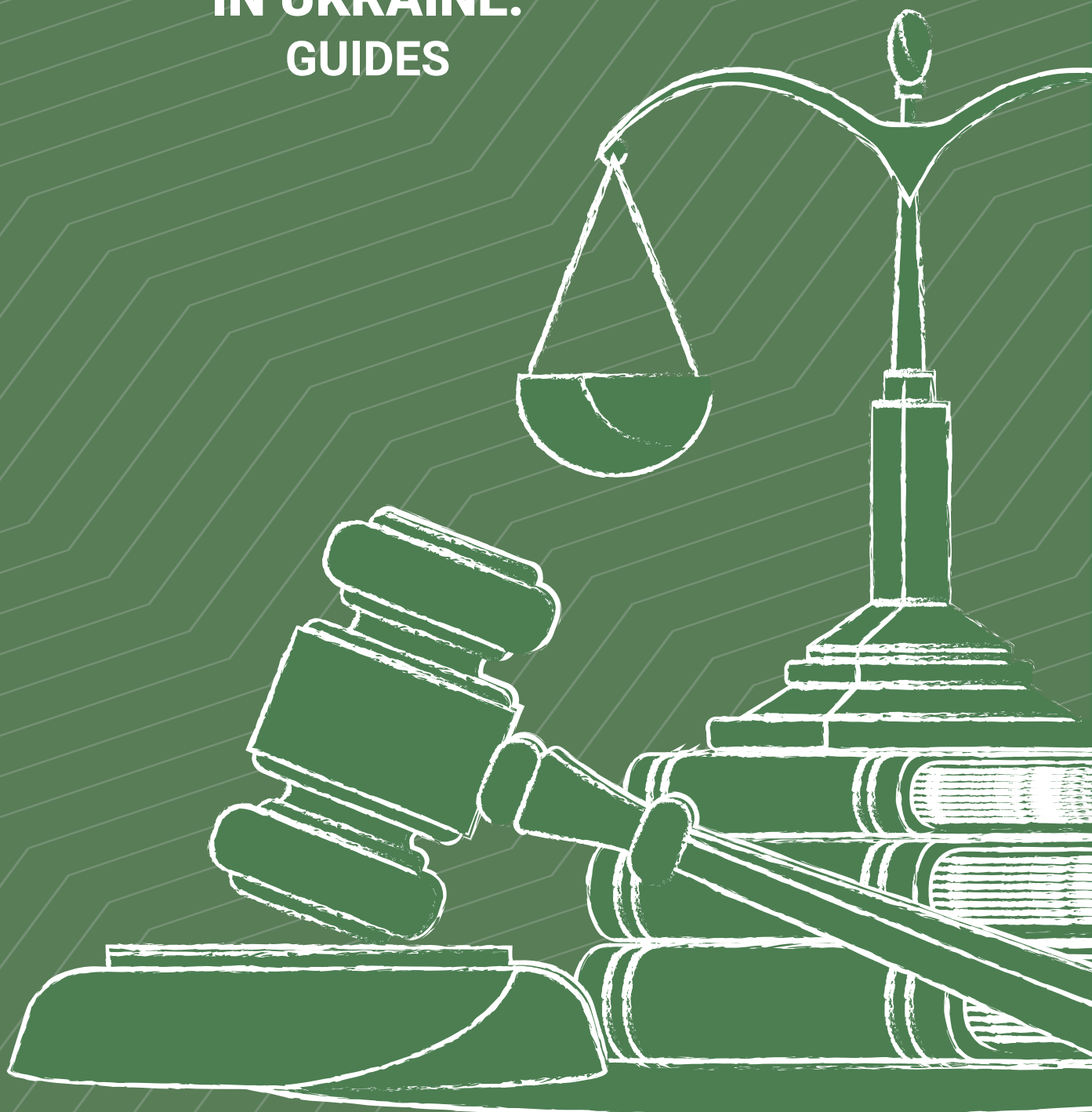


BASIC INVESTIGATIVE STANDARDS FOR DOCUMENTING INTERNATIONAL CRIMES IN UKRAINE: GUIDES



May 2023



Global
Rights
Compliance

These BIS Guides are designed to provide essential information in an easily-accessible format for individuals and organisations in Ukraine engaged in documenting and investigating international crimes. They accompany the [Basic Investigative Standards Manual for Documenting International Crimes in Ukraine](#). Please refer to the Manual for full details and information on sources.

This document is prepared within the MATRA-Ukraine project “Strengthening Ukraine’s Capacity to Investigate and Prosecute International Crimes” funded by the Dutch Ministry of Foreign Affairs. The project is a joint initiative of the T.M.C. Asser Instituut and Global Rights Compliance.

Six Essential Investigative Rules	3
Introduction to IHL, IHRL, ICL	5
Critical Elements of International Crimes	14
Preparing for Documentation	22
Introduction to Evidence	30
Collecting, Handling and Preserving Physical Information	36
Collecting, Handling and Preserving Documentary Information	45
Collecting/Creating, Handling and Preserving Digital or Audio-Visual Information	50
Collecting, Handling and Preserving OSINT/SOCINT Evidence	60
Survivor-Centred Principles for Dealing with Victims and Witnesses	71
Documenting Conflict-Related Sexual Violence Crimes	80



Global
Rights
Compliance

BIS GUIDE: SIX ESSENTIAL INVESTIGATIVE RULES



BIS GUIDE: SIX ESSENTIAL INVESTIGATIVE RULES

Six Essential Investigative Rules

1

DO NO HARM: ensure your documentation activities do no harm to yourself, victims, witnesses, colleagues and local communities.

2

MAINTAIN MINIMUM STANDARDS: ensure your conduct adheres to an explicit set of minimum standards of ethical and professional conduct.

3

IMPARTIALITY AND OBJECTIVITY: your role is not to take sides in the conflict, but to collect objective and reliable information.

4

KNOW YOUR LIMITS: refrain from undertaking tasks outside your competence and seek advice from qualified personnel.

5

OBTAIN INFORMED CONSENT of victims and witnesses prior to any engagement with them.

6

PROTECT CONFIDENTIALITY of information/ evidence and protect witnesses and sources.



Global
Rights
Compliance

BIS GUIDE: INTRODUCTION TO IHL, IHRL, ICL

This Guide provides an overview of international humanitarian law ('IHL'), international human rights law ('IHRL') and international criminal law ('ICL') with a view to explaining which legal regimes are applicable to Ukraine.

International Humanitarian Law (IHL)

IHL is the body of law that seeks to limit the effects of armed conflict for humanitarian purposes. It is only applicable during situations of armed conflict, including occupation.

Classifying Armed Conflicts

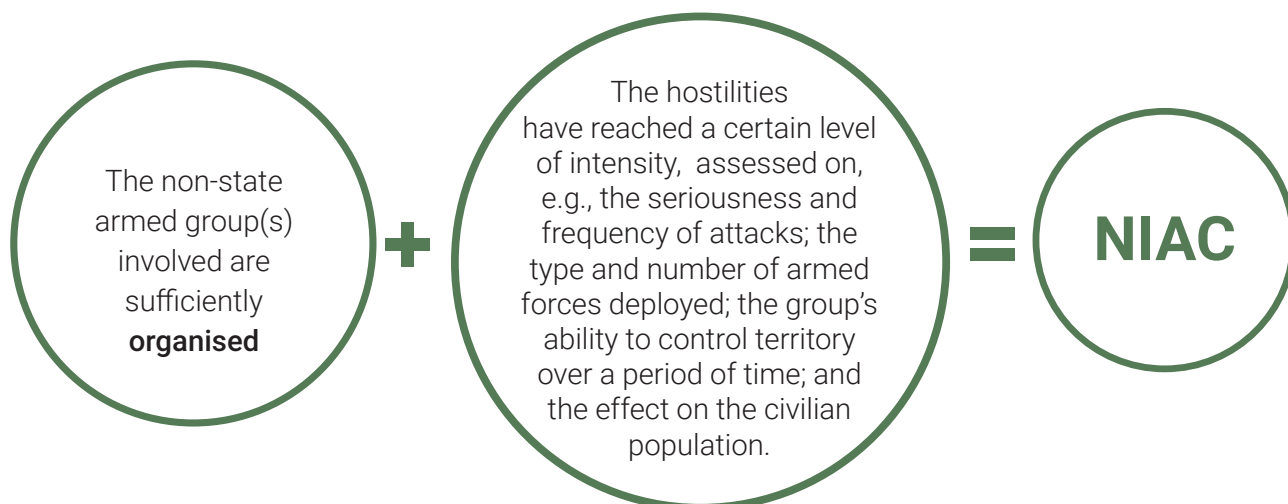
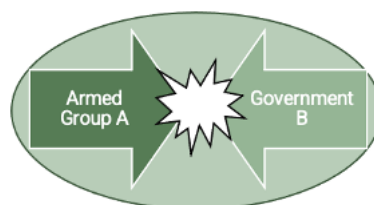
IHL distinguishes between international and non-international armed conflicts. Understanding when an armed conflict exists, and its classification is necessary to determine the applicability of IHL rules.

Non-International Armed Conflict (NIAC)

NIAC refers to “protracted armed violence between governmental authorities and organised armed groups or between such groups within a State” – Common Article 3 to the four Geneva Conventions

Applicable Law:

- Common Article 3 to the Geneva Conventions
- Additional Protocol II
- Customary IHL applicable in NIACs



International Armed Conflict (IAC)

An IAC occurs when one or more States have recourse to armed force against another State, regardless of the reason or the intensity – Common Article 2 to the four Geneva Conventions

Applicable Law

- Geneva Conventions
- Additional Protocol I
- Customary IHL applicable in IACs



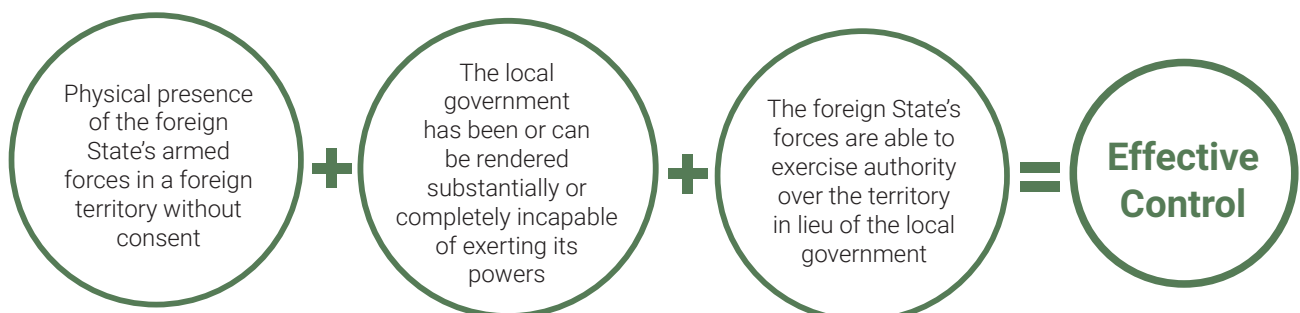
International armed conflict involves the use of armed force against an opposing State. This includes the use of force against the opposing State's armed forces, territory, civilian population/objects or infrastructure, and may involve deployment of troops, use of artillery or resort to jetfighters or combat helicopters on enemy territory.

A NIAC may turn into an IAC if another State intervenes directly or indirectly (through its control over a non-state armed group) in the conflict. In some cases this will establish a parallel IAC alongside the already existing NIAC.

Occupation

Occupation occurs where territory is placed under the 'effective control' of a foreign State's army and extends only to the territory where such control has been established and can be exercised – Common Article 2 to the four Geneva Conventions

The laws applicable in IACs also apply to situations of occupation, while some of the rules contained in these sources are specific to occupation situations.



Occupation by Proxy

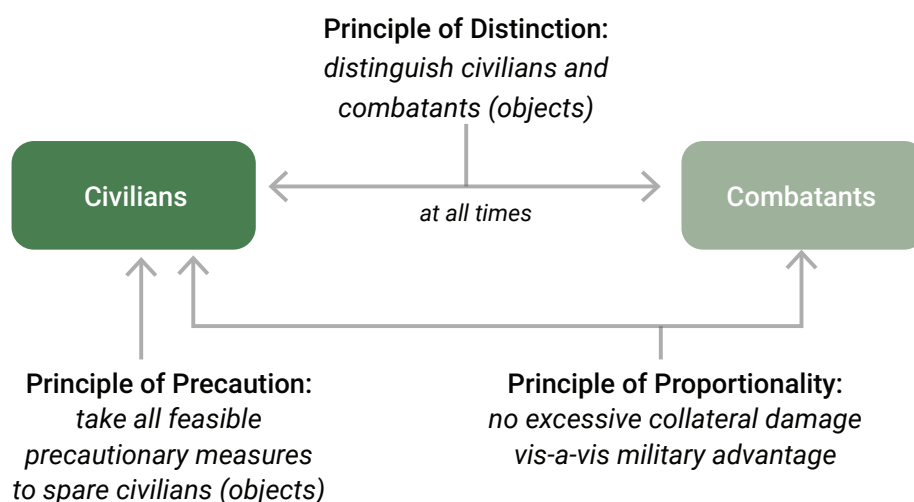
In addition to 'classic' belligerent occupation, a State can also be considered an Occupying Power in situations in which a territory is controlled by non-state armed forces acting on behalf of, and controlled by, that State (i.e., 'occupation by proxy').

Occupation by proxy will be established where the foreign State exercises indirect 'effective control' over the territory in question by virtue of the effective control exercised by proxy armed forces. The foreign State would be considered the Occupying Power, as it exercises 'overall control' over these proxy armed forces.



Foundational Principles of IHL

Regardless of the characteristics of the armed conflict (i.e., NIAC or IAC), the principles of distinction, proportionality, and precaution are foundational to the application of IHL and are the cornerstone of many war crimes.



Combatants vs Civilians

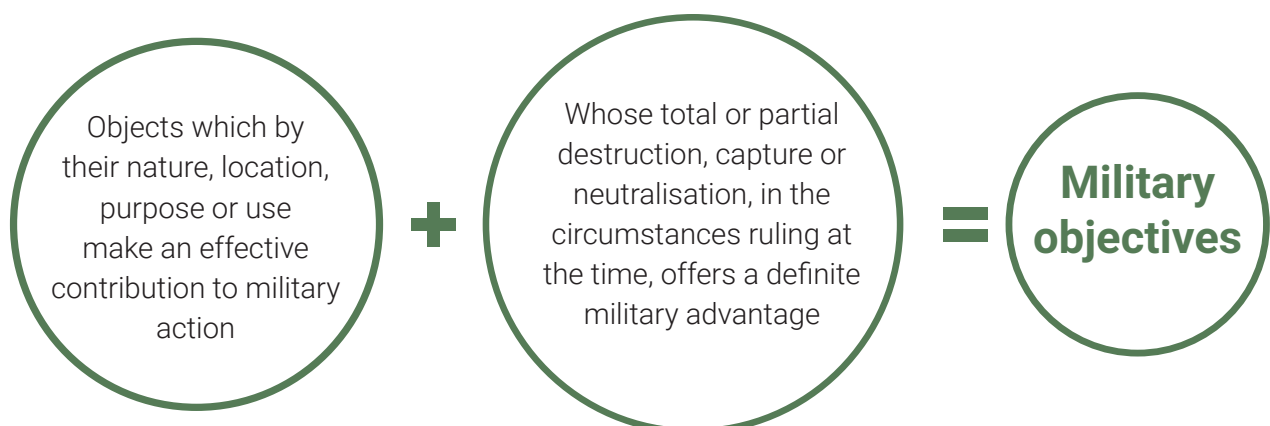
IHL makes a fundamental distinction between combatants and civilians.

IAC	NIAC
Combatants are members of the armed forces of the warring States	Members of the non-state armed groups engaged in hostilities are sometimes referred to as 'fighters'.
A civilian is any individual who is not a member of one of the following groups: 1) the regular armed forces; 2) the armed forces of a party to the conflict as well as militias or volunteer corps forming part of such armed forces; and 3) all organised groups and units, as long as those groups and units are under a command that is responsible for the conduct of its subordinates.	
A civilian directly participating in hostilities temporarily loses their protection under IHL and becomes a lawful target for attack.	

	Combatant	Fighter	Civilians	Civilians Directly Participating in Hostilities
Hostilities	participate		no right to participate but retain their civilian status if they do	
	lawful targets		cannot be deliberately targeted	temporarily lose protection and become a lawful target
Captured	entitled to POW status	entitled to humane treatment	should not have been detained and must be released	can be detained if conditions are met
Prosecution for participation?	immune from prosecution unless they breach IHL	may face prosecution	N/A	may face prosecution

Military Objects vs Civilian Objects

A **civilian object**, shall not be made the object of attack, is defined as an object which is not a military objective. Civilian objects temporarily lose their protection for such time as they are classified as military objectives. **Military objectives** can be legitimately targeted during armed conflict.



International Human Rights Law (IHRL)

IHRL is designed to safeguard the dignity of people and their fundamental freedoms. Human rights are granted to all individuals and are applicable during peacetime and armed conflict.

IHRL Framework

Ukraine has ratified all the below treaties (except ICMW):



In addition to the core IHRL treaties, there are also several important regional human rights treaties (and additional protocols). The [European Convention on Human Rights](#) ('ECHR') is most relevant for Ukraine and its additional protocols, to which Ukraine is a party.

Fundamental Protections under IHRL

Certain fundamental human rights protections are common to international and regional human rights treaties and are also guaranteed under the constitution of Ukraine.

Core Right	International Human Rights Conventions	European Convention on Human Rights	The Constitution of Ukraine
Right to life	Article 6 ICCPR	Article 2 ECHR	Article 27 of the Ukrainian Constitution
Right to freedom from torture	Article 7 ICCPR Article 2 CAT	Article 3 ECHR	Article 28 of the Ukrainian Constitution
Right to equality	Article 26 ICCPR Article 2 ICERD Article 2 CEDAW	Article 14 ECHR	Articles 24 and 26 of the Ukrainian Constitution
Right to liberty and security of person	Article 9 ICCPR	Article 4 ECHR	Article 29 of the Ukrainian Constitution
Right to freedom of expression	Article 19 ICCPR	Article 10 ECHR	Article 34 of the Ukrainian Constitution
Right to a fair trial	Article 14 ICCPR	Article 6 ECHR	Article 55 of the Ukrainian Constitution

When do Obligations Arise Under IHRL?

Application of IHRL During Armed Conflict

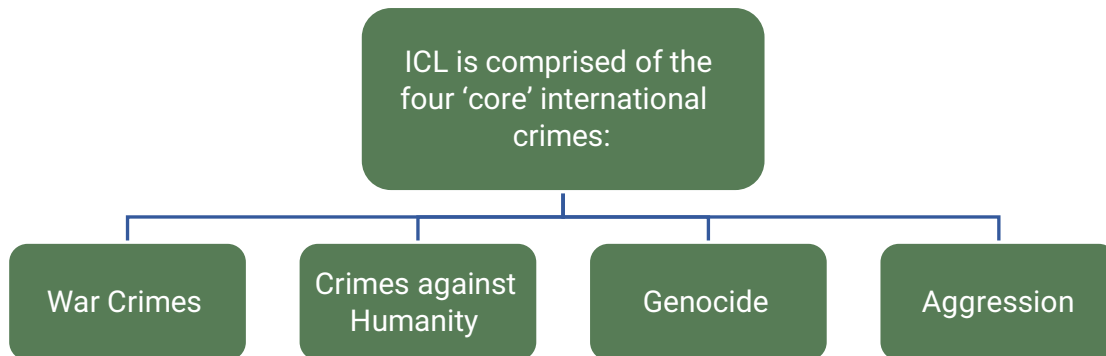
Generally, IHL regulates the obligations of warring parties during armed conflicts, while IHRL regulates the responsibility of States towards persons under their jurisdiction in times of peace. Nonetheless, during situations of armed conflict IHRL **continues to apply**.

IHRL is applicable extraterritorially (i.e., a State may be responsible for violations committed by its agents on the territory of another State). In sum, States will have jurisdiction where they exercise effective 'authority and control' over an individual (e.g., by placing them in detention), or over a territory (i.e., within their own borders and areas where they exercise effective control outside these borders, e.g., as an Occupying Power).

