

DOCUMENT PREPARED BY:



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

INVESTIGATOR'S TOOLKIT

Observe, analyze, act against transnational
organized crime in Central Africa

© 2026 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted
in any form or by any means without permission in writing from
the Central Africa Observatory on Organized Crime and Violence.

Cover: © *Sia Kambou/AFP via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

Contents

Context	1
Module 1: Defining the desired impact	2
Defining your objectives: Understanding the problem to take better action	4
Module 2: Planning the investigation and observation	5
Identifying credible leads	6
The role of hypotheses in building an investigation	7
Deciding whether to launch an investigation	8
Strategic planning	9
Module 3: Information-gathering techniques	13
Categories of information to be collected	14
Primary and secondary sources	14
Processing and organizing collected information	18
Module 4: Open-source research	19
OSINT information sources	20
Key tools and platforms for investigators	21
Module 5: Ethical issues for investigators	23
Why ethics are central	24
The issue of financial compensation for sources	26
Avoiding the pitfalls of manipulation	26
Ethics and conflicts of interest	26
Managing relationships with sensitive sources	26
Ethical guidelines for presenting findings	27
Establish guidelines for the organization's internal practices	27
Ethical approaches as a strategic lever	27
Module 6: Security issues – physical, digital and political	28
Integrating security from the planning phase	29
Physical safety and operational security of individuals	29
Digital security and data protection	30
Political pressure and psychological safety	31
Incident preparedness and response	32

Module 7: Analysis, information processing, reporting	33
Organization and centralization of collected data	34
Analysis of facts and cross-referencing of data	35
Writing a report or investigative dossier	35
Module 8: Advocacy and communication	38
Differences between advocacy and communication	39
Key steps for building an advocacy strategy	40
Creating an effective communication campaign	41
Dealing with retaliation and protecting spokespersons	41
Module 9: Monitoring and evaluation	42
Integrate M&E from the planning phase onward	43
Defining M&E indicators	43
Structure post-investigation or post-campaign follow-up	44
Organize internal debriefings	44
Involve communities in the evaluation	44
Assessing long-term effects	45
Highlight the results and lessons learned	45
Appendix 1: Survey plan (template)	46
Appendix 2: Consent form for sources	48
Appendix 3: Sample letter for a formal or community complaint	49
Appendix 4: Sample letter to local authorities to report concerns or request a meeting	50
Appendix 5: Useful apps and platforms	51
Resources	52

Context

Organized crime in Central Africa constitutes a major and evolving challenge to governance, economic stability and social cohesion. It operates through adaptive and often transnational networks that exploit structural vulnerabilities such as porous borders, uneven state presence and resource-rich environments. Illicit markets – including trafficking in goods and arms, illegal resource exploitation, informal mining and human trafficking – are not isolated phenomena, but interconnected systems supported by logistics, finance and protection mechanisms.

In many contexts, these criminal dynamics are embedded within broader political and economic systems, sometimes intersecting with public authorities, private actors or armed groups. This contributes to corruption, weakens institutions and, in certain cases, fuels insecurity and violence. Despite its scale, organized crime remains difficult to document due to limited access to reliable data, opaque operations and significant legal and security constraints.

Investigating organized crime is inherently complex. It involves working with fragmented, sensitive or concealed information, navigating environments shaped by risk and uncertainty, and addressing issues that may have political or economic implications. It is not a linear process and rarely produces immediate or complete results. As such, it requires analytical rigor, methodological discipline, ethical awareness and strong professional judgment.

This toolkit has been developed to support civil society organizations, investigative journalists, researchers and community actors engaged in understanding and addressing these dynamics. It proposes a structured yet flexible methodology that follows the full cycle of an investigation, from defining objectives to evaluating impact.

The process begins with defining the desired impact (Module 1), ensuring that the investigation is grounded in a clear understanding of the problem and guided by precise, measurable objectives. It then moves to planning the investigation (Module 2), including identifying leads, formulating hypotheses, organizing resources and anticipating constraints.

Effective investigation depends on the ability to collect and organize information (Module 3) from diverse sources such as interviews, field observations and documentation. This is complemented by open-source research (Module 4), which provides valuable tools for identifying actors and corroborating findings.

Throughout the process, ethical principles (Module 5) and security considerations (Module 6) are essential to ensure credibility, protect sources and mitigate risks. The transformation of information into evidence relies on analysis and verification (Module 7), enabling the production of coherent and actionable outputs.

To generate impact, investigations must be accompanied by advocacy and communication strategies (Module 8), aimed at informing stakeholders and influencing decision-making. Finally, monitoring and evaluation (Module 9) allow practitioners to assess outcomes, learn from experience and strengthen future actions.

Together, these elements form an integrated methodological framework designed to support rigorous, secure and impactful investigations. This toolkit encourages a professional, adaptable and context-sensitive approach, contributing to stronger knowledge production, informed action and more accountable systems in Central Africa.

Defining the desired impact

Module 1

Before launching an investigation into organized crime, it is essential to clarify the intended objective. Investigations into criminal markets can serve different purposes: documenting the existence of a network, understanding how trafficking operates, highlighting institutional interactions or complicity, or producing data useful to public policymakers.

Clearly defining the desired impact helps avoid two common pitfalls:

- >> Investigations that are too ambitious and spread resources too thin;
- >> Investigations that are too narrow, which fail to provide insight into criminal mechanisms.

In the context of an organized crime investigation, the objective might, for example, focus on:

- >> Mapping the actors involved in an illicit market;
- >> Clarifying the objectives and the theory of change;
- >> Identifying trafficking routes and strategic crossing points.

Accomplishing that objective will require deliberate planning, including:

- >> Identifying research that can illustrate and support the achievement of the objective, as well as priority research areas;
- >> Defining the data collection methodology;
- >> Developing a strategy for physical and digital security;
- >> Planning for needs and ensuring the availability of resources – human, logistical and financial – to achieve objectives;
- >> Ensuring at every stage that the research strategy supports the pursuit of impact;
- >> Establishing the foundations of an advocacy and communication strategy that can evolve over time.

Planning, as presented in this module, is a collaborative effort. It is important to identify a leader who can coordinate a core group within the research team. This core group must share a common vision of the objectives to be achieved, the methodology to be used and the resources to be deployed. This core group must embody trust, solidarity and mutual support. In turn, this core group will need to build other relationships of trust to help extend the information chain toward a common goal: change.

Defining the desired impact means providing a strategic direction for your efforts, maximizing the chances of engagement and ensuring that the resources invested produce a tangible and measurable effect.

Defining your objectives: Understanding the problem to take better action

Before setting a goal, it is essential to clearly understand the problem you wish to solve. This step relies on facts, reliable data and knowledge gathered from the field or through documentary research. A clear formulation of the problem then allows you to identify a goal that will guide your work: research, advocacy, community mobilization or communication.

Clearly state the problem

This involves describing what is observed, why it is a problem and who is affected by it.

Example: The expansion of organized crime networks contributes to the proliferation of armed violence, undermines state authority, fosters insecurity in urban and rural areas and exposes civilian populations – particularly young people and vulnerable communities – to increased risks of violence, exploitation and marginalization.

A well-formulated statement should be factual, neutral, well documented and understandable for a non-specialist audience.

Define a S.M.A.R.T. goal

Once the problem has been identified, the next step is to define the change you wish to bring about. To do this, use the S.M.A.R.T. approach:

- >> **Specific:** The goal must be clear and unambiguous.
- >> **Measurable:** Progress must be trackable.
- >> **Achievable:** The goal must be attainable with your resources.
- >> **Realistic:** The goal must take into account the political, social and institutional context.
- >> **Time-bound:** Set a deadline or timeframe.

Refine your objective

A well-defined objective allows you to:

- >> Determine research priorities, including topics, sources, methods, and level of evidence;
- >> Anticipate risks and develop mitigation strategies;
- >> Identify desired impacts, such as providing information to law enforcement authorities to combat impunity, or influencing legislators to revise a law;
- >> Guide the advocacy strategy, for instance by selecting target audiences (local authorities, lawmakers, media, communities, etc.);
- >> Tailor communication tools to the target audience.

