ANALYST

Co-funded by the European Union

Unit 6
Key Intelligence Concepts – Frameworks, Sources, and Disciplines

Fundamentals of Intelligence: History and Theory

MASSIVE OPEN ONLINE COURSE (MOOC)

Project N. 2023-1-IT02-KA220-HED-000161770
ANALYST - A New Advanced Level for Your Specialised Training

Alessandro Vivaldi

HOZINT HORIZON INTELLIGENCE · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · Centro Studi AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Intelligence Cycle

- The intelligence cycle is a fundamental framework that describes how intelligence is produced from start to finish. It consists of several phases that form a loop: Direction (Planning), Collection, Processing/Analysis, Dissemination, and Feedback. In short, first the needs are defined, then information is gathered, then it's analyzed into intelligence, then delivered to those who need it, and their feedback can refine what's needed next – and the cycle repeats. This structured process ensures intelligence work is organized rather than haphazard.

Direction/Planning: This is where it all begins – identifying what questions need to be answered or what problems need intelligence support. Leaders or analysts set requirements: for example, "We need to know if Organization X poses a threat to our company's network" or "What is Country Y's military planning to do next month?" Good direction means clear priorities so that efforts are focused.

HOZINT HORIZON INTELLIGENCE · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · Centro Studi AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Intelligence Cycle

Collection: In this phase, agencies or analysts gather raw information. This could be through various means (more on the sources in a moment). It might involve collecting documents, intercepting communications, conducting interviews, monitoring news and social media, taking photos via satellites – any method to get relevant data. Collection should follow the requirements set in the direction phase (no use collecting tons of data that isn't related to the question).

HOZINT HORIZON INTELLIGENCE · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · Centro Studi AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Intelligence Cycle

Processing and Analysis: Once information is collected, often it needs to be processed – translating foreign documents, decrypting messages, sorting and organizing data. Then comes analysis, where analysts evaluate the information, compare it with other data, and draw conclusions. This is the heart of creating "intelligence." Analysts ask: What does this information mean? Is it reliable? What might happen next? They may use analytic techniques (structured methods) to avoid bias and ensure thoroughness. The end result is usually findings or answers to the original questions.

ANALYST

Co-funded by the European Union

Intelligence Cycle

Dissemination: This is delivering the finished intelligence product to the people who requested it or who need to act on it. It could be a written report, an oral briefing, a dashboard – whatever format suits the customer. Timeliness is key: the intelligence must get to the decision-maker in time to be useful. Also, it needs to be presented clearly (no jargon overload) so the user can grasp the insights quickly.

HOZINT HORIZON INTELLIGENCE · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · Centro Studi AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Intelligence Cycle

Feedback: Although sometimes omitted in simple depictions, feedback closes the loop. The decision-makers might ask new questions after seeing the intel (“This is useful, but now I need to know about aspect Z”), or might say what was helpful and what wasn’t. That feedback guides the next cycle, refining direction and collection. Without feedback, the process can become less responsive to actual needs over time.

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

HUMINT (Human Intelligence): Information collected from human sources. This includes spies who clandestinely get secrets, diplomats or military attaches gathering info, defectors, or even just interviewing people who have knowledge. In a corporate setting, HUMINT might be talking to industry experts or insiders. HUMINT is as old as history (think spies), and it provides insights into intentions and thinking of adversaries that tech might not catch. However, it can be risky (agents can be caught) and sometimes less timely.

ANALYST

Co-funded by the European Union

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

SIGINT (Signals Intelligence): Intercepting communications and electronic signals. This ranges from listening to radio communications, tapping phone calls, to intercepting internet traffic. Agencies like NSA specialize in SIGINT. It can yield large volumes of data – sometimes highly secret info if communications are decrypted. A WWII example was reading encrypted messages; today it could be eavesdropping on terrorist cell phone chats. The challenge with SIGINT is dealing with encryption and picking out useful intel from a firehose of signals.

ANALYST

Co-funded by the European Union

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

IMINT (Imagery Intelligence): Obtaining information from imagery – photos or videos, traditionally from aerial or satellite cameras. Modern IMINT includes high-resolution satellite photos, drone imagery, even commercial satellite pics used in corporate intel (for example, a company might use satellite images to estimate a rival’s inventory by looking at shipping containers in their lot!). IMINT is great for understanding physical developments (e.g., new construction at a military base, or how many ships are in a port). It often provides the “hard proof” in an image, but analysts must correctly interpret what they see.

ANALYST

Co-funded by the European Union

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

MASINT (Measurement and Signature Intelligence): A less widely known category, MASINT refers to technical measurement of signatures of things. It can include chemical, radiological, acoustic, seismic, or other data. For example, detecting the distinct radar signature of a new missile, or analyzing air samples for traces of nuclear tests, is MASINT. It’s very science-heavy and often supports arms control monitoring or identifying weapons by their unique “fingerprints.”

ANALYST

Co-funded by the European Union

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

OSINT (Open-Source Intelligence): Information gathered from publicly available sources. This includes news media, academic articles, official reports, websites, social media, public data sets – anything openly published. OSINT has exploded in importance, especially with the internet. For instance, analysts might comb through social media posts to get ground truth during a conflict, or use online databases to research a company. OSINT is accessible and can provide broad context quickly. However, its volume is enormous and quality varies – part of the skill is sifting credible information from rumors or misinformation.

ANALYST

Co-funded by the European Union

Sources of Intel: the INTs…

- Intelligence practitioners categorize sources by the collection method, often using three-letter acronyms ending in “INT” (intelligence):

CYBINT (Cyber Intelligence): Often considered a subset of SIGINT or OSINT, but increasingly a category on its own, cyber intelligence involves gathering information from cyberspace – including the activities of hackers, dark web forums, network traffic that indicates intrusions, etc. It’s crucial for cybersecurity (like intelligence on a new malware threat) and also as a window into adversaries’ intentions (state hackers often tip off geopolitical moves). Cyber intel analysts might look at things like metadata of communications or patterns of cyber attacks to attribute them to certain actors.

ANALYST

Co-funded by the European Union

Evaluation of sources and info

- Not all information is equal – some sources are very reliable, others not so much. Intelligence professionals use frameworks to rate how much confidence to place in info. A classic is the "reliability-credibility matrix" (also called the Admiralty Scale). It rates the source's reliability (for example, A = completely reliable, B = usually reliable, … F = unreliable or unknown) and the information's credibility or likely truth (1 = confirmed by other sources, 2 = probably true, … 5 = improbable, 6 = unverifiable). So an intercepted message from a proven source might be rated A1 (high confidence), while a rumor from an unknown person might be E4 or F6 (low confidence). This helps analysts and consumers weigh how much trust to put in a piece of intel. A good intelligence product will often include these caveats: e.g., "Source is usually reliable, info not confirmed by other sources."

Corroboration

- A key practice in analysis is corroborating information – that is, checking if multiple sources say the same thing. If a satellite image shows unusual activity at a base and intercepts also pick up chatter about a “big exercise,” plus a human source reports troops moving – together these make a stronger case than any single source alone. Fusion centers exist to bring different streams (HUMINT, SIGINT, OSINT, etc.) together, giving a more complete picture. This multidisciplinary approach helps overcome the blind spots of any one method. It also helps detect deception – if one source is feeding false info, other sources might contradict it.