain the services of an interpreter during the interview.
- Ensure that the complainant is comfortable and that the interview room is private.
- The interview questions and methods applied should be age and gender appropriate.
- Inform the complainant that the specific online offence is serious and regarded as a criminal offence.
- Advise the complainant to be specific and accurate and to provide as much detail as possible.
- The possibility of stalking and the future risk of physical violence should be considered whenever an online violence-type offence is reported. 'The whole story needs to be heard' from the viewpoint of the complainant's past or relationship with the suspect to properly assess whether the fear is imminent.

4.1.4.2. Essential Information Required

- Obtain a detailed chronology of all relevant incidents.
- Provide a calendar and paper to the complainant to be able to make notes and to confirm dates.
- Determine whether the incident(s) involved others or occurred in the presence of others (such as family, friends, co-workers or neighbours).
- Determine which devices were used and whether the messages/images are still available on the devices.
- Search and Seizure protocols should be followed to obtain the evidence and the chain of evidence should be recorded.
- If the suspect is known to the complainant obtain personal details and background information on any previous relationship between the victim and the suspect.
- Consider whether there have been any previous incidents of domestic violence; whether the victim has communicated to the suspect any interest in a reconciliation; or whether any friends or family have been pressuring the victim to reconcile with the accused or to not contact the police).
- Obtain information about the impact that the suspect's conduct has had on the complainant:
 - One effective way to do this is to ask the complainant to describe a typical day before the online violent crime began, and then to describe a typical day since it has begun.
 - Has the conduct caused the complainant to fear for his or her safety, or that of someone known to him or her?

100 Department of Justice of Canada: Handbook for Police and Crown Prosecutors on Criminal Harassment (2012, p 22). Available online at: <https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/EN-CHH2.pdf>

- Has the complainant taken any security or preventative measures, such as getting an unlisted telephone number, or changing his or her residential or work address?
- Has the complainant sought medical treatment or counselling?

4.1.4.3. Protection measures to be considered

- Existence of Protection orders.
- Protection for children.
- Does the suspect have a firearm or access to firearms or other weapons?
- Does the complainant have access to and understanding of the process of the Criminal Justice System?
- Fear to disclose the sexual orientation of the complainant.
- Assist the complainant to contact victim support services if available.
- Advise the complainant to change passwords on her devices and change the privacy settings of all social media platforms.

4.1.5. Factors to consider when interviewing girls

4.1.5.1. Language and age-appropriate questions

The best way to gauge the developmental and linguistic ability of the child being interviewed is to pay close attention to her use and understanding of language. Consequently, it is important to encourage narrative responses from the beginning of the interview and assess her ability to respond to open-ended questions. It is also important to remember that a child who stumbles in one language might be very competent and able to provide full disclosure in another, usually his or her first language, the language they feel most comfortable using or the language they use at home. The child's linguistic and developmental abilities should be assessed in the language in which he or she is most competent. While it may be assumed that adults may be interviewed using everyday language, it is still important not to use medical or legal terms with which they may not be familiar.

When deciding on questions to ask children about the abuse event(s), it must be kept in mind that children use language differently than adults. Word choice and types of questions asked are of paramount importance. There are three basic types of questions discussed below.

4.1.5.2. Type of questions

(Open-ended questions are the most preferred, then focused, and then, forced questions.)

Open-ended questions do not assume anything about an event or experience. They allow the child to respond

in a free recall, narrative format. Examples of open-ended questions include 'What happened?' or 'What game were you playing or in which chat room did you meet?'

Focused questions focus the child's attention on a particular topic, place, or person, but refrain from providing information. These are the 'who, what, where, when, and how' questions. Multiple choice questions would also be examples of focused questions. However, when multiple choice questions are asked, the offered answers must include the option of 'or anything else' to allow the child to respond with an answer not provided. An example here would be the interviewer asking 'Was he using Facebook, Twitter, Instagram or something else?'

Forced choice is the final type of question. Here, the child is given a closed set of possible answers. An example of a forced-choice question would be any question where the only answers are 'yes' or 'no' or where the child can only choose from a closed set of possible answers.

There are also **additional strategies** to make questions easier for children to answer i.e.

- **Time segmentation questions** break down an event into smaller segments of time and probe for additional details. An example would be: rather than ask the child about the whole day, ask about what happened before she went to school, what happened at school and what happened when she got home from school.
- **Sensory focus questions**, ask about what the child saw, heard, touched, tasted or smelled during the abuse, to generate additional reliable details of the event(s).

4.1.5.3. Word Choice

The choice of the words themselves and recognising how children's understanding of words may differ from adults' understanding of them is critical. Several examples follow, but they all reflect the need for the interviewer to make certain the child has clarity about the question that is being asked, as well as the need for the interviewer's understanding of the child's answer.

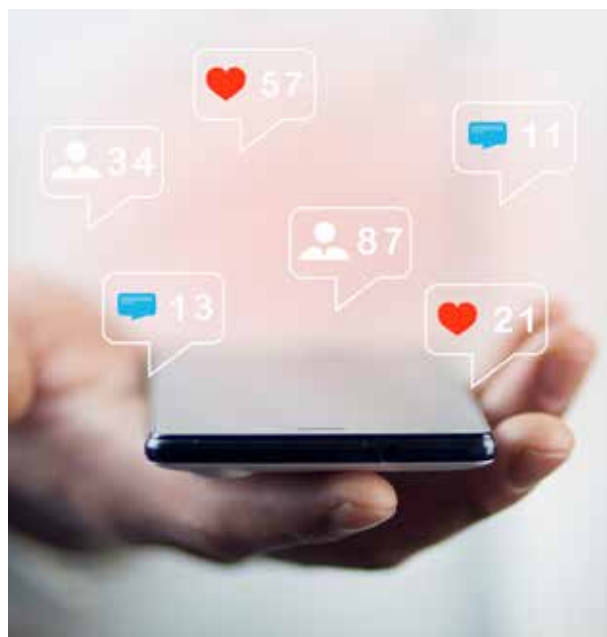
Under-extension: where a child gives a word only part of its adult meaning. An example is the word 'clothes'. A child may understand 'clothes' to mean only outerwear (clothes that can be seen by others), as opposed to underwear.

Over-extension: where a child gives a word a fuller meaning than an adult might. Again, using the word 'clothes' - to an adult 'clothes' may be any article of clothing, but to a child 'clothes' may mean all the clothes a person is wearing.

Concrete thinking and literal interpretation: children may be cognitively unable to expand their reasoning to incorporate the more general meaning of a word. Younger children will often interpret a question or command in the most narrow and literal sense. So if asked 'Do you see the man who hurt you in the courtroom?' and because of the configuration of the courtroom, the child does not have a direct line of sight to the defendant, she may say 'no'. When the child is put in a position to actually see the defendant, the answer becomes 'yes'.

Another example of literal interpretation is seen in the difference between asking the question 'Did he put his penis in your mouth?' and 'Did you put your mouth on his penis?' These are not the same question, though to an adult they may seem so. The first question makes the adult the actor, the one who is committing the act, whereas the second question reflects the child being the actor. So a child will answer the first question 'yes' and the second question 'no'. This might seem to be an inconsistency or even contradictory, but it is not.

Explaining feelings and hypothetical questions: many children will have difficulty explaining their thought processes of feelings. Examples would include asking 'Why are you sad?' or 'Why didn't you run?' or 'Why didn't you tell?' Asking 'why' to a child younger than 8 to 10 years is usually meaningless, as many children are 'pre-logical' until then. Hypothetical questions will be answered with 'I don't know' until approximately 12 years of age. Avoid word pairing such as 'if' and 'then', or conditional word choices such as 'would' and 'could'.



Meaning of words: often a child will use a common word, such as 'tickle' which to adults is understood one way. However, the child may describe being digitally penetrated by the abuser. Children can only describe the abuse using words they have in their vocabulary, so when a child uses a verb, the interviewer must follow up with questions such as 'where did he tickle you' or 'what did he tickle you with' to ensure the act described is either, in fact, innocent tickling or that it is being used to describe something very different.

Children will sometimes use a word that they have heard in conversation, or on the TV or elsewhere, without knowing exactly what it means. When a child uses a word that the interviewer feels is beyond the average vocabulary use of a child of that age, ask follow-up questions to ensure the child is using the word appropriately.

Finally, children can only describe what happened with the vocabulary they have at any given age or development level. Often, interviewers feel the child is fabricating or engaging in fantasy, when in fact, the child is giving an accurate description of what occurred, but using a child's vocabulary. A child may describe 'a giant bird looking down on the bed' which seems strange. Upon further investigation, it turns out that a huge tapestry was hung on the wall over the bed where the abuse occurred, which had a picture of a giant eagle on it. The child was telling the truth but didn't have the word for 'tapestry' or 'eagle'. Do not dismiss a child's statement simply because it does not fit the expectation of the interviewer. Investigate how the statement might be true, within the context of a child's vocabulary

4.1.5.4 Questions to avoid

A quick set of rules to follow in terms of what type of questions to avoid

- Avoid use of legal terms, e.g. defendant, accused
- Avoid use of technical terms, e.g. ejaculation
- Avoid use of multisyllabic/big words, e.g. preceding, accompany, incident
- Avoid use of words with more than one meaning e.g. play
- Avoid abstract terms e.g. justice, truth

Particularly with those under 10 years

- Avoid the use of relationship words. Use given names (e.g. Noah) rather than 'your uncle', etc. Because the child may not know the proper name
- Avoid pronouns – he, she, they, etc.

Until 10 years, kids have difficulty linking pronouns to reference noun

- Avoid negative constructions like, 'Mom wasn't home, was she?'
- Avoid using concepts of 'some', 'all', 'more' or 'less'

Particularly with under 7-year-olds

- Avoid the use of quantifiers, e.g. 'a couple', 'several' or 'few'
- Ask, 'Did this happen once or more than once?'
- What it means when a child says 'It happened a million times'

Avoid 'do you remember' questions

- With children under 10 years of age, to 'remember' may mean you must have forgotten once
- Do not ask 'Do you remember telling the police? Instead ask 'You talked to the police about something that happened. What was it that happened?'

Also avoid the following in general

- Avoid shifting back and forth between topics or in time without signaling to the child
- Try to link events to something important to the child
- Prior to the age of 9, children are usually poor with time concepts
- Avoid asking for units of measurements – e.g. size, distance
- Big vs. small, child uses self as the measure
- Avoid asking for estimates of elapsed time
- Children, like many adults, are notoriously bad with time estimates

4.1.5.5. The appropriate duration of the interview

Every child is unique and age guidelines for optimal interviews reflect average age norms. Some children who are five or six may have the developmental level of a four-year-old, while others may be more in line with the development of

a seven-year-old. Please note that these guidelines do not apply to children with developmental delays or other special needs, such as being deaf or blind. With 'special case' children, each interview must be crafted with additional care, to reflect the needs and abilities of each child.

Generally, an interviewer has approximately 3 to 5 minutes of focused attention time for every year the child is old. So, a five-year-old's interview should be between 15 and 25 minutes. As children approach their teens, they come more in line with adult standards of focus and attention. However, simply because a child is an adolescent, does not mean that protocols can now be shifted to those of interviewing adults.

Also, as a general rule, it is preferable to aim for shorter rather than longer interviews, especially with younger children. The interviewer should listen to the child's cues and be mindful of signals indicating fatigue, loss of concentration, etc. A one-hour interview is generally considered to be the maximum amount of time even an older child can focus on questions and not become fatigued or distressed.

4.2. Essential Services Package for women and girls subjected to violence

4.2.1. Introduction

This section outlines the importance of a multi-disciplinary team approach, followed by the Essential Service Package, its framework and guidelines for essential justice and policing services.

4.2.2. Inter-agency Collaboration and Coordination of the Multi-disciplinary Team

4.2.2.1. The multi-disciplinary team (MDT)

A multi-disciplinary team approach should be in place to respond to cyberviolence against women and girls.

A multidisciplinary team is a professional team of service providers that may be a composite of representatives drawn from law enforcement, prosecution, health, social services, and others brought together to coordinate the assistance needed to handle cases of gender-based violence. The establishment of such inter-agency teams reduces the number of survivor interviews and can reinforce the survivor's trust and confidence in the system, improve communication, pool knowledge and have greater access to information.

Other advantages of an MDT include:

- holistic, best outcomes approach, harmonising and correlating actions by psychosocial welfare, law enforcement, criminal justice and health
- based on inter-institutional partnership and cooperation

- requires a common philosophy and principles and standards
- coordinated, coherent plans that enable collaboration
- partnerships are critical because it offers a safety net for support and referral
- monitoring and evaluation are important issues for effective coordination and implementation.
- be aware of the roles, responsibilities, and limitations in an intervention
- roadmap on the provision, reporting and referral systems
- training together for improving quality and management.

The multi-disciplinary team also lessens the burden on the victim/survivor, optimally through the provision of services in a centralised location, while simultaneously maximising the opportunities to obtain corroborative evidence in an expedited manner, thereby increasing the likelihood of obtaining a conviction.

The United Nations Essential Services Package for Violence against Women and Girls¹⁰¹ is a programme developed in partnership by UN Women, UNFPA, WHO, UNDP and UNODC with the aim to provide greater access to a coordinated set of essential and quality multi-sectoral services for all women and girls who have experienced gender-based violence. The programme identifies the essential services to be provided by the health, social services, police and justice sectors (the 'Essential Services') as well as guidelines for the coordination of Essential Services and the governance of coordination processes and mechanisms (the 'Coordination Guidelines'). Service delivery guidelines for the core elements of each essential service have been identified to ensure the delivery of high-quality services, particularly for low and middle-income countries for women and girls experiencing violence. Taken together, these elements comprise the '**Essential Services Package**'.