The requirements for evidence, analysis and documentation will differ, depending on your objective. Hence the importance of clarifying the objective from the outset to effectively structure your approach. Enhance transparency in the management of public funds by helping to reduce financial losses and corruption.

Planning the investigation and observation

Module 2

In contexts heavily marked by organized crime and armed violence, an investigation cannot be based on an abstract idea; it must first be substantiated by the realities on the ground. What is both possible and relevant to investigate will be determined by local dynamics, the risks involved, the actors present and the information available. Not every issue necessarily lends itself to an investigation; from the outset, the choice must be guided by clear and realistic objectives that align with the team's capabilities and the specific demands of the context.

Identifying credible leads

Before any planning takes place, the team must determine whether it has credible and reliable leads that would justify opening an investigation. A credible lead is never based on a rumor or an isolated hunch, but on a set of preliminary elements that corroborate one another:

- >> Consistent interviews
- >> Internal or administrative documents
- >> Direct observations
- >> Geospatial images or data
- >> Physical or digital evidence
- >> Cross-checks from independent sources, including credible media outlets

These elements, which are sometimes fragmentary, allow you to piece together what is essentially a jigsaw puzzle with missing pieces: A structure, a mechanism, a network or an event may begin to emerge, but certain pieces of information are still missing that are vital to establishing the facts and completing the picture.

It is precisely from this incomplete puzzle that the stage of forming hypotheses begins – a preliminary and indispensable step in any investigative planning.

Importance and limitations of community-based investigations conducted by community liaison officers in the contexts of organized crime and armed violence

Community-based investigations conducted by community liaisons are particularly valuable for understanding and documenting phenomena related to organized crime and armed violence. Embedded at the heart of local social dynamics, these actors possess detailed knowledge of their immediate environments, the practices taking place there and the developments affecting community safety. Their proximity to the population and their familiarity with on-the-ground realities allow them to access information that is often difficult for external actors to gather.

In many contexts marked by insecurity, local communities are among the first victims of criminal activities and armed violence. Community liaisons can thus play a decisive role by helping with:

- >> early detection of signs of criminal activity or armed violence, such as unusual movements of armed groups, illicit trafficking or recruitment patterns;
- >> collecting and documenting field information based on direct observations, testimonies and contextual clues to better understand local dynamics;

- >> alerting relevant organizations or support structures to high-risk situations or concerning developments; and
- >> guiding subsequent investigations by providing preliminary information that facilitates the identification of priorities for analysis and intervention.

Through their local roots, community liaisons thus help enhance the capacity of civil society organizations, researchers and institutions to understand the local realities of organized crime and armed violence, while valuing the knowledge and expertise of the communities directly affected.

However, while community-based investigations represent an essential step in gathering information and detecting problematic situations early, they also have limitations. Community liaisons may face significant constraints, such as restricted access to certain areas controlled by armed groups, the risk of reprisals, or a lack of technical, analytical or legal resources to conduct in-depth investigations.

Furthermore, information gathered at the local level does not always, on its own, allow for the reconstruction of all the mechanisms at work within criminal networks, which often operate on multiple levels and extend beyond local borders. It therefore becomes necessary to supplement community-based investigations with more structured inquiries, enabling the cross-referencing of sources, the analysis of financial and logistical flows, the identification of involved actors and the documentation of chains of responsibility.

Community-based investigations conducted by community liaisons thus form a fundamental foundation for understanding the phenomena of organized crime and armed violence. However, their effectiveness and impact are enhanced when they are part of a broader investigative framework that combines technical expertise, in-depth analysis and institutional mechanisms capable of transforming the information gathered into concrete and sustainable actions.

The role of hypotheses in building an investigation

Hypotheses are provisional explanatory propositions that help make sense of the fragments of information already collected. They are neither evidence nor conclusion; they are possible explanations that the investigation may confirm, refine or reject. In this way, they play an essential role in transforming raw data, interviews, documents, images and observations into testable assumptions that guide the investigative process.

Each investigative hypothesis helps define concrete actions, identify necessary resources and shape the methodological approach. It serves as an operational framework for organizing information collection and structuring analysis.

For example, if initial information suggests the presence of arms trafficking in a border area, a possible hypothesis could be: *Arms are being trafficked through specific border routes using informal transit networks*. This hypothesis could then be tested by identifying transit routes, observing suspicious movements and gathering information from local actors.

If multiple accounts mention the recruitment of young people by armed groups, a possible hypothesis could be: *Armed groups are actively recruiting young people through local community networks or schools.* This could be tested by verifying testimonies and engaging with community leaders and institutions.

If collected information points to kidnappings or extortion, a possible hypothesis could be: *A structured criminal network is operating in the area and coordinating kidnapping and extortion activities.* This hypothesis could be explored by analyzing patterns, identifying areas of activity and examining communication and financial channels.

Thus, hypotheses serve as frameworks for transforming incomplete information into structured work plans. They help to determine what needs to be verified, where, how and with what resources. They act as methodological compasses and filters, helping eliminate irrelevant leads, assess feasibility and allocate resources effectively.

In short, hypotheses serve as the bridge between informed intuition drawn from the field and strategic planning. They enable us to determine whether the investigation is relevant to the initial objectives and feasible, secure and methodologically sound.

Deciding whether to launch an investigation

Between identifying credible leads and committing resources to implementing operations in the field, it is essential to evaluate whether an investigation is realistic and feasible. Consider the following:

- >> **Objectives and potential impact:** Does the investigation clearly align with the defined strategic objectives (mandate, thematic priorities, advocacy needs)? Does it offer a real opportunity for impact – in terms of change, awareness or accountability – or would another organization (specialized journalists, international NGOs, research institutions) be better positioned to carry it out?
- >> **Time constraints:** Can the investigation be conducted within the project's timeframe without compromising the quality of the work or the safety of the teams?
- >> **Human, technical and financial resources:** Do you have the necessary skills, technical support and budget? Do you have reliable and secure local partnerships?
- >> **Security, legal and political risks:** Could the investigation involve potential threats to the team, the communities involved or the data collected?
- >> **Logistical feasibility:** Is the area accessible? Are infrastructures and data available and of reasonable quality? Are there constraints related to the presence of sensitive stakeholders or local environmental conditions?

Decision-making process for launching an investigation



Strategic planning

Once feasibility is confirmed, the investigation can be structured to maximize safety, efficiency and impact. Strategic planning is the crucial process of transforming a preliminary, still uncertain and fragmentary investigative idea into a realistic mission aligned with set objectives. It enables investigators to define the conditions that will ensure its effectiveness, safety and impact.

Checklist for launching an investigation

- >> Identification of human and technical needs
- >> Budget preparation
- >> Timeline development
- >> Crisis prevention and management

Building a team

Once feasibility is confirmed, the investigation can be structured to maximize safety, efficiency and impact. Strategic planning is the crucial process of transforming a preliminary, still uncertain and fragmentary investigative idea into a realistic mission aligned with set objectives. It enables investigators to define the conditions that will ensure its effectiveness, safety and impact.

Example of an investigative team

Role	Main function
Coordinator / Project manager	Oversees logistics, budget and adherence to the schedule. Ensures that objectives are met at each stage.
Lead investigator	Gathers information in the field, verifies hypotheses and explores new avenues.
Analyst	Verifies and cross-checks information and data; conducts open-source research; performs literature reviews; and compiles, organizes and secures relevant information.
Legal counsel	Provides legal advice regarding applicable regulations related to the subjects of the investigation. Ensures compliance with laws and regulations and minimizes legal risks for the team (defamation, public order disturbances, potential charges).
Security focal point	Assesses risks, manages alerts and coordinates emergency measures.
Fixer or community liaison	Facilitates access to the field and local contacts, acts as an intermediary to collect images, documents and interviews, and helps the team gain acceptance in the communities being investigated. Serves as a security liaison, keeping the investigative team informed about the security situation on the ground.

Tip 1: A small, close-knit team that is on the same page and trusts one another is better than a large, poorly coordinated group that lacks trust.