During some serious public emergencies, States may either place **limitations** on, or **derogate** from, certain IHRL obligations.

International Criminal Law (ICL)

ICL is the branch of international law that deals with the prosecution of the four core international crimes.



The **International Criminal Court** ('ICC') is the court that has jurisdiction over the crimes of genocide, crimes against humanity, war crimes and aggression. The ICC is a 'court of last resort'.

Complementarity at the ICC

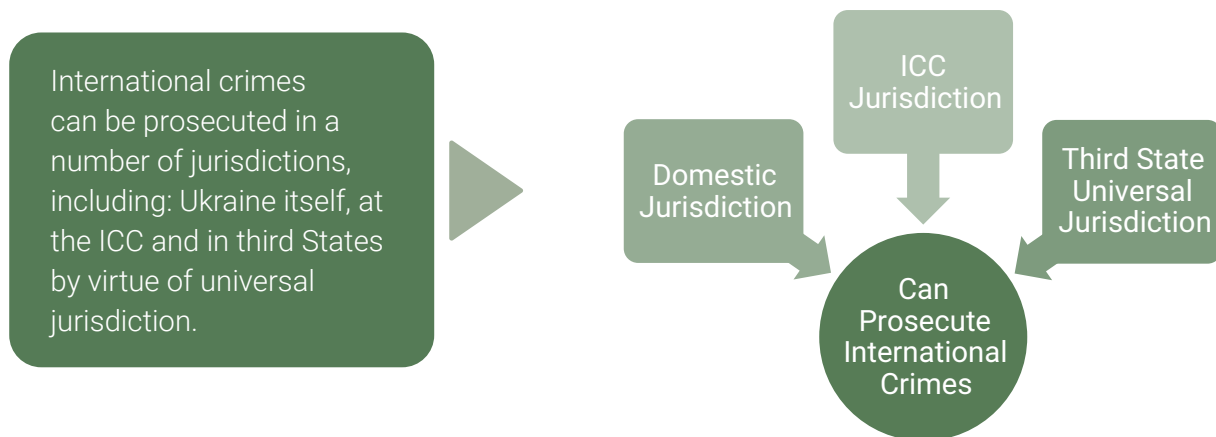
While ICL is generally known for its prosecution of high-level perpetrators within international court and tribunals, international crimes are primarily intended to be prosecuted at the domestic level. At the ICC, this is known as the principle of **complementarity**, according to which the ICC will only exercise jurisdiction where States parties are unwilling or unable to investigate / prosecute international crimes within their jurisdiction.

Ukraine and the ICC

While neither Ukraine nor Russia have signed the Rome Statute, Ukraine has submitted two declarations to the Court granting it jurisdiction over any war crimes, crimes against humanity or the crime of genocide committed on its territory from November 2013.

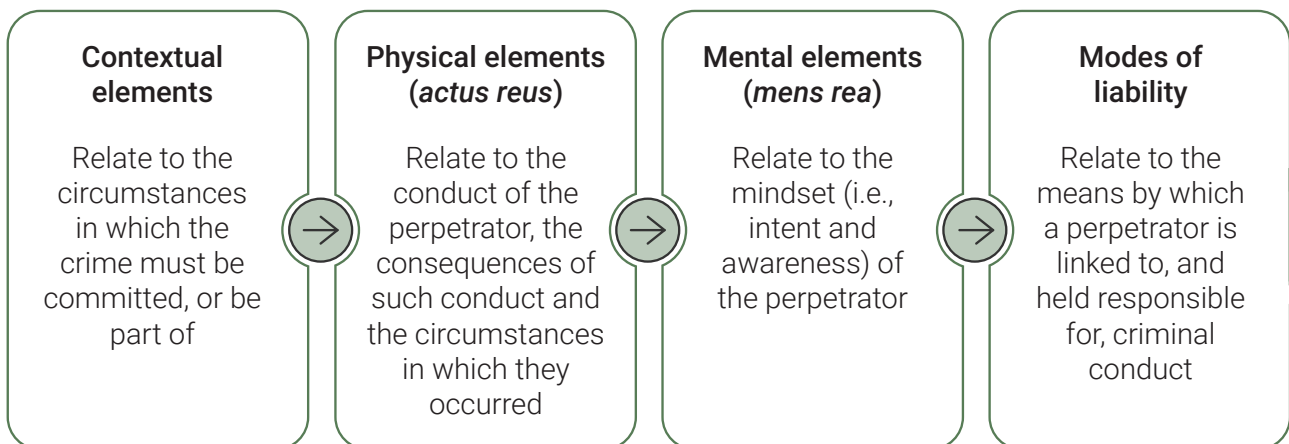
The ICC Prosecutor opened an investigation into the situation in Ukraine on 2 March 2022.

Investigation and Prosecution of Elements of International Crimes



To establish the individual criminal responsibility of a perpetrator for international crimes, the following core, internationally accepted elements of crimes must be established beyond a reasonable doubt:

Elements of International Crimes





Global
Rights
Compliance

BIS GUIDE: CRITICAL ELEMENTS OF INTERNATIONAL CRIMES

This Guide is designed to aid practitioners in the documentation of international crimes by setting out the elements necessary to establish a perpetrator's responsibility for such crimes. Accordingly, this Guide will enable practitioners to understand the elements of crimes under the Criminal Code of Ukraine ('CCU') (including future potential amendments to the CCU through Draft Bill 7290) in light of the international law and practice of the relevant international courts and tribunals, including the International Criminal Court ('ICC').

International crimes are prohibited under Articles 438 (war crimes), 442 (genocide) and 437 (aggression) of the Criminal Code of Ukraine ('CCU'). The CCU, however, does not currently prohibit crimes against humanity. Draft Bill 7290, if and when it enters into force, will introduce amendments to the CCU, including a crimes against humanity provision.

Investigation and Prosecution of the Elements of International Crimes

Regardless of whether they are investigated and prosecuted domestically or internationally, to establish individual criminal responsibility for international crimes, the following core, internationally accepted elements of international crimes must be established beyond a reasonable doubt:

- (i) *the contextual elements of international crimes*: elements that relate to the circumstances in which the crime must be committed, or be part of;
- (ii) *the physical elements (actus reus) of the crime*: elements that relate to the conduct of the perpetrator, the consequences of such conduct and the circumstances in which they occurred;
- (iii) *the mental elements (mens rea) of the crime*: elements that relate to the mindset/intent of a perpetrator in committing a crime; and
- (iv) *modes of liability*: principles that relate to the means by which a perpetrator is linked to, and held responsible for, criminal conduct.

The ICC [Elements of Crimes](#) set out the contextual and physical elements for each crime under the Rome Statute of the ICC.

Documenting the Contextual Elements

When documenting individual criminal acts, practitioners should be aware of the surrounding context that might suggest that crimes against humanity, war crimes and/or genocide may have occurred. These contextual elements are also relevant to international crimes prosecuted domestically (through Articles 438 or 442 of the CCU, or through future amendments made by Draft Bill 7290).

Evidence that establishes the existence of the contextual elements behind these types of crimes will be critical as it is these elements that turn an individual criminal act into an international crime.

Crimes Against Humanity

1. The conduct was committed as part of a widespread or systematic attack directed against a civilian population.

This element can be broken down as follows:

- (i) there was an attack directed against a civilian population;
 - (ii) this attack was widespread or systematic;
 - (iii) the attack was committed pursuant to or in furtherance of a State or organisational policy to commit such an attack; and
 - (iv) the conduct was committed as part of the attack.
2. The perpetrator knew that the conduct was part of or intended the conduct to be part of a widespread or systematic attack against a civilian population.

War Crimes

1. The conduct took place in the context of and was associated with an international or non-international armed conflict.

This element can be broken down as follows:

- (i) International armed conflict – resort to armed force between States.
 - (ii) Non-international armed conflict – *protracted* armed violence between governmental authorities and *organised* armed groups or between such groups within a State.
 - (iii) Nexus – the **conduct must have been closely linked** to the armed conflict taking place in any part of the territories controlled by the parties to the conflict.
2. The perpetrator was aware of the factual circumstances that established the existence of an armed conflict.

Genocide

1. The victim(s) belong to a particular national, ethnic, racial or religious group.
2. The perpetrator(s) intended to destroy, in whole or in part, that national, ethnic, racial or religious group, as such.
3. The conduct took place in the context of a manifest pattern of similar conduct directed against that group or was conduct that could itself effect such destruction.

Documenting the Individual Acts

‘Individual acts’ refers to the physical (or material) elements of the individual international crimes.

Crimes Against Humanity

Crimes against humanity are prohibited by, among other international instruments, Article 7 of the [Rome Statute](#). While the CCU does not currently prohibit crimes against humanity, Draft Bill 7290 will introduce these crimes into the CCU.

The following crimes are prohibited as crimes against humanity:

- **Murder:** occurs when a perpetrator kills or causes the death of another person.
- **Extermination:** involves the intentional infliction of conditions of life (e.g., the deprivation of access to food and medicine) calculated to bring about the destruction of part of a population.
- **Enslavement:** involves the exercise of any or all of the powers attaching to the right of ownership over a person.

- **Deportation and forcible transfer:** occurs when persons are forcibly displaced by expulsion or other coercive acts from the area in which they are lawfully present without grounds permitted under international law.
- **Imprisonment:** occurs when one or more persons are imprisoned or otherwise severely deprived of their physical liberty.
- **Torture:** means the infliction, by act or omission, of severe pain or suffering, whether physical or mental, for the purpose of obtaining information or a confession, or punishing, intimidating or coercing the victim or a third person, or discriminating, on any ground, against the victim or a third person.
- **Rape:** occurs when there is an invasion of the body of a person (i.e., penetration, however slight, of any part of the body of the victim or of the perpetrator with a sexual organ, or of the anal or genital opening of the victim with any object or any other part of the body), and this invasion is committed by force, by threat of force or coercion, by taking advantage of a coercive environment, or against a person incapable of giving genuine consent.
- **Sexual slavery:** occurs when a perpetrator exercises any or all of the powers attaching to the right of ownership over one or more persons, or by imposing on them a similar deprivation of liberty, and causes that person or persons to engage in one or more acts of a sexual nature.
- **Enforced prostitution:** occurs when a perpetrator causes one or more persons to engage in one or more acts of a sexual nature by force, by threat of force or coercion, or by taking advantage of a coercive environment or such person's or persons' incapacity to give genuine consent, and the perpetrator or another person obtained or expected to obtain pecuniary or other advantage in exchange for or in connection with the acts of a sexual nature.
- **Forced pregnancy:** means the unlawful confinement of a woman forcibly made pregnant, with the intent of affecting the ethnic composition of any population or carrying out other grave violations of international law.
- **Sexual violence:** occurs when a perpetrator commits an act of a sexual nature against one or more persons or causes such person or persons to engage in an act of a sexual nature by force, by threat of force or coercion, or by taking advantage of a coercive environment or such person's or persons' incapacity to give genuine consent.
- **Persecution:** means the intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity on political, racial, national, ethnic, cultural, religious, gender or other grounds that are universally recognised as impermissible under international law.
- **Enforced disappearance:** means the arrest, detention or abduction of persons by, or with the authorisation, support or acquiescence of, a State or a political organisation, followed by a refusal to acknowledge that deprivation of freedom or to give information on the fate or whereabouts of those persons, with the intention of removing them from the protection of the law for a prolonged period of time.
- **Other inhumane acts:** occurs when a perpetrator inflicts great suffering, or serious injury to body or to mental or physical health, by means of an inhumane act.

War Crimes

The CCU's war crimes provision, set out under Article 438, prohibits:

Cruel treatment of prisoners of war or civilians, deportation of civilian population to engage them in forced labour, pillage of national treasures on occupied territories, use of methods of the warfare prohibited by international instruments, or any other violations of rules of the warfare stipulated by international treaties, ratified by the Verkhovna Rada of Ukraine [...].

The reference to the “use of means of warfare prohibited by international law” and “other violations of the laws or customs of war envisaged by international agreements” does not specify which conduct is prohibited by Article 438. However, the reference in these phrases to “international law” and “international agreements” refers to the IHL treaties to which Ukraine is a party (e.g., the four [Geneva Conventions of 1949](#) and [Additional Protocol I to the Geneva Conventions of 1977](#)), and thus, the war crimes stipulated within each treaty. Accordingly, the international instruments that interpret these IHL treaties, such as the [Rome Statute](#) of the ICC and the jurisprudence of the ICC and other international courts and tribunals, can be relied upon when assessing the exact scope of Article 438.

The following list provides a representative example of some of the major war crimes:

- **Wilful killing:** occurs when a perpetrator kills (or causes the death of) one or more persons.
- **Extensive destruction and appropriation of property:** occurs when a perpetrator destroys or appropriates protected property in a manner that is extensive, wanton and not justified by military necessity.
- **Denying a fair trial:** occurs when a perpetrator deprives one or more protected persons of a fair and regular trial by denying judicial guarantees as defined, in particular, in the [Third Geneva Convention](#) and the [Fourth Geneva Convention](#).
- **Taking hostages:** occurs when detained persons are threatened with death, injury or the continuation of their detention in order to compel a third party to do or to abstain from doing something as a condition of the release of that person.
- **Attacking civilians:** occurs when the civilian population or civilians not taking direct part in hostilities are intentionally targeted during attacks.
- **Attacking civilian objects:** occurs when civilian objects (i.e., objects which are not military objectives) are intentionally targeted during attacks.
- **Excessive incidental death, injury or damage:** means the intentional launching of an attack in the knowledge that such an attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.
- **Compelling participation in military operations:** occurs when a perpetrator compels the nationals of a hostile party to take part in the operations of war directed against their own country, even if they were in the belligerent's service before the commencement of the war.
- **Outrages upon personal dignity:** occurs when a perpetrator humiliates, degrades or otherwise violates the dignity of one or more persons, and the severity of the humiliation, degradation or other violation is of such degree as to be generally recognised as an outrage upon personal dignity.

- **Rape, sexual slavery, enforced prostitution, forced pregnancy and sexual violence:** the definitions of these war crimes are the same as the crimes against humanity of rape, sexual slavery, enforced prostitution, forced pregnancy and sexual violence.
- **Using protected persons as shields:** occurs when the presence of a civilian or other protected person is used to render certain points, areas or military forces immune from military operations.
- **Starvation:** occurs when starvation of civilians is intentionally used as a method of warfare in an international armed conflict by depriving them of objects indispensable to their survival (e.g., crops, drinking water installations, and medical supplies).

Genocide

Genocide is prohibited by Article 442 of the CCU and by, among other international instruments, the [Genocide Convention](#) and Article 6 of the [Rome Statute](#).

The following crimes are prohibited as acts of genocide:

- **Killing:** occurs when a perpetrator kills one or more persons who belong to a national, ethnic, racial or religious group with the intent to destroy such group.
- **Causing serious bodily or mental harm:** occurs when a perpetrator causes serious bodily or mental harm (e.g., through acts of torture, rape, sexual violence or inhuman or degrading treatment) to one or more persons who belong to a national, ethnic, racial or religious group with the intent to destroy such group.
- **Inflicting conditions of life calculated to bring about physical destruction:** occurs when a perpetrator deliberately inflicts conditions of life (e.g., deprivation of food/water, systematic expulsion, or denial of medical services) calculated to bring about the physical destruction of a national, ethnic, racial or religious group.
- **Imposing measures intended to prevent births:** occurs when a perpetrator imposes measures intended to prevent births (e.g., forced sterilisation, sexual mutilation, or measures that cause severe mental trauma which has the effect of preventing procreation) on a national, ethnic, racial or religious group with the intent to destroy such group.
- **Forcibly transferring children:** occurs when a perpetrator forcibly transfers children belonging to a national, ethnic, racial or religious group to another group with the intent to destroy such group.

Aggression

The crime of aggression is prohibited by Article 437 of the CCU and Article 8bis of the [Rome Statute](#). The Rome Statute and the accompanying [ICC Elements of Crimes](#) provide useful guidance on the definition, interpretation and application of the crime of aggression. The elements of the crime of aggression are defined as follows:

1. The perpetrator planned, prepared, initiated or executed an act of aggression;
2. The perpetrator was a person in a position effectively to exercise control over or to direct the political or military action of the State which committed the act of aggression;
3. The act of aggression (i.e., the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations) was committed;
4. The perpetrator was aware of the factual circumstances that established that such a use of armed force was inconsistent with the Charter of the United Nations;
5. The act of aggression, by its character, gravity and scale, constituted a manifest violation of the Charter of the United Nations; and
6. The perpetrator was aware of the factual circumstances that established such a manifest violation of the Charter of the United Nations.

Documenting the Mental Elements

To hold an accused responsible for an international crime, it must be established, beyond a reasonable doubt, that they possessed the requisite mental elements (also known as *mens rea*) of the specific crime at the time of its commission. The mental elements describe the state of mind of the individual who perpetrated the acts that constitute the 'material elements' of the crime.

Mental Elements under the CCU

Under the CCU, *mens rea* is referred to as 'guilt' and can take two forms: intent (Article 24) and recklessness (Article 25). However, Ukrainian legislation does not recognise the applicability of recklessness for any international crimes.

Article 24 provides for two categories of intent:

- **Direct intent:** "where a person was conscious of the socially injurious nature of his/her act (action or omission), anticipated its socially injurious consequences, and wished them"; and
- **Indirect intent:** "where a person was conscious of the socially injurious nature of his/her act (action or omission), foresaw its socially injurious consequences, and anticipated, though did not wish them".

Intent under the CCU is comprised of two elements:

- The **intellectual element:** the perpetrator's knowledge of the socially injurious nature of the act or consequence; and
- The **volitional element:** whether the perpetrator 'wished' the socially injurious nature of the act and consequence.

Mental Elements under the Rome Statute

Article 30 of the [Rome Statute](#) provides that the default mental elements (intent and knowledge) must be established in relation to each material element of the specific crime, unless otherwise specified in the Rome Statute or the [ICC Elements of Crimes](#).

Article 30:

1. Unless otherwise provided, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court only if the material elements are committed with intent and knowledge.
2. For the purposes of this article, a person has intent where:
 - a. In relation to conduct, that person means to engage in the conduct;
 - b. In relation to a consequence, that person means to cause that consequence or is aware that it will occur in the ordinary course of events.
3. For the purposes of this article, 'knowledge' means awareness that a circumstance exists or a consequence will occur in the ordinary course of events. 'Know' and 'knowingly' shall be construed accordingly.

The Rome Statute's intent and knowledge requirement follows a similar logic to the CCU:

- The 'intent' requirement under Article 30 of the Rome Statute is similar to the 'volitional element' of guilt under the CCU, and certain elements of the 'intellectual element' of guilt are similar to the awareness requirement.
- The 'knowledge' requirement under Article 30 of the Rome Statute is similar to the 'intellectual element' of guilt under the CCU.

Documenting the Modes of Liability

To hold an individual responsible for an international crime, it must not only be demonstrated that a crime was committed, but also that the alleged perpetrator acted in a specific way, and those actions contributed to the commission of the crime.

The circumstances in which an individual will be held criminally responsible for committing a crime are governed by the principles known as ‘modes of liability’, which are set out in both domestic and international criminal law.