The Essential Services Package comprises of five overlapping modules:

- Module 1 Overview and Introduction
- Module 2: Health Essential Services
- Module 3: Justice and Policing Essential Services
- Module 4: Essential Social Services
- Module 5: Essential Actions for Coordination and Governance of Coordination

The international obligation to exercise due diligence requires States to establish effective measures to prevent, investigate and prosecute cases of violence against women. This includes effective means to respond to each case

101 UN Women: Essential Services Package for Women and Girls Subject to Violence Core Elements and Quality Guidelines, Partnership by UN Women, UNFPA, WHO, UNDP and UNODC (2015). Available online at: <https://www.unwomen.org/en/digital-library/publications/2015/12/essential-services-package-for-women-and-girls-subject-to-violence>

of violence, as well as address the structural causes and consequences of the violence, by ensuring comprehensive legal and policy frameworks, gender-sensitive justice systems and police, available health and social services, awareness raising activities, and ensuring the quality of all measures.

The purpose of the Essential Services Package is to support countries as they work to design, implement and review services for all women and girls who are victims and survivors of violence in a broad range of settings and situations. The Package is a practical tool for countries setting out a clear roadmap on how to ensure the provision and coordination of quality services of all sectors are coordinated and governed to respond in a comprehensive way, are women-centred and where necessary, children-centred and are accountable to victims and survivors and each other.

4.2.3. The Essential Services guidelines framework

The Framework for the Essential Services Guidelines for the delivery of quality essential services incorporates four interlinked components:

- **Principles** that underpin the delivery of all essential services.
- **Common characteristics** which describe a range of activities and approaches that are common across all areas and which support the effective functioning and delivery of services.
- **Essential services and actions** which set out the guidelines required for services to secure the human rights, safety and well-being of any woman, girl or child who experiences intimate partner violence and or non-partner sexual violence. Essential services are grouped into three sector-specific areas: **health, justice and policing and social services**. They are underpinned by a fourth element: essential actions for **coordination and governance of coordination**.
- **Foundational elements** which must be in place to enable the delivery of quality services across all essential services and actions.

ESSENTIAL SERVICES PACKAGE: OVERALL FRAMEWORK DIAGRAM

PRINCIPLES	A rights based approach	Advancing gender equality and women's empowerment	Culturally and age appropriate and sensitive
	Victim/survivor centred approach	Safety is paramount	Perpetrator accountability
COMMON CHARACTERISTICS	Availability	Accessibility	
	Adaptability	Appropriateness	
	Prioritize safety	Informed consent and confidentiality	
	Data collection and information management	Effective communication	
	Linking with other sectors and agencies through referral and coordination		
FOUNDATIONAL ELEMENTS	Comprehensive legislation and legal framework	Governance oversight and accountability	Resource and financing
	Training and workforce development	Gender sensitive policies and practices	Monitoring and evaluation

MINIMUM SERVICES TO BE PROVIDED BY EACH DISCIPLINE

ESSENTIAL SERVICES AND ACTIONS	HEALTH	JUSTICE AND POLICING	SOCIAL SERVICES
	<ol style="list-style-type: none"> 1. Identification of survivors of intimate partner violence 2. First line support 3. Care of injuries and urgent medical treatment 4. Sexual assault examination and care 5. Mental health assessment and care 6. Documentation (medico-legal) 	<ol style="list-style-type: none"> 1. Prevention 2. Initial contact 3. Assessment/investigation 4. Pre-trial processes 5. Trial processes 6. Perpetrator accountability and reparations 7. Post-trial processes 8. Safety and protection 9. Assistance and support 10. Communication and information 11. Justice sector coordination 	<ol style="list-style-type: none"> 1. Crisis communication 2. Crisis counselling 3. Help lines 4. Safe accommodations 5. Material and financial aid 6. Creation, recovery replacement of identity documents 7. Legal and rights information, advice and representation, including in plural legal systems 8. Psycho-social support and counselling 9. Women-centred support. Children's services for any child affected by violence. 10. Children's services for any child affected by violence. 11. Community information, education and community outreach 12. Assistance towards economic independence, recovery and autonomy.

ESSENTIAL ACTIONS REGARDING GOVERNANCE AND COORDINATION OF SERVICES

NATIONAL LEVEL: ESSENTIAL ACTIONS	LOCAL LEVEL: ESSENTIAL ACTIONS
<ol style="list-style-type: none"> 1. Law and policy making 2. Appropriation and allocation of resources 3. Standard setting for establishment of local level coordinated responses 4. Inclusive approaches to coordinated responses 5. Facilitated capacity development of policy makers and other decision-makers on coordinated responses to VAWG 6. Monitoring and evaluation of coordination at national and local levels 	<ol style="list-style-type: none"> 1. Creation of formal structures for local coordination and governance of coordination 2. Implementation of coordination and governance of coordination

ESSENTIAL ACTIONS REGARDING GOVERNANCE AND COORDINATION OF SERVICES

FOUNDATIONAL ELEMENTS	Comprehensive legislation and legal framework	Governance oversight and accountability	Resource and financing
	Training and workforce development	Gender sensitive and practices	Monitoring and evaluation

4.2.4. Unique features of the framework specific to essential justice and policing services

4.2.4.1. Principles

In applying the overall principles, justice service providers should keep the following in mind:

- The dynamics of inequalities between women and men create gender-specific vulnerabilities, such as economic and legal dependency, which among other things, impact women's use of justice services, create obstacles to accessing justice and even result in some justice remedies negatively impacting women (i.e. fines in intimate partner violence cases).
- Justice and policing services should not compromise the rights of women and girls, be non-coercive, and be grounded in a gender transformative approach.
- A women-centred approach to justice and policing service delivery puts the needs and realities of women and girls at the core of any justice service rather than the goals of the justice institutions. This means prioritising women safety, empowerment and recovery; treating every woman with respect; supporting and keeping them informed throughout the justice process.
- Holding perpetrators accountable requires justice and policing services to support and facilitate the victim's and survivor's participation in the justice process, promote her capacity of acting or exerting her power (woman's agency), while ensuring that the burden or onus of seeking justice is not placed on her but on the state.

4.2.4.2. Common Characteristics

In applying the overall principles, justice service providers should keep in mind:

- Failure to continually and consistently consider issues of protection and support, throughout the whole justice process can lead to catastrophic results.
- Systematic, timely, clear and effective communication, coordination of services, referral networks and mechanisms between justice and other services.

4.2.4.3. Foundational Elements

In applying the overall principles, justice service providers, should keep in mind:

- A criminal law framework that criminalizes all forms of violence against women, as well as criminal, civil, family and administrative law frameworks that ensure effective prevention, protection, prosecution, adjudication and provision of remedies in accordance with international standards.
- Regarding training and workforce development, conducting investigations, prosecution and adjudication of violence against women are often complex and require specialist knowledge, skills and abilities. Justice services should consider delivery through specialized and multi-disciplinary units within the justice sector (i.e. specialized domestic violence courts, gender-based violence prosecution units, and domestic violence units within police forces which include police officers and social workers).

4.2.5. Guidelines for essential justice and policing services

In the United Nations Essential Services Package for Violence against Women and Girls, Chapter 3 includes a detailed description of guidelines for essential Justice and Policing Services. The Essential Services include the following:

NUMBER	ESSENTIAL SERVICE	DESCRIPTION
1.	Prevention	It is important that justice service providers strongly support initiatives and organizations that seek women's equality; raise public awareness about violence against women, its causes, and the consequences to women, their families and communities as well as the punishment that perpetrators will face; and ensure that information about services and how to access them is readily available to all. The development and promotion of institutional cultures founded on gender equality and gender responsiveness and service delivery is crucial to prevention.
2.	Initial contact	A positive initial contact experience with the justice system is crucial for victims/survivors of violence. Services must be available and accessible to all women. But most importantly, the initial contact must demonstrate to the victim/survivor that the justice system and the justice service providers in the system are committed to her health and safety, take her complaint seriously, and want to ensure that she is well supported on her journey through the justice system.
3.	Investigation	Investigations of crimes of intimate partner and sexual violence against women must be started in a timely fashion, conducted in a professional manner, meet evidentiary and investigative requirements, and all available means to identify and arrest the suspect are exhausted. Throughout, the woman's safety, security and dignity are carefully considered and maintained. These guidelines are complemented by Essential Health Service number 6 – Documentation (medico-legal) detailed in the Health Module, particularly 6.2 Collection and documentation of forensic specimens and 6.3 Providing written evidence and court attendance.
4.	Pre-trial Processes	Criminal, civil, family and administrative pre-trial/hearing processes that are non-biased and sensitive to the specific needs of victims and survivors of intimate partner violence and sexual violence are essential to guarantee their right to justice. Essential pre-trial criminal justice services reflect the international obligation of the state and its justice service providers in exercising primary responsibility for investigation and initiating prosecution while balancing the importance of empowering victims and survivors to make informed decisions regarding their interactions with the criminal justice system. Essential pre-trial/hearing civil, family and administrative justice services emphasise the importance of timeliness, affordability and simplified and easy-to-use procedures.
5.	Trial / Hearing Processes	Victims and survivors of intimate partner violence and sexual violence who are involved at the trial stages in criminal and civil justice processes can feel vulnerable, overwhelmed by the unfamiliarity of the justice system or re-victimised through the insensitive or discriminatory treatment of justice service providers. International norms and standards call for measures to prevent further hardship and trauma that may result from attending the trial itself and to ensure that trial processes maximise the survivor's cooperation, and promote her capacity to exert agency during the trial stage while ensuring that in criminal matters, the burden or onus of seeking justice is on the State. The justice services that are considered essential during the trial processes reflect internationally agreed upon model strategies, including friendly and enabling court environments for survivors to feel safe and comfortable recounting what they have experienced; procedures to minimise experienced; procedures to minimise re-victimisation; and the application of evidentiary rules in a non-discriminatory manner.

NUMBER	ESSENTIAL SERVICE	DESCRIPTION
6.	Perpetrator accountability and reparations	The vast majority of perpetrators of intimate partner violence and sexual violence face no legal consequences. When they are held accountable, too often the sanctions, whether criminal, civil or administrative, are very low. In addition, the reparations that women receive from the perpetrator and/or the state following the violence often do not reflect the realities of the harm suffered by women and girls, particularly the patterned use of coercion, intimidation and the use or threat of violence. From a survivor's perspective, accountability and reparations can mean many things, from a criminal sentence, civil damages, state compensation and public condemnation of the violence, as well as including redress for the state's failure to provide essential justice services. The essential services relating to accountability and reparations reflect the international obligation of due diligence of imposing appropriate sanctions to hold perpetrators accountable for their actions and providing for just and effective remedies to the survivors for the harm or loss suffered by them.
7.	Post-trial Processes	The justice system can play an important role in preventing future violence, both by sending a strong message to the community that violence against women will not be tolerated, and also in its role in ensuring the accountability and rehabilitation of perpetrators and reducing recidivism. The international norms and standards urge States to develop and evaluate the treatment and reintegration/rehabilitation programmes for perpetrators that prioritize the safety of the victims as well as ensure that compliance is monitored. These standards also urge States to ensure that there are appropriate measures in place to eliminate violence against women who are detained for any reason.
8.	Safety and protection	Protection measures for women who have experienced intimate partner violence and sexual violence are critical to stopping the violence and preventing reoccurrence, escalation, and threats of violence. Women have the right to live free of violence and free of the fear of violence. This means that protection measures need to be available independent of any initiation of a criminal, civil, or family law case and be designed to empower women in their access to justice and enable them to stay safely engaged with the justice process.
9.	Support and assistance	A crucial element in guaranteeing access to justice for all women is the provision of support and assistance services during the justice process. The international norms and standards refer to the importance of legal assistance, practical, accurate and comprehensive information, victim and witness support services and the need for support from outside the justice sector (such as health, shelters, social services, counselling). These services can empower women, allowing them to make their own informed decisions based on knowledge of their rights and justice options.
10.	Communication	Communication is a key theme throughout the justice system. The victim/survivor needs to know that she is being listened to and that her changing justice needs are being understood and addressed. Information and the way it is communicated can empower the victim to make informed decisions regarding her engagement with the justice system. Information and communication management amongst the various justice service agencies and non-justice sectors, particularly prioritising confidentiality and privacy, can contribute to the minimisation of the risks victims face when seeking justice.
11.	Coordination among Justice Agencies	Given the different mandates of each justice agency and the various tasks of different justice service providers, a coordinated response is essential to ensuring that essential justice and policing services are delivered in a quality and effective manner and delivers the best outcome for victims/survivors. Coordination sets transparent standards and expectations from each justice agency and contributes to better communications and linkages between the different justice agencies and service providers. From the perspective of a victim/survivor, coordination of essential services means that she will be met with the same understanding of her rights and her situation and receive the same, high quality response from all justice service providers. Justice service providers are valuable members of multi-disciplinary coordination mechanisms, which have been discussed in Module 5 on Coordination and Governance.