Tip 2: Not all team members need access to all information. Restricting access to certain sensitive information – such as the identities of sensitive sources – helps protect those involved in the investigation.

Plan logistics and budget

Rigorous planning requires a realistic budget forecast. Main expense categories may include:

- >> **Human resources:** research teams, consultants, field informants, communities, intermediaries;
- >> **Travel:** per diems, flights, car rentals, fuel;
- >> **Logistics:** transportation, fuel, lodging, food;
- >> **Equipment:** recorders, dedicated phones, GPS, cameras, batteries;
- >> **Security:** satellite phones, secure vehicles, field training;
- >> **Communication:** credits for secure messaging services, VPNs; and
- >> **Documentation:** printing, archiving, secure storage, secure transmission methods.

Advice: Always set aside some finances for unforeseen circumstances.

Develop a realistic timeline

It is important to establish a timeline with clear objectives, recognizing that different phases may require varying amounts of time. The phases of the investigative process can include:

- >> **Advance research:** literature review, open-source research, mapping;
- >> **Fieldwork, or primary data collection:** observation, site visits, interviews;
- >> **Analysis:** verification and consolidation of data, analysis; and
- >> **Delivery:** reporting, publication, advocacy, outreach.

Prevent and manage crises

This step is a critical component of planning. It enables stakeholders to anticipate risks, protect those involved, including community observers and the organization's staff, and establish rapid response mechanisms in the event of threats or pressure from criminal actors. Thorough preparation and proactive incident management enhance the security, reliability and continuity of investigative work.

The steps involved in this process may include the following:

- >> **Preliminary risk assessment:** Identify potential threats, assess the accessibility and sensitivity of the areas to be visited, and map out stakeholders and their interests.
- >> **Safety protocols:** Establish travel guidelines (safe travel times, restricted areas, discreet cover), use secure communication procedures and implement an emergency contact plan.
- >> **Source protection:** Anonymize testimonies and sensitive data, vary meeting locations and methods, regularly assess risks to sources and informants, and plan safety measures.
- >> **Incident management:** Establish a clear protocol for dealing with intimidation, confiscation of equipment, surveillance or arrest; set up an internal chain of command for rapid incident reporting; and document each incident to facilitate follow-up and response.
- >> **Coordination with reliable partners:** Collaborate with local organizations, established networks of observers or journalists; exchange information with legal or security experts; and establish mutual support mechanisms in the event of a crisis.
- >> **Continuity planning:** Plan alternative methods for collecting or verifying data if access becomes impossible, secure evidence and plan strategies for a discreet exit if the situation escalates.

Assess constraints and unforeseen circumstances

The team must be able to adapt without ever compromising safety or ethics, which means that the best planning is flexible. It anticipates obstacles and provides for alternatives.

Risk	Planned response
Refusal of cooperation by a local authority	Rely on a community partner to gain access to the site.
High security risks	Modify the itinerary, postpone the mission or assign it to a local contact.
Adverse weather conditions	Plan for temporary fallback windows.

Evaluate legal considerations

Verify the legality of the investigation, including in sensitive areas, protected areas and mining zones. Obtain the necessary permits. Anticipate the legal risks associated with an arrest.

Information-gathering techniques

Module 3

Information gathering is at the heart of any investigation into transnational organized crime. Investigators can combine several methods and techniques to test different initial hypotheses. They should be mindful, however, that research in illicit or high-risk environments requires a context-sensitive, do-no-harm approach. Methodological choices should be guided primarily by risk to participants and researchers, rather than procedural completeness.

Categories of information to be collected

Investigations draw on a wide range of information sources. Some are available in the public domain, such as official documents, NGO reports or open databases. Others are not publicly available and require active efforts to obtain them, including through interviews, partnerships with experts or consultations with inside sources. The richness of an investigation lies in this patchwork of information, where a variety of sources – public and private, direct and indirect – combine to form a complete picture that allows us to understand the reality on the ground and the networks at play. The more these sources of information intertwine and corroborate one another, the more robust and credible the investigation becomes, offering a reliable and comprehensive view of the networks and activities under study.

Primary and secondary sources

Primary sources

- >> Interviews
- >> Documented direct observations
- >> Non-public documents

Secondary sources

- >> Official reports issued by governments, the UN, international organizations, etc.
- >> Media reporting
- >> NGO reports
- >> Social media
- >> Open-source databases (see Module 4 – OSINT)

Tip: Save everything and do not lose anything. Systematically cross-reference primary and secondary information to enhance verifiability.

Interviews

By building trusted relationships with intermediaries, investigators can arrange interviews with individuals key to the investigation. Identifying these sources relies on a solid network of reliable intermediaries, as well as open-source analysis.

Certain sources are of particular importance:

- >> **The eyewitness:** They can provide a firsthand account of the events they observed. The investigator must ask deliberate questions and accurately capture the witness's words and impressions in order to precisely document what they heard or saw.

- >> **The knowledgeable informant:** These sources may possess documents or in-depth knowledge of the activities under investigation, often from having been involved in the network as current or former employees, customs officers or competitors. They can provide access to technical and internal information.
- >> **Members of a criminal network:** These sources may provide crucial information on the network's structure and operations. They may be difficult to approach and must be handled with caution and security.
- >> **The victim:** Although they often lack detailed knowledge of the networks, they help document violations of the law and provide context for the harm caused.
- >> **Indirect sources:** Their testimony does not always carry the same weight as that of direct sources, but they can facilitate contacts, share documents or point to relevant information. They should therefore not be overlooked.
- >> **Diplomatic sources:** The testimony of these sources can be very useful, particularly for understanding transnational issues. The information they provide may be highly sensitive, however, and so must be handled with caution.

Tip: Cross-referencing information from these different types of sources helps enhance the reliability and credibility of the data collected.

In conducting interviews, remember that informed consent remains essential; it must be meaningful and freely given, taking into account power imbalances and situational pressures. In addition, the use of recording devices should be carefully assessed on a case-by-case basis, as their presence can:

- >> increase suspicion or risk in illicit environments;
- >> inhibit open communication; and
- >> create a permanent record that may endanger participants if accessed by third parties.

As a result, recording is not always appropriate, even with consent. In such cases, consider an approach that minimizes data capture and reduces the risk of sensitive data being exposed or misused, such as:

- >> contemporaneous or post-interview note-taking; or
- >> selective documentation focused on analytical relevance.

The interview

1. *Preparing for the interview*

- >> Clearly identify the objective of the interview and the information you are seeking.
- >> Select appropriate sources based on their role within the network being studied (e.g. witness, informant, victim).
- >> Prepare a flexible interview guide that allows you to follow the flow of the discussion while leaving room for unexpected elements.

2. *Listening and questioning techniques*

- >> **Open-ended questions:** Encourage the person to describe their experience in their own words.
- >> **Clarifying questions:** Clarify specific points without suggesting answers.
- >> **Paraphrasing and verification:** Repeat what was said to confirm understanding.
- >> **Active listening:** Observe non-verbal cues and hesitations, which can reveal important information.

3. *Adapting to the type of source you are talking to*

- >> **Eyewitness:** Have them accurately describe what they saw or heard, without interpretation.
- >> **Knowledgeable informant:** Explore the technical and documentary details of the network or activity.
- >> **Victim:** Gather an account of the violations and impacts suffered, while respecting their vulnerability.

4. *Verification and triangulation*

- >> Cross-reference information from different sources (interlocutors, documents, observations, open data) to enhance reliability.
- >> Carefully document interviews while protecting the confidentiality of sources.

When conducting interviews and capturing related data, protecting the identity of sources should be the top priority. The use of pseudonyms is standard, and researchers should take further steps towards robust anonymization, including by removing or altering indirect identifiers and by avoiding contextual details that could enable re-identification. Confidentiality should be treated as an ongoing responsibility, not a one-time step.

All collected data should be securely stored and encrypted, with access controlled. However, consistent with a risk-based approach, researchers should also consider only collecting and retaining information that is strictly necessary. In some cases, the safest course is not to create or retain sensitive records at all.