Mode of Liability Under the CCU	Corresponding Mode Under the Rome Statute	Corresponding Mode Under Customary International Law
Direct commission (or perpetration) (Article 18)	Direct commission (Article 25(3)(a))	Direct commission (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Perpetration through others not criminally liable (Article 27(2))	Indirect perpetration (Article 25(3)(a))	N/A – would be charged under direct commission
Liability for groups of persons, organised groups, and criminal organisations (Article 28 together with Articles 27(3) and 30)	<i>No direct comparison, but such conduct might be covered by:</i> Co-perpetration (Article 25(3)(a)) Indirect perpetration (Article 25(3)(a)) Indirect co-perpetration (Article 25(3)(a)) Other contributions to crimes as a part of a group of persons acting with a common purpose (Article 25(3)(d))	<i>No direct comparison, but such conduct might be covered by:</i> Joint criminal enterprise (JCE) (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Organising (Article 27(3))	<i>No direct comparison, but such conduct might be covered by:</i> Indirect perpetration (Article 25(3)(a)) Indirect co-perpetration (Article 25(3)(a)) Ordering (Article 25(3)(b))	<i>No direct comparison, but such conduct might be covered by:</i> Planning (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1)) Ordering (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Abetting (Article 27(4))	Soliciting or inducing (Article 25(3)(b)) <i>In some circumstances:</i> Aiding and abetting (Article 25(3)(c))	Instigation (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1)) Aiding and abetting (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Acting as an accessory (Article 27(5))	Aiding and abetting (Article 25(3)(c)) Other contributions to crimes as a part of a group of persons acting with a common purpose (Article 25(3)(d))	Aiding and abetting (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Ordering the commission of a war crime (Article 438(1))	Ordering (Article 25(3)(b))	Ordering (ICTY Statute, Article 7(1); ICTR Statute, Article 6(1))
Command responsibility as a mode of liability is not available under the CCU. However, <ul style="list-style-type: none"> Article 426 provides for the criminal offence of failure to act by Ukrainian military commanders; and Article 438 can be interpreted to include the criminal offence of failure to act for all military commanders (Ukrainian or Russian) by virtue of Articles 86 and 87 of Additional Protocol I. 	Command responsibility (Article 28)	Command responsibility (ICTY Statute, Article 7(3); ICTR Statute, Article 6(3))
Incitement to commit genocide (Article 442(2))	Incitement to commit genocide (Article 25(3)(a))	Incitement to commit genocide (ICTY Statute, Article 4(3)(c); ICTR Statute, Article 2(3)(c))



Global
Rights
Compliance

BIS GUIDE: PREPARING FOR DOCUMENTATION

The documentation of international crimes can differ greatly from the documentation of domestic crimes. **Preparation is essential.** This Guide describes the key steps that practitioners must undertake before commencing documentation activities.

Preparing the Documentation Kit and Folder

The Documentation Kit

1. Communications equipment, mobile telephone, satellite telephone, radio (or similar)
2. Laptop computer
3. Digital audio recording device that can be used to record interviews, oral notes of documentation activities or observations at a crime site
4. Digital storage media (thumb drives, memory sticks, etc.)
5. Global Positioning System ('GPS') navigators (and maps)
6. Camera (an Information Photo Board is a handy tool for photographic information: a small chalkboard or a blank piece of paper on which to write key information that will help identify the photo at a later time)
7. Other items that might be useful, such as: measuring tape; notepad; ropes and signs to secure the scene of an incident; computer tool kit for extraction of hard drives and devices; evidence bags in a range of sizes; evidence tape; evidence boxes; rubber gloves; cotton swabs; plastic bags; torch; first aid kit

Folder

Preparing a Documentation Folder

Practitioners should use a **Documentation Folder** to catalogue the information collected during documentation activities.

A Documentation Folder can be created either electronically or in hardcopy but **must include every record of your documentation activities and copies of the information collected.**

Information in the Documentation Folder must be carefully catalogued and clearly numbered.

For **documentation activities** that involve large quantities of information and/or multiple criminal allegations, a more extensive folder or database should be created, with the following:

1. **Case Management File:** containing an 'Activity Log' describing all the activities undertaken, and who they were taken by.
2. **Communications File:** containing a 'Communications Log' recording details of any relevant communication (including written correspondence).
3. **Witness Statement File:** containing copies of witness statements or summaries and a 'Witness Communications Log' (a chronological record of all the contact that the practitioner has had with each witness). Refer to the witness by a code number and keep identifying information separate.
4. **Confidential Witness Information File:** containing sensitive information about the witness that should be kept separate from the main Witness Statement File. Including a 'Witness Code Sheet' and 'Witness Information Sheet'.
5. **Information File:** containing a record of all the physical, photographic/video and documentary information collected, separated into different logs for each type of information (e.g., 'Physical Information Log').
6. **Sketch and Diagram File:** containing the sketches or diagrams created during the documentation process and a 'Sketch and Diagram Log'.

Recording Documentation Details in Documentation Notebooks

It is advisable that practitioners use **two notebooks** (or, where more practical, one notebook clearly divided) to record the details of the documentation process.

1

Notebook 1: To record all **objective** information discovered during the documentation process as well as the practitioner's actions. For each activity taken, include a short description of where you were, who was there, what you observed and when, and what information was unearthed. Try to record matters contemporaneously.

2

Notebook 2: To record any **subjective** analysis, personal reflections or other similar commentary.

Implementing a Storage System

Prior to any documentation activities, consider where and how any information collected will be stored and organised. If you cannot ensure the confidentiality and/or integrity of information, you must not collect it to avoid it being lost, damaged or rendered unusable.

How to Store Information

Practitioners should utilise a combination of manual/physical and digital storage systems.

- A **manual/physical storage** system is needed to store/inventory physical information. Everything in the physical archive should be digitalised to render it searchable, disclosable and protected.
- The **digital archive** will also include any items which originates in digital form.

Practitioners should conduct a risk assessment of all storage options available, and assess which systems are best suited based on physical space and security measures available as well as capacity and resources.

Basic Principles when Handling and Storing information	
All Information	Store information in a safe and secure manner and in a logical order (i.e., chronological).
	Implement a policy outlining who will have control over, and access to, the information.
	Catalogue all items with an established numbering system.
	Store public information separately from confidential information (including information that identifies a victim/witness and their statement).
	Ensure that the confidentiality requirements are followed and that the information is not disclosed.
	Keep a backup of the information collected in a second, secure location.
	Have emergency evacuation plans in place for securing the materials if needed.
	Access the information in a secure environment and avoid travelling with confidential documents or files.
Information Stored Manually	Keep a logbook to record any access to the storage facility. The logbook should contain details like the name of the person, the date, time and purpose of access, and what items were accessed.
	If the information is perishable (e.g., old notebooks), ensure that the storage conditions are appropriate. In particular, keep the evidence away from heat, light, damp and humidity as well as insects, mice or other animals that may damage it.

Basic Principles when Handling and Storing information	
Information Stored Digitally	Assess which technologies are the most appropriate for your purpose.
	Put in place a digital security protocol before collecting and storing information electronically.
	Protect and encrypt all sensitive electronic files using anti-virus software and passwords, and store passwords securely in a separate location. Encryption tools are often freely available on the Internet.
	Automatically record any access to the digital files and have an edit-trail function on the files to track any modifications made. Back up the digital files frequently so that all changes are securely saved.

Organisations like the **Human Rights Information and Documentation Systems** ('HURIDOCs') provide further guidance and useful resources.

How to Maintain a Chain of Custody

The chain of custody of information is an important indicator of authenticity and integrity. It is essentially a paper trail of the information's collection and handling. From the moment of collection to the time the information is used (for e.g., in a court process), there should be proof of secure, continuous possession from each custodian of the information in question.

Practitioners should have established procedures in place to track who maintained custody over all information collected. The chain of custody should not be broken, the information should be secured and all movements must be recorded.

The number of people who handle or otherwise access the information should be limited as far as possible.

A record/log of the information collection procedure should be created and stored in the **Documentation Folder** (see above).

In addition, it is recommended that practitioners undertake the following steps:

- Ensure evidence is **packaged and marked**. This guarantees that:
 - The items are protected from damage, substitution or alteration.
 - Essential information on the contents of the package, its origin, initial condition, etc., is included on the marking.
 - Record all movements of the information in the **logbook**.

A Documentation Plan

Practitioners should create a plan for **every** activity related to the documentation of international crimes. The Documentation Plan should be used as an overall guide for the documentation process.

A good Documentation Plan should be realistic and flexible; its scope, intended outcomes and methodology should be based on the team's capacity; and it should be amended as new information comes to light.

Preliminary Research and Identification of Objectives:

- Local context
- Alleged incidents and perpetrator groups
- Local political/military structures
- Legal, medical and social services available for victims
- Available documentation by other actors

Potential Alleged Offence and Elements:

- Information indicating alleged offences
- Understanding of the elements of potential crimes
- Information on links between alleged crime and (chain of) people responsible
- Avoid premature attempts to identify suspects

Documentation Team, Plan of Activities:

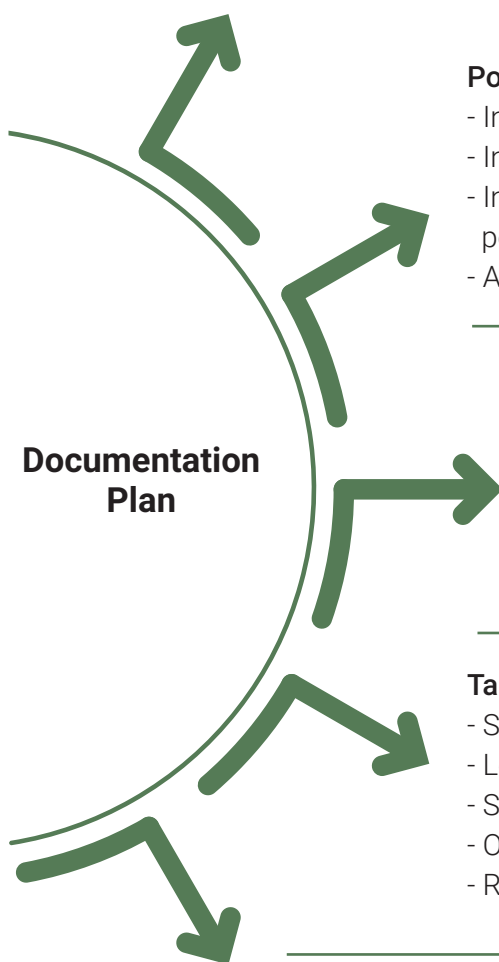
- What sort of information could be collected
- Where it is likely to be found
- Potential locations/witnesses
- Prioritisation and steps to collect evidence
- Assignment of roles within the team (including team lead)

Tasks to be Completed, Resources/Costs:

- Staff required
- Location of offices
- Storage system
- Other resources
- Roles and responsibilities

Review:

- Continual reassessment as new information is received
- Set out specific times for review



Preparing a Risk Assessment and Strategy

As part of the Documentation Plan, undertake a **risk assessment** and create a **risk strategy** to prevent and mitigate harm.

The risk assessment should identify potential risks to all members of the **team, victims and witnesses, and any other source of information**. Risk assessments should be conducted **before** you begin and continue **throughout** your documentation.

Where possible, practitioners should seek the advice of security professionals to ensure that the security procedures meet minimum standards. All risk assessments should comply with the principle of 'Do no harm'.

Assessment of risk is based upon:

The risk assessment should, at a minimum:	
Identify potential risks:	<ol style="list-style-type: none"> 1. The potential security risks where the team is located; 2. The potential or actual effect of gathering information, including on the team itself; 3. The potential risks facing the victim(s)/witness(es).
Assess the threat:	<ol style="list-style-type: none"> 1. Assess the likelihood of the risk becoming a reality 2. Assess the impact of the risk posed <p style="text-align: center;">Risk likelihood + Risk Impact = RISK LEVEL</p>
Integrate and act upon the findings of the risk assessment:	<p>Design and implement an adequate strategy to address the potential risks and integrate them into a Risk Strategy contained in the Documentation Plan (see above).</p> <p>Consider actors and/or institutions that can help mitigate certain risks, including, for example, NGOs or volunteers providing aid to victims and witnesses.</p>
Verify whether the risks have been addressed adequately:	<p>Risk assessments should continue throughout the documentation process, especially at the beginning of each new activity. If additional threats are identified, practitioners should update the Strategy accordingly.</p>
Establish a reporting system:	<p>In case any perceived risks are reported to the team by staff members, witnesses, victims or other stakeholders. Accordingly:</p> <ol style="list-style-type: none"> 1. The risk assessment should seek to obtain the opinion/likely response of local communities and stakeholders prior to, and during, documentation activities; 2. The risk assessment should establish a way of facilitating safe communication with victims, witnesses or other stakeholders to allow concerns to be promptly received.

Examples of Risk and Strategy to Mitigate

Risks to Victims/Witnesses and their Family/Community

- Retaliation, intimidation or threats by alleged perpetrators
- Punishment by members of community
- Re-traumatisation (through reporting crime)
- Rejection by family/community
- Loss of livelihood



Mitigation

- Only interview if absolutely necessary
- Ensure informed consent and confidentiality
- Tailor support based on individual safety and security needs
- Implement a trauma-informed approach
- Refer to social, medical, psychological support services
- Contact individual after interview for emotional support

Risk to Yourself and Your Team

- Environmental risks
- Stress, fatigue and secondary trauma
- Targetting by perpetrator groups/supporters
- Attacks by armed forces/armed groups



Mitigation

- Security planning
- Training on safety and security
- Dedicated resources and equipment
- Travel protocol (postpone travel until safe if possible)
- Know how to reach nearest medical facilities
- Provide access to trauma-trained counsellor
- Adopt a media strategy

Risk to the Information

- Leaking of confidential information (including victim/witness information) theft, alteration, or destruction of evidence
- Corruption or interception of digital information/communications



Mitigation

- Create an information management and security plan for confidential information/communications
- Use an encryption system
- Store information in a secure location
- Careful information sharing



Global
Rights
Compliance

BIS GUIDE: INTRODUCTION TO EVIDENCE

This Guide provides an introduction to information and evidence; the various types and categories of evidence; and the rules governing the admissibility of evidence.

Information and Evidence: The Difference

International crime investigations usually involve a significant body of **information**. CSOs may wish to ensure that collected information can be used as **evidence** during further proceedings, i.e., that it is admissible before a national or international court or tribunal including the International Criminal Court. **Not all information is evidence**. A large part of the information gathered during an investigation may only serve as a lead or merely help with the appreciation of the circumstances.

Information

Any facts, data, or objects that is of investigative value, regardless of its form:

- Testimonial
- Documentary
- Physical
- Electronic
- Audio-visual
- Telecommunications
- Open-Source, etc.

Evidence

Information which meets the standards of legality, relevance and probative value, and is admitted in a criminal trial.

Only evidence can be used to prove or disprove an alleged crime.

Type of Evidentiary Materials

Evidence can come in many forms, which can be broadly divided into testimonial, documentary, physical and, in more recent years, audio-visual digital. This is the type of information practitioners should attempt to collect as each can be relevant for proving the commission of international crimes before domestic and international courts.



Testimonial

- The evidence or statement(s) that a witness gives under oath whether written, oral or through a recorded deposition.
- Examples include information from: victims, a wide range of corroborative witnesses, insider witnesses or the suspect/ accused. Experts can testify orally to discuss and elaborate on the results of their analytical reports in court. Victims can also deliver victim impact statements at sentencing.



Physical

- Objects, including materials detected through scientific means.
- Examples include: remains of weapons or ammunition, uniforms, items collected at a crime scene, etc.



Documentary

- Any piece of evidence that can be introduced at a trial in the form of documents, as distinguished from oral testimony. Documentary information can be gathered from a variety of public and private sources.
- Examples include: laws, regulations, transcripts, medical records, prison records, newspapers, court records, public statements or announcements, diaries, orders, minutes, decrees and official logbooks (e.g., vehicle usage, guard shift changes and visitor logs), reports, among others.



Open-Source

- Information that is publicly available or available through request or purchase.
- While open-source information is “not defined by its specific source”, it can broadly be split into online and documentary information (see below).



Documentary Open-Source

- Documentary evidence accessible through public means, such as in print or online. Useful in establishing the background of a conflict and the extent to which certain information is known.
- Examples include: books, magazines, articles, microfiche materials, reports, public statements, testimonies, press releases, public records, library holdings, newspapers.



Online Open-Source

- Information publicly available on the internet. Verification and authentication can demonstrate the reliability and authenticity of this type of evidence.
- Examples include: online news articles; expert and NGO reports; images/videos posted on social media (Facebook, YouTube, Twitter, Instagram, LinkedIn, etc.).



Digital and Audio-Visual

- **Any privately owned** digital or audio-visual content that would not otherwise be classified as open-source information. Digital evidence may help establish the perpetrator’s intent, whereabouts at the time of a crime, relationship with other suspects, pattern of movement or existence of a common plan.
- Examples include: electronic health records, videos or photographs, etc.



Telecommunication

- Falls under the umbrella of audio-visual and digital evidence and covers a wide range of potential forms of information relating to telecommunications. Can be helpful for corroboration and may provide indications of networks, such as familial ties or chains of command.
- Examples include: communications service providers’ records, such as subscriber records; handset details (including applications and audio-visual files); etc.

Categories of Evidence

The above types of evidentiary materials may fall into the following categories:

Direct

- Directly proves a fact without the need for additional inferences to be made.
- **Example:** The testimony of a witness who saw a missile hitting a school or a soldier shooting an unarmed civilian.

Indirect

- Does not directly prove a fact, but, when corroborated, allows for a reasonable inference to be made that a fact exists. It can be important for establishing a fact in international trials, e.g., where there are no eye-witnesses or related documents.
- **Example:** Witnesses who did not see the exact moment of the attack on the residential district, but were able to identify the consequences, including the character of the damage and injuries.

Hearsay evidence

- Can be in oral or documentary form. First hand (i.e., a witness recounts information provided to them by another person); second hand; or more remote (i.e., information that has passed between two or more persons before being conveyed to the witness appearing in court). It is generally admissible, but its weight will depend on the circumstances.
- **Example:** a witness who testified that she heard from another person who the perpetrator of a crime was.

Exculpatory

- Evidence that may point to the innocence of the accused. Practitioners should make every effort to explore any exculpatory evidence.
- **Example:** video footage that the accused was in a different location when the crime was committed.

Corroborative

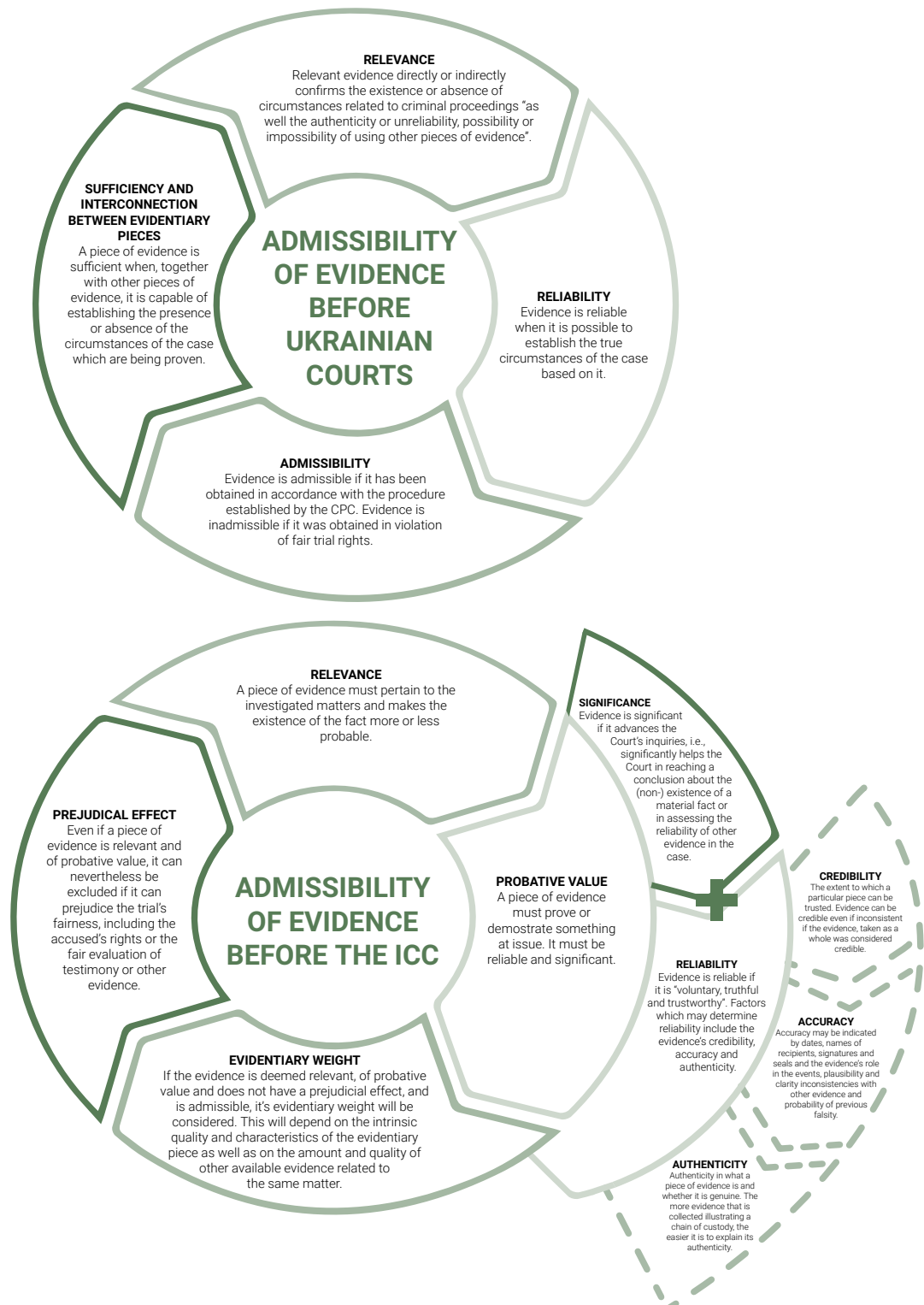
- Evidence from which a reasonable inference can be drawn that confirms and supports other categories of evidence or in some material way connects the relevant person with the offence. It strengthens or confirms what other evidence shows.
- **Example:** bullet casings found at the scene of a crime consistent with a witnesses testimony.