PART FIVE

Digital Investigation Proceedings of Electronic and Digital Evidence

LEARNING OBJECTIVES

Understanding cyber/digital evidence



Grasping the key issues involved in crime scene processing



Understanding how best to present digital/electronic evidence in court



Knowing how to assess which jurisdiction has priority in multi-jurisdictional digital/electronic evidence cases



5.1. Introduction

'Digital data is a fundamental pillar for most law enforcement investigations today. With the advent of the smartphone, social media, and internet personalisation with services like Google and Apple, a person leaves a digital trail and the digital trail must be captured and analysed for intelligence and evidence relating to the crime. The search and seizure phase is critical as this will safeguard the devices and the data held on them'.¹⁰²

5.2. What is digital evidence?¹⁰³

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device.

Properties of the Electronic Evidence:

- It is hidden, similar to fingerprint evidence or DNA evidence
- It can be broken, altered, damaged, or destroyed by improper handling
- It expires within a pre-set time.

Digital evidence refers to the recovery and investigation of material found in **digital devices**, often concerning computer crime. It covers the investigation of all devices capable of storing **digital data**. Several sub-branches are computer forensics, network forensics, mobile forensics and forensic data analysis.

5.3. First Responder

- Responsible for the process of search and seizure
- Responsible for obtaining the appropriate search warrant and having in place all necessary authorization before starting the search and seizure process
- Makes decisions about the methods of collecting or seizing electronic pieces of evidence
- Responsible for securing the scene, documenting the scene, and storage of evidence
- Responsible for the actions that could change the evidence
- Responsible for the state of the electronic evidence
- Responsible for identification of all possible storage of electronic evidence
- Responsible for the activities for the prevention of altering or losing the electronic pieces of evidence

5.4. Sources of evidence

Electronic evidence may be found in any number of locations, such as:

- Locally on an end-user device
 - Computer Systems: e.g. personal computers (PCs), laptops, servers, gaming consoles, etc.
 - Data storage mediums: e.g. Cloud storage, Optical Discs (CD, DVD, Blu-Ray), removable data storage drives (USB thumb drives, external SSD/HDD), memory cards, flash drives, external hard drives, etc.

¹⁰² INTERPOL: Guidelines for Digital Forensics First Responders (March 2021). Available online at: <https://www.interpol.int/content/download/file>

¹⁰³ Ibid

- Mobile devices: e.g. mobile/smartphones, tablets (with SIM Card and Removable Media Card), digital cameras, satellite navigation systems, automotive IT devices, smart watches, fitness trackers, etc.
- Network devices: e.g. NAS (Network Attached Storage), routers, wireless access points, smart sensors/actors/controls, etc.
- Internet of Things (IoT) devices: e.g. smartwatches, Smart TV, Home kits, sensors, actors, controllers, gateways, concealed cameras, etc.
- Automotive vehicles: e.g. automotive embedded information systems in cars
- Virtual assets devices: e.g. involving cryptocurrencies such as Bitcoin;
- Unmanned aerial vehicles: e.g. Drones
- Video surveillance devices: e.g. CCTV.
- Remotely on a public resource e.g. social networking sites, discussion forums and newsgroups
- Remotely on a private resource e.g. an ISP user's activity logs, a mobile phone company's customer billing records, a user's webmail account and a user's remote file storage
- In transit e.g. mobile phone text messages, or voice calls, emails, or internet chats. Special authorisation might be needed to obtain 'in transit' evidence.

5.5. Search and seizure: Standard Operating Procedures (SOPs) for dealing with electronic evidence

Standard Operating Procedures ensure that the integrity and chain of custody of electronic evidence are maintained from the stage where a cybercrime incident is reported at a police station up to the stage where the evidence is presented in court. Any deviation from the SOPs must be properly explained in writing. SOPs cover all the important stages and procedures in the collection of electronic evidence, namely: the preliminary steps, legal requirements, the search and seizure procedure, and the manner in which electronic evidence must be packed, transported, processed, stored and made available for criminal proceedings, and the responsibilities and qualifications of the persons who are involved in the investigation process and forensic examination process.¹⁰⁴

5.6. Five principles applicable to electronic evidence

Principle 1: Legality - The search for and seizure of all electronic evidence must be authorised by law. This could involve obtaining consent from a person entitled to give consent or procuring a search warrant. Where electronic evidence is obtained for purposes of criminal proceedings the rules governing admissibility of electronic evidence must be kept in mind.

Principle 2: Data Integrity - No action taken by law enforcement agencies or their agents should change electronic evidence which may subsequently be relied upon in a court of law. Where it is necessary to access data on a "live" computer system to avoid the loss of potential evidence, this process must be carried out in a manner which causes the least impact on the data and by a person qualified to do so.

Principle 3: Audit Trail - A record (audit trail) should be created of all actions which are undertaken when handling electronic evidence and it should be preserved for future reference. This is to ensure that an independent third party should be able to examine those actions and achieve the same results. The audit trail will also assist in proving the admissibility and reliability of the chain of custody during criminal proceedings.

Principle 4: Competence of person seizing electronic evidence - A person seizing electronic evidence must be competent to do so. If a member of law enforcement is not competent to do so, such member must request assistance from a person competent to do so. Said person must be able to give evidence explaining the relevance and the implications of his or her actions.

Principle 5: Oversight - The person in charge of the investigation has the overall responsibility for ensuring that the law and these SOP's are adhered to.

104 Association of Chief Police Officers: ACPO Good Practice Guide for Digital Evidence for Digital Evidence (2011). Available online at: https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.

5.7 Preparation prior to the search and seizure operation ¹⁰⁵

5.7.1 Planning

Several considerations must be taken into account when planning and preparing for a search and seizure operation:

- A **preparatory meeting** should be held to exchange information between the Unit in charge of the investigation and the digital forensic specialist supporting the mission.
- **Briefing and allocation of tasks:** All members of the law enforcement team involved in the search and seizure operation and other persons assisting them should be fully briefed and individual tasks should be assigned to the team members.
- **Background information:** Before arriving at a potential search scene, the investigator must obtain as much information about the offence, the suspect and his/her IT skills, and the scene as possible.
- **Suspect's Technical knowledge:** Information about the suspects and their technical skills must be assessed as they could have protected their equipment or data in some way that could compromise the acquisition of the evidence.
- **The objectives of the search and seizure:** Just because a digital device is found at the scene does not mean it has to be seized. It must first be considered whether an article is likely to contain evidence relevant to the suspected offence/s. The person in charge of the search must have reasonable and justifiable grounds to remove the property. Officers should ensure they are acting within the confines of the search warrant.
- **Nature of the electronic evidence:** The type of electronic evidence will determine the technical solutions which will be needed to acquire the electronic evidence, as well as the level of expertise that is required during the operation. This may include considerations such as whether there will be a seizure of equipment or capturing of live data or a combination of both.
- **Location of electronic evidence:** The location of electronic evidence may have a bearing on the required judicial authority and/or how the search and seizure operation should be conducted. It is not unusual for information to be stored in a place other than the physical computer equipment of the suspect. It might then be necessary to obtain additional legal authorization, especially if it is stored in a different jurisdiction and additional technical equipment is required to ensure the integrity of the evidence. Electronic evidence may also be held in more than one location. Consideration should be given to the different resources involved in obtaining the evidence from the different locations to determine which one would provide the easiest access.
- **Logistical aspects:** The logistical aspects of the investigation must be considered to ensure the availability of sufficient human resources and equipment.
- Time of the search and seizure operation.
- **Other forensic examinations:** Appropriate arrangements must be made where other forensic processes also need to be performed during the search and seizure operation, e.g. the taking of fingerprints or collection of DNA samples.
- **Safety:** Where necessary make appropriate arrangements to ensure the safety of law enforcement members and other persons present at the scene.
- **Securing of location:** Make appropriate arrangements to safeguard the electronic evidence against unwanted access. This will be especially important where the perpetrator/s is/are skilled in the use of computers.
- **Evidence destination:** The destination of the seized items must be defined before starting any activity of search and seizure. Forensic copies, as well as devices that require specific treatment, should be sent to the corresponding department/team for processing and analysis.

5.7.2 Authorisation

Regarding authorisation the following needs to be done:

- The necessary legal authorisation must be attained prior to the search and seizure operation.
- All officials involved must act in accordance with the provisions of the authorising legislation when they conduct a search for or when they seize electronic evidence.
- When making an application for a warrant in terms of the relevant legislation, the extent of the authority which is required to conduct a search and seizure operation must be clearly set out.
- A valid search warrant must, therefore, in a reasonably comprehensible manner:

105 Council of Europe Portal: Cybercrime Programme Office (C-PROC) - CyberSouth Activities: The CoE Standard Operating Procedures for the collection, analysis and presentation of electronic evidence (12 September 2019) Available online at: https://www.coe.int/en/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/the-coe-standard-operating-procedures-for-the-collection-analysis-and-presentation-of-electronic-evidence-have-been-released?inheritRedirect=false

- state the statutory provision in terms of which it is issued
 - identify the searcher/s
 - mention the authority it confers upon the searcher/s
 - identify the person, container or premises to be searched
 - describe the article/s to be searched for and seized, with sufficient particularity
 - specify the offence and (where relevant) the statutory provision which prompted the criminal investigation
 - name the suspected offender/s.
- appropriate forensic equipment, among others –
 - computer devices to undertake forensic examination, imaging or preview
 - hard drive storage media devices which have been forensically cleaned
 - approved forensic software
 - approved write blockers that permit read-only access to data storage devices without compromising the integrity of the data
 - forensic boot DVDs or equivalent
 - network cables (twisted pair and crossover)
 - gloves
 - power supplies, electric cables for digital devices and power banks, etc.

5.7.3 Personnel

Regarding personnel the following should be considered:

- Sufficient qualified law enforcement members should be made available to participate in a search and seizure operation.
- Participating members must be clearly identified in the search warrant.
- A Digital Forensic Examiner required to attend a search and seizure operation may require a written request before deployment and he/she must specifically be authorised in a warrant to participate in the investigation.
- Unless national legislation provides otherwise, persons who are not members of law enforcement cannot actively participate in a search and seizure operation. They can however be requested to provide remote advice during an investigation.

5.7.4 Equipment

Members involved in the process of search and seizure of electronic evidence should ensure the availability of:

- necessary tools for the disassembly and removal of electronic devices
- required documentation to be completed during the search and seizure
- photography or video recording equipment
- supplies to package and transport electronic evidence, such as exhibit bags (where necessary of an anti-static or Faraday type), labels, markers, appropriate containers, cable ties, etc.

5.8 During the search and seizure operation¹⁰⁶

5.8.1 Securing the location

The person in charge of the search and seizure operation must guarantee the safety of all persons at the location as well as the integrity of all seized electronic and traditional evidence by ensuring that:

- All national instructions for the securing of a crime scene are implemented
- The location where the search and seizure are to take place is secure. This includes identifying potential hazards, e.g. is the suspect likely to possess a firearm, resisting arrest or flee the scene
- All persons are accurately accounted for
- Electronic evidence is protected from interference, damage or power outage
- Unauthorised persons do not have access to electronic evidence which includes peripherals associated with electronic devices). It is, however, imperative to identify all persons at the scene and to record their location at the time of entry
- Assistance is not provided by persons who have not specifically been authorised by the person in charge of the investigation
- The suspect or his/her accomplice is not able to remotely or directly interfere with the relevant electronic evidence
- Electronic devices and possible sources of electronic evidence are kept away from magnetic devices, extreme temperatures, and moisture to prevent the loss or destruction of data.

106 Council of Europe. Electronic Evidence Guide-A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.1. March 2020. Available online at <https://www.forensicfocus.com/forums/general/coe-electronic-evidence-guide/>

5.8.2 Search and seizure

5.8.2.1 General

- (a) Identify all potential evidence and ensure that the integrity of both the digital and traditional evidence is preserved. Take note that digital devices containing potential evidence may be easily hidden, integrated, or contained within cupboards or drawers, i.e. memory cards, mobile phones, etc.
- (b) Identify all relevant removable electronic devices (e.g. CDs, Blu-ray Disks, Memory Cards, USBs, Tape Disks, etc.) and ensure that the integrity of the devices is preserved.
- (c) To take precautions to prevent the potential loss of critical data which is of temporary nature, the officer in charge of the operation should assess the volatility of digital evidence present at the location. Volatile electronic evidence must be seized first in order to prevent loss of data. The order of volatility of electronic evidence is as follows:
 - Network connections, ports, running processes
 - Open files such as unsaved documents
 - The contents of RAM
 - Open remote storage
 - Logical volumes
 - Physical disks
 - External media – such as USB, CD and DVD.
- (d) Collect instruction manuals, documentation and any notes that might have bearing on the collected electronic evidence.

5.8.2.2 Keeping record

- (a) The search and seizure location should be documented, photographed and/or video recorded from the moment of commencement of the operation up to the conclusion thereof.
- (b) A plan of the search and seizure location should be drawn up prior to seizure and must reflect the layout of the premises, the position of electronic devices, and any other relevant information.
- (c) A designated member of operation should be nominated to keep a full record of the search and seizure operation, which includes the finding, seizure, photographing, and packaging of exhibits.
- (d) All actions taken and decisions made by members involved in the operation should be fully recorded, in writing, by said member and be preserved for future reference or criminal proceedings.

- (e) All activities undertaken by a digital forensic examiner in the course of the operation should be fully and contemporaneously recorded in writing, by the said digital forensic examiner and be preserved for future reference or criminal proceedings.
- (f) All routers (including wireless routers), switches, telephone lines and cabling must be identified. Only authorised digital forensic examiners should undertake the examination of routers, switches, and other live network devices.
- (g) Exhaustive documentation of the location and original condition of the devices must be kept. The following are examples of information that must be documented:
 - Type (Computer, Hard drive, flash drive, DVD, etc.)
 - Brand and Model
 - Storage Capacity
 - Serial Number
 - State (if it is damaged specify the extent of the damage)
 - Security (access password, PIN)
 - Other comments (used by children, not connected to the internet, etc.)

