



WIKIPEDIA  
The Free Encyclopedia

# Signals intelligence

(Redirected from SIGINT)

**Signals intelligence** (**SIGINT**) is intelligence-gathering by interception of *signals*, whether communications between people (**communications intelligence**—abbreviated to **COMINT**) or from electronic signals not directly used in communication (**electronic intelligence**—abbreviated to **ELINT**).<sup>[1]</sup> Signals intelligence is a subset of intelligence collection management. As classified and sensitive information is usually encrypted, signals intelligence in turn involves the use of cryptanalysis to decipher the messages. Traffic analysis—the study of who is signaling whom and in what quantity—is also used to integrate information again.

## History

### Origins

Electronic interceptions appeared as early as 1900, during the Boer War of 1899–1902. The British Royal Navy had installed wireless sets produced by Marconi on board their ships in the late 1890s, and the British Army used some limited wireless signalling. The Boers captured some wireless sets and used them to make vital transmissions.<sup>[2]</sup> Since the British were the only people transmitting at the time, no special interpretation of the signals that were intercepted by the British was necessary.<sup>[3]</sup>

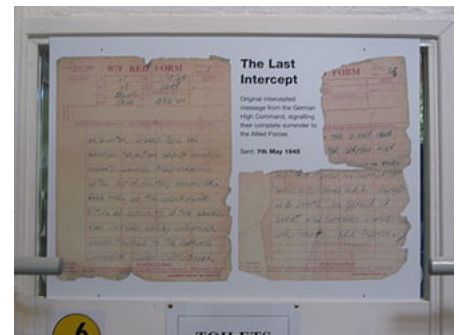
The birth of signals intelligence in a modern sense dates from the Russo-Japanese War of 1904–1905. As the Russian fleet prepared for conflict with Japan in 1904, the British ship HMS Diana stationed in the Suez Canal intercepted Russian naval wireless signals being sent out for the mobilization of the fleet, for the first time in history.<sup>[4]</sup>

### Development in World War I

Over the course of the First World War, the new method of signals intelligence reached maturity.<sup>[5]</sup> Failure to properly protect its communications fatally compromised the Russian Army in its advance early in World War I and led to their disastrous defeat by the Germans under Ludendorff and Hindenburg at the Battle of Tannenberg. In 1918, French intercept personnel captured a message written in the new ADFGVX cipher, which was cryptanalyzed by Georges Painvin. This gave the Allies advance warning of the German 1918 Spring Offensive.



RAF Menwith Hill, a large site in the United Kingdom, part of ECHELON and the UKUSA Agreement in 2005



A German message intercepted by the British during World War II, signaling Germany's unconditional surrender

The British in particular built up great expertise in the newly emerging field of signals intelligence and codebreaking (synonymous with cryptanalysis). On the declaration of war, Britain cut all German undersea cables.<sup>[6]</sup> This forced the Germans to use either a telegraph line that connected through the British network and could be tapped, or through radio which the British could then intercept.<sup>[7]</sup> Rear Admiral Henry Oliver appointed Sir Alfred Ewing to establish an interception and decryption service at the Admiralty; Room 40.<sup>[7]</sup> An interception service known as 'Y' service, together with the post office and Marconi stations, grew rapidly to the point where the British could intercept almost all official German messages.<sup>[7]</sup>

The German fleet was in the habit each day of wirelessly the exact position of each ship and giving regular position reports when at sea. It was possible to build up a precise picture of the normal operation of the High Seas Fleet, to infer from the routes they chose where defensive minefields had been placed and where it was safe for ships to operate. Whenever a change to the normal pattern was seen, it immediately signalled that some operation was about to take place and a warning could be given. Detailed information about submarine movements was also available.<sup>[7]</sup>

The use of radio-receiving equipment to pinpoint the location of the transmitter was also developed during the war. Captain H.J. Round, working for Marconi, began carrying out experiments with direction-finding radio equipment for the army in France in 1915. By May 1915, the Admiralty was able to track German submarines crossing the North Sea. Some of these stations also acted as 'Y' stations to collect German messages, but a new section was created within Room 40 to plot the positions of ships from the directional reports.<sup>[7]</sup>

Room 40 played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea. The battle of Dogger Bank was won in no small part due to the intercepts that allowed the Navy to position its ships in the right place.<sup>[8]</sup> It played a vital role in subsequent naval clashes, including at the Battle of Jutland as the British fleet was sent out to intercept them. The direction-finding capability allowed for the tracking and location of German ships, submarines, and Zeppelins. The system was so successful that by the end of the war, over 80 million words, comprising the totality of German wireless transmission over the course of the war, had been intercepted by the operators of the Y-stations and decrypted.<sup>[9]</sup> However, its most astonishing success was in decrypting the Zimmermann Telegram, a telegram from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico.