Expert

- Experts are persons with specialised skills and knowledge acquired through training who may be called to assist the court in dealing with issues that are beyond the understanding and experience of the average judge, such as specific issues of a technical nature, or requiring knowledge in a particular field.
- **Example:** military expert who can provide evidence of the command structure and weaponry used by a military organisation.

Overview of the Principal of Admissibility

Information source(s) must meet the characteristics above to be classified as evidence, and that evidence must be admissible. Those collecting evidence of international crimes should be cognisant of the applicable domestic rules on admissibility and the rules in any international court (i.e., the ICC) that also has jurisdiction.

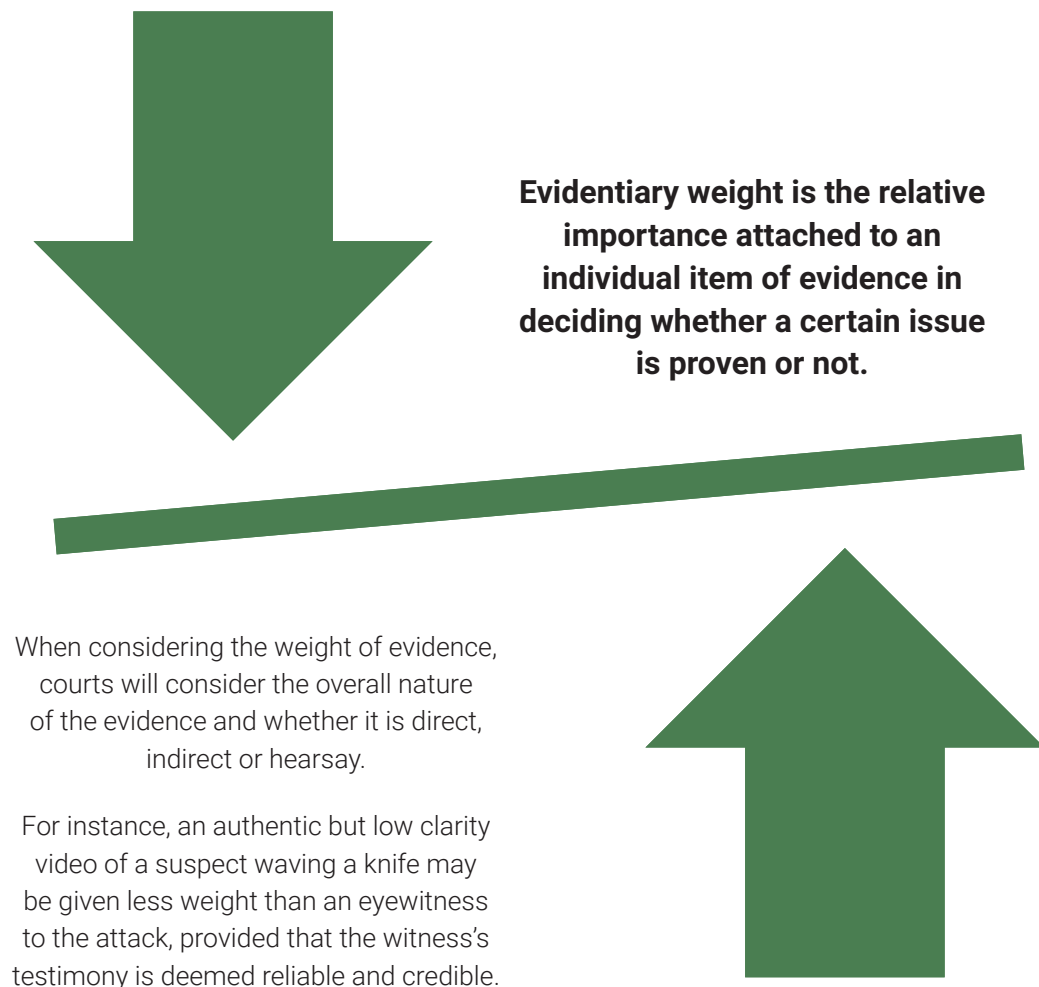


In addition, when determining whether a piece of information is admissible, consider:

Has a violation of an internationally recognised human right taken place to obtain the information?	
No	The information can be admitted provided that other requirements (relevance, probative value, etc. – see above) are met.
Yes	The information is not automatically excluded. Assess whether the violation of the accused's rights was so serious and substantial as to impact the reliability of the information.

Evidentiary Weight

Provided that these admissibility tests are satisfied, the court will also assess the relative importance attached to each item of evidence (i.e., the 'evidentiary weight').





Global
Rights
Compliance

BIS GUIDE: COLLECTING, HANDLING AND PRESERVING PHYSICAL INFORMATION

This Guide outlines the basic principles that should be maintained when practitioners collect or receive physical information.

Physical Information: Definition and Characteristics

Physical information refers to physical objects, including materials detected through scientific means.

Examples include

- weapons or ammunition
- explosive devices
- human remains
- communications equipment
- prints (such as fingerprints, etc.) found at a crime scene

Article 98 of the Ukrainian Criminal Procedure Code describes physical evidence as material objects or documents that:

- 1 Were an instrument for the crime's commission;
- 2 Preserved traces of a crime; or
- 3 Contain other information proving a fact or circumstance relevant to the proceeding, including items that were the crime's object or were acquired as a result of the crime.

Physical information is commonly linked to the 'first' linkage level used to uncover a suspect, i.e., the identification of direct perpetrators and the organisations of which they are members. It is equally helpful for establishing the victims of a crime, such as those exhumed from a mass grave.

Observation and documentation of crime scenes and the collection of physical information may involve risks to health and safety. **Exercise extreme caution when collecting and handling physical information or accessing crime scenes.** It usually requires a high degree of training and expertise.

This document provides advice on:

Observing and
documenting
a crime scene

Receiving
information
from a source

Safely recording,
handling and
storing physical
information

Collecting and Receiving Physical Information from a Crime Scene

The management of a crime scene is a highly technical process that requires the expertise of a professional criminal investigator. An inexperienced practitioner may easily contaminate a crime scene in a variety of ways. Therefore, as a general rule:

- do not attempt to enter, secure, manage, or intervene in, a crime scene; and
- if practicable, contact the appropriate domestic or international authorities within your locale to process the crime scene.

Only observe, document and, if needed, collect information from a crime scene if:

- Professional investigators are not willing or able to access the crime scene;
- Information arising from the crime scene would be lost or damaged; and
- You are confident of your expertise and have carried out appropriate risk assessments to ensure you and others remain safe.

1 PLANNING AND SAFETY

Establish a documentation team, including a team lead. Ensure a plan is created and a security briefing is undertaken.

Make sure the site is safe and free of any dangers.

1. Identify and plan escape routes
2. Identify nearby medical facilities and your ability to access medical care
3. Consider collaboration with local authorities/actors if appropriate
4. Ensure capable personnel have swept the area for landmines, unexploded ordnance, etc.
5. Make initial observations (look, listen, smell)
6. Wear protective clothing
7. Prioritise assisting injured persons found at the scene

DO NOT ENTER IF IT IS UNSAFE.

2 IDENTIFY THE CRIME SCENE

Once safety is established, identify the crime scene.

1. Identify the central point of the crime scene
2. Consider whether there are any possible secondary crime scenes
3. Cordon off an area around the scene that is large enough to contain all relevant physical information

The perimeter must allow for safe interaction with the local population. The contact information of persons should be recorded so interviews can be arranged, if necessary.

3 SECURE THE CRIME SCENE

Ensure trained security personnel are present to secure the crime scene and where possible **consult with local military or police personnel to assist with security.**

1. Accurately record the location of the site
2. Establish a common entry point to the scene
3. Monitor access to the crime scene
4. Keep a log of all those who enter the crime scene
5. If outdoors, promptly photograph and shelter if from the weather

4 OBSERVE THE CRIME SCENE

Produce an accurate and reliable overview of the **original state** of the crime scene. Comprehensively map the crime scene by drone, video, photographs and sketches.

Prepare a detailed birds-eye sketch of the crime scene:

1. The direction of north;
2. The central point of the crime scene;
3. The location(s) where the crime(s) may have occurred;
4. The location of identified information or objects (including human remains);
5. Any landmarks, roads or buildings with a label and description; and
6. Any measurement of pertinent objects and spaces between them.

5 WALK THROUGH & INITIAL DOCUMENTATION

The team lead should conduct a walk through of the crime scene.

The team lead should keep professional, accurate and tidy notes detailing the following:

1. The date/ time of the incident and date/ time the team arrived and left
2. The location and size of the crime scene through GPS coordinates and on a map
3. The type of crimes that may have occurred at the crime scene
4. All additional observations (such as: how the crime scene looks, potentially important information, potential witnesses)

6 MORE FOCUSED DOCUMENTATION

Under the direction of the team lead, team members should document the scene in the following ways:

Photographs: photograph the overall scene, as well as close-ups of notable parts/ objects. Plan the photography route.

Video: Video recordings may be made to supplement the photographs.

Sketches: Sketches should be made of the immediate area of the scene, noting the relative location of items of evidence, and distances to adjacent buildings and landmarks. Sketches are an important way to record the spatial relationships of objects.

General notes: Document the location of the scene, the time of arrival and departure. Initial notes about the incident should answer the who, what, where, why and how questions.

It is likely logical to conduct this step simultaneously with Step Seven (below).

It is vital to maintain a permanent record of all crime scene activities.

7**COMPREHENSIVE COLLECTION OF EVIDENCE**

The lead prosecutor must identify which type of search methodology is most appropriate considering the size and layout of the scene:

- i. Lane or strip search
- ii. Grid search
- iii. Zone search
- iv. Spiral search

Evidence found during the search should be record in a Physical Information Log and collected in line with the standards explained below.

Note the details and photograph all evidence which cannot be collected.

8**COMPLETE THE COLLECTION OF EVIDENCE AND DEBRIEF**

Debriefing must:

1. Determine what evidence was collected
2. Discuss preliminary scene findings with team members
3. Discuss potential technical forensic testing to be performed
4. Initiate any action identified in discussion that may be required to complete the crime scene investigation
5. Brief the person(s) in charge upon completion of an assigned crime scene task

The team lead should then conduct a final survey of the crime scene and final walk-through of the scene. Both must ensure the following:

1. Each area identified as part of the crime scene is visually inspected
2. All evidence collected at the scene is accounted for
3. All equipment and materials generated by the investigation are removed
4. Any dangerous materials or conditions are reported and addressed
5. Photographs are taken depicting the condition of the scene at exit

Collecting and Receiving Physical Information from a Source

Physical information can be provided by various sources, such as a victim, witness or third party, for evidence purposes. In this case, **those receiving the information** should:

- Avoid receiving information in exchange for money;
- Ensure that the source obtained the information without violating internationally recognised human rights;
- Consider the motivation of the creator / source in creating / providing the physical information;
- Record the personal contact details of the source;
- Wear protective clothing when handling the object;
- Avoid altering the original state of the information in any way (e.g., by stapling a document, or washing a piece of clothing);
- Never promise the source that the information or their identity will remain confidential in all circumstances;
- Explain to the source that confidentiality and/or security concerns may be addressed through the implementation of protective measures; and
- Make copies of the original information as soon as practical and store the original appropriately (see below).

Recording, Handling, and Storing Physical Information

All physical information should be properly recorded, handled and stored to ensure its reliability and, consequently, its successful admission as evidence before a court in the future.

Recording Physical Information

Ensure that all documentation activities and other documentation pertaining to the crime scene is recorded in the Documentation Folder (see BIS Guide: Collecting, Handling and Preserving Documentary Information).

The section of the Documentation Folder on physical information should include:

- A Physical Information Log to register the collection of physical information, indicating:
 - The reference number of the object assigned
 - A description of the object
 - When, where and by whom the object was provided and/or collected
 - Any additional comments
- Photographs of the collected information

In addition, if a crime scene has been inspected, include the following:

- The overall description of the crime scene and notes taken by the team members (detailing their activities and evidence)
- Any videos / photographs, maps, or sketches which were created
- Documentation forms regarding the initial securing of the crime scene
- Entry / exit documentation

Handling and Storing Physical Information

PACKAGING



All forms of information must be packaged and sealed for evidence purposes.

As a **general rule**:

The packaging method must ensure that the item cannot be altered or substituted without distorting the integrity of the package, and that it is adequately protected from damage, spoilage, deterioration or loss of its properties.

A piece of evidence can be packaged in a plastic storage bag or paper bag / envelope. Seal the bag / envelope with adhesive tape.

LABELLING & MARKING



All forms of packaged information must be labelled with the following information:

1. The reference number assigned to the object upon collection;
2. The name of the person who originally collected the item, the date and time, and the location it was found;
3. A description of the object (appearance, quantity, size, weight, etc.); and
4. The names of all persons who have had possession of the item, the date, time and location of handlings, and the purpose for which they handled it.

This will help to maintain a **chain of custody**.

STORING



Store the information in a secure, safe place, such as a room or a closet space with a lock, free from environmental factors (extreme heat or cold, water, etc.) and unauthorised access.

Appoint a person to be responsible for the storage area and control who gains access to the physical items.

Institute a logbook to record who enters the room and for what purpose.

Record any handling of the item after storage.

Contact the authorities to pass the item(s) to professional investigators as soon as practicable.

See *below* the basic rules for using either of these storage methods.

Basic Rules for Storing Evidence

When storing evidence, the following basic rules should be maintained:

- Physical evidence must be stored in **a condition preserving its essential features and properties and protecting it from destruction or damage.**
- If the information is perishable, **keep it away from extreme heat or temperature drifts, light and humidity, as well as insects, mice, or other animals that might damage it.**
- **Only a limited number of responsible persons should have access.**
- **Keep a record of the handling, movement and custody of the evidence in a logbook** in a chronological order reflecting who, when, where and how any activity was undertaken related to an evidentiary item in question (chain of custody).

If these minimum requirements cannot be met, practitioners should secure the location in which the information was found and return later when it can be safely collected and properly stored.



Global
Rights
Compliance

BIS GUIDE: COLLECTING, HANDLING AND PRESERVING DOCUMENTARY INFORMATION

This Guide explains documentary information, and the basic principles which must be followed when dealing with documentary information.

Documentary Information: Definition and Characteristics

Documentary information is anything which comes in the form of a document, as distinguished from oral testimony. In this sense, documentary information refers to a broad range of evidentiary sources.

For example:

1

Examples of documentary information include:

Laws, regulations, transcripts, medical records, prison records, newspapers, court record, public statements or announcements, minutes, diaries, orders, decrees, and official logbooks (e.g., vehicle usage, guard shift changes, and visitor logs).

2

Documentary information can be gathered from sources including:

Victims/witnesses, State authorities, NGOs, international organisations, national or international media, including radio broadcasts, private individuals and organisations, newspapers and online sources.

If a piece of documentary information meets the characteristics of physical evidence, it will be classified as such (see BIS Guide: Collecting, Handling and Preserving Physical Information). If the document is in digital form, follow the advice contained in BIS Guide: Collecting/Creating, Handling and Preserving Digital or Audio-Visual Information.

Authenticating Documentary Information

Authenticating documentary information is intrinsically linked to its **reliability** and **probative** value forming part of **admissibility** assessments. A document's authenticity must be established for it to be admitted as evidence before a court.

According to international standards, documentary information can be authenticated for evidentiary purposes if the document concerned is:

Self-authenticating:

such as an official document publicly available from an official source.

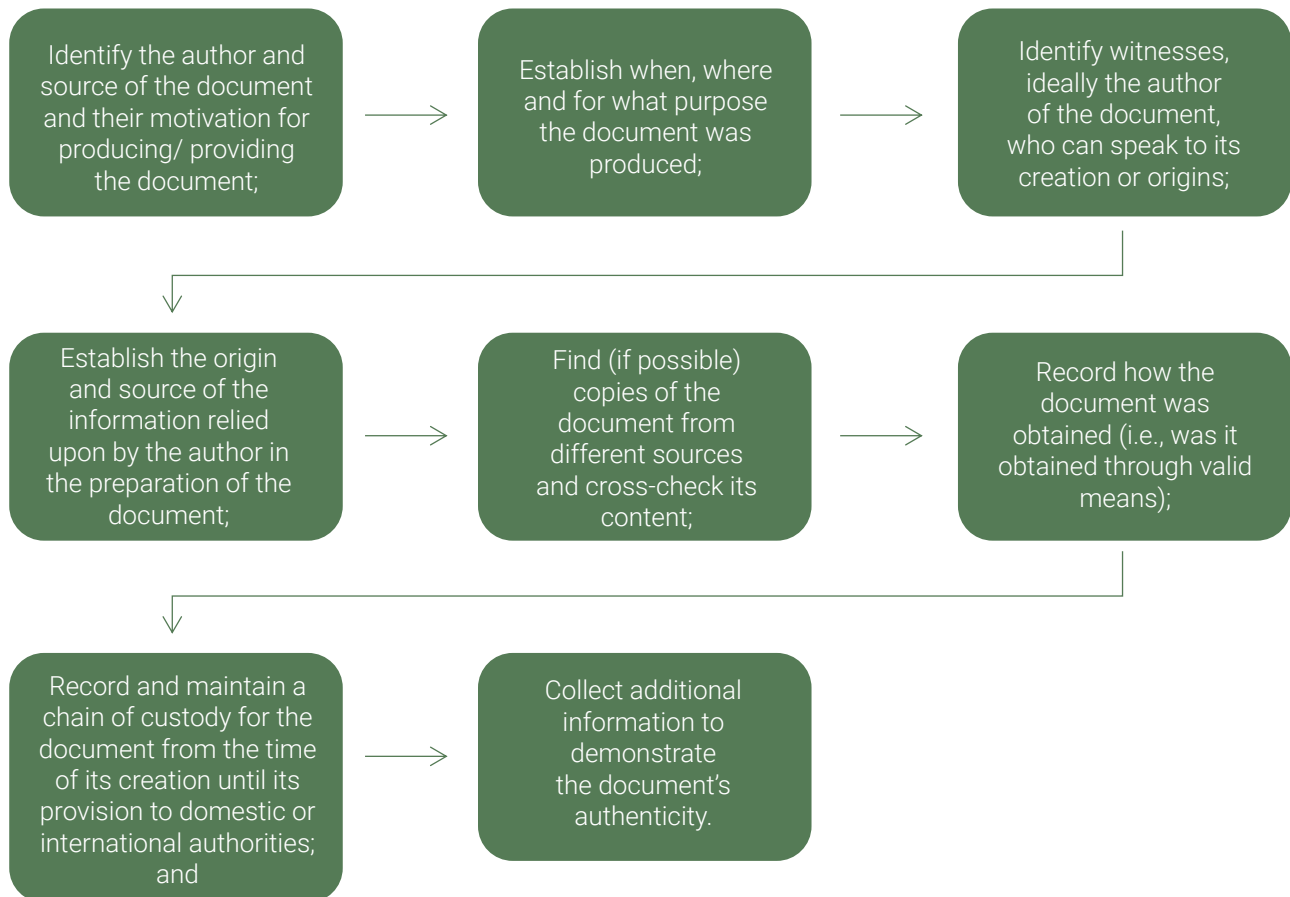
Prima facie reliable:

meaning it bears sufficient indicia of reliability such as a logo, letterhead, signature, date, or stamp and appears to have been produced in the ordinary course of the activities of the person or organisation that created it; or

Lacking sufficient indicia of reliability:

meaning that its authenticity must be established to enable the court to verify that the document is what it purports to be.