5.8.2.3 Electronic devices which are switched off ¹⁰⁷

NOTE that a computer may only *appear* to be switched off:

- Check if the monitor has power and connection to the equipment
- Check if the computer has power
- Check if LEDs are blinking or if you can hear any fan or hard drive noise
- Try moving the mouse or pressing SHIFT on the keyboard. Do not press RESET or ENTER
- Take note of time of actions for record purposes.

Where an electronic device which is to be seized, is switched off DO NOT TURN IT ON. The following procedures should be followed:

- Document all connections to the PC before disconnecting connectors.
- Remove any power supply connected to the equipment - not from the wall.
- Check if there is a disc inside the CD-DVD reader and remove it with a clip in the mechanical unlocking hole.
- Check if there are any USB devices connected.

107 INTERPOL: Guidelines for Digital Forensics First Responders (March 2021). Available online at: <https://www.interpol.int/content/download>

- Search the scene for any evidence of passwords.
- After documenting the status and situation in which the equipment is found, the entire device is sealed.
- If disks have been configured in RAID or the PC has an encryption chip or any other particular element, the equipment must be seized together with the hardware to facilitate its subsequent reconstruction.
- In the case of simple or standardized equipment, it will not be necessary to seize the entirety of the equipment.
- Peripherals, monitors, mice, keyboards and their cables should not be seized unless they are proprietary models.
- Where an emergency requires the system to be booted the device should be booted in read-only mode through a blocker or from a bootable media with its own forensic operating system (CAINE, DEFT Linux, KALI Linux, SANS SIFT, AUTOPSY WinFE, FTK Imager, etc.). This operation should only be carried out by an expert.

5.8.2.4 Electronic devices which are switched on

- (a) Where an electronic device is found to be switched on, it should be examined in order to determine –
- i. If the device is connected to a power outlet that is switched on
 - ii. If encryption or similar software is used on the device
 - iii. If there is a possibility that digital evidence has not been saved to a storage medium such as the hard drive
 - iv. If any anti-forensic systems have been installed on the device
 - v. Other possibilities of probable loss of digital evidence.

Where the circumstances referred to in items (i) to (v) are present, it may be necessary to capture digital evidence from electronic devices before they are turned off or disconnected from networks or power supplies (live acquisition of digital evidence).

Device isolation from the network should also be assessed, as cutting off the device from its access ‘lifeline’ could assist in preventing existing digital evidence from changing, or even disappearing altogether.

Screensavers and screen locking should also be disabled.

- (b) The information referred to in paragraphs (a) (i) to (v) should be brought to the attention of the member in charge of the operation, who must decide whether a live acquisition of digital evidence should be undertaken.
- (c) live acquisition of digital evidence must only be undertaken by a digital forensic examiner.

USEFUL TIPS

- Take a picture of the screen.
- Check for the user's activity. If any destructive action is on going, it must be interrupted immediately, even pulling the power cable.
- Is the device networked?
- Disable screensaver and power options.
- Check the available volumes and verify if they are encrypted.
- Check if there are connections with online services, like Dropbox or OneDrive.
- Check activity of the browser, webmail, social networks, etc.
- Can it now be disconnected from the network?

- (d) The live acquisition of digital evidence should be done in the following manner: ¹⁰⁸
- i. Only appropriate accredited forensic tools should be used.
 - ii. Only appropriate accredited write blockers should be used during a live acquisition.
 - iii. A forensic image of the electronic device being examined should be saved to an external memory storage device that has been forensically cleaned and provided during the planning phase.
 - iv. Appropriate forensic tools should be used to obtain forensic images of the memory dump (RAM).
 - v. Where pre-acquisition viewing is undertaken, appropriate write blocking and forensic devices must be used.
 - vi. Where files and/or data are copied at the pre-acquisition viewing stage for use in interviews or other investigative processes, a full record must be kept and the files and/or data should also be retrieved during the full examination undertaken at a Digital Forensics laboratory.
- (e) Once a full image of the electronic device has been obtained on-site, the device should be powered down and packed in accordance with the prescribed provisions.
- (f) Where an electronic device that communicates via radio frequencies is switched on and a decision is made to leave it powered on, there is a risk that someone may interfere with, or connect to the device and remotely wipe the device. In such instances, appropriate packaging should be used to prevent remote interference with the electronic device via the radio frequency spectrum. Appropriate packaging

108 Ibid

would typically include a Faraday Bag that blocks radio signals to the electronic device.

- g) In circumstances where it is not viable to physically seize an electronic device, such as a shared server, it should be left in place and a full record of that decision should be made and retained for future reference or judicial proceedings.

NOTE

- The HASH function or summary function is used to verify the integrity of a data set. In other words, it is about obtaining its 'fingerprint'.
- In the case of electronic evidence, this procedure is applied when making copies of the original devices, so that, once the HASH value of the origin and destination has been calculated, they must be identical. This process is known as verification.
- This procedure is also used to detect known files within the evidence. There are reliable file databases (from the installation of operating systems or other applications), such as those of the NSRL (National Software Reference Library) that allow them to be discarded, and other databases with the signatures of known files, for example, of child sexual abuse material, which allow investigators to identify, track, and even share them amongst law enforcement without the need to distribute the original files.
- It is important to remark that some technologies like SSD are becoming a new challenge when considering evidence verification methods. Due to how the SSDs work they can sometimes purge data all by themselves even if they are not connected to any interface with only the power on.
- Alternatives to traditional evidence hashing must be considered, such as hashing of logical partition or file hashing.

5.8.3 Packing of electronic evidence

Electronic evidence must be placed in a sealed forensic evidence bag which should be appropriately marked with a permanent marking ink pen. An exhibit label should be attached to it and must contain the following information:

- i. The case number
- ii. The unique reference number of the exhibit
- iii. A description of the device (computer, laptop, phone, etc.)
- iv. Any identifying marks found on the device (make, model, serial number)
- v. A description of the location of where the item was found at the crime scene with reference to the plan contemplated in paragraph

- vi. Who found and seized the exhibit
- vii. Who sealed the exhibit in the evidence bag
- viii. The date and time seized
- ix. Date and time sealed
- x. The particulars of the person who was in possession of or under control of the electronic evidence.

Each electronic device should be placed in its own individual exhibit bag. When seizing a laptop include its own laptop bag, charger, cables and accessories. The officer in charge of the search and seizure operation must ensure that all exhibits are accounted for at all times and not left unattended at any time. The packaging of the electronic evidence and the subsequent handling thereof must be documented and kept for future reference or criminal proceedings.

5.8.4 Transportation of electronic evidence¹⁰⁹

When transporting digital devices and electronic evidence the following should be ensured:

- i. The officer in charge must ensure that all exhibits are accounted for at all times.
- ii. Electronic devices should be securely packaged during transportation to prevent damage from shock, temperature and vibrations.
- iii. Ensure that there are no external dongles or external storage devices plugged into electronic devices. All dongles and external storage devices must be removed and dealt with as separate exhibits.
- iv. The transportation process should allow for a conducive and controlled environment. Appropriate storage and transport containers and protective packaging should be provided for safe storage and transportation. The levels of moisture, humidity and temperature should be controlled.
- v. Adequate grounding should be provided during packaging and transporting in order to circumvent electrostatic discharges.
- vi. Avoid keeping potential electronic evidence in the transportation vehicle for prolonged periods in order to circumvent damage or loss of evidence due to Ultra Violet Light.

The member responsible for the loading and transportation of the electronic evidence must document the following:

- i. The exhibits which were received
- ii. The person from which the exhibits were received
- iii. The integrity of the packaging of the exhibits which were received

109 Ibid

- iv. The date and time on which the exhibits were received
- v. The way the exhibits were packed in a vehicle for purposes of transportation
- vi. The persons which took possession of the documents after it was transported to their destiny
- vii. The date and time on which the exhibits were handed over to another person
- viii. The integrity of the packaging and conditions of the exhibits when it was handed over to other persons
- ix. Any incidents which may have affected the integrity of the exhibits during transportation.

5.8.5 Witness statement of the digital forensic expert

Regarding the witness statement the following need to be considered:

- i. The contents of any digital forensic report should be introduced as evidence in the format of an affidavit in accordance with the relevant national legislation.
- ii. Prior to making an affidavit, it is good practice for the digital forensic expert to liaise with the prosecutor in the case. This is to ensure that the prosecutor is aware of the full details of the digital forensic report.
- iii. The full digital forensic report or agreed parts thereof shall be incorporated by reference in the witness statement.
- iv. At the start of the affidavit, the digital forensic examiner should introduce himself or herself and outline his or her qualifications, experience and training.
- v. Each page of the affidavit and attached documents must be initialed.
- vi. Where discs or similar media are presented, the disc or media should be initialed by the digital forensic examiner and sealed in an appropriate container.

5.8.6 Preparation for criminal proceedings

A digital forensic examiner must always be fully prepared when required to consult with a prosecutor regarding a case or when giving evidence in criminal proceedings.

5.8.7 Consultation with prosecutor

Regarding the consultation process with the prosecutor the following need to be considered

- i. The investigating officer must consult with the prosecutor who is assigned to prosecute a matter to make adequate arrangements to consult with the digital forensic examiner/s who prepared the abovementioned affidavit.
- ii. The investigating officer must attend any consultation between the prosecutor and digital forensic examiner and keep a record of the consultation on SAP 5 of the case docket.
- iii. Disclosure of information to the defence or any other person must only take place in accordance with the policy of the prosecuting authority, law enforcement, and applicable legislative provisions.
- iv. Before the commencement of criminal proceedings the investigating officer must liaise with the prosecutor in order to identify all of the exhibits that are needed for purposes of criminal proceedings and the ambit and extent of evidence that a digital forensic examiner must give during proceedings.
- v. Where exhibits are to be presented in criminal proceedings and need to be demonstrated the investigating officer must make arrangements with the prosecutor and digital forensic examiner to ensure the availability of any specialised equipment.

5.8.8 Non-consensual pornographic and child sexual abuse images

Regarding the non-consensual pornographic and child sexual abuse images the following need to be considered:

- i. Where electronic evidence is recovered which contains non-consensual pornographic and child sexual abuse images or other sensitive evidence, special care must be taken to restrict access to such evidence in order to prevent secondary victimisation of the victims or other persons.
- ii. Viewing of such evidence should be restricted to persons who, in accordance with their official duties and responsibilities or in terms of an order of the court, have to deal with the evidence in question.

5.8.9 Criminal proceedings

Regarding the criminal proceedings the following need to be considered

- i. A digital forensic examiner should be fully prepared for criminal proceedings.
 - ii. A digital forensic examiner must ensure beforehand that any specialised equipment which is to be used to demonstrate exhibits are available and fully functional.
 - iii. When giving evidence, a digital forensic examiner must introduce himself or herself and give an outline of his or her qualifications, experience and training. The digital forensic investigator must satisfy the court that he or she is sufficiently qualified to give evidence regarding the subject matter.
- The evidence presented by the prosecutor must prove that the integrity of the data or digital evidence presented in court is intact. This would imply proving that the evidence remained unaltered between the time of its seizure by law enforcement and its examination up to the moment it is being presented in court.
 - If for some reason the data has been altered, the examiner will need to explain exactly how and why.
 - The witness should be able to discuss the type(s) of evidence examined, how it was analysed, and the results.
 - The witness needs to convey all technical information to a non-technical trier of fact in the way that best facilitates understanding.

SAMPLE QUESTIONS FOR A FORENSIC EXAMINER

- Please state your name and by whom are you employed.
- What is your current rank?
- How long have you worked in law enforcement?
- What assignments have you had in law enforcement?
- What is your current assignment?
- How long have you been assigned to that unit?
- What are your specific duties?
- What is 'computer forensics'?
- What is a forensic examination as it relates to computer evidence?
- Is there a standard procedure that you follow in performing computer forensic examinations?
- Briefly, describe the steps in an examination (e.g. identification, preservation, acquisition, recovery, reporting).
- How many examinations have you done to date?
- (Keep in mind that one case may have multiple pieces of evidence and each piece of evidence counts as a separate examination)
- Do you ever assist other law enforcement agencies in doing forensic examinations?
- What is your educational background? (if relevant)
- Do you belong to any relevant professional organisation/s?
- Discuss the organization, its membership, and its purpose where relevant.
- What are your activities within each organisation – if relevant?
- Have you received any training specifically related to computer forensics?
- From whom?
- Have you received any type of certification by any of those organisations?
- Do you have any other specialised training in the use, operation and functioning of computers or software?
- Have you received any additional certification based on that training?
- Have you ever provided training to others on computer forensics?
- For whom, when and where?
- In addition to receiving ongoing training, what else do you do to stay current with developments in computer forensics?
- Have you ever participated in the execution of a search warrant in the field?
- Have you ever conducted an exam outside the lab setting?
- Have you ever testified before?
- If so, how often and in what field(s)?
- Have you ever been qualified as an expert witness before?
- If so, how often and in what field(s)?

5.8.10 Mutual legal assistance

Mutual legal assistance, international cooperation and the presence of INTERPOL and SADC in cases of cross-border cyber violence against and exploitation of women and girls are becoming increasingly prevalent, e.g. online sexual exploitation cases, romance scams, cyberstalking and sextortion, etc.