When referencing information collected through interviews, consider what information can be shared and how best to cite sources. While transparency is a core research principle, in a conflict-affected setting, protecting sources takes precedence over full attribution. There may be instances in which using information gathered through interviews could retraumatize victims or citing a source could put their safety or security at risk. Researchers should avoid including identifying details when doing so could expose individuals to harm; they should instead use anonymized or generalized references.

Field observation

Direct observation is an essential technique because it provides visual and contextual details that enrich and supplement other sources of information. It allows for the objective documentation of suspicious activities and the collection of usable physical evidence.

Essential steps for effective observation:

- >> **Prepare a notebook:** Record dates, locations, atmosphere, activities and any anomalies observed. Note behaviours, interactions and any details that could serve as evidence.
- >> **Capture high-quality images and videos:** Use a dedicated device with geotagging capabilities, rather than a personal phone. Ensure that the images allow you to zoom in on key details: faces, licence plates, logos, uniforms, vehicles and markings. Always include the date, location and context to ensure the legal and analytical value of the evidence.
- >> **Note specific details:** These include licence plates, logos, uniforms, vehicle types, phone numbers, names – any element that will help reconstruct the facts and corroborate other sources.

Observations should be:

- >> **Risk-minded:** Activities should not expose the researcher or others to harm.
- >> **Ethical:** Observation should not infringe on the dignity, privacy or safety of individuals.
- >> **Self-aware:** Researchers must recognize that their presence and perspective shape what is observed and recorded.

The quality of the observation is just as important as the way the facts are recorded. A photograph or video without metadata (e.g. date, GPS location) loses much of its value. The analysis of the collected information generally takes place after the fieldwork, and the relevance of the investigation depends directly on the investigator's ability to have secured as much reliable and detailed data as possible.

Non-public, confidential documentation

Confidential documentation can be obtained from internal whistle-blowers and sources met during the investigation. These documents include anything not available in the public domain, such as contracts, agreements and correspondence. It is essential to follow best practices: scan and save the documents immediately, never alter the original, and record the conditions under which the documents were obtained (source, date, context) to ensure the reliability and traceability of the evidence.

Secondary sources

Not all publicly available secondary sources carry the same weight or value in an investigation. An official report from an international organization, such as the UN, is based on rigorous methodologies, cross-checks and reliable data and therefore serves as a solid reference. Conversely, an article published in a little-known magazine or on a dubious website may be unreliable or biased or contain unverified information. During analysis, it is crucial to assess the credibility of each source, consider the expertise and reputation of the publisher and cross-reference this information with other evidence to avoid erroneous conclusions. In short, the quality of public sources varies considerably, and their use must always be critical and contextual.

Processing and organizing collected information

Processing and organizing the collected information is essential to ensure that nothing is lost during the investigation. Upon returning from the field, it is advisable to prepare a compiled grid that categorizes the information by type, source, location, reliability and follow-up actions, linking each item to the corresponding file to facilitate analysis. Information gathering is a rigorous and sensitive process; it is not simply a matter of 'taking whatever we can', but of seeking out what is accurate, useful and actionable. Every interaction, photograph or testimony serves as a building block for reconstructing a criminal network that is often well concealed.

Sample data collection table

Date	Source	Key information	Location	Reliability	Follow-up

Open-source research

Module 4

In the digital age, an increasing proportion of organized crime can be documented and verified remotely using open-source intelligence (OSINT). This approach allows investigations to be conducted without investigators being on the ground, and it helps strengthen evidence derived from direct observation by leveraging local media, social media, public databases, digital archives and mapping platforms. It also makes it possible to include actors who may not be physically present, but who may be managing or financing networks from tax havens or other opaque structures. OSINT thus offers the ability to track illegal cross-border flows, identify actors and their structures, and collect and verify videos, photographs and online testimonies, all while securing the research to prevent losing it.

Accessible even with limited technical resources, OSINT is a powerful and complementary tool for supporting complex investigations and circumventing the opacity of the institutions or companies involved. In high-risk contexts, such as mining or forestry areas under armed control, OSINT is sometimes the only feasible investigative approach without direct physical risk.

OSINT information sources

Types of open sources	Possible information to collect
Social media	Relevant photographs and videos, employee comments, names of executives, company details.
Official websites	Licences issued, calls for bids, laws, concessions.
Commercial registries	Shell company names, shareholders, connections between firms.
Local and international press	Current events, scandals reported, legal precedents, prevailing sentiments.
Satellite imagery	Areas of deforestation, new roads, evidence of mining operations.
Public databases or leaks	Public data on exports, individuals, blacklists, banking details.

Key tools and platforms for investigators

Tools and platforms	Recommended use
Advanced Google Search	Search by site, date, language and keywords.
Wayback Machine	View the history of modified and deleted pages; preserve current versions of webpages.
Google Earth or Sentinel Hub	Track changes in an area over time.
Open Corporates, Societe.com, Orbis	Research details about companies and their executives.
Maltego or Aleph	Map the connections between individuals, organizations and places.
Social Searcher or TweetDeck	Search for geolocated posts or keywords.
Intelligence X	Search databases, internal documents and leaks.
Organized crime databases: CITES, Forest Trends, Environmental Investigation Agency, TRAFFIC	Gather trade, wildlife, timber and sanctions statistics.

Verification and validation of OSINT information

OSINT can be manipulated through doctored images, false statements or disinformation. As a result, it is essential to:

- >> **Verify the source:** Determine whether the account is official or anonymous and whether the media outlet is reliable.
- >> **Cross-check the data:** A single piece of information is never enough.
- >> **Geotag and date:** Pinpoint the location and verify the date for every photograph or video.
- >> Verify metadata using FotoForensics or Metadata2Go.

Use OSINT without putting yourself at risk

Even without going into the field, OSINT can expose you to retaliation if it is not used properly. Practice strong digital hygiene:

- >> Never use personal accounts; use a fake account or a dedicated account instead.
- >> Use a VPN to hide your location.
- >> Never leave traces of your searches on shared devices.
- >> Be wary of booby-trapped or malicious documents, unknown links or corrupted files.
- >> Use secure platforms (e.g. Signal) for communication.

When to use OSINT in the investigative cycle

OSINT can be utilized at every stage of an investigation: during the preparatory phase to identify companies, individuals and backgrounds; during the investigation to supplement field intelligence and monitor social media; and after the investigation to verify facts before publication and to track reactions.

Although OSINT is a powerful tool for generating leads, cross-checking testimonies, identifying hidden networks and tracking illicit flows, it does not replace the richness of fieldwork, the emotional impact of testimony or the complexity of local context. It works in tandem with direct observations and human interactions. When properly mastered, OSINT is an indispensable strategic tool in investigations involving organized crime, revealing hidden truths, strengthening the robustness of collected data and protecting investigators by limiting their direct exposure.

Ethical issues for investigators

Module 5

When power imbalances are pronounced and certain communities live in situations of heightened vulnerability, any investigative process carries a risk of unintentional harm. The fundamental principle of 'do no harm' must therefore guide every interaction, all information gathering and every decision to publish. The goal is not merely to document the facts, but to do so without unnecessarily exposing those involved to reprisals, stigmatization or internal conflicts. In a context often marked by impunity, corruption and violence, investigators must demonstrate rigour, integrity and responsibility.

This module sets out the fundamental ethical principles that must guide any investigation, namely:

- >> respect for the free and informed consent of sources. This basic principle includes exceptions in very specific cases, which must be properly regulated in compliance with the law;
- >> protection of the identity, dignity and safety of those interviewed; and
- >> rejection of any form of corruption, manipulation or exploitation of facts.

It also provides practical tools for:

- >> preparing interviews in a respectful manner;
- >> assessing ethical dilemmas in the field; and
- >> integrating transparency and accountability practices into every stage of the investigation.

By ensuring a strong ethical stance, investigators strengthen community trust, the credibility of their work and the long-term impact of their actions.

Why ethics are central

Ethics are not constraints that slow down the investigation; they are a prerequisite for robustness and credibility. An investigation conducted without a clear ethical framework can produce fragile, legally questionable or counterproductive information. Unethical behaviour can also erode trust between the investigator, those who agree to provide information and those who will receive it. Conversely, a structured and responsible approach strengthens the evidentiary value of the documented facts and protects the organization against attempts to discredit it.