If the document is not **self-authenticating** or **prima facie reliable**, you should implement the following steps to assess whether the document is authentic, as soon as possible upon receipt of a document(s):



Authenticating Particular Types of Documentary Information

1. Reports from NGOs, inter-governmental organisations ('IGOs') or third State Governments.



Generally, reports that appear to be well-researched from well-known and respected NGOs, IGOs or governmental bodies will be considered *prima facie* reliable if they provide sufficient guarantees of non-partisanship and impartiality.

Focus on collecting reports issued by impartial, independent, and respected NGOs, IGOs or governmental bodies (such as Human Rights Watch, Amnesty International, the United Nations ('UN'), including the Human Rights Monitoring Mission in Ukraine ('HRMMU') and the Independent International Commission of Inquiry on Ukraine).

Necessary steps to ensure authentication:

- Note when and where the document was obtained.
- Assess whether the document provides information on its sources.
- Consider the methodology to analyse and present the factual claims within the report.

2. Official documents



Official documents refer to any authenticated documents from organisations performing public functions (even if they do not belong to regular State authorities) and may include documents such as pay records, records of employment, orders, police reports, meeting reports, court records, military personnel records, daily military reports, land and property reports or State legislation.

Generally, these types of documents constitute highly probative information before a court.

Necessary steps to ensure authentication:

- Note when, from where and how the document was obtained.
- Check whether the document is authorised and signed by an identified representative or agent of an official body or organisation. If so, the document will be presumed authentic, as long as the authenticity of that signature is not called into question.
- If there is no identified author, check whether the document is self-authenticating.
- In case the document is not self-authenticating, ensure the document is certified by the relevant issuing authority or an identified representative from that authority.

3. Private documents



Private documents are those provided by private individuals or organisations.

Necessary steps to ensure authentication:

- Note when and where the document was obtained.
- Ensure that the document provides proof of authorship or possesses other indicia of reliability proving its authenticity, e.g., a signature, stamp, watermark, date, self-evident meaning or indication of distribution, and whether it is properly structured and formatted.
- If the document does not provide any indicia of reliability, have the author authenticate it or find corroborating information to authenticate it and establish its date (e.g., through another document or witness referring to it).

4. Media articles and reports



Media articles and press reports may provide highly relevant information on the occurrence of crimes, statements made by alleged perpetrators or associated groups, or details on the scope of the victims or affected communities. However, media articles/reports often do not provide detailed information about their sources and, thus, will likely be considered an unreliable opinion. This information is often only admissible when presented in court by an expert.

Necessary steps to ensure authentication:

- Note the date and source of the press article/report and how it was retrieved.
- Note the author of the article/ opinion and how they have come to their conclusions, e.g., the background of the journalist(s) and their sources and other material relied upon in publishing the article/report.

5. Letters, manifestos, political statements, and similar documents.



Letters, manifestos, political statements, and other documents emanating from persons or entities involved in contemporaneous events related to the commission of crimes will likely be considered as opinion information and will therefore often only be admissible when presented in court by an expert. More often than not, these documents will merely contain assertions by people with subjective interests, limiting their probative value. If, however, the documents make factual assertions about relevant military or political events, practitioners should take steps to authenticate.

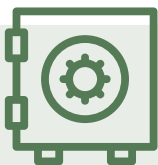
Necessary steps to ensure authentication:

- Note when, from where and how the document was obtained.
- Note the date of the document.
- Find corroborating information (allowing crosschecking) demonstrating that the document contains reliable and objective statements.
- Ask the author for further information concerning how they arrived at the conclusions or opinions contained in the document.

Recording and Storing Documentary Information

The original version of the document needs to be preserved. The process of recording, storing documentary information and maintaining its chain of custody in the Documentation Folder are identical to the rules related to physical information (see BIS Guide: Collecting, Handling and Preserving Physical Information).

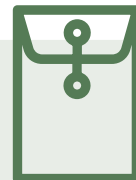
For documents specifically:



The documents must be stored in a condition suitable for their further use in criminal proceedings (if passed on to the relevant authorities), i.e., in a secure, safe place that preserves their essential features and properties and precludes conditions that may lead to their destruction or damage. The storage of documents must be free from environmental factors (e.g., extreme heat or cold, water, etc.) and unauthorised access.



All documents should be labelled with an established numbering system (chronologically). Where relevant, the number of an item should include a link/reference to the connected piece of information. For example, documents referred to in a witness statement should be clearly marked as such.



When the document is stored, it must be kept enclosed between blank sheets of paper in envelopes. Do not make any notes or inscriptions on such documents or bend them. If there is a large number of documents, they are to be compiled into a separate package. The envelope (package) should indicate the list of documents attached to it.



Global
Rights
Compliance

BIS GUIDE: COLLECTING/CREATING, HANDLING AND PRESERVING DIGITAL OR AUDIO-VISUAL INFORMATION

This Guide focuses on digital information stored on, received or transmitted by an electronic device, i.e., how to collect/create, handle and preserve digital or audio-visual information, including photographs and videos, information contained on electronic devices and digital information collected from third parties.

Digital or electronic materials can fall in **two broad categories** depending on their nature:

- 1 Open-source intelligence ('OSINT') and social intelligence ('SOCINT') information:** Open source information on the internet that any member of the public can obtain by request, purchase or observation.
- 2 Other digital information stored on, received or transmitted by an electronic device:** Audio-visual content that would not otherwise be classified as open-source information (e.g., photos or videos of the crime scene created by the practitioner).

For information on collecting OSINT/SOCINT information, see BIS Guide: Collecting, Handling and Preserving OSINT/SOCINT Evidence.

Collecting or Creating Digital Information

Creating Photographic and Video Information



BASIC PRINCIPLES:

Before being admitted as evidence, a court will require proof of the photograph or video's originality, reliability and integrity.

Always provide the date, time and location the video/photograph was created, to establish its relevance.





Taking a Video

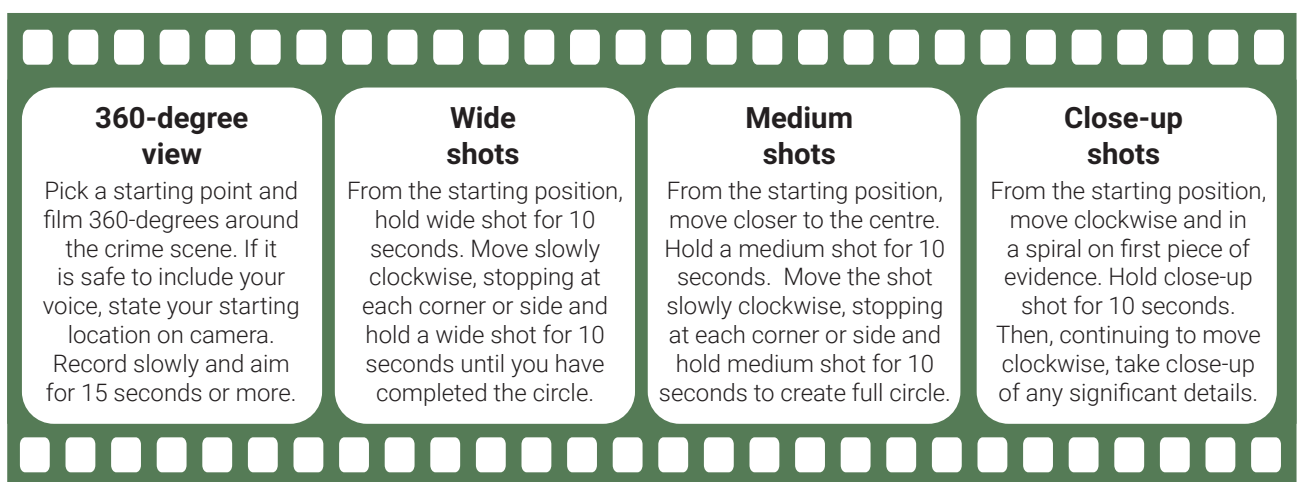
Always ensure that the person taking the footage has experience in doing so.

When taking a video, **take care to:**

- Record time, date, and location.
 - Ensure the location is clearly visible in the video itself and/or activate GPS.
 - Ensure the camera or cell phone is set to the correct date and time.
 - Record your voice saying the date, time and location, write them on a piece of paper and record it for 10 seconds or film anything that shows this information.
- Take the video immediately, i.e., before the crime scene or information is disturbed.
- Prioritise quality over quantity.
- Film strategically and logically to ensure that viewers will understand what happened and where.
- Avoid narration and film silently (apart from voicing the date, time and location if needed).
- Continuously film the same incident or location, i.e., try to not stop and start the video.
- Ensure that the video captures all aspects of the scene, not just what you think is important.
- Hold all your shots for 10+ seconds.
- Move the camera slowly when changing your position or when zooming in or out.
- If you were unable to add basic information to the video recording, create a separate document summarising the key information about the footage.
- Record the contact details of the person who is filming.
- Keep memory card safe from physical damage or confiscation.
- Do not attempt to alter the video. If an alteration is necessary, record the reason why.

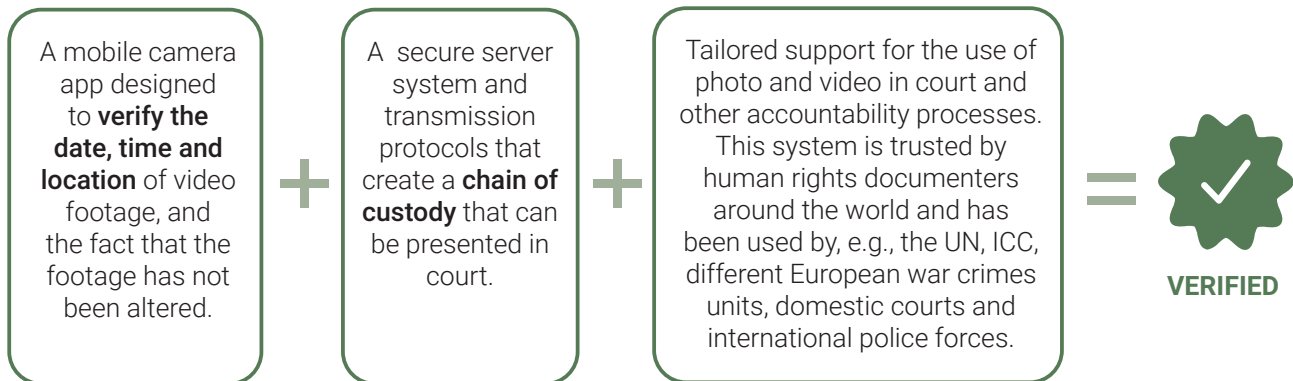
Types of Video Footage

For more information, see [Witness, Video as Evidence Field Guide](#).



Digital Tools: the eyeWitness system

Be aware of digital tools that allow photos and videos to be verified during their creation. The eyeWitness system (<https://www.eyewitnessproject.org/>) includes:



Taking Videos of People



Taking a Photo

When taking a photo **take care to:**

- Use the camera's date and time capabilities or show the date/time by using, e.g., a newspaper.
- Activate GPS settings on the device, or ensure the location is clearly visible in the photograph.
- Transient objects, such as bloodstains or latent prints, should be photographed as soon as possible.
- Take a series of photographs to ensure good quality images and from different angles. Remember that quality takes priority over quantity.
- Photographs should move from the exterior to the interior of the crime scene, and from general to specific focus.
- Take close-up and mid-range photographs of the individual pieces of information.
- Take wide-angled photographs that show the location of the information within the context of the entire scene.
- Use a ruler next to objects to indicate their dimensions.
- Record the author, location, date and time of the particular photograph, a description of the part of the crime scene the photograph depicts (e.g., "investigative scene facing north") and a description of the information the photograph shows, if any (e.g., "bullet casings found at the south entrance to the crime scene").
- Take photographs of victims and potential perpetrators that may still be at the crime scene (provided that all security and consent issues have been adequately addressed).

Photographing Recovered Bodies



Collecting Digital or Audio-Visual Information

E-Devices

Digital information can also be collected directly from an e-device. E-devices can include computers, digital cameras, mobile phones, and electronic devices. They can be found at the crime scene, belong to deceased victim, or be retrieved from a third party.

Handle e-devices with extreme care – the integrity of the device could be compromised, and the data lost due to mishandling.

Always seek expert (e.g., a digital forensic expert) advice.

Do not do anything to change the data contained on a device to ensure its integrity.

Follow the rules of handling and preserving digital information (below).

When receiving e-devices from third persons:

- Avoid receiving information in exchange for money.
- Check that the provider obtained the information through valid means, i.e., not in breach of human rights.
- Consider if the person can provide information to verify the digital information received, e.g., by describing what is in the photograph/video, when, where and why the photograph/video was taken and by whom, and by providing context.

E-Device Evidence Collection Check List

- What type of collection/retrieval methods will be used?
- What equipment may be needed on site?
- What is the level of instability of data and information related to potential digital evidence?
- Is remote access to any digital device possible, and does it threaten the integrity of the evidence?
- What happens if data/equipment is damaged?
- Can the data be compromised?
- Can the digital device be configured to destroy, damage or confuse the data if turned off?

Techniques to **identify**, **extract**, and **collect** evidence from e-devices:

Keyword Searches

Searching the content of devices using likely or known file names and/or key phrases of text, which allows for searches of specific, topical information and digital documents.

File Signature Searches

Searching the device for specific types of electronic files, e.g., doc, PDF, JPEG, etc.

Searching Known Evidential Locations

Focusing on electronic files and folders that are most likely to contain the relevant information. E.g., folders whose name corresponds to an issue being investigated, or folders that were most recently accessed prior to seizure of the device.

Hash Searches

Hashes are a unique string (text data) used to identify a file and ensure it has not been tampered with since its seizure. In order to search for a file using hashes, a practitioner must be familiar with the 'command' function of a computer device.

Handling and Preserving Digital Information

Chain of Custody

For the purposes of digital information, a complete chain of custody should record:

- i. A precise description of the item collected and a detailed record of the activities conducted in relation to that item;
- ii. The whereabouts of the piece of digital information from the moment someone receives it to the moment it is handed over to the relevant court or other proper authority;
- iii. All persons who handled that information, including those that provided the information and those responsible for the storage of that information;
- iv. The purpose for which the information was handled; and
- v. Any alterations of digital information made and the person responsible for making such alterations.

Preservation of Digital Information

Digital preservation refers to the storage of both:

- **physical devices and data carriers** on which digital information is stored.
- **information within the digital storage system, e.g., I-DOC.**

Packaging and Storing Physical E-devices

General rules related to packaging and storing physical devices and data carriers are the same as those applicable to physical evidence. In addition, consider the following basic principles.



Basic Principles on Packaging and Storing E-devices

Packaging, transportation and storage conditions for e-devices must ensure protection from shock, vibration, altitude, heat, electromagnetic sources, radiation exposure, dust, oil, chemical contaminants, etc., as such conditions can potentially interfere with the device and corrupt the data contained therein. Ensure that access control systems, surveillance systems or intrusion detection systems, etc., are in place.

Extra precaution should be taken to not fold, bend or scratch media such as diskettes, CDs and tapes. Avoid placing adhesive labels directly on the surface of e-devices – label the outer cover so as to avoid damage from scratches, etc.

Where a device is comprised of multiple parts and components, pack each individual component separately. For instance, separate the computer monitor from the attached wires.

Clearly label and photograph each device and any associated parts or equipment. For instance, for a computer system, label the monitor, connections, cables, user manuals and any peripheral devices like scanners, printers, etc. Make note of any serial or identification numbers on these items.

Leave cellular, mobile or smart phone(s) in the power state (on/off) in which they were found.

Devices with batteries should be checked regularly to ensure that they always have sufficient power.

Digital information may also contain hidden information, fingerprints or biological evidence, so appropriate action should be taken to preserve this potential evidence.

If possible, record the passwords, codes or PINs needed to access the device.

Create a complete back up of the information, and store in a separate location.

When preserving digital information on data carriers or the e-devices themselves:

1

Prevent unauthorised access to the data, including by limiting access to files to persons with security clearance and by maintaining strong passwords on all devices and information.

2

Encrypt files with particularly sensitive information with encryption software, such as VeraCrypt. It is also recommended to install firewalls, antivirus and anti-spam software on all devices to protect from malicious software, such as MalwareBytes, Avira or AVG.

Using Digital Storage Systems



Basic Principles when Using Digital Storage Systems

Conduct a risk assessment and put in place a digital security protocol before starting to collect and store information electronically. Ideally, in addition to open-source guidance (such as Security in-a-Box Guide to Digital Security), specialists should be consulted.

If the system does not already provide for high-level protection, protect and encrypt all sensitive electronic files with a password. Encryption tools are often freely available on the Internet. Some examples are: AxCrypt, BitLocker, GNU Privacy Guard, and 7-Zip.

Consider whether to keep a record of relevant passwords in a secure and off-site location.

Limit access to protected files to specific staff. There should be a clear policy on who can access the information.

Use the backup system or make and keep two copies of all digital files by transferring and storing them on a computer, memory key/USB and/or read-only CD kept separately in case of malfunctions.

Have an emergency security plan to ensure the personal safety of staff with access to relevant passwords and protected files.

Use anti-virus software and back up database files.

Automatically record any access to digital files and have an edit-trail function on the database.

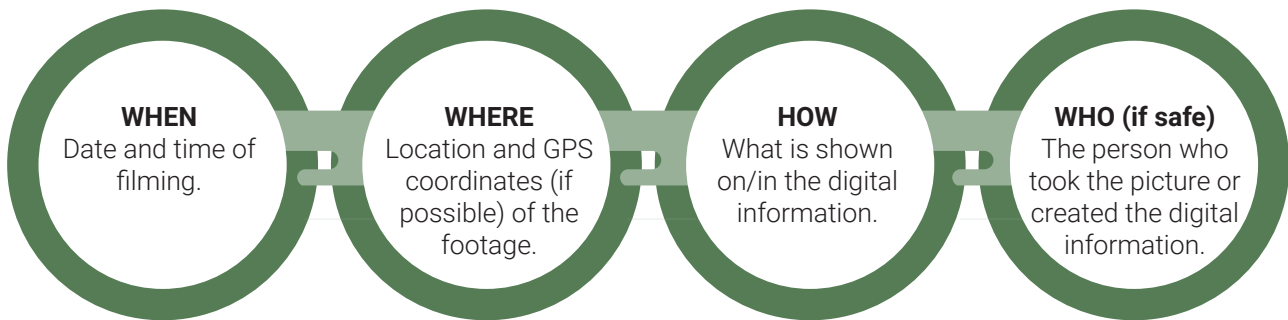
Ensure digital storage systems are demonstrably inaccessible and sufficiently protected against tampering.

Develop a clear policy and guidance containing the rules of the digital storage system's use, which will be accessible to all staff members.

Authenticating and Verifying Digital Information

Work on the presumption that digital information will require **authentication** and **verification**, to demonstrate it retains its **integrity** (i.e., that it has not be tampered with, manipulated and is otherwise reliable).