Where multiple jurisdictions are involved in a matter, decisions should be made as early as possible as to which investigation/prosecution will be given priority and what can be done to minimise the trauma to the victim by avoiding pursuing the matter in multiple jurisdictions. The decision of which state has jurisdiction, and which state will be given preference in terms of proceeding with prosecution first is a complex matter which mandates a case-by-case analysis and decision.

Factors reviewed in coming to that determination include:

- **Procedural issues:** these would include issues of double jeopardy between jurisdictions, Memorandums of Understanding (MOUs) that may apply, and extradition issues, such as whether there is an extradition treaty in place between the countries and do the states involved permit extradition of their nationals.
- **Substantive issues:** these would assess which jurisdiction has the strongest case and can reasonably expect a successful prosecution. Quantity and quality of admissible evidence, as well as past success or failure in prosecuting similar cases, would be relevant to making this determination.
- **Best interest of the victim(s):** where is the victim located? How can the victim experience the least amount of distress and inconvenience (e.g. having to testify more than once, having to travel internationally versus locally, etc.)? Which jurisdiction(s) has protocols in place to lessen the trauma to victims? How will location interact with any compensation claims the victim may have against the perpetrator(s)?
- **Witnesses:** which jurisdiction will impose the least burden on the witnesses? Where are the majority of witnesses located? Where are witness protection plans in place, if needed?
- **Defendant:** will the defendant's state permit extradition? What alternatives to in-person presence, if any, might be available?
- **Evidence:** will key, relevant evidence be able to be shared electronically, through statements/testimony being given by audio-visual link (such as CCTV), or through the production of physical evidence in another jurisdiction?
- **Mutual Legal Assistance (MLA) treaty:** If an MLA is in place between the countries, it may provide guidance.¹¹⁰
- **Law enforcement investigative investment:** This will entail considering the length of the investigation to date and the resources already invested in the case. Which jurisdiction has the greatest connection to the crime? Which jurisdiction has sufficient resources to bear the burden of costs of the prosecution?
- **Prescriptive period/statute of limitations:** Are there any time limits on prosecuting that make one jurisdiction more or less appealing than another?
- **Sentencing power:** What are the available offences and penalties which appropriately reflect the seriousness of the criminal conduct in each possible jurisdiction? Which jurisdiction can secure a sentence that deters similar conduct and results in just punishment?¹¹¹
- Any other relevant factors not mentioned above.

As each case is inherently unique, any determination about which jurisdiction is best positioned to prosecute should be based on the facts and merits of each case with all relevant factors considered. Which criteria should be applied, and the order of priority must be determined on a case-by-case basis.

110 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters (2004). Article 1.2 states: Mutual assistance to be rendered in accordance with this Treaty may include: (a) taking of evidence or obtaining voluntary statements from persons; (b) making arrangements for persons to give evidence or to assist in criminal matters; (c) effecting service of judicial documents; (d) executing searches and seizures; (e) examining objects and sites; (f) providing original or certified copies of relevant documents, records and items of evidence; (g) identifying or tracing property derived from the commission of an offence and instrumentalities of crime; (h) the restraining of dealings in property or the freezing of property derived from the commission of an offence that may be recovered, forfeited or confiscated; (i) the recovery, forfeiture or confiscation of property derived from the commission of an offence; (j) locating and identifying witnesses and suspects; and (k) the provision of such other assistance as may be agreed and which is consistent with the objects of this Treaty and the laws of the Requested Party. Available online at https://www.jus.uio.no/english/services/library/treaties/04/4-07/asean_mutual_legal_assistance.xml

111 International Association of Prosecutors (IAP). Prosecutorial Guidelines for Cases of Concurrent Jurisdiction (2014), pp 10-16. Available online at http://www.iap-association.org/IAP/media/IAP-Folder/IAP_Guidelines_Cases_of_Concurrent_Jurisdiction_FINAL.pdf.



PART SIX
Annexures

ANNEXURE 1

ACRONYMS

ACPO	Association of Chief Police Officers
ACRWC	African Charter on the Rights and Welfare of the Child
ASEAN	Association of Southeast Asian Nations
AU	African Union
BPfA	Beijing Declaration and Platform for Action
CCTV	Closed-circuit television
CEDAW	Convention on the Elimination of all Forms of Discrimination Against Women
COE	Council of Europe
C-PROC	Cybercrime Programme Office
CRC	Convention on the Rights of the Child
CSAM	Child sexual abuse materials
CSO	Civil society Organisation
CSVr	The Centre for the Study of Violence and Reconciliation
CVAWG	Cyber Violence Against Women and Girls
DDF	Data Disclosure Framework
DVA	Domestic Violence Act
ECPAT	End Child Prostitution and Trafficking
EVAW	Elimination of Violence Against Women
EC	European Commission
EU	European Union
GBV	Gender-based Violence
GBVF	Gender-based Violence and Femicide
GRKWG	Gender-related killing of women and girls
HIPSSA	Harmonisation of ICT Policies in Sub-Saharan Africa
IAP	International Association of Prosecutors
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IGF	Internet Governance Forum
ISPs	Internet Service Provider(s)
IAWJ	International Association of Women Judges
ICT	Information Communications Technology
IoT	Internet of Things
IPDV	Inter-Partner Domestic Violence
IPV	Intimate Partner Violence
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, Asexual and other extensions

M&E	Monitoring and Evaluation
MAUCORS	The Mauritian Cybercrime Online Reporting System
MDT	Multi-disciplinary Team
MISA	Maintenance and Internal Security Act
MLA	Mutual Legal Assistance
NAPs	National Action Plans
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organisation
NGO	Non-governmental Organisation
NPA	National Prosecuting Authority
OGBV	Online gender-based violence
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organisation for Security and Co-operation in Europe
PO	Protection Order
PPO	Permanent Protection Order
PTSD	Post-Traumatic Stress Disorder
RWPC	Regional Women's Parliamentary Caucus
SADC	Southern Africa Development Community
SAIK	Sexual Assault Investigation Kit
SDGs	Sustainable Development Goals
SGM	Sexual and Gender Minority
SH	Sexual Harassment
SOC	Sexual Offences Court
SOPs	Standard Operating Procedures
SRHR	Sexual and Reproductive Health and Rights
TIP	Trafficking in Persons
TFGBV	Technology Facilitated Gender-based Violence
UDHR	The Universal Declaration of Human Rights
UN	United Nations
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UNFPA	United Nations Population Fund
UNICEF	United Nations International Children's Emergency Fund
UNODC	United Nations Office on Drugs and Crime
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women
VAW	Violence Against Women
VAWC	Violence Against Women and Children
VAWG	Violence Against Women and Girls
WHO	World Health Organisation

ANNEXURE 2

GLOSSARY

Child/minor¹¹² – a person under the age of 18 years, regardless of the age of majority or age of consent nationally/locally. This is based on the Convention on the Rights of the Child.

Child sexual abuse materials (CSAM)¹¹³ – this is the preferred term for child pornography as it more accurately reflects the fact that sexualised material that depicts or otherwise represents children is indeed a representation and a form, of child sexual abuse, and should not be described as ‘pornography’.¹¹⁴ To refer to these images as ‘pornography’ may ‘contribute to diminishing the gravity of, trivialising, or even legitimising what is actually sexual abuse and/or sexual exploitation of children’.

Compensation¹¹⁵ – means quantifiable damages resulting from the violence and includes both pecuniary and non-pecuniary remedies, such as an injunction. When compensation is not fully available from the offender or other sources, States should provide financial compensation.

Criminal justice¹¹⁶ – refers to a system that is derived from criminal law and focuses on concepts such as accountability of the person who commits a crime or offends public order/violates the rights of another; protection and compensation/redress of the victims; and fairness in terms of all parties. Criminal justice also refers to a mechanism for administering criminal justice that can provide a fair outcome and has appropriate capacity and authority.

Cyberbullying¹¹⁷ – is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include: spreading lies about or posting embarrassing photos of someone on social media; sending hurtful messages or threats via messaging platforms; impersonating someone and sending mean messages to others on their behalf.

Cybercrime – is generally defined as meaning illegal acts, the commission of which involves the use of information and communication technologies; ‘any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them’. These can be traditional criminal offenses committed with the use of a computer and newer crimes that originated with the advent of computers and networks.

Cyberviolence¹¹⁸ – the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual’s circumstances, characteristics or vulnerabilities.

Essential Services¹¹⁹ – encompass a core set of services provided by the health care, social service, police and justice sectors. The services must, at a minimum, secure the rights, safety and well-being of any woman or girl who experiences gender-based violence.

Formal justice systems – are justice systems that are the responsibility of the State and its agents. They include government-supported laws, and institutions such as police, prosecution services, courts, and prisons that have the responsibility to enforce and apply the laws of the State and to administer the sanctions imposed for violations of laws.

112 UNICEF: Convention on the rights of the child. Available online at <https://www.unicef.org/child-rights-convention>

113 ECPAT, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Available online at <https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf>.

114 Interpol, ‘Appropriate Terminology’. Available online at <http://www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology>

115 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

116 Ibid

117 UNICEF: Cyberbullying-What it is and how to stop it – What teens want to know about cyberbullying. Available online at <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>

118 Cybercrime Convention Committee: Mapping study on Cyberviolence. Available online at <https://www.coe.int/en/web/cyberviolence>

119 United Nations: Essential Services Package for Women and Girls Subject to Violence – Core Elements and Quality Guidelines. Partnership by UN Women, UNFPA, WHO, UNDP and UNODC (2015). Available online at <https://www.unodc.org/documents/justice-and-prison-reform/EN-Modules-AllInOne.pdf>

Gender ¹²⁰ – refers to the roles, behaviours, activities and attributes that a given society at a given time considers appropriate for men and women. In addition, ‘gender’ refers to the social attributes and opportunities associated with being male and female and the relationships between women and men and girls and boys. These attributes, opportunities and relationships are socially constructed and are learned through socialisation processes. They are context- and/or time-specific and changeable Gender determines what is expected, allowed and valued in a woman or a man in a given context. In most societies, there are differences and inequalities between women and men in responsibilities assigned, activities undertaken and access to and control over resources and decision-making opportunities. Gender is part of the broader sociocultural context, as are other important criteria for sociocultural analysis, such as class, race, poverty level, ethnic group, sexual orientation and age.

Gender-based violence against women and girls (GBVAG) ¹²¹ – is violence directed towards, or disproportionately affecting women because of their gender or sex. This term makes explicit the gendered causes and impacts of the violence. Such violence takes multiple forms, including acts or omissions intended or likely to cause or result in death or physical, sexual, psychological or economic harm or suffering to women, threats of such acts, harassment, coercion and arbitrary deprivation of liberty. GBVAG can be defined differently under national laws.

Gender equality ¹²² – refers to the equal rights, responsibilities and opportunities of women and men and girls and boys. Equality does not mean that women and men will become the same, but that their rights, responsibilities and opportunities will not depend on whether they are born male or female. Gender equality implies that the interests, needs and priorities of both women and men are taken into consideration, recognizing the diversity of different groups of women and men. Gender equality is not a women’s issue; it should concern and fully engage men as well as women. Equality between women and men is seen as both a human rights issue and a precondition for, and indicator of, sustainable, people-centred development.

Gender identity ¹²³ – refers to each person’s deeply felt internal and individual experience of their own gender, which may or may not correspond to the sex assigned at birth. This includes an individual’s personal sense of their own body (which may involve, if freely chosen, modification of bodily appearance or function by medical, surgical or other means) and other expressions of gender, including dress, speech, mannerisms and choice of personal pronouns (he/him; she/her; or gender-neutral and non-binary pronouns e.g. they). Gender identity is not restricted to male or female, as individuals may choose to identify as neither male nor female, as both male and female or as a third gender (irrespective of anatomy).

Gender-related killing of women and girls (GRKWG)¹²⁴ – refers to the killing of women and girls by their intimate partners or family members, ‘honour’-related killing of women and girls, dowry-related killing of women, killing of women in the context of armed conflict, gender-based killing of aboriginal and indigenous women, extreme forms of violent killing of women, killing as a result of sexual orientation and gender identity, killing of women due to accusations of sorcery and witchcraft, or killing of sex workers. In some countries GRKWG was criminalized as ‘femicide’ or ‘feminicide’ and has been incorporated as such into national legislation in those countries. Intimate partner/family-related homicides are one of the most visible and widely researched forms of GRKWG, with data from the 2018 UNODC Global Study on Homicide showing that 137 women across the world are intentionally killed by current or former intimate partners each day.

Gender-responsive justice ¹²⁵ – means ensuring that laws, justice institutions, justice processes and justice outcomes do not discriminate against anyone on the basis of gender. It necessitates taking a gender perspective on the rights themselves, as well as an assessment of access and obstacles to the enjoyment of these rights by women and men, and adopting gender-sensitive strategies for protecting and promoting them.

120 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

121 Ibid

122 Ibid

123 Ibid

124 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

125 Ibid

Gender sensitivity¹²⁶ – means using respectful and non-discriminatory language and taking into account the different situations, needs and attributes of women, men and others, in order to make sure behaviours, mind sets or programmes respect the human rights of all persons.

Grooming – a process by which a person prepares a person and the environment for the abuse of this person. Specific goals include (1) gaining access to the person, (2) gaining the person's compliance, and (3) maintaining the person's secrecy to avoid disclosure. The grooming process serves to strengthen the offender's abusive pattern, as it may be used as a means of justifying or denying their actions.