In an environment where organized crime is transnational and often linked to powerful networks (political, economic, military) and where local populations are vulnerable, an ethical approach can become a moral shield and a protective strategy. It can safeguard:

- >> the integrity of the investigation against manipulation or corruption;
- >> those involved, including sources, investigators and communities; and
- >> the organization's credibility, which is essential for advocacy and building alliances.

Strong ethics are a powerful defense against those who may wish to discredit you.

Fundamental principles of investigative ethics



Do no harm

Avoid and minimize risk to the participants, the researcher and the affected community.



Safety

Mitigate risks to researcher safety and avoid unnecessary exposure to danger.



Informed consent

Inform all participants of the purpose of the research, the risks involved and how the collected information will be used.



Responsible use

Ensure sensitive data is properly managed and that any information shared does not expose the source or enable harmful activities.



Confidentiality

Never reveal the identity of sensitive sources unless explicitly agreed.



Accuracy

Never exaggerate or manipulate the facts; accuracy takes precedence over sensationalism.



Awareness

Be aware of researchers' positionality, biases and influence on the research process and findings.



Independence

Do not become a judge or executioner; document the facts and do not settle scores.



Internal transparency

Ensure that your team is familiar with the methods used and validate any sensitive information.

The issue of financial compensation for sources

Paying sources is prohibited because paying for information:

- >> compromises the credibility of the investigation;
- >> creates a relationship of dependency; and
- >> obscures the source's true motivation.

However, certain forms of compensation may be considered acceptable. For example:

- >> covering the cost of a meal or a drink during an interview, within reasonable limits and without excess; and
- >> reimbursing transportation, communication or logistical expenses.

Avoiding the pitfalls of manipulation

Some sources may have intentions that could undermine the credibility of the research. They may provide false or incomplete information to manipulate the analysis.

The golden rule is to always cross-check all information gathered, because an unverified fact poses a risk to the investigator's credibility and entails legal and ethical risks.

Ethics and conflicts of interest

Conflicts of interest may include situations such as an investigator having a personal or business relationship with a party under investigation, or a partner organization receiving funding from a company under suspicion.

To avoid such situations, one should:

- >> maintain complete transparency internally: these situations must be disclosed and discussed;
- >> revise the strategy if necessary: change the investigator or reposition the investigation; and
- >> never allow a conflict of interest to compromise the primary mission.

Managing relationships with sensitive sources

Some sources put their lives or jobs on the line to speak out. These individuals may include internal employees, security personnel, members of armed groups or government agencies, victims and whistle-blowers.

It is recommended that you do not record them without permission, do not expose them by publishing their names or photographs and do not ask them for evidence that they cannot safely provide. Building a relationship based on listening, following up and establishing trust over time is key to a successful investigation.

Ethical guidelines for presenting findings

Even when you have damning information, it is crucial to:

- >> not label a person as 'guilty' without formal, corroborated evidence;
- >> use legally prudent language, such as 'potentially involved parties', 'suspected practices' or 'alleged perpetrators';
- >> allow those implicated the right to respond (see Module 7); and
- >> avoid rushing to publish under the influence of emotional or political pressure.

Establish guidelines for the organization's internal practices

Ethics do not rest solely on an individual investigator. The organization must establish clear guidelines, such as an ethical code of conduct to be signed before each assignment and protocols for data and personal protection. An organization should consider establishing an ethics or legal liaison within the team.

These actions could help prevent misconduct, protect team members from risky or illegal decisions and strengthen the organization's position in the face of any allegations.

Ethical approaches as a strategic lever

A rigorous ethical stance allows you to:

- >> gain the trust of communities and key sources;
- >> convince donors and institutional partners;
- >> make the organization more difficult to attack legally or in the media; and
- >> serve as a model of good governance.

In short, ethics in investigations are not an option – they are a guarantee of safety, effectiveness and legitimacy. In a minefield of conflicting interests, opacity, and risks, an ethical approach is our only reliable compass.

Security issues – physical, digital and political

Module 6

Investigations into organized crime frequently expose those involved – including civil society organizations, journalists, lawyers and communities – to physical, psychological, legal or digital threats. Political pressure, intimidation, arbitrary arrests, data hacking and digital surveillance are not theoretical risks: they are realities experienced by many investigators.

This module offers a structured and preventive approach to security in hostile environments. It covers:

- >> the physical safety of teams (travel, accommodation, sensitive areas, crisis management);
- >> digital protection (secure communications, anonymous browsing, data storage);
- >> measures to protect sources, particularly vulnerable witnesses; and
- >> approaches to managing political, legal or social threats against civil society organizations and whistle-blowers.

It also provides practical tools, including alert sheets, risk matrices, secure mission plans and protocols for handling arrests or information leaks. The module aims to equip actors to operate without exposing themselves unnecessarily, strengthen team resilience and make security a shared priority at every stage of the investigation.

Integrating security from the planning phase

In the context of investigations into organized crime, the dangers are not theoretical. Indeed, actors are often operating in areas under armed control and regularly face:

- >> administrative or police repression;
- >> seizures of equipment and arbitrary arrests;
- >> risks of reprisals against communities, journalists and whistle-blowers; and
- >> hacking or digital surveillance.

Security is not just another module. It is a central thread that must be integrated from the very beginning.

Physical safety and operational security of individuals

Duty of care and risk mitigation

Investigators and organizations must prioritize the safety of participants and research teams, avoiding activities where risks outweigh potential benefits and adapting methods to the context.

Risk assessment

To assess risks before beginning any investigation, use a risk matrix to:

- >> identify potential threats, including poachers, military personnel, traffickers, wildlife or difficult terrain;
- >> assess the likelihood and severity of each risk; and
- >> propose mitigation measures, alternative routes, safe travel times or local support points.

Example: When conducting fieldwork in a remote mining area under the influence of armed groups, it is advisable to plan the fieldwork with local guides, have an exfiltration plan, avoid travelling at night and check in with a contact person daily.

Developing a secure mission plan

Every field mission must have:

- >> a security focal point, responsible for monitoring the team's movements;
- >> a mission sheet listing locations, dates, objectives and emergency numbers;
- >> an alert procedure in case of prolonged radio silence (e.g. 24 hours); and
- >> an evacuation plan in case of an incident, such as illness, assault or threat.

Tip: At a minimum, always work in pairs. Never go out alone, especially in sensitive areas.

Practical safety measures

You should always carry safety equipment with you during investigative assignments, including:

- >> a dedicated phone with a portable charger;
- >> local and backup SIM cards;
- >> a GPS and printed maps in case signal is lost;
- >> neutral clothing (avoid military-style attire);
- >> a basic first-aid kit; and
- >> a paper list of contacts in case the phone is lost.

The role of local fixers and informants

Fixers are the eyes and ears of investigators in the field. They provide information on the actual security situation, help avoid high-risk areas and can negotiate safe passage or act as intermediaries in case of an attack. It is advisable to build relationships based on trust, respect, transparency and moral – and sometimes logistical – support.

Digital security and data protection

Why is digital security vital?

Digital security is vital because the consequences of failing to be vigilant in this regard are severe and sometimes irreversible. Technology is a double-edged sword that should be used wisely.

Example: A seized phone makes it easier to reveal the names of sources and puts their lives at risk. A hacked email account compromises an entire ongoing investigation. A video shared without protection allows a witness to be located – in just three clicks.

Basic rules for protecting your data

Action	Recommended tools
Messaging	Signal, not WhatsApp or Facebook Messenger
File sharing	Tresorit, Proton Drive, CryptPad
Browsing	VPN and a private browser (Brave, Tor)
Email	Proton Mail, not Gmail
Storage	Automatic encryption, strong password, 2FA enabled

Never use your personal phone during an investigation; use an ‘investigation’ device that is disconnected from your social media accounts.

Back up and protect evidence

Tips for saving and protecting evidence:

- >> Always keep two copies of evidence: one on site (e.g. on an SD card) and one in a secure cloud.
- >> Name files in a way that does not reveal the names of the sources.
- >> Never store sensitive video or audio files in your phone’s gallery.
- >> Disconnect devices during important meetings.