Authentication



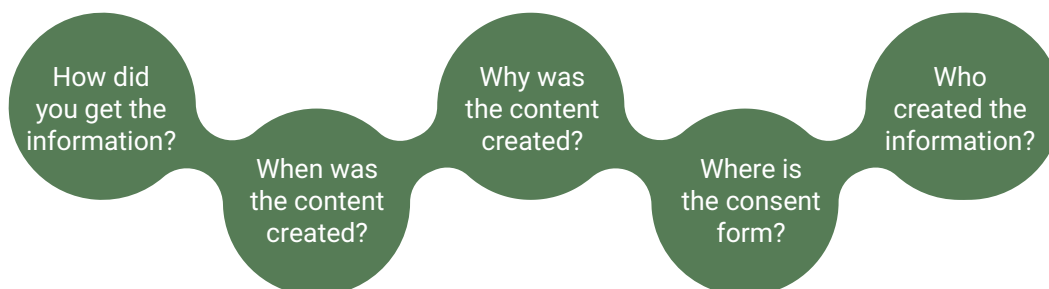
The **metadata** should also be recorded, which includes:

- The description of the lifecycle of the digital information, i.e., the chain of custody;
- The details of any person/organisation that played a role in the creation of the digital information;
- How the digital information was created, collected or received;
- The languages used in the digital content (if any);
- The type (e.g., photograph, voice recording or video) and format (e.g., JPEG, MKV, mp3, etc.);
- The tools(s) used to create the digital content (e.g., the type of camera, recorder, etc.);
- The size or duration of the digital content;
- The subject of the digital content explained through single keywords (e.g., crime scene, attack, weapons, etc.) so the content can be retrieved quickly through key searches;
- A brief description of the content of the digital information; and
- The location of the digital information depicts (if applicable), by geolocating the landmarks in the image either automatically (by enabling GPS on the e-device used) or manually (by, e.g., including street signs, clocks, landmarks, etc. in photographs and video footage).

For more information, see [the Dublin Core Metadata Initiative, User guide – Creating Metadata](#).

Verification

Verification purports to tell you something about the who, what, where and when of a certain event. To verify digital information that is not OSINT or SOCINT, the following cues can be used:



For information on how to verify OSINT/SOCINT information, see BIS Guide: Collecting, Handling and Preserving OSINT/SOCINT Information.

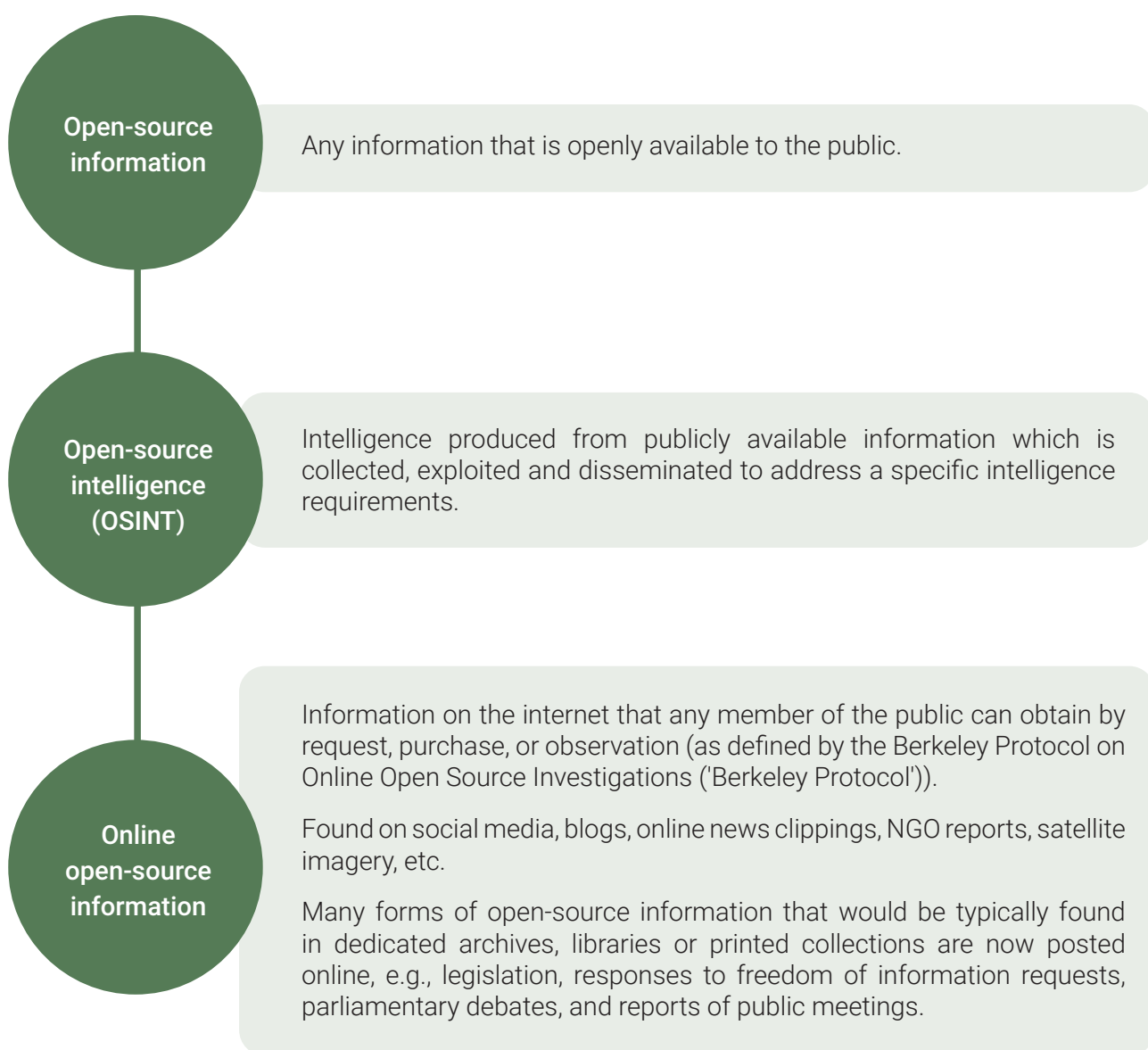


Global
Rights
Compliance

BIS GUIDE: COLLECTING, HANDLING AND PRESERVING OSINT/SOCINT EVIDENCE

This Guide presents an overview of the key definitions and processes involved in open-source investigations. Open-source investigations can be a valuable tool for CSOs seeking to document international crimes and human rights abuses.

Concepts and Definitions



The [Berkeley Protocol](#) provides the most comprehensive guidelines for conducting online research with guidance on methodologies and procedures, analysis and preserving.

Uses, Limits, and Pitfalls



Open-source investigative techniques should **not** be seen as a means to replace traditional, on the ground investigations.



Advantages of Using OSINT:

- Generating lead evidence that can provide concrete avenues for further enquiry.
- Developing an initial investigation plan.
- Overcoming access barriers when gathering information from inaccessible locations.
- Amplifying marginalised voices and hearing from a broader range of perspectives.
- Providing direct evidence of violations upon which findings can be based.



Disadvantages of Using OSINT:

- Investigations may distance practitioners from local communities and grassroots organisations, thus undermining the execution of survivor-centred investigations (the analysis of OSINT is far better carried out by, or involving, those with local knowledge).
- Gaps and 'blind spots' can be attached to the information itself, or arise from cognitive or technical biases.
- It can reflect some of the power imbalances and structural inequalities that lead to certain groups or perspectives being marginalised in the first place.
- The presence and use of dis and mis-information (whether intentionally or not).

The 'Hidden' Nature of Open-Source Research Methods



There is a prevalent idea that types of crime may be less likely to be identified through open-source research methods because of their 'hidden' nature.

For example, in the context of conflict-related sexual violence ('CRSV'), open-source information may exist but is often "hiding in plain sight" due to coded language used on social media. Information on war crimes and crimes against humanity in Ukraine, too, may be hiding in plain sight. For example, satellite imagery can show the destruction of a civilian area through the use of prohibited weapons. Intent to commit the crime against humanity of persecution may potentially be shown through social media posts calling for the collective punishment of a particular group.

Fundamental Principles

As with all human rights work, open-source investigations must be driven by the **'Do no harm'** principle. Throughout the collection stage, the following rules from the **Berkeley Protocol** must be followed:




Preparation

Preparation is key to a successful open-source investigation. From the outset, this requires **setting up**:

- 1

An **information collection plan** for each question you want to answer, outlining the process for how you propose to answer it. Keep questions in clear view, and avoid 'rabbit holes'.
- 2

A **workstation** including which browser to use and which tools to download in advance (such as WeVerify and Google Earth Pro).



Tip: Stick a post-it note with your research question onto your computer screen to keep it in mind throughout.

Before getting started it is recommended to:

- 1

Devise a **workflow** for the investigation (see Workflow Design, below) and the parameters of the investigation.
- 2

Determine how the investigation is going to be **documented** and all of the steps to be taken.
- 3

Consider **security and online safety**: alias accounts should be used for online search platforms which may require purchasing new SIM cards and creating new email addresses; use separate devices for personal and investigative use (when possible); create separate Google accounts (if using Google Chrome), etc. Security in a Box provides a helpful toolkit for digital security.
- 4

Decide if you need to install Hunch.ly or similar **software for recording your steps** online.
- 5

Decide whether you are going to use a site like archive.org to **archive relevant webpages** as seen on that date and time, and whether you need a plugin, like GoFullPage, to take screenshots of the whole page.
- 6

For important videos and images, which may be taken down by the platform or otherwise become unavailable later, determine how and where you are going to **preserve and store this sensitive information**. Do you have a data management plan in place?
- 7

If you are working as part of a **team**, decide how you are going to share information on what avenues you or others have investigated and how you are going to prioritise what information gets selected for verification.

In addition to the above, you should implement measure for self-care and clear work/life boundaries online:



Workflow Design

A structured and well-organised workflow is key to a successful investigation. **Two sample workflows** are set out below which highlight the steps to be taken in an open-source investigation. The process is **iterative** and **cyclical**:

1

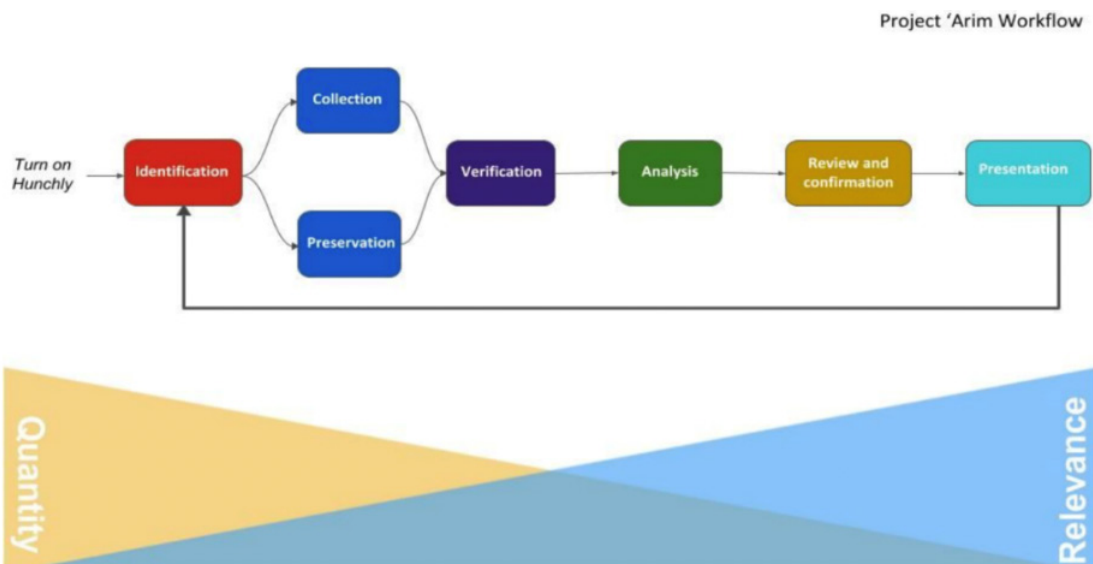
Berkeley Protocol Workflow Design

Open source investigation cycle



2

Bellingcat/GLAN Workflow Design



Discovery, Preliminary Assessment and Collecting Data



The **Berkeley Protocol** recommends that the open-source investigation process should:

1. Start with an **online inquiry**. This requires:
 - 1.1. **Searching**, i.e., discovering information sources through the use of general or advanced search methodologies; and
 - 1.2. **Monitoring**, i.e., discovering new information through the consistent and persistent review of a set of constant sources.
2. Follow with a **preliminary assessment**. This requires practitioners to identify any materials to avoid over-collection and to comply with the principles of data minimisation and focused investigation.
3. Move to the **collection phase**. This requires gaining possession of online information through a screenshot, conversion to PDF, forensic download or other form of capture. Various collection methods can ensure the authenticity of a digital item (for more information, see [Berkely Protocol](#), pp.155-6).

No search is neutral

Tips for maintaining a neutral search:

- Consider your location, search history, device and other factors which will lead the search engine or platform to tailor the results you see.
- Go to the second or third page following a Google search – where relevant information may appear.
- Actively clear the browser's search history and use an anonymous browser tab using a VPN to hide the user's location.
- Log out of all personal accounts before beginning a search.



For example: when conducting a search for expressions of persecutory intent in social media posts, setting the preferred language of the web browser to Russian – rather than Ukrainian, English or another language – may return more relevant results.

Preservation and Storage

The **Berkeley Protocol** recommends to:



Save open-source items as soon as possible

Social media companies remove harmful or violent content from their platforms which can also remove valuable evidence of human rights violations in the process.



Preserve a clean original of the collected digital item in the format(s) in which it was collected

Original copies should be made when edits/manipulation is needed for analysis or verification. Preserve metadata links, networks, content, and all comments from social media and other sites.



Store information locally

For example, save to a password-encrypted hard drive kept in a locked cabinet, to a networked drive that is part of a local area network or remote server, or to the cloud.

Use a standardised data collection system (such as an itemised spreadsheet) to keep track of what is stored, where, and what items have been verified or require verification.

Obtain the informed consent of the person who first shared the information online to store and use that piece of information (unless it would put the uploader at risk to do so).

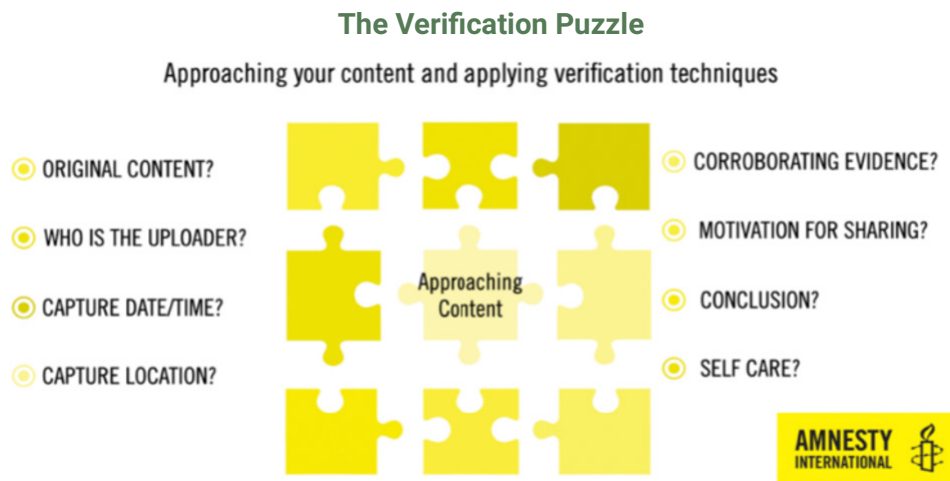
Verification

Ethical Concerns

Verification may reveal sensitive information, such as the uploader's real name or their political affiliation. Before the investigation starts: the value of this information should be weighed carefully against the risk of harm to the creator, uploader, people featured in the content, practitioners themselves, the investigating organisation, and other stakeholders.

According to the Berkeley Protocol, 'verification' is *"the process of establishing the accuracy or validity of information that has been collected online."*

Think about verification as a 'puzzle' where each of the pieces can **work together to help assess whether the piece of content is what it purports to be:**



Common tools and techniques that can be used in verification:

- Reverse image searching
- Viewing Exchangeable Image File Format ('EXIF') Data
- Geolocating content
- Other advanced tools e.g., **SunCalc** to calculate shadow lengths in photographs and videos; new tools hosted by the **OSR4Rights Tools Hub** for open-source human rights investigations; **Twitter** to learn more about these tools; specialist training programmes, etc.

Amnesty International 'Checklist for Verifying Content'

- Is the content you are viewing original?
- Who is the uploader?
- When was the content captured?
- Where was the content captured?
- Can you identify any other corroborating evidence?
- What is the source's motivation for sharing this content?
- What conclusions can be drawn from the content analysed?
- Are you practicing effective self-care?

Analysis

When analysing open-source information, be mindful of what you **can** and **cannot** conclude from the information. Devise multiple working hypotheses and be careful not to fall into the trap of confirmation bias. Helpful **cues** from the **Berkeley Protocol** include:

How was the content obtained?

- Think about what information channels the content travelled through before arriving on your desk.
- How many times did it change hands?

Who created the content?

- Is the person who shared or uploaded the content online also the creator, or was it someone else? Ask if you do not know.

Where is the content from?

- Descriptions and metadata can be forged. Are there visible landmarks or sounds (like police sirens or dialects) that can help you verify a location or time? If you are concerned about the authenticity of the images, you should employ an experienced member of your investigation team or other professional to geolocate the landmarks in the images.

When was the content created?

- You may not always be able to trust the date stamp on a file. Are there visual clues like the weather?

Why was the content created?

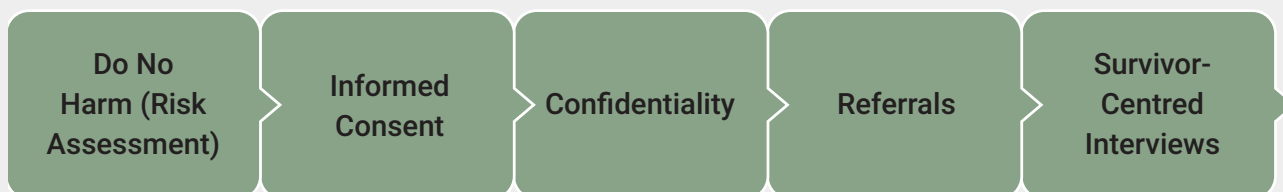
- Can you determine the motivation for sharing the content? What interests does the uploader have?



Global
Rights
Compliance

BIS GUIDE: SURVIVOR-CENTRED PRINCIPLES FOR DEALING WITH VICTIMS AND WITNESSES

This Guide explains the fundamental principles for dealing with victims and witnesses in the context of conflict-related crimes. A survivor-centred approach to dealing with victims and witnesses encompasses:

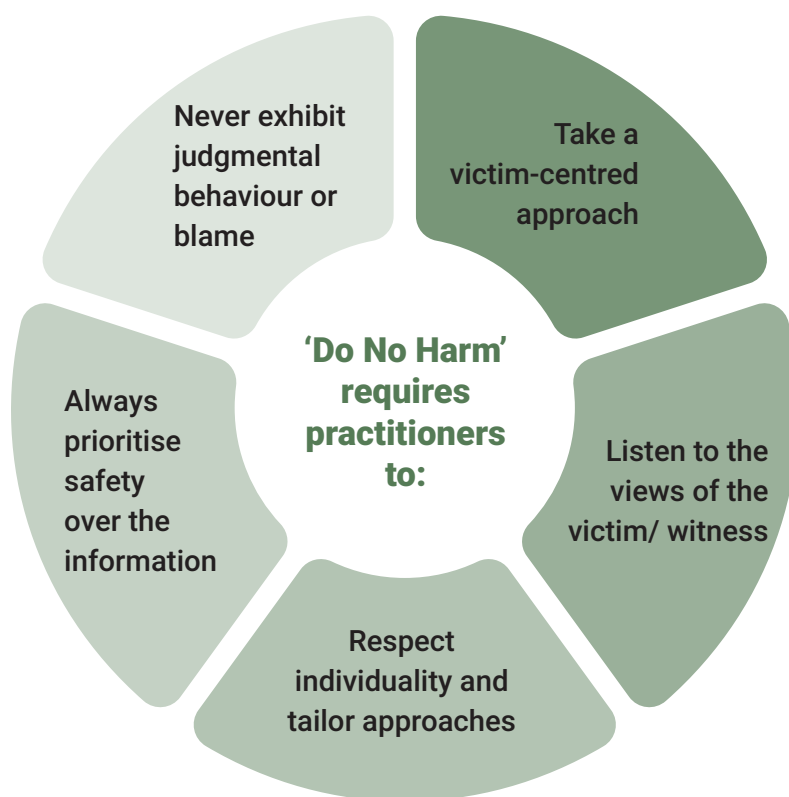


The ‘Do No Harm’ Principle

‘Do No harm’ is an ongoing principle that requires practitioners to listen to the views of the victim / witness, and ask them what they want, their priorities, their concerns, and any risks they may face.

