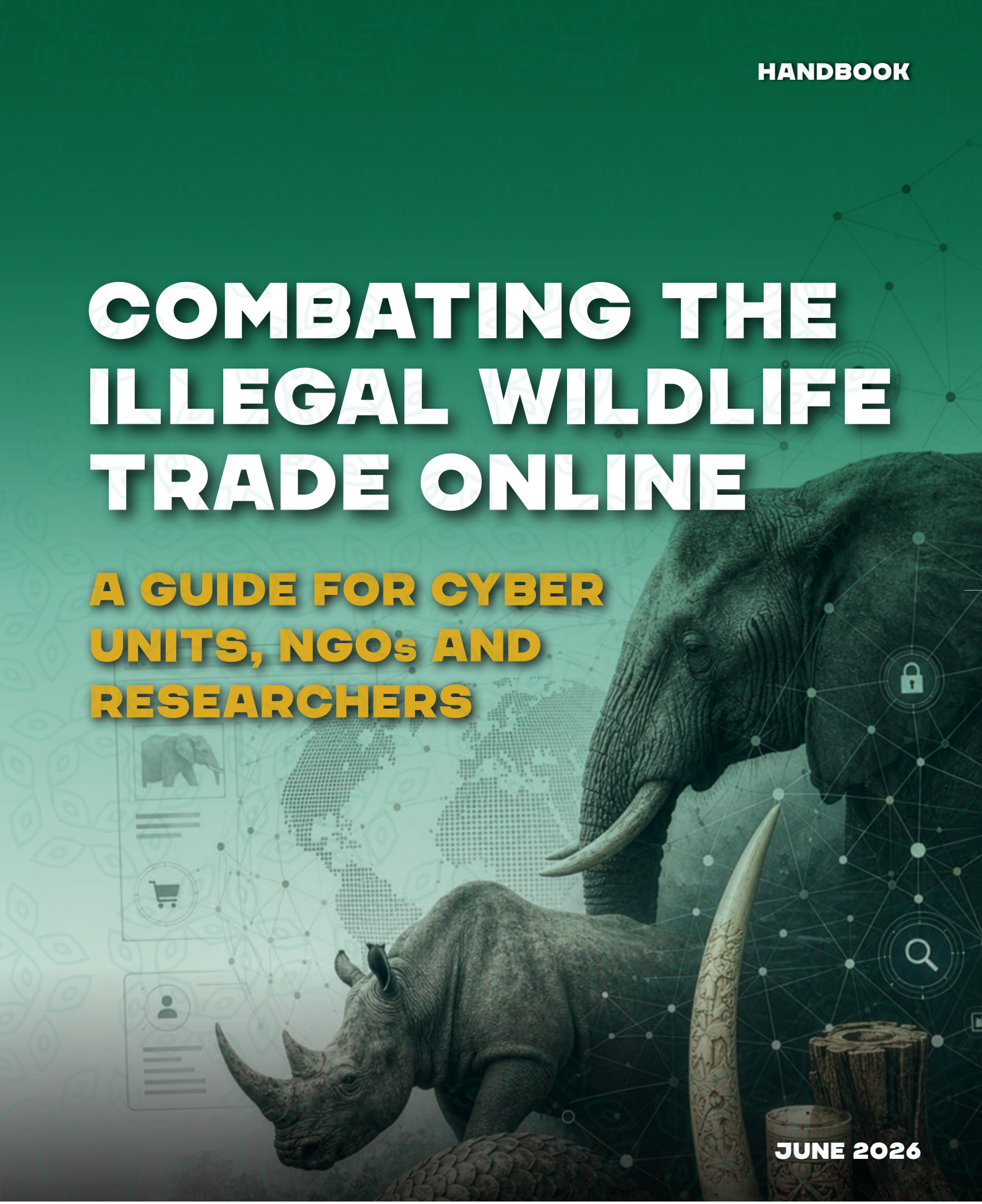
HANDBOOK

COMBATING THE ILLEGAL WILDLIFE TRADE ONLINE

A GUIDE FOR CYBER UNITS, NGOs AND RESEARCHERS



JUNE 2026

ECO SOLVE
GI-TOC
GIFP
Global Illicit Flows Programme
Funded by the European Union