Intimate partner violence – is 'the most common form of violence experienced by women globally . . . and includes a range of sexually, psychologically and physically coercive acts used against adult and adolescent women by a current or former intimate partner, without her consent. Physical violence involves intentionally using physical force, strength or a weapon to harm or injure the woman. Sexual violence includes abusive sexual contact, making a woman engage in a sexual act without her consent, and attempted or completed sex acts with a woman who is ill, disabled, pressurised, or under the influence of alcohol or other drugs. Psychological violence includes controlling or isolating the woman and humiliating or embarrassing her. Economic violence includes denying a woman access to and control over basic resources.'

Justice continuum – extends from a victim/survivor's entry into the system until the matter is concluded. A woman's journey will vary, depending on her needs. She may pursue a variety of justice options, ranging from reporting or making a complaint that initiates a criminal investigation and prosecution or seeking protection, and/or pursuing civil claims including divorce and child custody actions and/or compensation for personal or other damages, including from State administrative schemes, concurrently or over time. Multi-disciplinary response teams are groups of stakeholders who have entered into agreements to work in a coordinated manner to respond to violence against women and girls within a community. These teams are focused on ensuring an effective response to individual cases and may contribute to policy making.

Judicial stereotyping¹²⁷ – is the practice of judges ascribing to an individual specific attributes, characteristics or roles by reason only of her or his membership in a particular social group and perpetuating harmful stereotypes through their failure to challenge those stereotypes

Non-partner sexual violence¹²⁸ – refers to violence by a relative, friend, acquaintance, neighbour, work colleague or stranger. It includes being forced to perform any unwanted sexual act, sexual harassment and violence perpetrated against women and girls frequently by an offender known to them, including in public spaces, at school, in the workplace, and in the community.

Secondary victimisation¹²⁹ – is the victimisation that occurs not as a direct result of the criminal act but through the inadequate response of criminal justice institutions and providers to the victim.

Sexual abuse¹³⁰ – means the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions. It includes sexual slavery, pornography, abuse and sexual assault.

Sexual exploitation¹³¹ – is defined as an actual or attempted abuse of someone's position of vulnerability differential to power or trust, to obtain sexual favours, including but not only, by offering money or other social, economic or political advantages. It includes trafficking and prostitution.

Victim/survivor¹³² – refers to women and girls who have experienced or are experiencing gender-based violence to reflect both the terminology used in the legal process and the agency of these women and girls in seeking essential services.

Violence against women (VAW)¹³³ – means 'any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.'

126 Ibid

127 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at: https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

128 Ibid

129 Ibid

130 UNHCR: What is Sexual Exploitation, Abuse and Harassment? Available online at <https://www.unhcr.org/what-is-sexual-exploitation-abuse-and-harassment.html>

131 Ibid

132 UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

133 WHO: Violence against women, 2021. Available online at: <https://www.who.int/news-room/fact-sheets/detail/violence-against-women>

ANNEXURE 3

EXAMPLE OF A TRAINING INTERVENTION: DRAFT PLANNING AND PREPARATION PLAN

1. Target audience:

2. Probable number of attendees

3. Training intervention topic:

4. Objective of training intervention and outcomes to be achieved:

5. Objective:

6. Outcomes to be achieved:

7. Planning and organising a team:

Name	Contact number	Email

8. Possible dates and times for training intervention:

9. Will it be done virtually or in-person? If virtual, what platform will be used? If in-person, what are the possible venues and estimated cost (if any)? Will refreshments be needed? Copies? Costs?

.....

.....

.....

10. Method/s of presentation to be used:

.....

.....

.....

11. Methodology to be used:

Guest Speaker/s? Who?

Why this speaker/s?

Costs involved?

Peer facilitators to be used?

Who?

Group discussions?

Other training techniques?

.....

.....

Other activities?

.....

.....

12. Materials needed:

For facilitators:

.....

.....

For participants:

.....

.....

To be developed:

.....

.....

13. Tools needed:

14. Presentation plan:

Topic	Objective	Time needed	Speaker/Facilitator

15. Draft programme:

Time	Topic		

16. Action Plan for Intervention:

Action	By when?	Person/s Responsible?	

ANNEXURE 4

EXAMPLE OF A TRAINING PROGRAMME



TRAINING AGENDA FOR INVESTIGATORS AND PROSECUTORS ON CYBERVIOLENCE AGAINST WOMEN AND GIRLS (CVAWG)

DAY 1		
INTRODUCTION TO CYBERVIOLENCE AGAINST WOMEN AND GIRLS (CVAWG) CYBERCRIME: CONVENTIONS, PROTOCOLS CHARTERS AND MODEL LAWS		
08:30 - 09:00	Opening Remarks and Welcome	
09:00 - 09:15	Guest of Honour Remarks (optional)	
09:15 - 09:30	Pre-test Introduction of Agenda	
09:30 - 11:00	Video on Gender-based Violence (GBV) Plenary Discussion	
11:00 - 11:15	BREAK	
11:15 - 12:15	<ul style="list-style-type: none"> • GBVF Statements and Discussion • Cyberviolence and GBVF • Human Rights Perspective 	
12:15 - 13:15	<i>What is cybercrime?</i> – defining the digital world and its crimes	
13:15 - 14:00	LUNCH	
14:00 - 15:00	Cybercrime: Conventions, Protocols, Charters and Model Laws	
15:00 - 16:00	SADC Model Law on GBVF	
16:00 - 16:15	Wrap up, homework assignment and overview of Day 1	
DAY 2		
UNDERSTANDING GENDER-BASED VIOLENCE AND FEMICIDE (GBVF), CYBERCRIMES AND RELATED ISSUES		
08:30 - 08:40	Welcome and Recap (10 mins)	
08:40 - 10:45	Understanding Gender-based Violence and Femicide <ul style="list-style-type: none"> • Group Activity 1: <i>What is Gender-based Violence and Femicide?</i> • Report Back on Group Activity 1 Gender-based Cyber Offences: <ul style="list-style-type: none"> • Cyberstalking • Practical Investigation of cyber devices use in Cyberstalking 	

10:45 - 11:00	BREAK	
11:00 - 13:15	Gender-based Cyber Offences: <ul style="list-style-type: none"> • Revenge Pornography / Harmful disclosure of an intimate image • Sexting • Sextortion • Online Exploitation: Catfishing • Cyberbullying • Grooming 	
13:15 - 14:00	LUNCH	
14:00 - 14:50	Train the Trainers Part I – Development of Training Programmes and Adult Learning Principles	
14:50 - 15:00	Wrap up, homework assignment and overview of Day 2	
DAY 3		
BRIEF OVERVIEW OF LOCAL LEGISLATION INVOLVING CYBERVIOLENCE IDENTIFYING, SEIZING AND HANDLING OF ELECTRONIC EVIDENCE		
08:30 - 08:40	Welcome and Recap (10 mins)	
08:40 - 09:40	Digital evidence in Cyberviolence Against Women and Girls	
09:40 - 10:45	<ul style="list-style-type: none"> • The Computer Misuse and Cybercrime Act 22 of 2003 • The Cybersecurity and Cybercrime Act 2021 was enacted on 19 November 2021 <ul style="list-style-type: none"> ◦ A brief overview of relevant offences • Important cybercrime-related concepts 	
10:45 - 11:00	BREAK	
11:00 - 13:15	<ul style="list-style-type: none"> • Important cybercrime-related concepts (continues) • Identifying, seizing and handling Electronic Evidence <ul style="list-style-type: none"> ◦ Chain of custody ◦ Standard Operating Procedures (SOPs) ◦ International Cooperation 	
13:15 - 14:00	LUNCH	
14:00 - 14:50	Train the Trainers Part II – Training Tools and Tips	
14:50 - 15:00	Wrap up, homework assignment and overview of Day 3	

DAY 4		
PRESENTING ELECTRONIC EVIDENCE IN COURT OBTAINING A WITNESS STATEMENT		
08:30 - 08:40	Welcome and Recap (10 mins)	
08:40 - 10:45	<ul style="list-style-type: none"> Types of Electronic Evidence Admissibility and proof of Electronic Evidence in Court Other types of relevant evidence (e.g. circumstantial evidence) that can be used to prove the offence Presenting the Evidence in Court 	
10:45 - 11:00	BREAK	
11:00 - 13:15	Victim Impact Reports and Secondary Victimisation Interviewing Survivors <ul style="list-style-type: none"> Video of Trauma on the Brain Aggravating Factors with regards to Sentencing 	
13:15 - 14:00	LUNCH	
14:00 - 14:50	Train the Trainers Part III – Using Training Tools	
14:50 - 15:00	Wrap up, homework assignment and overview of Day 4	
DAY 5		
MULTI-DISCIPLINARY APPROACH TO COMBATING GBVF SADC PROTOCOL ON MLA AND EXTRADITION TRAIN THE TRAINER LESSON PLANS		
08:30 - 08:40	Welcome and Recap (10 mins)	
08:40 - 9:30	Multi-disciplinary Approach to Combating GBVF	
09:30 - 10:45	Policing Capabilities	
10:45 - 11:00	BREAK	
11:00 - 11:45	The Forensic Process	
11:45 - 12:30	SADC Protocol on Mutual Legal Assistance (MLA) in Criminal Matters and the SADC Protocol on Extradition	
12:30 - 13:15	LUNCH	
13:15 - 14:15	Train the Trainers Part IV – Presentation of Lesson Plans	
14:15 - 14:30	The Way Forward	
14:30 - 15:00	Post-test Conclusory Remarks and Dismissal	

ANNEXURE 5

CHECKLIST FOR GENDER-BASED CYBERCRIMES

Station _____

CAS No./CASE No./Inquiry No. _____

PRE-ARREST CHECKLIST FOR GENDER BASED CYBERCRIMES			
Suspect Name	Suspect ID No./DOB/ Passport No.	Suspect Address	Suspect Phone Number
Victim Name(s)	Victim DOB(s)	Victim Address(es)	Victim Phone Number(s)
Primary Investigator		Forensic Analyst	Prosecutor
Preliminary Information		Interviews	
<input type="checkbox"/> Google suspect if/when identified <ul style="list-style-type: none"> Identify social media, etc 	<input type="checkbox"/> Victim/Survivor <ul style="list-style-type: none"> mechanisms of victimization Impact safety 	EVIDENCE COLLECTION Photographs: <input type="checkbox"/> Suspect Profile/victims/witnesses <input type="checkbox"/> Residence <input type="checkbox"/> Devices: <ul style="list-style-type: none"> Before During After <input type="checkbox"/> Other _____	
ITC Check	<input type="checkbox"/> Witnesses <input type="checkbox"/> Associates	Items to Collect: <input type="checkbox"/> Cellphones <input type="checkbox"/> Computers/iPads/PDA's <input type="checkbox"/> Gaming consoles <input type="checkbox"/> external storage <ul style="list-style-type: none"> hard drives, thumbdrives, etc. <input type="checkbox"/> Misc. data storage/collection devices <input type="checkbox"/> Credit Cards (Debit/Credit/Prepaid) <input type="checkbox"/> Ledgers/logs/notes <input type="checkbox"/> Passwords <input type="checkbox"/> Trash can(s) <input type="checkbox"/> Identification <input type="checkbox"/> Cameras <input type="checkbox"/> GPS device (vehicle)	
Does Suspect have firearm?	Suspect interview: <input type="checkbox"/> General factual interview <input type="checkbox"/> Possession and control of devices <ul style="list-style-type: none"> when purchased <ul style="list-style-type: none"> proof? Who uses <ul style="list-style-type: none"> different accounts? How used Passwords 		
Identify IP (WHOIS, IPChicken)	COLLABORATIVE PARTNERS <input type="checkbox"/> Call forensic investigator re: evidence collection <input type="checkbox"/> Forensic Social Worker <input type="checkbox"/> SACMEC/ICMEC/NCMEC <input type="checkbox"/> Medical/Mental Health Professionals <input type="checkbox"/> Stakeholders/FPB/DSD/Dept of Home Affairs <input type="checkbox"/> NPA <input type="checkbox"/> Civil Society/NGO		
Preservation Letters	Open Source Tools: <input type="checkbox"/> WHOIS/ IP Chicken <input type="checkbox"/> MX Toolbox <input type="checkbox"/> Reverse Image Search Plugin Windows <input type="checkbox"/> Powershell Cell info: www.porting.co.za/public-website/ Cell phone: <ul style="list-style-type: none"> Passwords Dial *#06# Gmail/geo-tracking 		
Search Warrant(s)/Subpoena(s)	MISCELLANEOUS INFORMATION <input type="checkbox"/> Car registration <input type="checkbox"/> DNA sample from Defendant <input type="checkbox"/> DNA sample from victim (w/ consent) <input type="checkbox"/> DNA collection on scene	Physical Toolkit <input type="checkbox"/> Police ID card <input type="checkbox"/> Camera <input type="checkbox"/> Packaging/Evidence bags/labeling materials (include markers, and large bags for blankets) <input type="checkbox"/> Zip ties for cords <input type="checkbox"/> screwdriver/ other tools <input type="checkbox"/> power sources <input type="checkbox"/> gloves <input type="checkbox"/> Faraday Bag (or other signal blocking method) <input type="checkbox"/> SAPS 138 book	
Cellphone:			
<input type="checkbox"/> Call history <input type="checkbox"/> Call records <input type="checkbox"/> Text messages <input type="checkbox"/> Contact list <input type="checkbox"/> Cell tower <input type="checkbox"/> Internet history			
Social media			
Cell phone			
Residence/storage/garage			
Financial records			
IP records			
IP Address Subpoena			
Internet Advertisement Subpoena			
Email Subpoenas			
Social Media Subpoena			
Cloud Storage Subpoena			
IMEI/MEIN			

MORE INFORMATION ON REVERSE →

ANNEXURE 6

Checklist for Cyberviolence

WORKSHOP ON CYBERVIOLENCE AGAINST WOMEN AND GIRLS

PRE-POST TEST

Participant Full name: _____

Date: _____ Sex (Male/Female): _____

Dear participant, this Pre and Post-training evaluation will provide us with an **overview of the knowledge** you possess before and after the workshop, and whether this workshop has contributed to your knowledge levels or not. Please **answer all questions** honestly. Your responses will be treated **confidentially**.