When taking a **victim-centred approach**, practitioners must tailor their interventions to the victim’s/ witness’s specific identities and characteristics (e.g., age, gender, socio-economic/political situation).

Pay particular attention to victims of conflict-related sexual violence (‘CRSV’), torture and other vulnerable groups. These individuals, initially harmed by their perpetrators, can be further harmed by the criminal justice process.



Risk Assessments

A risk assessment is an essential element of Do No Harm and one of the first steps practitioners should take in the documentation process. Risk assessments should be updated throughout investigation processes. There are three stages involved:



Risk Mitigation

Engagement with a victim / witness comes with risks for that person including:

- Retaliation, intimidation and threats by the alleged perpetrator;
- Punishment (including criminal punishment);
- Re-traumatisation during the investigation process; and
- Rejection and stigmatisation.

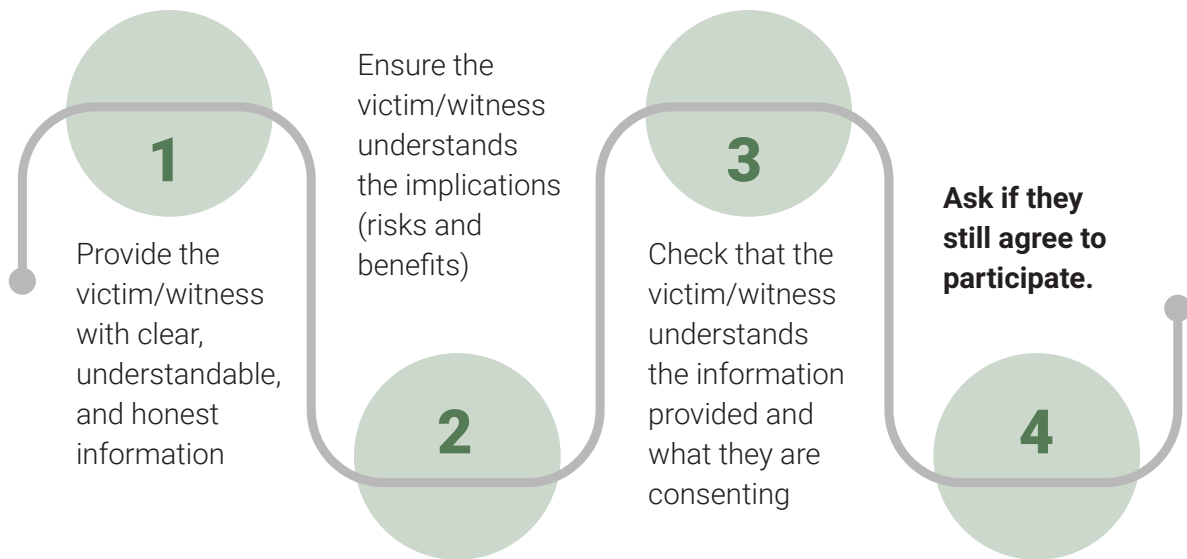
Coordinated safety plan

This may involve implementing protective measures, such as:

- Referring victims/witnesses to psychological or medical assistance prior to interviews;
- Conducting interviews at a certain time or location;
- Conducting interviews using staff of a particular gender or with trauma expertise;
- Providing safe transportation to and from interviews; and
- Contacting foreign partners to secure rehabilitation or relocation abroad (if applicable).

Informed Consent

A victim's / witness's consent must be obtained **prior** to any investigative activity. It must be **explicit** and **ongoing**. Informed consent ensures that victims of crime maintain full control over their experiences and are **informed, willing** participants in the investigative process. However, consent to any aspect of the documentation process **can be withdrawn at any time**.



Individual characteristics of the victim / witness may impair their ability to fully comprehend the relevant facts and their competency to provide informed consent, such as: age (e.g., children), severe intellectual disabilities, literacy issues, mental illness (including traumatisation), physical conditions.

In such cases, translation should be provided to ensure they can understand what they are consenting to, or the permission of a legally authorised representative in accordance with applicable law must be sought in place of informed consent (where appropriate).

Sharing Information

Pro-actively and continuously inform victims / witnesses about:

- Their rights and their case;
- Their safety and security;
- The progress of the documentation process, investigation, or proceedings; and
- The consequences of sharing their information with the ICC and/or Ukrainian authorities.

Explain the criminal justice process to the victim / witness, the potential pitfalls (to counter unrealistic expectations about their participation) and the possibility of obtaining reparations.

Confidentiality

Confidentiality is an ethical obligation, a legal imperative, and an operational necessity. It requires practitioners to protect the information they gather throughout all stages of the documentation process.

Practitioners must inform victims/witnesses that there are limits to confidentiality. This should be clearly explained and their informed consent to continue should be obtained.

Generally, when information is passed on to the ICC or Ukrainian authorities, it will be disclosed to judges or the defence. Inform victims / witnesses of this, and tell them that any confidentiality measures (pseudonyms, etc.) will only be implemented if the prosecutor / judge decides.



Referrals

Referrals involve placing victims / witnesses in contact with social and other support networks. Referrals should never be dependent on participation in the documentation / justice process. Depending on the circumstances, it may be necessary to make a referral prior to, or after the documentation process.

Be aware of what discrete formal and informal social, legal, medical and other services are available for the victim in order to provide the most suitable referral options.

Special Consideration for Victims of Sexual Violence

Victims of sexual violence need access to services that can facilitate their recovery from sexual violence.

1

Referrals prior to documentation

- For example, when the victim requires urgent medical, psychological or security assistance.
- This will be particularly relevant to those areas of Ukraine where active hostilities are taking place or where the victim has been displaced.

2

Referrals after documentation

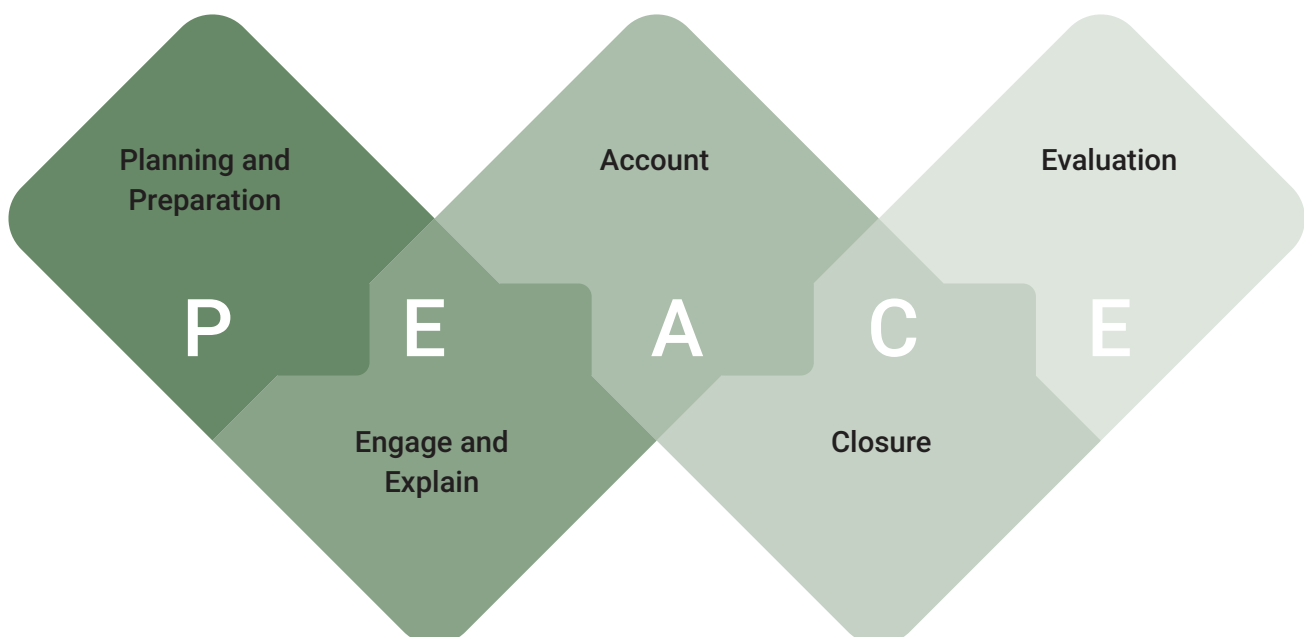
- For example, where the documentation process has been emotionally difficult / traumatic, or has placed the victim at additional risk.

Principles Relating to Witness Statements and Interviews

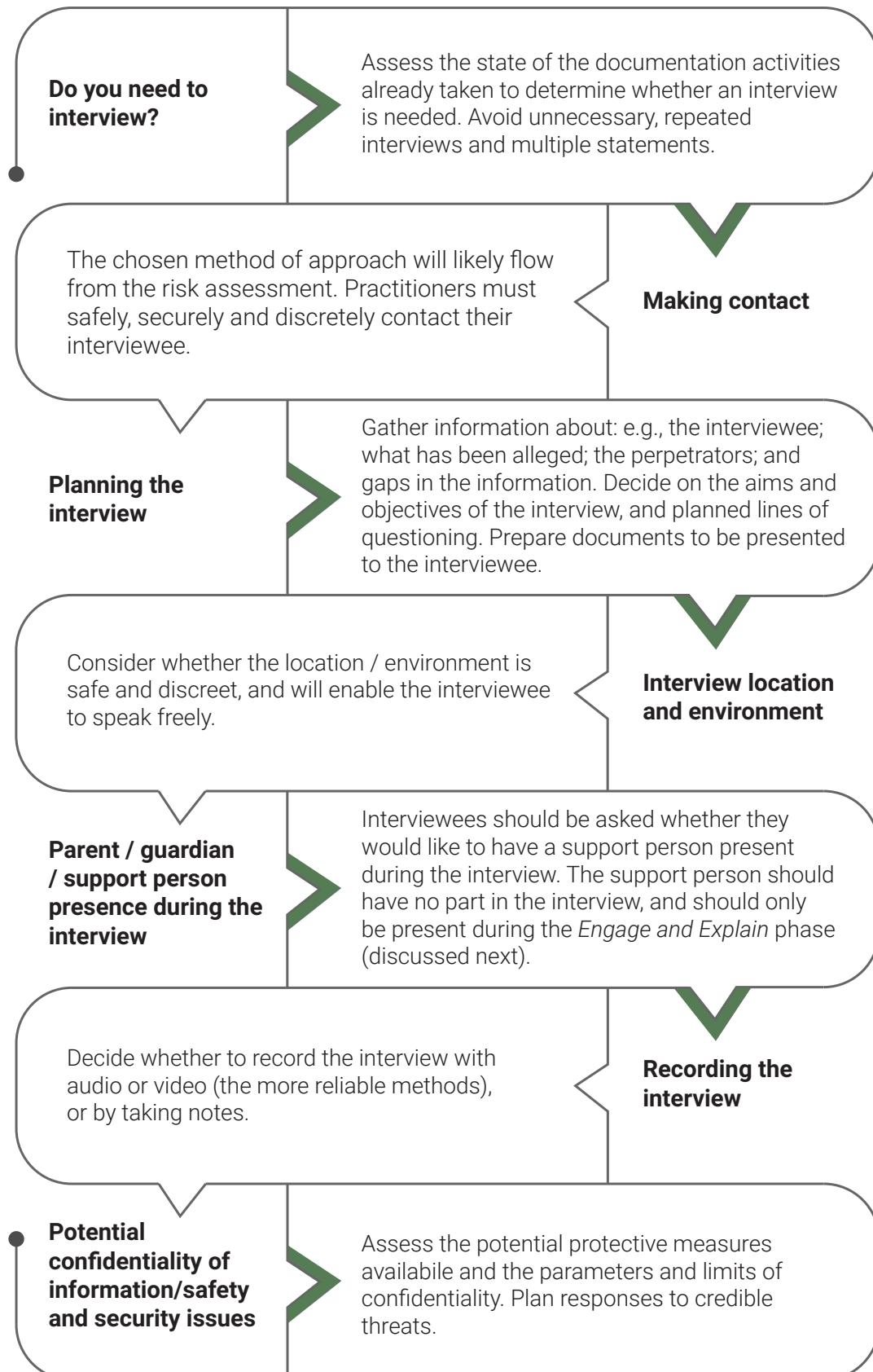
Survivor-Centred Best Practices in Interviewing

Only practitioners who are confident in their own training and competences should conduct witness interviews.

Use the internationally accepted PEACE model when conducting interviews



PEACE – Planning and Preparation



PEACE – Engage and Explain

This is the first stage of the actual interview, in which practitioners should make every possible effort to ensure interviewees feel comfortable and secure. Explain to the interviewee that they have control over the situation, and that they can pause or terminate at any time.

At this stage, practitioners should:

- Create a positive atmosphere, and ensure the interviewee is comfortable.
- Develop trust and rapport.
- Ask the interviewee if they have given any previous interviews.
- Explain the purpose of the interview clearly, and the nature of the questions that will be asked.
- Explain your mandate and how their information will be used.
- Secure informed consent.
- Explain that they should tell the truth, and to ask questions if they don't understand or if the interviewer has got something wrong.
- Record the personal information of the interviewee.

PEACE – Account

During the interview, be attentive and avoid creating an intimidating atmosphere.

Questioning

- Start broad then move on to the specific.
- Start by allowing the interviewee to provide an uninterrupted narrative of events.
- Use clear and accessible language.
- Ensure questions are short, simple, and open-ended.
- Avoid interrupting the interviewee and 'topic-hopping'.
- Use the 'who/what/where/when/and how do you know' questions.
- Use 'TEDS' Questions:

TEDS Questions	
Tell	Could you tell me exactly what happened?
Explain	Could you explain to me what happened afterwards?
Describe	Could you describe to me what that person looked like?
Show	Could you show me on the map where this happened?

Avoid asking the following types of questions:

- **leading** (e.g., He hit you, didn't he?)
- **compound** (e.g., What did they look like and what did they say?)
- **closed** (e.g., Did he shoot?)
- **forced-choice** (e.g., Were the uniforms green or blue?)
- When dealing with victims of sexual violence, do not ask victim-blaming questions like "Why didn't you leave?"

Clarify and Challenge

Expand and clarify the account given focusing on **P**eople, **L**ocations, **A**ctions and **T**ime (PLAT).

- Establish the basis for knowledge of every statement of fact. How did they find out? Who told them?

Inconsistencies in testimony are not something that must be eradicated. They can be indications of reliability and credibility and can arise for many reasons, including:

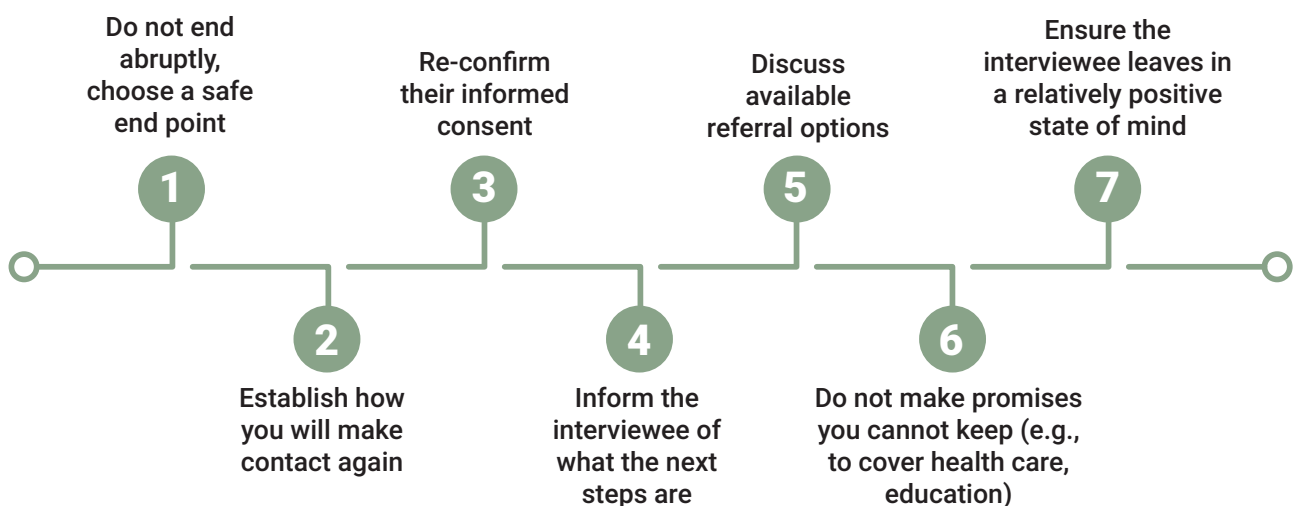
- The victim's lack of understanding;
- Trauma-induced inability to recollect events; or
- Fear of retaliation, shame, or embarrassment.

When faced with inconsistencies, practitioners should seek to clarify rather than confront by taking them back through their story step-by-step, or by posing questions differently and using specific questions.

If this does not reconcile an inconsistency, **note it and move on.**

PEACE – Closure

Concluding an Interview



PEACE – Evaluation

Evaluate the information obtained during the interview:

- Consider whether the interview has revealed any **new or changed risks** to the interviewee or another person.
- Assess the information received including its effect on your current investigation and whether it is consistent.
- Based on the interview, pursue possible further lines of inquiry, and amend documentation strategies accordingly.
- Evaluate whether you obtained all the information you could (be self-critical) and whether further investigation is required.

Interviewing Particularly Vulnerable Individuals

The conflict in Ukraine has affected the population as a whole. However, **some groups face specific threats and impacts**, *including* women, children, older persons, persons with disabilities, national and ethnic minorities, LGBTQI+ people, human rights defenders/activists and IDPs and refugees.

*** Be cognisant of the special needs and problems faced by these groups ***

Collecting Testimonial Information from Children

Practitioners should only interview children in exceptional circumstances where the information they possess is critical and cannot be obtained through other means. And this should only be done after a careful assessment of the child's best interests.

*** Do not interview children unless you have the expertise to do so ***



Global
Rights
Compliance

BIS GUIDE: DOCUMENTING CONFLICT-RELATED SEXUAL VIOLENCE CRIMES

This Guide explains the process involved in documenting conflict-related sexual violence ('CRSV'). **CRSV is a form of gender-based violence that occurs during armed conflict, it is discriminatory and a serious violation of human rights law.**

Sexual violence is underreported in Ukraine due to, among other reasons:

- Community stigma
- A reluctance or unwillingness of some criminal justice actors to initiate CRSV investigations
- Fear of re-traumatisation and reprisals
- Negative investigative practices, such as requiring corroboration

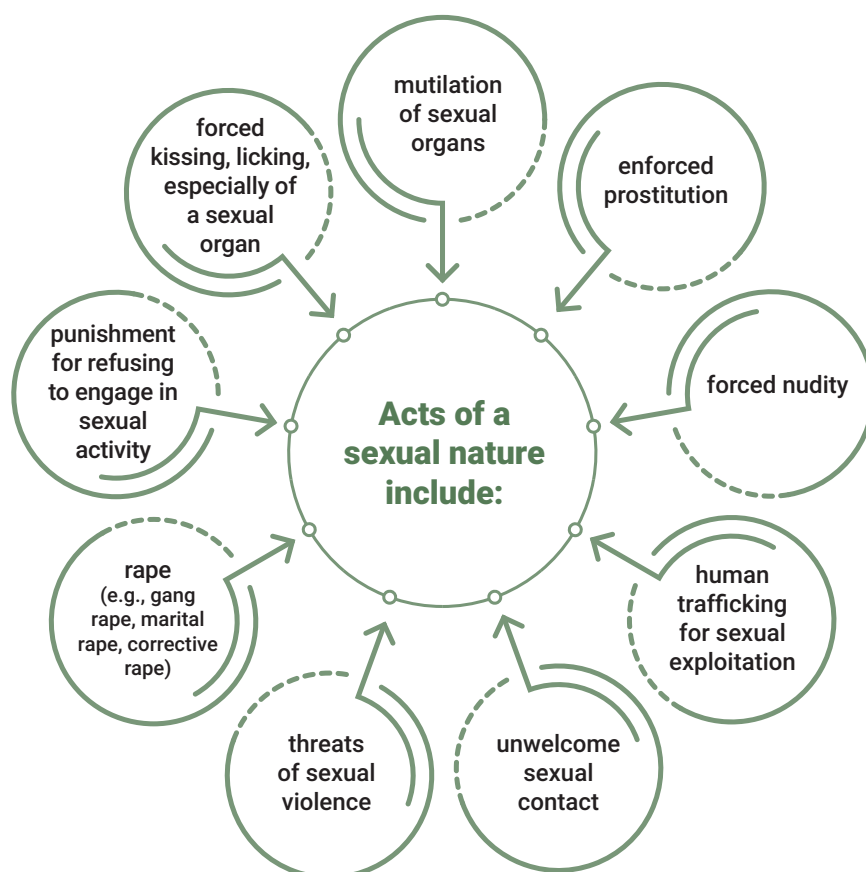
Understanding and Identifying CRSV Crimes

CRSV involves the commission of intentional, non-consensual, acts of a sexual nature. There is a broad range of conduct which may amount to CRSV, including non-physical acts.

