INTELLIGENCE · CONCEPTS AND HISTORY

Signals Intelligence (SIGINT): Extracting Knowledge from Intercepted Data

Signals intelligence is knowledge drawn from intercepted communications and electronic emissions. This short article explains its main forms, its history from codebreaking to metadata, and why its power raises lasting questions about privacy and oversight.

ModQu research article · 715 words · 7 references (APA 7th edition)

Signals intelligence, or SIGINT, is intelligence derived from intercepting signals: communications between people, and electronic emissions from radars, weapons and other equipment. It is one of the main collection disciplines of national intelligence and, for some states, the largest by budget and staff (Lowenthal, 2022).

Three kinds of signal

Practitioners divide SIGINT into three parts. **Communications intelligence** (COMINT) comes from intercepted messages: telephone calls, radio traffic, emails and data. **Electronic intelligence** (ELINT) comes from non-communication emissions, such as radar signals, which reveal the location and capability of equipment. **Foreign instrumentation signals intelligence** comes from the telemetry that missiles and spacecraft send back during tests (Lowenthal & Clark, 2016).

From codebreaking to data

For most of its history SIGINT meant breaking codes. Kahn (1967) traces cryptography and cryptanalysis from the ancient world to the twentieth century and shows how interception and decryption repeatedly shaped diplomacy and war. The most celebrated case is the British effort at Bletchley Park against German Enigma and other cipher systems in the Second World War. Ferris (2020), in an authorised history of Britain's signals intelligence agency, GCHQ, describes how codebreaking became an industrial enterprise employing thousands of people and machines, and how its product influenced military operations.

Shannon's (1948) mathematical theory of communication, which treats information as a measurable quantity transmitted through noisy channels, provided part of the scientific foundation for modern signal processing and cryptography alike. As communications moved from radio to cables, satellites and the internet, SIGINT agencies shifted from intercepting individual messages to processing vast streams of digital data.

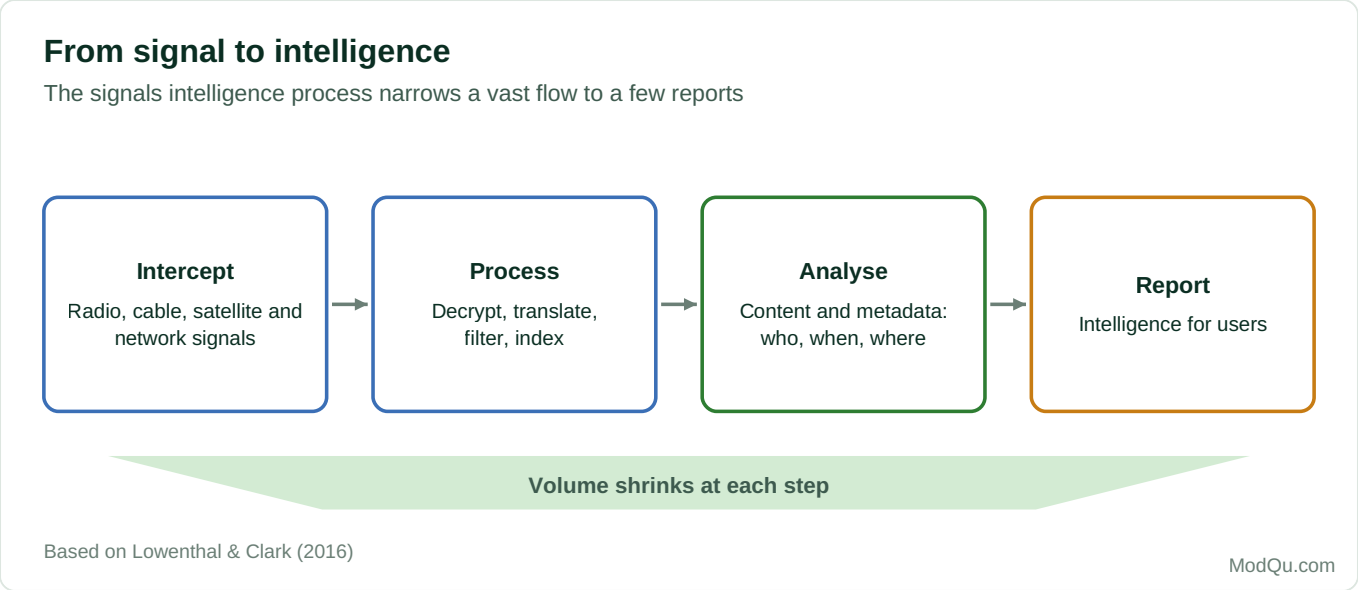


Figure 1. From signal to intelligence. Most raw intercepts are never read by a person; processing and filtering decide which few reach an analyst. Based on Lowenthal and Clark (2016); diagram by ModQu.

Strengths and weaknesses

SIGINT has distinctive strengths. It can be collected at a distance, without placing people at risk, and it often captures what targets say to each other in private, which may reveal plans and intentions that no outside observer could see. It can also be very timely: an intercepted order can be read before it is carried out.

Its weaknesses are equally distinctive. Targets who know they may be monitored change their behaviour, switch channels, use code words or encrypt their messages. Intercepted conversations are often fragmentary, informal and full of references that only the participants understand, so their meaning must be inferred. Translation adds another layer of interpretation. And a skilled adversary can feed false messages into channels it knows are monitored, turning SIGINT into a vehicle for deception. For these reasons analysts treat signals intelligence as evidence to be weighed alongside other sources, not as a direct window into the adversary's mind.

The power of metadata

Encryption now protects much message content, but the **metadata** of communications, who contacted whom, when, for how long and from where, remains highly informative. Mayer et al. (2016) studied the telephone metadata of hundreds of volunteers and showed that it could reveal sensitive facts, such as medical conditions and religious affiliations, and that individuals could often be identified from call patterns alone. Metadata are also easier than content to analyse at scale, which makes them central to modern SIGINT.

Businesses face a version of the same issue. Records of customer calls, website visits and app use are a kind of metadata, and analysing them can reveal far more about individuals than customers expect. The lesson from SIGINT is to treat such patterns as sensitive data in their own right, not as harmless by-products.

Oversight and trust

The disclosures made by Edward Snowden in 2013 showed how extensively some agencies collected domestic and foreign communications data. Landau (2013) argued that the most significant revelations concerned the scale of collection, the reliance on metadata and the weakening of commercial security standards, and that they raised questions not only about privacy but about the security of the communications systems everyone depends on.

What SIGINT teaches about intelligence

SIGINT illustrates three general lessons. First, volume is not knowledge: the challenge is selecting the few relevant signals from an overwhelming flow. Second, patterns can reveal as much as content, which applies equally to business data such as transaction and web logs. Third, the most powerful collection methods need the strongest legal limits and independent oversight if they are to keep public trust.

References

Ferris, J. (2020). *Behind the enigma: The authorised history of GCHQ, Britain's secret cyber-intelligence agency*. Bloomsbury.

Kahn, D. (1967). *The codebreakers: The story of secret writing*. Macmillan.

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, *11*(4), 54–63. https://doi.org/10.1109/MSP.2013.90

Lowenthal, M. M., & Clark, R. M. (Eds.). (2016). *The five disciplines of intelligence collection*. CQ Press.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, *113*(20), 5536–5541. https://doi.org/10.1073/pnas.1508081113

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, *27*(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x