Please circle the number representing your view using the legend below.

1	2	3	4	5
Very low/Little ☹️☹️	Low/Little ☹️	Neutral 😐	Very/Sufficiently 😊	Very High/Much 😊😊

1. What is your level of knowledge in interviewing victims of online crimes against women and children?

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

2. Rate your level of knowledge of who are the victims and offenders in these cases?

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

3. Rate your level of knowledge in identifying and responding to online crimes against women and children

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

4. Rate your level of knowledge on identifying, collecting, preserving and presenting online evidence in court

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

5. Rate your level of knowledge of relevant legislation that may be used in these cases

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

6. Rate your level of knowledge on international dimensions to online crimes against women and children

BEFORE WORKSHOP							AFTER WORKSHOP						
Very low ☹️	1	2	3	4	5	Very high 😊😊	Very low ☹️	1	2	3	4	5	Very high 😊😊

The end. Thank you for your time 😊😊

ANNEXURE 7 ADMINISTRATIVE TRAINING FORMATS



ATTENDANCE REGISTER

DATE:

PURPOSE OF MEETING:

#	NAME	ORGANISATION	SEX	DISABILITY	EMAIL	MOBILE

Workshop Evaluation Questionnaire: CVAWG

Location : _____

Date: _____

Dear participant, we constantly strive to improve our programme delivery to ensure that it is relevant to *your work* and *your needs*. In this context, we would like to ask you for your constructive feedback on this event.

Your views are of crucial importance for us and will be helpful to 1) assess the programme (e.g. relevance, usefulness, quality), 2) generate information on the event, and 3) determine areas of improvement for further workshops

Please **answer** all questions. Your responses will be **anonymous** and treated **confidentially**.

Please **circle** the number closest to your view using the legend below.

1	2	3	4	5
Very low/Little ☹️☹️	Low/Little ☹️	Neutral 😐	Very/Sufficiently 😊	Very High/Much 😊😊

A. Satisfaction, Relevance and Usefulness

1.	Overall how satisfied were you with the venue?	Very low ☹️	1	2	3	4	5	Very high 😊
2.	Overall how satisfied were you with the event?	Very low ☹️	1	2	3	4	5	Very high 😊
3.	How relevant was this event to your professional activities?	Very low ☹️	1	2	3	4	5	Very high 😊
4.	How likely will you use the skills learned over the next 6 months?	Very low ☹️	1	2	3	4	5	Very high 😊

B. Content

5.	How much prior knowledge (prior to the current workshop) on CVAWG did you have?	Very low ☹️	1	2	3	4	5	Very high 😊
6.	How much new knowledge did you gain through this event?	Very low ☹️	1	2	3	4	5	Very high 😊
7.	How satisfied were you with the overall course content/topics covered ?	Very low ☹️	1	2	3	4	5	Very high 😊
8.	To what extent did the following sessions/days meet your needs (e.g. to improve your expertise on the subject)? You can highlight areas you found particularly useful or disappointing in the free comments section below.							
Session and Topic								
9.	Part 1: Skills Development for Trainers	Very low ☹️	1	2	3	4	5	Very high 😊
10.	Part 2: GBV and CVAWG	Very low ☹️	1	2	3	4	5	Very high 😊
11.	Part 2.5 International and Regional Legal Frameworks and Standards on GBV	Very low ☹️	1	2	3	4	5	Very high 😊
11.	Part 3: Understanding CVAWG	Very low ☹️	1	2	3	4	5	Very high 😊

12.	Part 4: Interviewing survivors	Very low ☹	1	2	3	4	5	Very high ☺
13.	Part 4.2.2: Inter-agency collaboration and coordination of the multi-disciplinary team	Very low ☹	1	2	3	4	5	Very high ☺
14.	Part 4.2.3: Essential Service Package for women and girls subjected to violence	Very low ☹	1	2	3	4	5	Very high ☺
15.	Part 5: Digital investigation proceedings of electronica and digital evidence	Very low ☹	1	2	3	4	5	Very high ☺

C. Material and Organisation

16.	How satisfied were you with the training content (<i>i.e. presentations, etc.</i>)?	Very low ☹	1	2	3	4	5	Very high ☺
17.	How satisfied were you with the course guidance and instructions (<i>i.e. course clarity, pace, explanations, etc.</i>)?	Very low ☹	1	2	3	4	5	Very high ☺
18.	How satisfied were you with the overall organisation and administration of the event?	Very low ☹	1	2	3	4	5	Very high ☺

D. General points

19. What topics were of **special interest** to you? What did you **like most** about the training?

20. Do you have comments on how the course could be **improved**? (*i.e. topics that were missing, irrelevant topics, changes in the methodology, or any other changes you could suggest*)

21. What **additional training/topics** would be relevant to improve your work?

Many thanks! We highly appreciate your feedback!

ANNEXURE 8

RESOURCE AND READING LIST

RESOURCES

1. Amnesty International: Violence against Women Online in 2018. Available online at: <https://www.amnesty.org/en/latest/research/2018/12/rights-today-2018-violence-against-women-online/>
2. Association of Chief Police Officers: ACPO Good Practice Guide for Digital Evidence for Digital Evidence (2011). Available online at: https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.
3. Association of Southeast Asian Nations (ASEAN): Treaty on Mutual Legal Assistance in Criminal Matters – Article 1.2 (2004). Available online at: https://www.jus.uio.no/english/services/library/treaties/04/4-07/asean_mutual_legal_assistance.xml.
4. British Journal of Psychiatry - The impact of stalkers on their victims [Abstract]: Pathé, M. and Mullen, P.E. January 1997, 170(1) 12 – 17. Available online at: <https://pubmed.ncbi.nlm.nih.gov/9068768/>
5. Broadband Commission: Please see in particular the various reports. Available online at: <http://www.broadbandcommission.org/resources/Pages/default.aspx>
6. Center for Innovative Public Health Research: New Report Shows that 4% of U.S. Internet Users Have Been a Victim of “Revenge Porn” (13 December 2016). Available online at: <https://innovativepublichealth.org/press-releases/revenge-porn-report-findings/>
7. Child Welfare Information Gateway. Forensic Interviewing: A Primer for Child Welfare Professionals (2017). Children’s Bureau. U.S Department of Health and Human Services. Available online at: <https://www.childwelfare.gov/pubs/factsheets/forensicinterviewing/>
8. Council of Europe: Cyberviolence against children. Available online at: <https://www.coe.int/en/web/cyberviolence/cyberviolence-against-children>
9. Council of Europe: Istanbul Convention: Action against violence against women and domestic violence (2011). Available online at: <https://www.coe.int/en/web/istanbul-convention/country-monitoring-work>
10. Council of Europe: Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse: Lanzarote Convention (2007). Available online at: <https://www.coe.int/en/web/children/convention>
11. Council of Europe. Electronic Evidence Guide-A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.1. March 2020. Available online at <https://www.forensicfocus.com/forums/general/coe-electronic-evidence-guide/>
12. Council of Europe. Newsroom: CEDAW launches General Recommendation No.35 on general-based violence against women, 2017. Available online at: <https://www.coe.int/en/web/istanbul-convention/-/cedaw-launches-general-recommendation-35-on-gender-based-violence-against-women>
13. Council of Europe: Protecting Women and Girls from Violence in the Digital Age: Adriane van der Wilk (December 2012). Available online at: <https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3>
14. Council of Europe: Types of cyberviolence. Available online at: <https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence>
15. Council of Europe Portal: Cybercrime Programme Office (C-PROC) - CyberSouth Activities: The CoE Standard Operating Procedures for the collection, analysis and presentation of electronic evidence (12 September 2019) Available online at: https://www.coe.int/en/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/the-coe-standard-operating-procedures-for-the-collection-analysis-and-presentation-of-electronic-evidence-have-been-released?inheritRedirect=false

16. Council of Europe. Why is gender-based violence a problem? Available online at: <https://www.coe.int/en/web/gender-matters/why-is-gender-based-violence-a-problem>
17. Cross, C. and Dragiewicz, M. Domestic violence and online romance scams use similar psychological tricks (1 April 2018). Available online at: <https://www.abc.net.au/news/2018-04-05/online-romance-scams/9622066>
18. CSVR Gender-based Violence: A Brief Overview (April 2016 p15). Available online at: <https://www.csvr.org.za/pdf/Gender%20Based%20Violence%20in%20South%20Africa%20-%20A%20Brief%20Review.pdf>
19. Cyberbullying.org.za: Cyberbullying Definition – Safety & Security guide (South African portal for resources and information on Cybercrime. Available online at: <https://cybercrime.org.za/>
20. Cybercrimes Act 19 of 2020, South African Government. Section 13: Definitions. Available online at: <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000>
21. Cybercrime Convention Committee: Mapping study on Cyberviolence. Available online at <https://www.coe.int/en/web/cyberviolence>
22. Daly M. & Wilson M. Evolutionary Social Psychology and Family Homicide. *Science*. Oct 1988, 242(4874), 519 - 524. Available at: <https://www.science.org/doi/abs/10.1126/science.3175672>
23. Department of Justice of Canada: Handbook for Police and Crown Prosecutors on Criminal Harassment (2012, p 22). Available online at: <https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/EN-CHH2.pdf>
24. Douglas, D. 'Doxing: a conceptual analysis', *Ethics and Information Technology*, vol. 18, (2016), pp. 199–210. Available at: <https://www.studocu.com/row/document/mekelle-university/international-criminal-law/doxing-a-conceptual-analysis/10452762>
25. Eckert, S. and Metzger-Riftkin, J. (2020). Doxing. *The International Encyclopedia of Gender, Media, and Communication*. Available online at: <https://doi.org/10.1002/9781119429128.iegmc009>
26. ECPAT, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Available online at <https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf>.
27. European Institute for Gender Equality. EIGE-2021 Gender Equality Index 2021 Report: Health. Available online at: <https://eige.europa.eu/publications/gender-equality-index-2021-report/gender-based-violence>
28. Europe Institute for Gender Equality (europa.eu): Cyber violence against women and girls (2017). Available online at <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.
29. European Parliament, Directorate-General for Internal Policies of the Union, Wilk, A. Cyber violence and hate speech online against women, European Parliament, 2018. Available online at: <https://data.europa.eu/doi/10.2861/738618>
30. European Union Agency for Fundamental Rights (2014). Violence against women: an EU-wide survey – Main results. Luxembourg: Publications Office of the European Union, p. 104. Available online at: <http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>
31. Flynn, A., Powell, A. & Hindes, S. 2022. Technology-facilitated abuse: Interviews with victims and survivors and perpetrators. Available online at: <https://apo.org.au/node/309987>
32. Freed, D., Palmer, J. Minchala, D.E, Levy, K., Ristenpart, T. and Dell, N. 'Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders', *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, (2017), pp. 1–22. Available online at: <https://doi.org/10.1145/3134681>
33. Goldberg, C.A.: Top 5 Myths about Online Abuse. Available online at: <https://www.cagoldberglaw.com/top-5-myths-about-online-abuse/>

34. Halder, D. & Karuppanan, J.: Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India (October 2010). Available online at: <https://www.tandfonline.com/doi/abs/10.1080/15564886.2011.607402>
35. Hasinoff, A. A. Sexting and Privacy Violations: A case study on sympathy and blame. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>
36. Henry, N. Flynn, A. and Powel, A. 'Technology-facilitated domestic and sexual violence: a review', *Violence Against Women*, vol. 26, no. 15–16, (2020), pp. 1828–1854. Available online at <https://doi.org/10.1177/1077801219875821>
37. Hess, A. On the Internet, Men are called Names. Women are Stalked and Sexually Harassed (22 October 2014). Available online at: <https://slate.com/human-interest/2014/10/pew-online-harassment-study-men-are-called-names-women-are-stalked-and-sexually-harassed.html>
38. HIPSSA (Harmonization of ICT Policies in Sub-Saharan Africa): Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law (2013). Available online at: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf>
39. International Association of Prosecutors (IAP): Prosecutorial Guidelines for Cases of Concurrent Jurisdiction (2014) pp 10-16. Available online at: http://www.iap-association.org/IAP/media/IAP-Folder/IAP_Guidelines_Cases_of_Concurrent_Jurisdiction_FINAL.pdf
40. International Association of Women Judges (IAWJ): Naming, Shaming, and Ending Sextortion – A Toolkit (2012). Available online at: https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sexortion/naming_shaming_ending_sexortion.pdf
41. Internet trolling: A definition. Available online at: <https://www.endsleigh.co.uk/blog/post/what-is-internet-trolling/>
42. INTERPOL and ECPAT: Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018. Available online at: <https://www.iicsa.org.uk/key-documents/3720/view/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf>
43. INTERPOL: 'Appropriate Terminology'. Available online at <http://www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology>
44. INTERPOL: Guidelines for Digital Forensics First Responders (March 2021). Available online at: <https://www.interpol.int/content/download/file>
45. Inter Press Service News Agency: Cyber Bullies Target Kenya's Women (30 January 2014). Available online at: <http://www.ipsnews.net/2014/01/cyber-bullies-target-kenyas-women/>
46. Lewandowski L.A., Mcfarlane, J., Campbell, J.C., Gary, F & Barenski, C. 'He killed my mommy!': murder or attempted murder of a child's mother. *Journal of Family Violence*, 2004, 19:211–20. Available online at: <https://link.springer.com/article/10.1023/B:JOFV.0000032631.36582.23>
47. Lornard, T., Martland, T. & White, D. A Legal Examination of Revenge Pornography and Cyber Harassment (2016). *Journal of Digital Forensic Security and Law* Volume 11(3) 79 – 92. Available online at: <https://commons.erau.edu/jdfsl>
48. Marganski, A. Special Issue on Sexting: Sexting in Poland and the United States: A Comparison Study of Personal and Social-Situational Factors. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>
49. MacAllister, J.M. The doxing dilemma: seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, vol. 85, (2017), pp. 2451–2383. Available online at: <https://ir.lawnet.fordham.edu/flr/vol85/iss5/21/>
50. MAUCORS (The Mauritian Cybercrime Online Reporting System). Available online at: <https://maucors.govmu.org/maucors/>