CRSV may be committed against one or more persons, by causing a person to engage in an act of a sexual nature (e.g., on the perpetrator, themselves or a third party), and by or against any person.

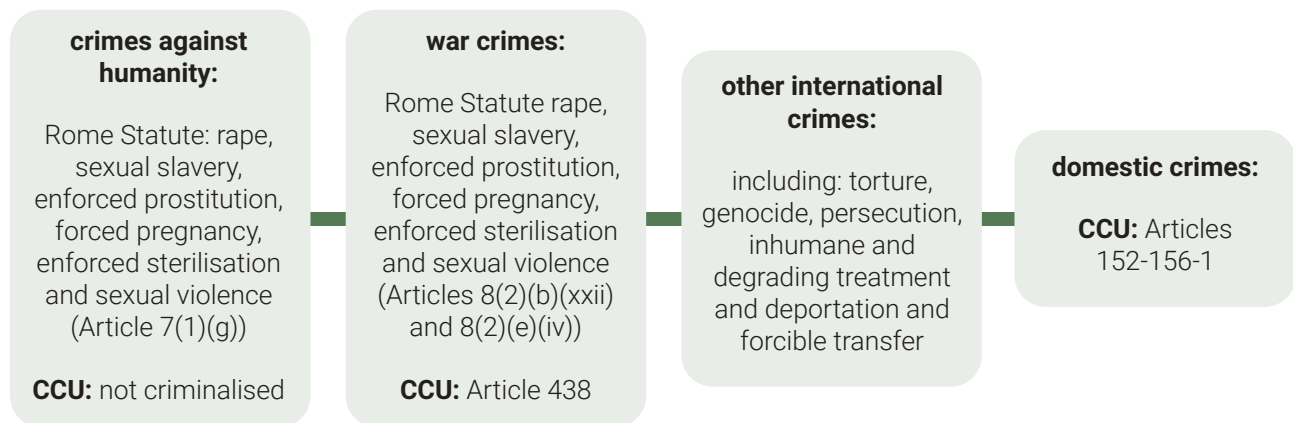
Recognising Acts of a Sexual Nature

The sexual nature of an act is rooted in the perceptions of the victim, the perpetrator and/or their respective communities. CRSV does not need, or be intended, to produce sexual gratification, and it does not have to cause physical injury, or even involve physical contact.



Classifying CRSV in Ukraine

CRSV is criminalised as an international crime and in the Criminal Code of Ukraine ('CCU'):



Lack of Consent and Coercive Circumstances

Sexual violence takes place under a broad range of coercive circumstances. Focusing on coercive circumstances surrounding an act, rather than the non-consent of the victim, removes the focus from the acts and conduct of the victim to the actions of the perpetrator.

Under the CCU, the domestic crimes of rape, sexual violence and compulsion to sexual intercourse occur when a 'sexual act' or 'sexual violence' is committed **without the voluntary consent** of the victim. **Consent will be 'voluntary'** if it is the result of a person's free act and deed, "with due account of attending circumstances" (Note to Article 152).

"Due account of attending circumstances" can be interpreted in line with international standards to cover *physical force, threats or coercion, coercive circumstances and incapability of giving voluntary consent due to age, disability, illness, etc.*

'Coercive Circumstances' under International Standards

Free, voluntary and genuine consent cannot be given to a sexual act imposed by actual or threatened force; coercion (i.e., that caused by fear of violence, duress, detention, psychological oppression or abuse of power); by taking advantage of a coercive environment (e.g., armed conflict or occupation); or when committed against a person incapable of giving genuine consent.

Only one of these coercive circumstances is necessary, but often there will a combination of multiple coercive circumstances. **Proving a lack of consent or demonstrating the non-consent of the victim (i.e., by their physical or verbal resistance) is not required.**

Documenting coercion and coercive circumstances requires practitioners to **take a context-based approach**, which involves exploring a wide variety of lines of questioning with the victim to uncover:

- Details about the victim themselves (e.g., name, date and place of birth, address) and whether they have any particular vulnerabilities (e.g., gender identity, age, disability, poverty).
- Information about the sexual violence they experienced and whether any coercive circumstances existed at the time (e.g., whether weapons, occupation forces or military activity were present in the area where the sexual violence occurred, whether the perpetrator(s) were armed and with what, whether the victim was detained or held against their will).
- A description of the appearance, demeanour and language of the perpetrator(s) (e.g., did they wear a uniform, have identifiable insignia on their clothing, speak in a different language or identifiable dialect, arrive in a vehicle?).
- A detailed description of the physical and mental harm suffered as a result of the violence.

Physical Force

Physical force provides clear evidence of non-consent but is not necessary to establish coercive circumstances.

Examples of physical force include:

- acts of violence directed towards the victim, such as hitting or slapping the victim, including with an object (i.e., a gun)
- physically restraining the victim, such as pinning them down or grabbing their hands
- pushing the victim to the ground or dragging the victim
- acts of violence directed towards another person
- using a knife to tear off the victim's clothes

CRSV does not always result in physical injury or leave any visible traces on the body. Evidence of physical injuries may also no longer exist where reporting of the crime was delayed or where medical evidence is unavailable. Practitioners should draw no adverse conclusions about the credibility of the victim in cases where there is no evidence of physical injuries.

The victim should not be expected to explain why they bear no marks of physical violence.

Threats of Force

Threats of force against the victim can also constitute coercive circumstances.

The threats (express or implied) may be of physical force or of other harm (e.g., against a family member or to reveal the sexual encounter). Physical force does not need to actually occur. The threat itself is sufficient if it creates a reasonable fear in the victim that they or a third person will be harmed.

Examples of threats of force include:

- threats or intimidation using a weapon
- threats to kill or injure
- threats to harm sexual body parts
- threats to harm a person's health
- threats of being subjected to sexual violence

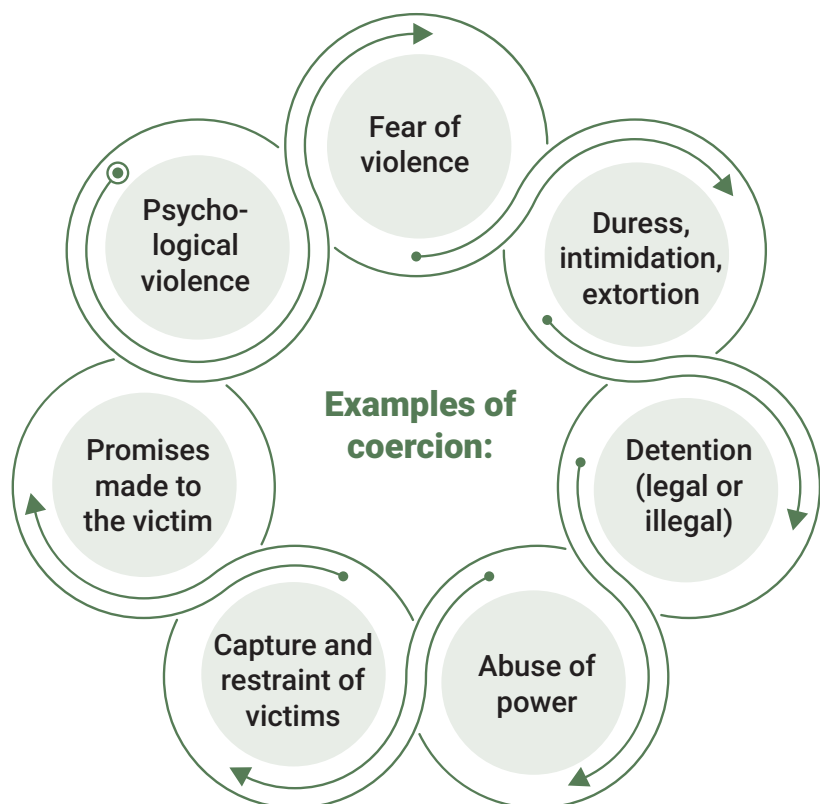
Coercion

Coercion or **coercive behaviour** involves the use of subtle behaviours – e.g., verbal or psychological abuse or controlling behaviour – by perpetrators of CRSV to create or exploit vulnerabilities and make victims dependant on, or subordinate to, them.

Practitioners should adopt a flexible, context-based approach when documenting CRSV cases to uncover the full range of coercive behaviours and circumstances that may have given rise to CRSV.

The following types of coercion (discussed below) are particularly relevant to Ukraine:

- Detention
- Psychological violence and abuse of unequal power relations



Coercion – Detention

Detention reflects unequal power structures and is always coercive

Sexual violence in any form of detention or captivity (legal or illegal, formal or ad hoc) vitiates consent and is therefore coercive

Coercion – Psychological Violence and Abuse of Unequal Power Relations

Psychological violence

May occur in a broad array of contexts and is particularly likely where there is an unequal power relationship between the perpetrator and the victim

Unequal power relations

Occurs when individuals have an official or unofficial position of authority in relation to their victims, e.g., soldier, police, border guard, guardian, doctor

Occupation forces

Have an unequal power relationship with those under their occupation. By definition, this entails an element of control

The following factors may be indicative of unequal power relations:

- the perpetrator has an official or unofficial position of authority (e.g., soldier, detention guard, police officer, guardian or care giver, doctor, teacher, community or tribal leader, etc.)
- the victim knows that the perpetrator previously used violence against them or a third party
- the victim has any type of dependency (e.g., financial, legal, familial, etc.) on the perpetrator
- the victim has certain vulnerabilities or personal characteristics that open them to exploitation
- there is inequality in familial or intimate relationships (e.g., where there is domestic violence or where the perpetrator is the head of the household)

A number of circumstances may, individually or collectively, indicate the existence of psychological violence or abuse of power, including:

- detention, border crossings or military check-stops
- active combat or attacks that force civilians to take shelter from shelling, sniping, the opposing military, etc. in locations where CRSV can take place
- isolation of the victim from others in their group (e.g., taking the victim to another room away from the individuals with whom they are sheltering)
- making the victim feel obligated to have sex by threatening to hurt another person or to disclose the location where the victim and others are sheltering
- using intimidating and aggressive language or gestures (e.g., yelling, destruction of objects)
- publicly humiliating, degrading or dehumanising the victim

Taking Advantage of an Inherently Coercive Environment

CRSV can also be committed by taking advantage of an inherently coercive environment. In this case, the perpetrator does not directly coerce the victim, but takes advantage of a coercive environment that exists independently to sexually abuse the victim.

Inherently coercive environments include:

- the presence of the military in the area
- armed conflict or occupation
- situations where other war crimes or crimes against humanity are being committed

Often, the other coercive circumstances will be present concurrently with the inherently coercive environment, all of which converge to create a situation where the victim is unable to provide genuine consent. **Practitioners must therefore consider evidence pointing to all forms of coercion in their totality.**

Incapacity to Give Genuine Consent

Incapacity – due to induced, natural or age-related causes – can also prevent individuals from giving free, voluntary and genuine consent

The causes of incapacity include:

- intoxication with alcohol or drugs, whether self-administered or by the perpetrator
- a temporary or permanent physical or mental condition
- being asleep or unconscious
- certain disabilities or conditions that affect ability to consent or communicate consent
- age, including old age

Corroborating Evidence of CRSV

To demonstrate that an act of CRSV has occurred, practitioners need to obtain evidence of that act. Corroborating evidence is evidence that strengthens, adds to, or confirms already existing evidence. However, **corroborating evidence is often difficult to obtain for CRSV cases** as they typically happen in isolated locations and/or in situations where the perpetrator is in a position of authority over the victim and the victim is unable to seek help.

Under both international and Ukrainian criminal law, judges may rely on the evidence of a single witness to enter a conviction without the need for corroboration.

Linking Perpetrators to Acts of CRSV

Even if the elements of the offence have been established, **practitioners also need to uncover linkage evidence to help demonstrate that the accused perpetrated the sexual violence offence.**

Perpetrators of CRSV may include those who physically commit the crime and those who do so indirectly through others, without ever meeting the victim or visiting the scene of the crime. These remote perpetrators can include individuals, groups, political or State entities, or organisations. Such perpetrators may have, for example, ordered or aided and abetted the sexual violence or had command responsibility over the direct perpetrators of the sexual violence.

Practitioners should consider the full range of modes of liability when examining potential perpetrators and consider evidence which may establish these links. For example, does the evidence show:

- The suspect had the authority to issue orders to subordinates and issued an order to commit sexual violence.
- The suspect a military commander who had effective control over subordinates and knew or should have known they were committing sexual violence, and failed to take reasonable measures to prevent, punish or report the crimes.
- The suspect provided the direct perpetrator with practical assistance, encouragement or moral support.
- The suspect formed a common plan with a group of people to commit sexual violence or contributed to the sexual violence committed by a group acting with a common purpose.

Victims and Impact of CRSV

1

Victims of CRSV

- **Anyone can be a victim of CRSV.** While CRSV disproportionately affects women and girls, it also affects men and boys, as well as non-binary, transgender and intersex persons.
- Practitioners should therefore **consider all reported incidents of CRSV without bias**, assess each case on a case-by-case basis and take into account the individual circumstances and needs of the victim based on their personal characteristics.

2

CRSV Against Men and Boys

- **It is important that the experience of men and boys with CRSV does not get lost or ignored when documenting CRSV.** In particular, it is common for CRSV against men and boys to be discussed in coded language or be characterised as other crimes that do not reflect the sexual nature of the conduct due to social stigma and shame.

3

Impact of CRSV

- The long and short-term impact of CRSV can be severe and sometimes life-threatening.
- The impacts of CRSV can be physical, psychological, social or socioeconomic and legal, and can affect not just the victim, but also families, family communities and communal structures.
- Practitioners should seek to gather impact evidence throughout the documentation process. Such evidence may be an indicator, and provide corroborating evidence, that CRSV has occurred and warrants further examination.

Vulnerable Categories and Intersectional Discrimination

How an individual experiences, and is affected by, CRSV will be very specific to the victim themselves, their gender and personal circumstances, the context in which the violation was committed and the relationship and power dynamics between the victim and the perpetrator.

Taking a victim's personal circumstances into account, by **adopting an intersectional approach**, will help practitioners understand how inequality and discrimination interact and operate together to create different experiences of CRSV.

Taking an intersectional approach will also enable practitioners to better understand the potential coercive circumstances affecting the victim's ability to consent, and to implement the most appropriate practices to protect the victim from additional harm caused during the documentation process.

These intersecting identities and factors include, among others

- | | | |
|---------------------|---------------------------------|--------------------------|
| • ethnicity/race | • indigenous / minority sta-tus | • social economic status |
| • language | • sexual orientation / gender | • religion or belief |
| • political opinion | • armed conflict | • national origin |
| • age | • being HIV positive | • health status |
| • being in sex work | | • displacement |
| • culture | | |

Best Practice Approaches to Documenting CRSV

To properly document CRSV and ensure that victims are able to access meaningful justice, it is crucial to **separate the misconceptions and falsehoods surrounding sexual violence from the facts**.

Practitioners should take a victim-centred approach to documentation, which requires them to ensure that no aspect of their documentation activities is affected by their personal views about sexual violence, gender or other stereotyping against women, or any other intersectional factors.

Understanding stigma and shame

A common impact of CRSV is stigma and shame felt by the victim. **Stigma entails negative, gender-based stereotypes that result in the victim's marginalisation and shifts blame from the perpetrator to the victim**. Victims of CRSV may internalise stigma / shame themselves, or it may be imposed on them by their families, community or the authorities investigating and prosecuting crimes.

Practitioners should remain objective and non-judgemental at all times and accept the victim's evidence at face value.

Ending Myths, Assumptions and Stereotypes

How an individual experiences, and is affected by, CRSV will be very specific to the victim themselves, their gender and personal circumstances, the context in which the violation was committed and the relationship and power dynamics between the victim and the perpetrator.

Promiscuity and Virginity: Irrelevance of Prior Sexual Conduct

Consent to a specific sexual act is only genuine if it is given voluntarily, consciously, and freely.

It does not matter if the person has consented to similar conduct, consented previously or withdrew consent after initially consenting.

Questions about a victim's prior sexual conduct are irrelevant to assessing whether they consented to a sexual act and to assessing whether a victim or witness is credible.

Practitioners should therefore focus only on establishing that the act of a sexual nature:

1. **occurred** (e.g., "what happened?", "where did he touch you?")
2. **under coercive circumstances** (see above).

Questions about sexual history, prior partners and relationships (e.g., "were you a virgin?", "how many people have you had sex with?") are irrelevant to proving the crime.

Irrelevance of the Victim's Conduct or Behaviour

The conduct of the victim (e.g., what they were wearing; whether they had make-up on; their sexuality; whether they had been drinking / taking drugs; their engagement in sex work) is **irrelevant to any assessment of consent.**

Focus on the behaviour of the perpetrator and avoid blaming the victim for the perpetrator's actions.

Flight, Fright or Freeze: Irrelevance of Behaviour During and After Sexual Violence

There is no correct way for a victim to behave during or after sexual violence. Victims do not have to say no or physically resist. Freezing or failing to call for help is not a sign of voluntary participation.

If there is evidence that a coercive behaviour or environment existed, consent cannot be inferred from the words or conduct of the victim. Victims may submit to CRSV for reasons associated with the unique, coercive environment surrounding the violence, e.g., they were overpowered, detained, genuinely feared for their lives, feared resisting would provoke more violence, or choose to not resist as a coping mechanism for dealing with the trauma of being sexually assaulted.

Active Participation and Physiological Responses

A victim's active participation in the sexual act or any physiological reaction (such as an orgasm, erection or ejaculation) does not indicate consent. Questions, such as: "did you enjoy it?", "did you have an erection/orgasm?" are biased, unfair and rooted in gender stereotypes.

Subsequent Behaviour

How the victim reacted after an act of CRSV (e.g., whether they remained in the location or ran away, acted upset or not, gave birth to a child conceived during rape or told anyone about the violence) may provide evidence that the CRSV occurred, but should not be used to infer the victim's consent. The victim's subsequent sexual conduct with the perpetrator and/or others is equally irrelevant.

No Adverse Inference from Delayed Reporting

Failure or delay in reporting acts of CRSV, including not revealing all the facts immediately or leaving out or minimising certain acts, does not imply that a victim is lying or lacks credibility.

Do not draw adverse inferences about the credibility of victims who have delayed reporting their case.

Reporting of CRSV crimes is often delayed for many reasons, including a lack of understanding about what CRSV is and if it has occurred; the ongoing armed conflict which may make reporting impossible; the influence of trauma upon a victim; fear of retaliation; fear of not being believed or being blamed.

Hymen Examination

Hymen examination (or virginity testing) is the practice of assessing a person's 'virginity' based on the state of their hymen. **Virginity testing should not be undertaken to establish whether a victim has been raped or sexually abused.** However, medical examinations of female genitalia for signs of sexual assault may be useful corroborating evidence where the purpose is to evaluate and treat injuries, and not to assess 'virginity'.

If approached by a victim of sexual violence, practitioners should help them seek medical treatment from a reputable medical practitioner who can also conduct a medical examination that will be admissible in a court of law.