Example: After an investigation, a participant stored her photographs on Tresorit and deleted them from her phone. Even if the phone were confiscated, the data would be inaccessible.

Political pressure and psychological safety

Common pressures and threats

Common pressures and threats that have been documented include:

- >> interrogations without warrants;
- >> intimidation, including surveillance and anonymous phone calls;
- >> public discrediting through state- or corporate-linked media; and
- >> administrative investigations into tax ‘irregularities’ or legal status.

Tip: Always document your requests (e.g. letters, emails) and keep records of every interaction with the authorities.

Managing stress and emotional fatigue

Psychological safety is integral. An investigator is not a machine. They may be prone to fatigue, anxiety and paranoia. It is advisable to maintain good discipline and incorporate practices to manage stress and prevent burnout.

Best practices:

- >> Regular group debriefings after each mission.
- >> Scheduled rest periods.
- >> Emotional support among colleagues or from a psychologist.
- >> Information exchanges with other engaged civil society organizations.

Incident preparedness and response

Teams should establish clear protocols for responding to threats, arrests, data breaches or other incidents, ensuring rapid coordination and well-documented action.

How to respond to an incident

In the event of an incident, be prepared to respond swiftly and appropriately:

- >> **Assault or direct threat:** Withdraw immediately, notify the team and document the facts.
- >> **Interrogation or arrest:** Remain calm, demand a lawyer and contact the parent organization.
- >> **Seizure of equipment:** Have a backup phone and offline copies.

Useful protocol: A team member who is not in the field should maintain constant vigilance and be ready to alert embassies or partner NGOs.

In short, security is not optional: it determines the viability of the investigation, the protection of sources and the very survival of the team. By integrating a culture of physical, digital and emotional security, investigators become more effective, more resilient and better prepared to face the realities on the ground.

Analysis, information, processing, reporting

Module 7

A successful investigation is not measured solely by the quantity of information collected, but by how that data is processed, analyzed and utilized. Analysis gives meaning to the facts; reporting provides strategic significance to the work accomplished.

This module guides participants in:

- >> organizing data, including testimonies, documents, images and videos;
- >> verifying, cross-checking and validating sources;
- >> transforming raw information into clear, structured and actionable results; and
- >> producing reports tailored to specific audiences such as decision-makers, media, donors, communities and legal professionals.

It also emphasizes source protection, respect for the truth and rigour in presenting facts. Through simple tools such as tables, data sheets and report templates, this module strengthens the capacity of civil society organizations to produce credible and impactful investigations.

Organization and centralization of collected data

An investigation often involves cataloguing:

- >> various documents (audio, video, scanned papers, photographs, handwritten notes);
- >> various sources (interviews, OSINT, direct observations); and
- >> information that needs to be structured and verified.

To structure this data, consider developing tools such as:

- >> a structured spreadsheet for sorting data (e.g. Excel, LibreOffice, Airtable);
- >> a folder-based filing system for sources, photographs, recordings, official documents; and
- >> a consistent file naming convention (e.g. date_location_source_type).

Source classification and prioritization

Not all information is created equal. Sources must be classified according to their:

- >> origin (primary/secondary);
- >> level of reliability (verified, probable, questionable); and
- >> strategic value (direct evidence, context, illustration, narrative support).

Classification example

Source	Type	Reliability	Usefulness
Photograph of a convoy	Primary	High	Direct evidence
Testimony of a villager	Primary	Medium	Local context
Newspaper article	Secondary	Variable	Public illustration
Scanned official document	Elementary	High	Legal element

Analysis of facts and cross-referencing of data

Analysis does not consist of accumulating facts, but of connecting them to identify trends and key actors, map flows and networks (e.g. from an extraction site to export) and to demonstrate the transnational or organized nature of the crime. This can be done through:

- >> maps and flowcharts, including ‘actor mapping’;
- >> timelines;
- >> responsibility matrices (who does what, when); and
- >> geographic cross-referencing (e.g. location of operations vs location of authorization).

Fact-checking and verification

Before publication or any external use, it is necessary to:

- >> cross-reference at least two different sources for each major fact;
- >> verify the authenticity of documents (dates, signatures, stamps);
- >> confirm the location and timing of photographs or videos (metadata, OSINT); and
- >> identify areas of uncertainty and acknowledge them.

Tip: Verified information is better than a sensational but unsubstantiated revelation.

Writing a report or investigative dossier

Reporting depends on the target audience: decision-makers, journalists, the general public or legal partners, among others. A good general framework for a report may include:

1. Executive summary (1 page maximum)
2. Context and rationale
3. Methodology (fieldwork, OSINT, limitations, ethics)
4. Findings, impacts and analysis
5. Conclusions and recommendations
6. Appendices (evidence, key documents, photographs)

Adapt the language and presentation

The language and presentation of the collected information should be tailored to the target audience. For instance, you may choose to be:

- >> technical and legal for authorities or legal professionals;
- >> educational and visual for the general public; or
- >> concise and strategic for donors and partners.

Useful tools:

- >> Graphics (Datawrapper, Flourish, Canva)
- >> Maps (QGIS, Google Earth Pro)
- >> Timelines (TimelineJS)

Caution: Never publish identifying information without the consent of the individuals involved (faces, names, exact locations).

Preparing a responsible publication

Responsible publication requires balancing accuracy, fairness and risk mitigation. When appropriate and feasible, researchers should provide named individuals or entities with an opportunity to respond to the relevant findings, allowing sufficient time for engagement prior to publication. This process should be guided by a context-specific risk assessment, as in some cases, contacting subjects may increase risk to researchers or sources, jeopardize the integrity of the investigation or simply be unfeasible.

When reaching out to individuals or entities, use language that is cautious and measured. Avoid making accusations. Instead, ask questions that will help you confirm the information you already have and that will potentially lead the respondent to provide further information. You should be careful to protect your confidential sources; you are not obligated to reveal your sources when requesting a response.

When responses are received, they should be accurately reflected in the publication. At times, it may be appropriate to note that attempts to seek comment were made but that no response was obtained.

Overall, decisions around engagement and publication should prioritize doing no harm, protecting sources and safeguarding research integrity.

Share the results strategically

The types of dissemination channels to consider may include:

- >> a report sent directly to decision-makers;
- >> an article published in a partner media outlet;
- >> an infographic or excerpt shared on social media;
- >> a press conference or webinar; or
- >> a publication on a regional platform (e.g. Central African Forest Commission – COMIFAC, observatories).

Channels for distributing reports or findings



Anticipate reactions and ensure follow-up

A published report can shift the status quo by sparking reforms or judicial investigations; provoke retaliation against the civil society organization, sources or partners; or generate requests for evidence or challenges.

It is therefore necessary to plan:

- >> a response strategy in the event of controversy or attacks;
- >> a post-publication monitoring system; and
- >> an approach to follow up on recommendations (see Module 9).

In short, how information is handled is what gives an investigation its shape, strength and credibility. Without rigour, information is lost; without strategy, it fades away; without ethics, it turns against you.

Advocacy and communication

Module 8

Advocacy is what enables an investigation to generate concrete change. It can transform the collected data into community mobilization, constructive pressure on decision-makers or public policy reform. Communication, for its part, serves to make the invisible visible, to inform, raise awareness and rally support.

Even the most rigorous investigation will only have an impact if it is translated into strategic advocacy action. In a context where authorities regularly turn a blind eye, companies lack transparency and communities have little voice in the public sphere, advocacy is the primary tool of civil society organizations. Advocacy is not 'complaining'; it is:

- >> documenting a problem;
- >> identifying the right levers of influence;
- >> mobilizing allies; and
- >> convincing decision-makers to act.

In this module, civil society organizations and partners will learn to:

- >> define a clear, targeted and measurable advocacy strategy;
- >> identify and engage the right stakeholders, including authorities, journalists, legal professionals and community allies;
- >> develop messages tailored to different audiences;
- >> prepare and launch strategic media campaigns locally, nationally and digitally; and
- >> anticipate the risks associated with speaking out publicly, including reprisals.