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the organizations and individuals who contributed to discussions, shared technical insights and provided input into our Data Interoperability Working Group. These contributions helped shape and refine the best practices set out in this document. Their experiences and feedback were valuable in strengthening the practical relevance, clarity and applicability of the guidance. We also thank representatives from the Environmental Investigation Agency, TRAFFIC, the African Conservation Centre, the Royal Botanic Gardens – Kew, CITES, Freeland, the Wildlife Trust of India, the International Fund for Animal Welfare, Education for Nature Vietnam, ADM Capital Foundation, the World Wide Fund for Nature, the World Parrot Trust, the French Gendarmerie and the Asia for Animals Social Media Animal Cruelty Coalition. In particular, we acknowledge the contributions and engagement of Melanie Butler, Martina Aerne, Shaliza Malik, Edwin Pickard, Martin Page, Dan Stiles, Antony Bagott, Sharon Baruch-Mordo, David Whitehead, Onkuri Majumdar, Debobroto Sircar, Deeya Bhattacharjee, Eugénie Pimont, Doug Hendrie, Sam Inglis, Jayasri Srikantan Lakshminarayanan, Rowan Martin, Stephanie Leterme, Jean-Baptiste Munoz, Nicola O'Brien, Stephanie Pendry, Melanie Heath and Dominique Prinsloo. This acknowledgement does not imply that the individuals or organizations listed endorse all of the contents, recommendations or conclusions of this document. Any errors, omissions or interpretations remain the responsibility of the authors.

Cover based on an image created using ChatGPT Images 2.0

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

CONTENTS

INTRODUCTION ... 2

OBJECTIVE, SCOPE AND METHODOLOGY ... 4

Geographic focus ... 5

Priority species and products ... 5

Platform and market selection ... 6

Data types and methodology ... 7

Tolerance for uncertainty and success metrics... 8

DATA COLLECTION AND MANAGEMENT ... 9

Manual and passive monitoring ... 9

Automated and assisted monitoring ... 13

INTELLIGENCE GATHERING AND OSINT ... 16

Verification and enrichment ... 17

LAW ENFORCEMENT ENGAGEMENT AND PARTNERSHIPS ... 18

Data sharing, sanitization and legality ... 19

THE SHIFTING LANDSCAPE ... 20

APPENDIX: GLOBAL DATA MODEL ... 21

INTRODUCTION

The illegal wildlife trade (IWT) is one of the world's most lucrative criminal activities, and a growing share of it happens online. Traffickers use social media, e-commerce platforms, messaging apps and other digital channels to advertise and sell live animals and wildlife products. This harms biodiversity and animal welfare, and can increase the risk of zoonotic diseases.

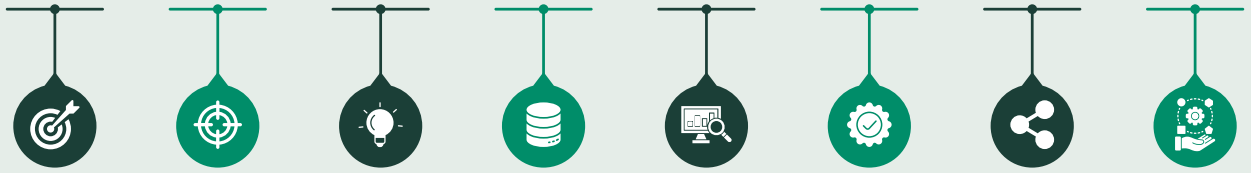
This guide responds to this threat by helping legitimate agencies and organizations move from ad hoc online searching to structured, accountable and comparable monitoring of online IWT. The guide's value lies in providing a practical framework for setting objectives, prioritizing species and platforms, managing data, applying safeguards and sharing intelligence responsibly. It is intended for agencies and organizations mandated to combat wildlife crime, including cyber units, wildlife authorities, customs, police, NGOs and research partners. The goal is to help them design and run effective online monitoring regimens in their countries or regions.

To reduce the risk of misuse, the guide stays at the level of governance, prioritization, data standards, analytical workflow and responsible intelligence sharing. It deliberately avoids operationally sensitive detail, such as platform-specific detection methods, covert engagement tactics, or information that could help offenders identify monitoring thresholds or evade law enforcement. The focus is on helping legitimate actors generate insights that support enforcement and policy.

Combating the illegal wildlife trade online

A framework for lawful, structured, interoperable online monitoring

Objective > Scope > Data model > Collection > Monitoring > Verification > Sharing > Adaptation



USE THE FRAMEWORK ITERATIVELY: DEFINE THE PURPOSE, CHOOSE A REALISTIC SCOPE, STANDARDIZE WHAT YOU COLLECT, VERIFY WHAT MATTERS, AND SHARE ONLY WHAT IS LAWFUL AND USEFUL.

1. DEFINE THE OBJECTIVE

Be explicit about what decisions the monitoring must support: investigative leads, market mapping, trend analysis, platform engagement or policy reform.

2. SET THE SCOPE

Choose the geography, priority species or products, platforms, and the level of certainty needed. Start broad, then explore, pilot and refine.

3. STANDARDIZE THE DATA MODEL

Use common fields and formats for record IDs, dates, locations, species names, prices, quantities, confidence and legal-risk coding.

4. CHOOSE THE COLLECTION MODEL

Match methods to purpose: manual monitoring, assisted searches, alerts, automation and secure data management with audit trails.

5. RUN ADAPTIVE MONITORING

Search in local languages, use platform-specific methods, capture evidence consistently and classify risk carefully with regular quality assurance.

6. SCALE CAREFULLY WITH TECHNOLOGY

Use alerts, APIs, web scraping, classifiers, dashboards, and case tools to extend reach, but keep humans in charge of judgement.