51. McGlynn, C. & Rackley, E. 'Image-Based Sexual Abuse', *Oxford Journal of Legal Studies*, vol. 37, No. 3, (2017), pp. 534–561. Available online at <https://doi.org/10.1093/ojls/gqw033>
52. MISA-Zimbabwe in partnership with Konrad Adenauer Stiftung: *Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights* (2021). Available online at: <https://www.ictworks.org/wp-content/uploads/2021/11/Cybersecurity-Laws-SADC-Region-Human-Rights.pdf>
53. National Center for Missing & Exploited Children: *Trends identified in CyberTipline sextortion reports* (2016). Available online at: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf>
54. Newstrom, J.W. & Scannell, E.E.: *The Big Book of Presentation Games: Wake-Em-Up Tricks, Icebreakers, and Other Fun Stuff* (1997). Available online at: <https://www.amazon.com/Big-Book-Presentation-Games-Icebreakers/dp/0070465010>
55. Ngo, F., Jaishankar, K. Agustina, J.R. Special Issue on Sexting: Current Research Gaps and Legislative Issues. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>
56. O'Connor, K., Drouin, M., Yergens, N. and Newsham, G. Sexting Legislation in the United States and Abroad: A Call for Uniformity. *International Journal of Cyber Criminology (IJCC)*: 2017, July to December, Volume 11, Issue 2. Available online at: <https://www.cybercrimejournal.com/IJCC-July-December-2017-Vol11-No2.php>
57. Office of the Council of Europe (C-PROC): *Cybercrime Programme. Standard Operating Procedures for the collection, analysis and presentation of electronic evidence - Version 12* (September 2019). Available to Law Enforcement online at [The CoE Standard Operating Procedures for the collection, analysis and presentation of electronic evidence have been released - Action against Cybercrime](https://www.coe.int/en/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/the-coe-standard-operating-procedures-for-the-collection-analysis-and-presentation-of-electronic-evidence-have-been-released?inheritRedirect=false). Available online at: https://www.coe.int/en/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/the-coe-standard-operating-procedures-for-the-collection-analysis-and-presentation-of-electronic-evidence-have-been-released?inheritRedirect=false
58. Office of the Council of Europe. *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges*. Cybercrime Division - Version 12 (March 2020). Available online at: www.coe.int/cybercrime
59. OHCHR: *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective* (2018). Available online at: <https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx>
60. OHCHR: *Rape is a monstrous crime, perpetrators must be held accountable – but death penalty and torture are not the answers - Bachelet* (15 October 2020). Available online at: <https://www.ohchr.org/en/press-releases/2020/10/rape-monstrous-crime-perpetrators-must-be-held-accountable-death-penalty-and-torture>
61. OHCHR: *Women's human rights and gender-related concerns in situations of conflict and stability, 1996-2022*. Available online at: <https://www.ohchr.org/en/women/womens-human-rights-and-gender-related-concerns-situations-conflict-and-instability>
62. Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C. & Deibert, R. (2019). *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. The Citizen Lab. Available online at: <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/>
63. Republic of the Philippines – Philippine Commission on Women: *Beijing Platform for Action*. Available online at: <https://pcw.gov.ph/beijing-platform-for-action>
64. SADC Protocol on Extradition (2002). Available online at: <https://www.sadc.int/document/protocol-extradition-2002-0#:~:text=The%20SADC%20Protocol%20on%20Extradition,in%20the%20requesting%20Member%20State>
65. SADC Protocol on Mutual Legal Assistance in Criminal Matters (2002). Available online at: https://www.sadc.int/sites/default/files/2021-08/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf

66. SADC (Southern Africa Development Community): The NATO Cooperative Cyber Defence Centre of Excellence. Available online at: <https://ccdcoe.org/organisations/sadc/>
67. Sepec, Miha. Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence (2019). *International Journal of Cyber Criminology: Volume 11, Issue 2, July to December*, p418-438. 21p.
68. Social Shepherd: 30 Essential Facebook Statistics You Need to Know in 2022. Available online at: <https://thesocialshepherd.com/blog/facebook-statistics>
69. Spitzberg, B.H. and Hoobler, G. Cyberstalking and the Technologies of Interpersonal Terrorism (2002). *New Media & Society*, 4, 71 – 92. Available online at: <https://doi.org/10.1177/1461444022226271>
70. Statista: The Universe of Data – Number of monetizable daily active Twitter users (MDAU) worldwide from 1st quarter 2017 – 2nd quarter 2022 (2022). Available online at: <https://www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/>
71. Stopbullying.gov - A federal government website managed by the U.S. Department of Health and Human Services: What Is Cyberbullying. Available online at: <https://www.stopbullying.gov/cyberbullying/what-is-it>
72. The New Yorker: The Story of Amanda Todd by Michelle Dean, 18 October 2012. Available online at: <https://www.google.com/search>
73. UNICEF: Convention on the rights of the child. Available online at <https://www.unicef.org/child-rights-convention>
74. UNICEF: Cyberbullying-What it is and how to stop it – What teens want to know about cyberbullying. Available online at: <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>
75. United Nations: Essential Services Package for Women and Girls Subject to Violence Core Elements and Quality Guidelines - Partnership by UN Women, UNFPA, WHO, UNDP and UNODC (2015). Available online at: <https://www.unodc.org/documents/justice-and-prison-reform/EN-Modules-AllInOne.pdf>
76. UNFPA-Technology-Facilitated GBV (TFGBV) -Making All Spaces Safe, 2021. Available online at: https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf
77. United Nations Human Rights Council: Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective (2018). Available online at: <https://digitallibrary.un.org/record/1641160?ln=en>
78. United Nations Human Rights - Office of the High Commissioner: General recommendation on the Elimination of Discrimination against Women. Available online at: <https://www.ohchr.org/en/treaty-bodies/cedaw/general-recommendations>
79. UNHRC: What is Sexual Exploitation, Abuse and Harassment? Available online at: <https://www.unhcr.org/what-is-sexual-exploitation-abuse-and-harassment.html>
80. United Nations Human Rights - Office of the High Commissioner: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (25 May 2000) – Human Rights Instrument. Available online at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>
81. United Nations: Policy Brief: The Impact of COVID-10 on Women (April 2020). Available online at: <https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/policy-brief-the-impact-of-covid-19-onwomen-en.pdf?la=en&vs=1406>
82. UNODC: Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector (23 January 2013). Available online at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf

83. UNODC: Cybercrime. Available online at: <https://www.unodc.org/unodc/en/cybercrime/index.html>
84. UNODC: Cybercrime. Available online at: <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>
85. UNODC Data Disclosure Framework (DDF) (August 2021). Available online at: [https://sherloc.unodc.org/cld/en/st/evidence/ddf.html#:~:text=The%20Data%20Disclosure%20Framework%20\(DDF,respecting%20the%20right%20to%20privacy](https://sherloc.unodc.org/cld/en/st/evidence/ddf.html#:~:text=The%20Data%20Disclosure%20Framework%20(DDF,respecting%20the%20right%20to%20privacy)
86. UNODC: Facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children, 2014. Available online at: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf
87. UNODC: Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls Women and Girls, 2019. Available online at: https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf
88. UNODC: Strengthening Crime Prevention and Criminal Justice Responses to Violence Against Women, 2014 Available online at: https://evaw-un-inventory.unwomen.org/en/agencies/unodc?pageNumber=2&un_inventory_period
89. UNODC: Treaties Database. Available online at: <https://sherloc.unodc.org/cld/v3/sherloc/treaties/search.html?>
90. UNODC: Database of legislation. Available online at: <https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?>
91. UN Women: Policy Brief No. 17. Covid-19 and Ending violence against Women and Girls (2020). Available online at: <https://www.unwomen.org/en/digital-library/publications/2020/06/policy-brief-covid-19-and-violence-against-women-and-girls-addressing-the-shadow-pandemic>
92. UN Women: Cyberviolence against women and girls: A Worldwide Wake-up Call – A discussion paper from the UN Broadband Commission on digital development working group on broadband and gender (OSCE, 2009). Available online at: <https://en.unesco.org/sites/default/file/genderreport2015final.pdf>
93. UN Women: Facts and figures: Ending violence against women. Available online at: <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures>
94. UN Women: Gender equality: Women's rights in review 25 years after Beijing (2020). Available online at: <https://www.unwomen.org/en/digital-library/publications/2020/03/womens-rights-in-review>
95. UN Women: Online and ICT facilitated violence against women and girls during Covid-19. Available online at: <https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19>
96. UN Women: Press Release: Ahead of International Women's Day, new UN Women report warns that progress towards gender equality is lagging and hard-fought gains are under threat (5 March 2020). Available online at: <https://www.unwomen.org/en/news/stories/2020/3/press-release-ahead-of-international-womens-day-report-warns-that-progress-is-lagging>
97. UN Women: Safe Digital Spaces: Protection of Women and Girls from Technological Violence – A Background Paper (2019). Available at: <http://africa.unwomen.org/en/digital-library/publications>
98. VAW Learning Network (2013). Technology-related Violence Against Women. Available online at: http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html
99. Watson, J & Silkstone, C. Human Trafficking as a Form of Gender-based Violence: Protecting the Victim. Agenda: Empowering Women for Gender Equity. No. 70, Gender-Based Violence Trilogy, Volume 1,2: Trafficking (2006), pp. 110-118. Available online at: <https://www.jstor.org/stable/4066741>
100. West, Jessica: Cyber-Violence Against Women (2014). Available online at: <http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf>

101. WHO Departmental news. Gender-based violence is a public health issue: using a health systems approach, 2021. Available online at: <https://www.who.int/news/item/25-11-2021-gender-based-violence-is-a-public-health-issue-using-a-health-systems-approach>
102. WHO: Global Plan of Action to strengthen the role of the health system within a national multisectoral response to address interpersonal violence, in particular against women and girls, and against children (2016). Available online at: <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>
103. WHO: Understanding and addressing violence against women - femicide (2012). Available online at: https://apps.who.int/iris/bitstream/handle/10665/77421/WHO_RHR_12.38_eng.pdf
104. WHO: Violence against women, 2021. Available at <https://www.who.int/news-room/fact-sheets/detail/violence-against-women>

READING LIST

1. Department of Justice, United States of America: Model Treaty on Mutual Assistance in Criminal Matters (Adopted by General Assembly resolution 45/117, subsequently amended by General Assembly resolution 53/112 – 14 December 1990 and 9 December 1998). Available online at: https://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf
2. Netherlands Institute for the Study of Crime and Law Enforcement (Leukfeldt, Rutger -editor): Research Agenda The Human Factor in Cybercrime and Cybersecurity (2017). Available online at: https://www.researchgate.net/publication/317191029_Research_agenda_The_human_factor_in_cybercrime_and_cybersecurity
3. Malanga, D.F.: Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic (2020). Available online at: <https://www.apc.org/es/node/36765>
4. Meta Public Policy Department for Southern Africa: Understanding Online Gender-based Violence in Southern Africa: An eight-country analysis of the prevalence of digitally enabled gender-based violence (2022). Available online at: <https://genderlinks.org.za/wp-content/uploads/2022/05/Understanding-Online-GBV-in-Southern-Africa-FINAL.pdf>
5. Thailand Institute of Justice: Towards Gender-Responsive Criminal Justice from Good practices Southeast Asia in responding to violence against women (2018). Available online at: <https://icclr.org/publications/towards-gender-responsive-criminal-justice-good-practices-from-southeast-asia/>
6. United Nations Office on Drugs and Crime Vienna: Strengthening Crime Prevention and Criminal Justice Responses to Violence against Women (2014). Available online at: https://www.unodc.org/documents/justice-and-prison-reform/Strengthening_Crime_Prevention_and_Criminal_Justice_Responses_to_Violence_against_Women.pdf



United Nations Office on Drugs & Crime - Southern Africa

1059 Francis Baard Street (Formerly Schoeman Street),
1st Floor, Hatfield, Pretoria, South Africa
P.O. Box 12673, Hatfield 0028, Pretoria, South Africa

Tel: +27 12 432 0820

Fax: +27 12 342 2356

www.unodc.org/southernafrica