Through planning frameworks, message templates and media kits, this module provides the tools to make a real impact and turn every investigation into a lever of influence in the service of justice.

Differences between advocacy and communication

Advocacy	Communication
Aims for lasting change: law, policy, behaviour	Aims for visibility and awareness
Targets decision-makers and institutions	Targets the general public and grassroots citizens
Based on evidence, facts or legal arguments	May include emotional narratives or slogans

Advocacy and communication are complementary: well-thought-out communication supports advocacy by mobilizing public opinion.

Key steps for building an advocacy strategy

To build a robust advocacy strategy, you must:

- >> **Confirm the objective:** What specific change are you aiming for?
- >> **Identify the targets:** Who has the power to bring about change?
- >> **Develop the message:** What information will move the targets to implement change?
- >> **Choose channels of influence:** For instance, face-to-face meetings, official letters, petitions, media campaigns, radio or television coverage, online press, alliances with civil society organizations or symbolic actions. How can the message be delivered most effectively?

Steps in developing an advocacy strategy



Mobilize allies and build coalitions

Isolated advocacy carries little weight. It is advisable to:

- >> identify other affected or engaged organizations;
- >> pool resources such as reports, contacts, translators or airtime;
- >> establish common goals with differentiated roles; and
- >> align regional strategies.

Example: An investigation in Gabon helped mobilize civil society organizations to produce a joint advocacy brief.

Use the media wisely

Journalists act as amplifiers, but they have their own logic and goals. It is therefore advisable to:

- >> create a concise, well-sourced press kit;
- >> build trusting relationships with committed journalists;
- >> prepare trained and protected spokespersons; and
- >> implement an embargo, meaning a coordinated release between civil society organizations and the media.

Avoid:

- >> sharing unprotected sensitive data;
- >> making accusations without evidence and thus risking a defamation lawsuit; and
- >> relying too heavily on media ‘buzz’ without a follow-up plan.

Creating an effective communication campaign

Creating an effective communication campaign involves identifying:

- >> **The targets:** The general public, young people, the diaspora or consumers.
- >> **The tools:** Short explanatory videos (e.g. voice-over and images), anonymized testimonials, interactive maps and infographics.
- >> **The approach:** Coordinated social media campaigns with hashtags, visuals and local influencers.

Tip: Combining human stories with statistics makes the report or campaign more memorable and engaging.

Follow-up and sustained pressure

Once the report or campaign is launched, the next steps are to:

- >> regularly follow up with authorities;
- >> update the case file based on positive or negative feedback;
- >> monitor the media, social networks and political forums; and
- >> organize a press briefing or an update webinar 1 or 2 months after the campaign launch.

Dealing with retaliation and protecting spokespersons

Advocacy can be disruptive; you should therefore:

- >> prepare legal responses in case of an attack;
- >> document any form of threat or harassment;
- >> protect whistle-blowers and investigators (see Module 6); and
- >> report attacks to international networks for support.

Ultimately, successful advocacy involves a well-thought-out investigation, a clear message, a carefully chosen channel and strong allies. It can transform a written report into a political turning point, the protection of an ecosystem or the recognition of community rights.

Monitoring and evaluation

Module 9

Monitoring and evaluation (M&E) are often overlooked in investigative processes, yet they are essential for measuring real impact, adjusting approaches and strengthening the credibility of civil society organizations over time. They help determine whether an investigation was useful, what it achieved and how to improve future initiatives.

An investigation or advocacy effort cannot be limited to a single publication or one-off event. Real change – whether legal, political, ecological or community-based – is built over time.

M&E allows you to:

- >> measure the concrete effects of the initiative, including results, reforms and reactions;
- >> learn from successes and mistakes;
- >> improve future investigations and strategies; and
- >> strengthen the legitimacy and transparency of civil society organizations in the eyes of partners, donors and communities.

This module equips teams to:

- >> conduct structured post-investigation follow-up regarding reactions, effects and outcomes;
- >> identify realistic indicators of success, whether institutional, community-based or media-related;
- >> organize internal and community feedback sessions;
- >> maintain a learning journal to reflect on successes and mistakes; and
- >> build a collective record of action to support accountability, organizational strengthening and advocacy.

This module reinforces the sustainability of investigations by embedding them within a framework of continuous improvement, collective learning and strategic resilience.

Integrate M&E from the planning phase onward

M&E cannot be improvised at the end. It must be planned before the investigation even begins to ensure that it aligns with the initial objectives.

Example: If the objective is to secure the suspension of a mining or forestry permit, monitoring will involve verifying whether an administrative measure has been taken, within what timeframe and with what impact.

Defining M&E indicators

Indicators of success should be established early on and should align with the initial objectives.

Quantitative indicators

- >> Number of documents collected/verified
- >> Number of sources consulted
- >> Number of publications distributed
- >> Number of meetings held with authorities
- >> Number of shares and views
- >> Number of media outlets covering the project or number of articles published

Qualitative indicators

- >> Level of community engagement
- >> Level of response or reaction from authorities
- >> Quality of dialogue with journalists or partners
- >> Perceived reliability of the information by stakeholders
- >> Perceived influence on the development of a policy or law

Structure post-investigation or post-campaign follow-up

Create a follow-up sheet that considers:

- >> actions taken: survey, publication, advocacy;
- >> targeted parties: government agencies, companies, civil society organizations;
- >> reactions received: official responses, silence, intimidation;
- >> corrective actions taken: meetings, follow-up, rebuttals;
- >> observed effects: positive or negative.

Keep this form updated for 3 to 6 months after the report's release.

Organize internal debriefings

After each assignment or action, it is advisable to:

- >> organize a structured team meeting to discuss what worked and what did not;
- >> listen to feedback, including regarding emotional and psychological impacts;
- >> review safety, ethical and reliability issues; and
- >> gather ideas for methodological improvements.

Example: If a local fixer has been threatened, consider better anonymizing data in the future or strengthening organizational protection for these individuals.

Involve communities in the evaluation

Communities are not merely sources or targets. They must also be beneficiaries and evaluators. To ensure collaborative M&E, conduct community feedback sessions to assess what impacts have been observed; readjust organizational priorities based on their feedback. These sessions should be tailored to the specific communities in terms of language, format and channel.

Example: A survey on illicit arms trafficking may reveal that the main concern of the affected community is not solely the circulation of arms, but the resulting increase in robberies, kidnappings or clashes between armed groups. Communities may also identify specific areas – markets, secondary roads or isolated villages – where the presence of weapons creates a particularly acute sense of insecurity. This feedback can then guide future investigations towards the locations and dynamics that most directly affect the safety of local populations.

Assessing long-term effects

Different types of impact may unfold over different timelines.

Short term

- >> Media responses
- >> Responses from authorities

Medium term

- >> Changes in local practices
- >> Regional shifts
- >> Language or terminology adoption

Long term

- >> Policy reform
- >> Case law establishment
- >> Institutional transformation

Recommendation: Schedule an evaluation after 6 or 12 months to measure the profound effects, including those that are not immediately apparent.

Highlight the results and lessons learned

In order to best identify the results of the investigation and the lessons that have been learned:

- >> prepare internal evaluation reports;
- >> share lessons learned with other civil society organizations;
- >> create an internal database of cases, successes and obstacles; and
- >> leverage this knowledge to train new teams.

Appendix 1: Survey plan (template)

1. Background and objective

Survey title: _____

Background: _____

Main objective (SMART): _____

Central question: _____

2. Information already collected (preparatory phase)

Sources and data identified by type of information (primary and secondary sources):

Key observations/notes:

3. Hypotheses and avenues for further investigation

Main hypotheses:

1. _____
2. _____
3. _____

Serious avenues to explore:

1. _____
2. _____
3. _____

4. Data collection techniques

Interviews

Interviewees: _____

Key questions: _____

Monitoring method: ☐ Notes ☐ Recording ☐ Other: _____

Direct observation

Sites to observe: _____

Details to record: ☐ Name tags, logos, uniforms ☐ Activities ☐ Other: _____

Equipment needed: _____

Documentation and evidence

Type of documents: _____

Collection methods: _____

Security: ☐ Scanner ☐ Backup ☐ Secure storage

OSINT

Tools and platforms: _____

Feeds to monitor: _____

Verification method: _____

5. Logistics and planning

Team and responsibilities: _____

Budget and resources: _____

Timeline/milestones: _____

Risks: _____

Security: ☐ On-site ☐ Digital ☐ Other: _____

6. Risk mitigation and crisis management

Crisis mitigation

Potential risks identified: _____

Planned mitigation measures: _____

Crisis management plan

Emergencies: _____

Alert procedure: _____

Internal/external communication: _____

Appendix 2: Consent form for sources

To be completed before or after an interview, depending on the level of sensitivity. To be adapted according to the local language or oral tradition.