7. VERIFY AND ENRICH

Apply structured OSINT, translation, cross-reference checks, and lawful geolocation to strengthen findings before escalation or sharing.

8. SHARE RESPONSIBLY AND ADAPT

Use legal review, privacy safeguards, minimization, partner protocols and regular updates as markets, platforms and tactics change.

CROSS-CUTTING RULES

• Operationally useful and risk assessed • Interoperable data structures • Human-reviewed decisions •
• Secure and privacy aware • Iterative and adaptive •

EXPECTED OUTPUTS

Actionable leads
Referrals, cases, target packages

Market intelligence
Species, routes, sellers, patterns

Trend evidence
Volume, price, displacement, seasonality

Platform and policy input
Engagement, reform, governance

OBJECTIVE, SCOPE AND METHODOLOGY

Before collecting any data, start by defining the objective of the monitoring. Be explicit about what you need the information for and what decisions it should support, because that objective should drive the scope, methods and data fields you choose.

- **The objective may be operational, strategic, analytical or mixed** – Common examples include generating investigative leads, mapping actors and markets, tracking trends in species or product availability, assessing displacement of an illicit market after an intervention, supporting policy reform, or documenting platform misuse to assist advocacy and engagement.
- **Once the objective is clear, define the scope and methodology around it** – Which geographic areas and platforms you will focus on, which species or products you will prioritize, what data fields you will capture, and what level of certainty you need for later use.
- **The appendix outlines a Global Data Model for online IWT monitoring** – Selecting a subset of fields relevant to project goals while using similar formats enables comparison and data sharing across initiatives.
- **A good scoping process is usually iterative** – Begin with a short exploratory phase to understand where activity appears, then pilot a draft method, review its outputs and blind spots, and only then lock in a routine monitoring design.

Geographic focus

Decide whether you will monitor globally, regionally, along specific trade routes, or within countries, hotspots or platform-based communities. Geographic focus should reflect the objective of the work, not simply the nominal origin of a website, because many of the online platforms used in IWT serve transnational markets.

- Are you primarily tracking trends and demand?
- Are you trying to identify and remove or de-platform illegal content?
- Are you building actionable intelligence packages for law enforcement?

In practice, geographic relevance can often be inferred from a combination of signals such as seller language, stated location, shipping options, currencies, phone area codes, time zone patterns, delivery claims, trade route references and repeated seller behaviour. Most projects start with a country, corridor or market segment and expand later, but it can also be valid to focus on blind spots where monitoring is weak or absent.

Priority species and products

In cases where resources are limited, it is best to establish a shortlist of priority species or product types. Priority-setting should balance conservation urgency, enforcement relevance and the practical likelihood that the species or product can be identified and assessed online with enough confidence to make monitoring useful. Criteria can include:

- **Conservation status and vulnerability to trade pressure** – Endangered and Critically Endangered species on the International Union for Conservation of Nature (IUCN) Red List of Threatened Species often deserve high attention, but a less endangered species may still face acute pressure from trade, have a restricted range, or be heavily affected by collection from the wild.
- **International protection** – Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) listings (especially Appendix I, but also high-risk Appendix II species) indicate where international trade is banned or tightly regulated.
- **National laws and permitting regimes** – Consider species protected by national legislation, species requiring permits that are rarely issued for commercial trade, and species subject to different levels of protection, such as fully protected, conditionally tradeable, or legal only with demonstrable lawful origin.
- **Enforcement priorities and crime links** – Species commonly traded by organized crime networks, money laundering, corruption or other priority offences, or products that syndicates rely on financially.
- **Online detectability and identifiability** – Prioritize species or products that can realistically be detected and interpreted online, considering visual ambiguity, lookalike species, whether products are processed or mixed, and whether the listing shows the product directly or declares it only in text.

A simple weighted scoring system across these criteria can help rank species or product groups. For example, the system below is used by analysts as part of the initial scoping exercise to prioritize species monitoring priorities for the ECO-SOLVE Global Monitoring System (GMS). The GMS uses open-source intelligence (OSINT) and artificial intelligence (AI) to track, analyze and disrupt illicit wildlife markets on social media and e-commerce platforms (Figure 1).

CRITERION	SCORE RANGE	DESCRIPTION
Legislative protection	**0–3**	Score is based on both international and national protections. **(3)** = The species is protected under CITES Appendix I and has a national trade ban/protection; **(2)** = It meets only one of these criteria (or if protected under CITES Appendix II with significant law enforcement rationale) and/or permit-based trade; **(1)** = General protections or legal-origin requirements; **(0)** = None.
Expert-identified concern	**0–2**	**(2)** = Strong evidence of emerging threat or conservation concern; **(1)** = Some concern but insufficient data; **(0)** = No flagged issues. Expert review ensures species of potential concern are not excluded due to limited monitoring.
Enforcement priority	**0–3**	**(3)** = High (organized crime link); **(2)** = Medium (significant trafficking); **(1)** = Low; **(0)** = Not identified as a priority.
Trade relevance (global/local)	**0–2**	**(2)** = High relevance in global and local markets; **(1)** = Medium relevance (either global or local); **(0)** = Low relevance. For species traded primarily for traditional medicine, cultural purposes or bushmeat, classify as local unless there is significant international demand.
Ecological impact	**0–2**	**(2)** = Critical Endangered/Keystone; **(1)** = Vulnerable; **(0)** = Least Concern.

