The OSINT Intelligence Cycle – Planning and Direction

Maria Cattini | 30/12/2025 | Open source intelligence

Why most OSINT investigations fail before they start

Ask ten beginners how they approach an OSINT investigation and nine will talk about tools. Scrapers. Dashboards. Automation. Visual graphs.

That instinct feels logical. It is also risky.

When a platform changes its rules, a tool goes offline, or an account gets flagged, the investigation collapses. Not because the data vanished, but because there was no plan behind the clicks.

If you want to sharpen your OSINT skills, there is a boring but powerful move: go back to the intelligence cycle. This first article focuses on the opening phase — **Planning and Direction** — and how it actually plays out in real OSINT work.

The OSINT intelligence cycle, stripped of theory

The intelligence cycle is often explained in academic terms. In practice, it is a discipline that forces you to think before you collect.

Planning and direction answer one question:
What am I trying to find out, and under what constraints?

Skip this phase and you drift. Do it properly and every later step becomes cleaner, faster, and safer.

Planning and Direction: what happens in this phase

This phase defines the shape of the entire investigation. It is where you set boundaries, expectations, and operational safeguards.

Four decisions matter more than anything else.

OSINT Investigation Planning

Essential Steps for Effective Digital Investigation

1

Define the questions — and write them down

Every OSINT investigation needs a clear core question.

"Who is behind this account?" works. "So what can I find about this profile?" does not.

Strong investigations usually follow a structure:

- one main question
- several smaller questions that support it

A single identity-focused case might break down into:

- What name does this person use elsewhere?
- Which country are they likely operating from?
- What age range fits their digital footprint?
- Do they maintain accounts on other platforms?

These questions are not static. They evolve. Adding or removing them during the investigation is normal. What matters is avoiding side paths that do not serve the main goal.

2

Anticipate the platforms you may need

Before opening a browser tab, check whether you can actually access what you are looking for.

Some platforms are easy. Others are not.

Mainstream social networks usually require:

- a sock puppet account
- email or phone verification

Niche forums, closed communities, or ideologically tight groups often demand more. Vetting by an existing member is common. Sometimes access depends on reputation, history, or shared context.

Failing to prepare accounts in advance creates two problems:

- wasted time mid-investigation
- rushed setups that raise suspicion

Good planning assumes friction and prepares for it early.

3

Gauge the target's technical awareness

Not every target understands operational security. Some do. A few understand it very well.

This matters for two reasons:

- detection risk
- interpretation of mistakes

A technically skilled target is less likely to leak metadata accidentally. A less skilled one might overshare without realizing it.

You will not always know this at the start. Still, assume a higher level of awareness than you expect. That mindset reduces careless exposure.

Using anonymous or hardened browsing environments when assessing technical behavior adds an extra layer of protection during early reconnaissance.

4

Decide what "success" looks like

An investigation without a defined endpoint drifts endlessly.

Before collecting anything, be honest:

- Is the output a written report?
- Is the goal attribution, pattern mapping, or risk assessment?
- Will the result be shared with authorities, editors, or internal teams?

Clear end goals shape every later decision. They influence what data you keep, what you discard, and how cautious you need to be.

Planning without an end state is just curiosity dressed as analysis.

Why this phase saves more time than any tool

Planning feels slow. It is not.

Most wasted hours in OSINT come from:

- chasing irrelevant leads
- creating accounts mid-investigation
- realizing too late that access is blocked
- backtracking after contamination or detection

Planning and direction eliminate these failures early. They reduce noise and protect the analyst as much as the investigation itself.

What comes next

Once planning is done, collection begins — with purpose, constraints, and awareness.

That is the difference between clicking around and conducting intelligence work.

Next step: the Collection phase, where discipline matters even more than curiosity.

Want to go deeper?

Subscribe to the **OSINT & AI for Everyone** newsletter and join the Telegram communities to follow the full intelligence cycle, tested on real investigations.

- Newsletter: https://coondivido.substack.com/
- Telegram: https://t.me/osintaipertutti
- Telegram: https://t.me/osintprojectgroup