Informed consent form

Survey on organized crime and armed violence

Date of interview: ____/____/____

Location: _____

Name or alias of the person (optional): _____

Purpose of the interview

I hereby declare that I have been informed that this interview is part of a citizen survey concerning phenomena related to organized crime and/or armed violence observed in my locality, community or region. This interview aims to gather information, observations or testimonies that may contribute to a better understanding of these phenomena and their impact on the population.

Intended use of the information

The information I provide may be:

- >> used anonymously in analyses, reports or research documents, without mentioning my name or any details that could identify me;
- >> cited, in whole or in part, in publications or presentations, only with my explicit consent;
- >> used in the context of awareness-raising, advocacy or information-sharing efforts with relevant organizations, public institutions or the media, in compliance with confidentiality and security rules.

Recording

Regarding the recording of the interview:

- ☐ I authorize the audio recording of my statements.
- ☐ I do not consent to the recording, but I agree that the interviewer may take notes during the interview.

Confidentiality and security

I understand that:

- >> my safety, anonymity and the confidentiality of the information provided will be respected at all times;
- >> I may refuse to answer certain questions;
- >> I may interrupt the interview or withdraw my statement at any time, without having to provide a reason;
- >> the investigator agrees not to use my statements outside the context described here without my consent.

Signature of the witness or recorded verbal consent:

Signature/verbal statement: _____

Investigator's name: _____ Investigator's signature: _____

Appendix 3: Sample letter for a formal or community complaint

[Place], on ____ / ____ / _____

To the attention of the [public prosecutor/regional delegate/district chief]

[Insert the competent institution]

Subject: Complaint regarding alleged organized crime and related criminal activities

Dear Sir/Madam,

We, the undersigned [name of organization/community representatives/affected individuals], respectfully bring to your attention serious incidents that may constitute organized crime and that affect public safety and order in the locality of _____.

Information gathered through field observations, testimonies and documentary evidence suggests the existence of activities that may constitute, in particular:

- >> illicit trafficking (of weapons, goods or other prohibited items) in the area of _____;
- >> acts of violence, intimidation or extortion targeting members of local communities;
- >> the alleged involvement of a structured network or individuals acting in an organized manner to facilitate or conceal these activities;
- >> direct consequences for the safety of the population, the functioning of local economic activities and the stability of the area concerned.

Preliminary information (testimonies, observations, documents, photographs or other available evidence) is attached to this correspondence to support these reports.

In light of the gravity of these facts, we respectfully request that your high authority:

1. Open a judicial investigation to verify the reported facts and identify the individuals involved.
2. Adopt appropriate measures to prevent the continuation of these criminal activities in the affected area.
3. Protect witnesses and community members who may be at risk due to their cooperation with the authorities.
4. Strictly enforce existing legal provisions to ensure the safety of the population and respect for the rule of law.

We remain, of course, at the disposal of the competent authorities for any additional information that may assist in establishing the facts.

We look forward to your prompt attention to this matter and remain, Sir/Madam, with our highest regards.

Name and title of signatory: _____

Organization/community represented: _____

Contact information: _____

Appendix 4: Sample letter to local authorities to report concerns or request a meeting

[Place], on ____ / ____ / _____

To the attention of the [mayor/sub-prefect/district delegate] [City/town]

Subject: Request for a meeting to report concerns regarding activities suspected of being related to organized crime in the town of [xxx]

Dear Sir/Madam,

We are writing to respectfully bring to your attention a concerning situation that has been observed in our community for several weeks and may be linked to organized crime or related violence.

Indeed, several incidents reported by residents and observed in the area of [specify the locality or neighbourhood] are causing serious concern among the population, notably:

- >> the recurring presence of armed or unidentified individuals or groups in certain areas;
- >> unusual movements of people, vehicles or goods that may suggest illicit activities (trafficking, extortion, circulation of weapons or other criminal practices);
- >> acts of intimidation, threats or insecurity affecting residents and disrupting the community's economic and social activities.

In the spirit of civic responsibility and dialogue and to prevent tension, we would like to discuss these concerns with the relevant administrative authorities.

To this end, we respectfully request:

1. The organization of a meeting with you and/or your staff to present in greater detail the concerns expressed by the community.
2. An investigation into the reported facts by the relevant authorities to verify the nature of the observed activities and, if necessary, to provide appropriate responses.
3. The implementation of preventive and consultative measures aimed at strengthening security and trust between the authorities and local residents.

Our approach is part of a commitment to constructive cooperation with the authorities, in order to contribute to the preservation of public safety, social cohesion and the rule of law in our region.

Thank you for your consideration of this request.

Sincerely,

Name and title of signatory: _____

Organization/community represented: _____

Contact information: _____

Appendix 5: Useful apps and platforms

Tools and platforms	Recommended use
Advanced Google Search	Search by site, date, language and keywords.
Wayback Machine	View the history of modified and deleted pages; archive live web pages.
Google Earth, Sentinel Hub, OpenStreetMap	Track changes in an area over time; review maps.
Open Corporates, Societe.com, Orbis	Research companies and their executives.
Maltego, Aleph	Map connections between individuals, companies and locations.
Social Searcher, TweetDeck	Search for geolocated posts or key data sets.
Intelligence X	Search databases, internal documents and leaks.
CITES, Forest Trends, Environmental Investigation Agency, TRAFFIC, other environmental databases	Access data on trade statistics, wildlife, timber, sanctions.
Signal	Communicate securely.
Tresorit	Store and share files securely.

Resources

There are a wealth of resources available on how to plan and conduct investigations. We have included just a few to help get you started.

Planning

KoboToolbox. Mobile survey platform for humanitarian contexts or areas with limited connectivity.

Security In-a-Box. Ethical and security tools for field investigators.

Front Line Defenders. Facilitation manual on risk analysis and protection planning for human rights defenders.

Journalism 101 Toolkit. Resources, tip sheets and guides for writing, editing, reporting and interviewing from the International Center for Journalists.

Datawrapper. Free tool to visualize data and create tables and graphics.

Namati. What do we know about legal empowerment? Mapping the evidence.

Monitoring and Evaluation. Resources and tools from ALNAP to support humanitarian M&E.

Writing with Libel in Mind. A guide for non-profits and bloggers on what libel is and how to avoid it.

OSINT Safety. Bellingcat resources for safety in OSINT research.

Journalism Resource Center. More than 2 000 items in 14 languages – from tip sheets and guides to instructional videos from the Global Investigative Journalism Network.

OSINT Research Guides. Bellingcat guidance on various digital investigation techniques and tools.

Resilient Fund Security Modules. Practical training on risk assessment, digital security, mission planning and incident response.

Ethics, security and methodology

GI-TOC: Approach and Ethics (Network of Experts). Ethical standards for researchers and experts that emphasize integrity, professionalism and the protection of sources.

Investigation and research

OCCRP ID. A service that helps investigative journalists in the Organized Crime and Corruption Reporting Project network conduct research quickly and effectively.

OCCRP Aleph. A vast archive of current and historic databases, documents, leaks and investigations.

World Bank Open Data. A compilation of high-quality and internationally comparable statistics.

UNODC Data Portal. Topical data and statistics from the UN Office on Drugs and Crime.

Offshore Leaks Database. A database from the International Consortium of Investigative Journalists of more than 810 000 offshore companies, foundations and trusts from the Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers and Offshore Leaks investigations.