FIGURE 1 The ECO-SOLVE/GMS Rapid Species Basket Review scoring system.

NOTE: Species scoring 8 or more are kept, those scoring 6–7 are considered through an internal expert vote, and those scoring 5 or less are automatically disqualified.

Platform and market selection

Compile an initial longlist of platforms and channels by reviewing reports, scientific papers, seizure cases and the following:

- Mainstream social media (e.g. Facebook, Instagram, TikTok)
- E-commerce and classifieds platforms
- B2B and auction sites
- Forums and niche hobby platforms.
- Messaging apps (e.g. WhatsApp, Telegram)
- Dark web or closed sites where appropriate and legally possible

Then, run a short exploratory phase across the longlist to identify which species, platforms, countries and trade behaviours appear. Use the findings to build a draft routine methodology, pilot it (including the time and resources required for routine data collection), review what it misses, then refine a shortlist of priority platforms, search terms and target taxa. Keep a flexible 'bycatch' field so analysts can still record relevant species or products outside the core scope and detect changes in illicit markets.

Data types and methodology

Decide how you will collect data and which Global Data Model fields you need (see the appendix). The field set should follow the objective of the project, but maintaining a common core across projects improves comparability. Across project types, it is useful to distinguish between directly observed, seller-declared, inferred and estimated information, and to record confidence where relevant.

- **For trend monitoring** – you will probably record platform, URL or post ID, date/time, species, product type, quantities, price, language, search terms used, and relevant descriptive text that may help interpret market narratives, such as provenance claims, wild-sourced language, rarity claims or quality cues.
- **For online advertisement monitoring for enforcement** – you will probably record platform, URL or post ID, date/time, species, product type, quantities, price, language, seller handle, contact details where lawfully collected, the basis for the species identification, provenance claims where stated, and reason codes for suspected illegality.

Use consistent formats:

- **Standardized species names** – scientific names, including synonyms or past classifications where relevant for searching; common names, with a controlled vocabulary for vernacular names, aliases and spelling variants; one preferred reporting name per species, but broader synonym lists for search and matching.
- **ISO 8601 dates and times** (with time zone or Coordinated Universal Time [UTC]) – one for date/time of the post; one for data entry date/time (they are typically not the same).
- **Structured location data** (country code, admin levels [level 0 = country, level 1 = state/province, level 2 = district/commune]), including coordinates where possible (in EPSG:4326 longitude/latitude format).
- **A unique record ID** for each post or incident (with a standard ID format – e.g. mmddYYYY_HHMM_Spp_Analyst Initials). These can often be autogenerated in data collection tools.

Tolerance for uncertainty and success metrics

Your objective determines the depth of data you need and your tolerance for uncertainty.

- Intelligence mapping and exploratory monitoring often benefit from recording a wider set of lower-confidence signals, provided they are clearly labelled as such.
- Operational referrals, enforcement packages, and legal follow-up usually require stronger verification, fuller metadata and more cautious interpretation.
- For some regulated species or products, illegality cannot be determined confidently from online material alone. In such cases, it is often better to code the record as possibly legal, probably illegal, unclear, or as a level of concern or risk, rather than forcing a false binary.

Define success metrics early. They should reflect the objective of the project and may include:

- the number of actionable leads generated, according to an internally defined referral threshold;
- the number of advertisements detected, screened and analyzed in depth, to show monitoring coverage and analytical effort;
- changes in volume, price, seller behaviour or distribution of online listings over time; and
- the number of platforms engaged, policy changes influenced, or other intervention-related outcomes where relevant.

DATA COLLECTION AND MANAGEMENT

Once scope is defined, you need a data collection strategy that matches it. Monitoring programmes may combine automated collection with human verification, human-led collection and secure data management.

Ensure that data is stored and managed properly:

- Use a database or structured spreadsheet that follows the Global Data Model fields and relies on dropdown lists or other controlled inputs wherever possible, so that entry is faster, cleaner and easier to analyze.
- Log key metadata (e.g. URL, platform, date/time collected, collector, collection method, editor name, edit notes, edit date/time, reviewer name, review date/time).
- Tag records with simple indicators if necessary (e.g. priority level, suspected illegality, relevant species group).
- Secure the database (access control, encryption where appropriate) and maintain backups.
- Keep an audit trail to support later analysis and any evidentiary needs.

Manual and passive monitoring

Manual and passive monitoring should help authorized agencies, NGOs and research teams collect information in a structured, lawful and accountable way, while remaining flexible enough to adapt to changing online trade patterns.

Data collection techniques

Teams should create a structured but adaptive monitoring routine that defines what will be checked while allowing enough flexibility to detect changes in trader behaviour.

- Decide which platforms, species and markets are checked, but vary timing and search terms so the routine does not become blind to temporal shifts in trader behaviour.
- Employ 'snowball sampling' methods where possible by using known wildlife selling accounts and their network of social contacts and groups to identify others.
- Sequence tasks (e.g. social media → classifieds → seizure/news scan).

Structured and consistent monitoring reduces effort bias by ensuring that analysts search comparable platforms, species, keywords and time periods, rather than only capturing the most visible or easily found content. This makes analyses of online IWT more reliable across countries, platforms, taxa and time periods.

- Analyze and document key findings on top of data.
- For each platform, keep a live document describing how to search, what typical red flags look like, how to capture evidence, and where species or product identification is especially difficult. For difficult taxa or processed commodities, include access to subject-matter guidance or image/product identification guides so analysts know what can and cannot be inferred confidently from online material.
- Update the live document whenever new tactics, platforms, slang or concealment methods appear, and feed urgent changes into intelligence sharing or operational briefings in near real time, where appropriate.
- Synthesize this live document into a briefing document for various time periods (e.g. bi-monthly or seasonally) to construct a record of changes in trends in species, sales volumes, coded language or other key factors.

Design smart search terms

- Search terms should be targeted, manageable and regularly refined, because a smaller set of well-designed searches is usually more useful than a large volume of poorly focused results. Build keyword sets for each priority species or product: scientific names, common names, local names, synonyms, key product words (horn, scales, skins, trophies, medicine) and sales terms ('for sale', 'available', 'delivery'). Keep search lexicons manageable and iteratively refine them based on what previous search rounds returned.
- Use Boolean operators (simple words such as 'AND', 'NOT' and 'OR' to combine or exclude keywords) and simple 'dorking' strings (quotes for exact phrases, 'OR' for synonyms, minus to exclude, site: for platform scoping).
- Maintain an internal spreadsheet of slang, emojis, misspellings and evasive phrases that appear repeatedly in suspicious contexts, and use iterative searches that add newly validated terms from previous rounds of monitoring and analysis.

Work in local languages

Analysts should not rely only on English. Search planning and data recording should be able to accommodate all relevant languages, including character-based scripts used in the market being monitored (e.g. sellers may be domestic in Spanish-speaking countries, but target consumers may be Chinese-speaking, so search terms in both languages would be necessary).

- Build keyword sets in the main local languages and relevant dialects.
- Use native speakers or trusted local partners to refine terminology; use machine translation mainly to interpret content.
- Include English where relevant for export-oriented offers, but treat it as a secondary layer on top of local language monitoring.

Read each platform on its own terms

Monitoring techniques should be adapted to how each platform works, since sellers use different behaviours, categories and visibility settings across social media, e-commerce sites, classified platforms and messaging apps.

- On social media, focus on group/page names, hashtags, recent posts, and comments under popular content.
- On e-commerce and classifieds, focus on high-risk categories, newest listings and seller history, but also check miscategorized content, as IWT products may be deliberately placed under unrelated sections such as pets, agriculture, decor, furniture or hobby goods.
- For messaging apps, pay attention to public channels, invitation links shared on other platforms, and metadata of channels where IWT transactions are commonly discussed.

Each platform should be treated as its own ecosystem, with its own search logic, user behaviour, risk indicators and possible evasion patterns.

Standardize evidence capture

Evidence capture should be standardized from the start, because inconsistent documentation makes later analysis, intelligence sharing and potential evidentiary use much weaker.

- For each suspect post, capture: URL or group/channel ID, date and time, platform, full screenshot (content plus context) and raw text.
- Use consistent file naming and link everything to the record's unique ID in your database.
- Keep hashed versions of any personal identifying information, and enable controls restricting access to raw datasets only to permitted personnel.

Consistent documentation makes records easier to verify, compare, share and, where appropriate, use in follow-up action.

Apply simple illegality categorizations

Use fast, consistent categories such as 'possibly legal', 'probably illegal', 'confirmed illegal' and 'unclear'. Base these on a documented set of criteria matched to the objective, species and product form being monitored.

- Species and product legal status, including jurisdiction, relevant domestic law, CITES status where relevant, and any stated or inferred source claims such as wild, captive-bred, ranched, antique or pre-Convention.
- Mention or absence of permits.
- Trade routes and cross-border shipping.
- Evasive behaviours (e.g. 24-hour video reels) or coded language.
- Repeated appearance of the same contact information across high-risk offers.

Some monitoring projects may use bespoke scoring parameters for live animals versus parts and derivatives, or different thresholds for research, disruption or enforcement workflows. The goal at monitoring stage is risk assessment, not final legal judgment.

Build light but constant quality control

Quality assurance should be simple enough to apply routinely, but regular enough to detect errors, inconsistent interpretation and uncertainty in key fields.

- Have a second analyst review a sample of records to check species identification, geographic data and other essential fields. Where the purpose requires strong evidential certainty, involve a subject-matter expert for species or product verification.
- Run occasional calibration sessions on ambiguous cases and update guidance.
- Allow analysts to flag uncertainty rather than forcing guesses, especially for any record that might go to law enforcement.

Track changing trends

Adaptation should be built into the workflow so that monitoring routines keep pace with new platforms, terminology, product types and displacement patterns.

- Maintain a short trend log of new platforms, code words, product types and seasonal shifts (this can be aggregated into your bi-monthly or seasonal briefing documentation).
- Run periodic exploratory checks on new platforms mentioned in seizures, media or partner reports.
- After major platform policy changes or crackdowns, look for displacement of illicit markets to other spaces and adjust routines.

Automated and assisted monitoring

Software, alerts and automation should be used to extend manual monitoring, not replace it. Human judgement remains essential for interpreting context, legality and risk. Automated and assisted monitoring are intended for teams that already have a manual monitoring regimen and want to scale up. The below outlines what is possible for authorized agencies and NGOs without treating automation as a substitute for human judgement.

Automate recurring searches and alerts

Once manual monitoring has identified viable and recurring search patterns, teams can turn repeat tasks into standing queries, alerts or scheduled reviews.

- Use tools such as Google Alerts or media monitoring services for species, code words and key platform terms in your region. Use dorking queries with previously mentioned syntax, such as site:website.com location species sales-term, while recognizing that search engine returns may still misstate country relevance or miss platform-internal content.
- Where platforms provide application programming interfaces (APIs), configure saved queries that pull new content matching your criteria into a central inbox or database. Pay attention to API limitations and platform terms and conditions.
- For sites without APIs, run web scrapers for specific time frames (e.g. weekly or monthly) on a schedule and have analysts review the new results.

Automation should reduce repetitive searching, but humans should retain control over interpretation and decisions.

Automation and web-scraping

Where manual monitoring cannot cover the volume of content on major platforms, and where it is legally and technically permissible, web-scraping and similar tools may help collect structured information for analysts to review.

- Use web scrapers or crawlers to collect structured data from relevant categories or search pages (text, images, etc.).
- Use search APIs or search engine results page-style (SERP-style) services to run complex queries at scale and feed URLs into your system. Use Google dorking syntax for ideal results (i.e. site:website.com location species sales-term).
- Respect platforms' legal terms, technical limits and Robots Exclusion Protocols (robots.txt), and always build in error handling and IP address-blocking safeguards.

Under the ECO-SOLVE GMS, for example, a combination of manual and AI-assisted scrapers is used to reduce manual workload and surface probable IWT posts for analyst review.

Machine learning and AI filters

AI can help manage high-volume scraper returns by prioritizing content, but it requires sustained resources, appropriate expertise, benchmark testing and continuous maintenance.

- Text classifiers can help distinguish probable wildlife sale posts from noise, but they should be trained and tested against domain-relevant examples and reviewed regularly, since trader language changes.
  - **Caveats:** returns often include news reports, conservation content or other non-sale material, and classifiers can drift or silently degrade when websites change, labels are inconsistent or the monitored market evolves.
- Image models can suggest probable species or product types from photographs, but they are vulnerable to concealment, lookalikes, cropped imagery, screenshots, reels, overlays and poor-quality media.
  - **Caveats:** many online sellers use tactics to bypass image recognition, such as videos, disappearing content, obstructed images, edited backgrounds, or partial views that make species identification unreliable.
- Risk scores can combine species status, quantities, price, location, provenance claims, seller history and contact patterns to help sort returns.
  - **Caveats:** risk scores are only as good as the data and assumptions behind them, and they should be calibrated to the objective rather than treated as self-evident truth.

Web scrapers and AI are not replacements for manual monitoring and human validation. False positives and false negatives are unavoidable, so teams should build in regular quality control, benchmark testing, failure detection, and a clear plan for what happens when websites change, APIs are revoked, or automated workflows silently stop working.

Many web scrapers are limited to surface-level search-engine returns, and many priority platforms restrict APIs, access or scraping. In practice, hybrid systems that combine automated collection with analyst review are often more realistic than fully automated models.

Integrate dashboards, case management and alerts

The greatest efficiency gains come when monitoring tools are joined into a single workflow that connects data collection, review, escalation, case management and follow-up.

- A central dashboard where data collection, classifiers and external alerts feed into a single queue sorted by risk, species, platform and geography.
- Integration with a case management system so that high-priority hits (categorized by risk scoring) can be escalated, enriched with further OSINT, linked to past activity and tracked through to outcome.
- Targeted alerts when, for example, a top-priority species appears on a monitored platform in a particular country, a well-known seller resurfaces, or a known IWT group becomes active again after a pause.

Monitor semi-closed and changing channels

As platforms strengthen enforcement or change their policies, traders may move towards semi-closed spaces, niche platforms or regional channels. Monitoring teams can respond by documenting legally accessible signals and assessing whether new spaces should be added to routine monitoring.

- Use OSINT tools and suites (e.g. Maltego or other network and link analysis tools) to pivot from public data to connected accounts, domains or infrastructure (within legal limits).
- Record invitation links and basic metadata for messaging app channels advertised in open spaces.
- Assess new or regional platforms quickly with exploratory monitoring, then either add them to the monitoring routine or deprioritize them.

Governance, testing and safeguards

Online monitoring raises legal, ethical, operational, digital security and psychological risks, so teams need explicit governance before collecting, storing, automating or sharing information.

- Have clear standard operating procedures for what is collected, where from, how often, on what legal basis, how it is stored and protected, and who is authorized to do what. These procedures should be backed by a documented risk assessment covering legal, moral, security and welfare issues.
- Any interaction with sellers or suspects should be exceptional, justified, recorded, risk-assessed, and compliant with national law and internal policy. Routine monitoring guidance should not assume covert, undercover or engagement-based methods.
- Test classifiers and alert rules in order to understand false positives, false negatives, blind spots and silent system failures. Use secure infrastructure, and where appropriate, consider protective measures such as dedicated devices, segregated environments, virtual private network (VPN) use subject to policy, or virtualized research setups.

INTELLIGENCE GATHERING AND OSINT

OSINT here refers to the structured collection of information from publicly available online sources. Staff carrying out this work should receive appropriate training in lawful OSINT practice, documentation, browser hygiene and digital security. Analysts should be trained to:

- Maintain cybersecurity standards, use dedicated research identities or avatars where policy permits, and protect personal identity and organizational infrastructure.
- Search effectively across platforms using advanced operators (e.g. Google dorking syntaxes, reverse image searches).
- Identify and track high-risk groups, pages and accounts.
- Recognize code words, euphemisms, emojis and obfuscation used in wildlife trading.
- Respect and work within legal and ethical limits. This guide does not treat covert engagement, undercover activity or access to closed forums through deceptive means as routine OSINT; such activity requires separate legal authority, specialist training and high-level risk management.

OSINT is not just 'Googling' – it is planned, documented, and aligned to your scope and legal framework.

Verification and enrichment

Many online posts lack enough information to judge legality, identify species or assess risk, so teams should build simple verification and enrichment processes into their workflow.

- Run reverse image searches to detect stock, reused or misleading images, which may indicate scam listings, copied content, or media that does not match the product being sold.
- Use translation tools to understand content in unfamiliar languages.
- Cross-reference names, numbers and email addresses across your own data and, where appropriate, external sources (e.g. business directories or public registries).
- Add or refine location information using image context or metadata, where legally accessible.

Treat each data point (handle, phrase, phone number) as a possible pivot into related information, but document your steps and stay within legal bounds.

- Define intelligence questions (who is involved, what is traded, where, when, how and why).
- Use structured OSINT methods to map networks (accounts, contacts, pages, companies) and digital footprints (usernames, phone numbers, emails, domains).
- Apply basic geolocation techniques where lawful, using context, metadata and open mapping tools.
- Document methodology and respect legal and ethical boundaries at every step.

LAW ENFORCEMENT ENGAGEMENT AND PARTNERSHIPS

Online monitoring has limited impact if findings are not connected to enforcement, regulatory action or credible platform response. At the same time, expectations should be realistic: many agencies or platforms may not act on every alert because of legal thresholds, priorities, capacity constraints or other institutional limits. Below are the key steps involved in turning online monitoring into real-world cases, seizures and policy improvements, rather than reports that sit on a shelf or in the cloud. An essential aspect of this is good partnerships.

Map the landscape:

- Identify which agencies in your country are responsible for wildlife, customs, cybercrime, financial crime and environmental enforcement.
- Understand their mandates, investigative powers, resource constraints, evidence thresholds and preferred data formats. The same principle applies to online platforms and other partners: knowing their constraints is often essential to eliciting useful action.

Initiate contact:

- Approach relevant units with a concise summary of who you are, what data you collect, and how it may support their work.
- Offer a small, well-presented sample of findings rather than a data dump, and ask what they can realistically pursue, what format they prefer, and what threshold of information they need before they can act.

Build trust:

- Share clear, well-structured intelligence products (briefs, case leads, trend summaries) rather than raw records.
- Be honest about limitations and uncertainty.
- Respect confidentiality and legal constraints, and where appropriate, present information in a professional intelligence product format using recognized evaluation standards and clear handling caveats.

Institutionalize cooperation:

- Where possible, formalize relationships through memorandums of understanding or standard procedures for information sharing, referrals and feedback.
- Set up regular check-ins to understand what is useful, and adjust your monitoring outputs accordingly.

Data sharing, sanitization and legality

Because IWT is transnational, cooperation and data sharing are essential, but they must be handled carefully. Multi-jurisdictional legal rules, evidential requirements, ethical issues and partner mandates all affect what should be shared, with whom, and for what purpose.

- **Data protection and privacy** – Comply with relevant laws, ensure you have a lawful basis for collecting and processing personal data present in online content, and tie collection and onward transfer to a defined purpose. If a transfer does not map to a clear purpose, it should not go ahead.
- **Minimization, purpose limitation and sanitization** – Collect and retain only the data needed for your mandate; do not stockpile personal data 'just in case'. Where necessary, apply pseudonymization, anonymization, hashing, blurring, aggregation or redaction, depending on the recipient and use case.
- **Secure storage and access** – Protect data with appropriate technical and organizational measures, restrict access to those who need it (with two-factor authentication where necessary/possible), and keep audit logs.
- **Cross-border sharing** – Use formal channels and agreements where possible. When direct sharing of raw data is not allowed or appropriate, apply privacy-preserving approaches and handling codes or data classes – for example, distinguishing public data, controlled sharing data, and restricted personal or operational data. Consider separately when it is appropriate to share data with platforms for takedown or disruption purposes and when that would be counterproductive.
- **Legal review** – Engage legal counsel early when designing data collection regimens, automation and data sharing protocols.

The aim is to enable cooperation and actionable intelligence while respecting privacy, due process and human rights.

THE SHIFTING LANDSCAPE

Online IWT and the tools used to fight it will continue to develop and expand. Below are some of the changes we can expect to see.

- **Platforms and channels** – New social networks, marketplaces and messaging apps will emerge; some will be more encrypted or decentralized, making monitoring more challenging.
- **AI and automation** – Traffickers and enforcement actors will make greater use of AI. Traffickers may experiment with fake identities, generate AI images of documents and permits, automated posting or AI-generated images/videos; enforcement and NGOs will rely more on classifiers, anomaly detection and cross-dataset correlation.
- **Regulation and platform policy** – More jurisdictions are exploring platform liability and transparency requirements, which may open new avenues for collaboration or data access but also impose new compliance duties on monitoring projects.
- **Convergence with other crime types** – Wildlife trafficking is intertwined with other illicit markets; future risk models and monitoring systems will increasingly integrate data from broader organized crime, financial flows and environmental harm.

Projects launched now should be designed to adapt. Modular systems, clear data models, and investments in people and partnerships are required, so that when technology changes, institutions are ready.

APPENDIX: GLOBAL DATA MODEL

Each organization can subset this model to fields that fit its context and capacity, while still maintaining comparability and interoperability across projects. The same logic applies across fauna and flora, although the plant trade may require additional attention to cultivar naming, artificial propagation claims, wild collection risk and lookalike legal trade.

The complete Global Data Model, including subsettable categories, can be viewed and downloaded here: https://gitoc-digitaltool.github.io/GMS-Global-Data-Model-App. At a minimum, general data models should consider the following eight categories, which represent the high-level structure.

1. RECORD AND CASE METADATA

- Unique record ID
- Case or operation ID (if applicable)
- Date and time collected
- Collector/source project
- Data source type (online post, seizure record, partner information, public reporting, etc.)

2. PLATFORM AND CONTENT METADATA

- Platform name and type (social media, e-commerce, messaging, etc.)
- URL or platform ID
- Group/page/channel names where relevant
- Post title/text, language, media presence (image/video)

3. SPECIES AND PRODUCT INFORMATION

- Standardized scientific name and common name
- Product type (live animal or plant, meat, skin, horn, ivory, scale, timber, medicinal ingredient, ornamental specimen, horticultural material, ornament, etc.)
- Quantity and unit
- Packaging or form, where relevant

4. LOCATION AND MOVEMENT

- Country and subnational location fields (standardized codes)
- Coordinates where available and lawful
- Mentioned origin, transit and destination locations for trade

5. ACTORS AND CONTACTS

- Seller and buyer identifiers (handles, IDs)
- Contact details present in the content (phones, emails, websites), with appropriate handling under data protection laws
- Role tags (seller, broker, shipper, etc.), where known

6. TRADE CHARACTERISTICS

- Price and currency (with standardized numeric field and original text)
- Delivery or shipping methods mentioned
- Frequency and diversity of listings per seller, including where possible, the apparent number of items or stock units offered over time

7. LEGAL AND RISK ASSESSMENT FIELDS

- Legal status coding (possibly legal, probably illegal, confirmed illegal, unclear)
- Relevant legal instruments (CITES appendix, national law references)
- Priority or risk score fields
- Flags for links to other crime types (where known)

8. FOLLOW-UP AND OUTCOME

- Whether the record was forwarded to law enforcement or partners
- Response received (if any)
- Outcomes such as takedowns, seizures, investigations or prosecutions (if known)

ECO SOLVE

GI-TOC

GIFP
Global Illicit Flows Programme

Funded by the European Union