## Postwar consolidation

With the importance of interception and decryption firmly established by the wartime experience, countries established permanent agencies dedicated to this task in the interwar period. In 1919, the British Cabinet's Secret Service Committee, chaired by Lord Curzon, recommended that a peace-time codebreaking agency should be created.<sup>[10]</sup> The Government Code and Cypher School (GC&CS) was the first peace-time codebreaking agency, with a public function "to advise as to the security of codes

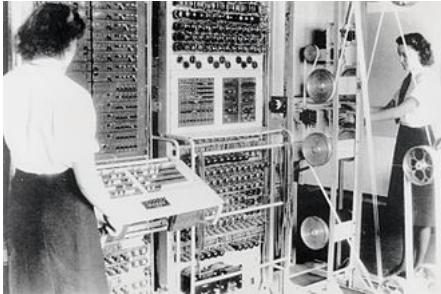
4458	gemeinsam
17149	Friedensschluss.
14471	⊙
6706	reichlich
13850	finanziell
12224	unterstützung
6929	und
14991	einverständnis
7382	ausserseits.
158(5)7	2a/3
67893	Mexico.
14218	in
36477	Texas
5670	⊙
17553	neu
67893	Mexico.
5870	⊙
5454	AR
16102	IZ
15217	ON
22801	A

Zimmermann Telegram, as decoded by Room 40 in 1917

and cyphers used by all Government departments and to assist in their provision", but also with a secret directive to "study the methods of cypher communications used by foreign powers".<sup>[11]</sup> GC&CS officially formed on 1 November 1919, and produced its first decrypt on 19 October.<sup>[10][12]</sup> By 1940, GC&CS was working on the diplomatic codes and ciphers of 26 countries, tackling over 150 diplomatic cryptosystems.<sup>[13]</sup>

The US Cipher Bureau was established in 1919 and achieved some success at the Washington Naval Conference in 1921, through cryptanalysis by Herbert Yardley. Secretary of War Henry L. Stimson closed the US Cipher Bureau in 1929 with the words "Gentlemen do not read each other's mail."

## World War II



A Mark 2 Colossus computer. The ten Colossi were the world's first programmable electronic computers, and were built to break the German codes.

The use of SIGINT had even greater implications during World War II. The combined effort of intercepts and cryptanalysis for the whole of the British forces in World War II came under the code name "Ultra", managed from Government Code and Cypher School at Bletchley Park. Properly used, the German Enigma and Lorenz ciphers should have been virtually unbreakable, but flaws in German cryptographic procedures, and poor discipline among the personnel carrying them out, created vulnerabilities which made Bletchley's attacks feasible.

Bletchley's work was essential to defeating the U-boats in the Battle of the Atlantic, and to the British naval victories in the Battle of Cape Matapan and the Battle of North Cape. In 1941, Ultra exerted a powerful effect on the North African desert campaign

against German forces under General Erwin Rommel. General Sir Claude Auchinleck wrote that were it not for Ultra, "Rommel would have certainly got through to Cairo". Ultra decrypts featured prominently in the story of Operation SALAM, László Almásy's mission across the desert behind Allied lines in 1942.<sup>[14]</sup> Prior to the Normandy landings on D-Day in June 1944, the Allies knew the locations of all but two of Germany's fifty-eight Western Front divisions.

Winston Churchill was reported to have told King George VI: "It is thanks to the secret weapon of General Menzies, put into use on all the fronts, that we won the war!" Supreme Allied Commander, Dwight D. Eisenhower, at the end of the war, described Ultra as having been "decisive" to Allied victory.<sup>[15]</sup> Official historian of British Intelligence in World War II Sir Harry Hinsley argued that Ultra shortened the war "by not less than two years and probably by four years"; and that, in the absence of Ultra, it is uncertain how the war would have ended.<sup>[16]</sup>

## Technical definitions

The United States Department of Defense has defined the term "signals intelligence" as:

1. A category of intelligence comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted.



Unit 8200 (the SIGINT unit of the Israeli Intelligence Corps) base on Mount Avital, Golan Heights

2. Intelligence derived from communications, electronic, and foreign instrumentation signals.<sup>[17]</sup>

Being a broad field, SIGINT has many sub-disciplines. The two main ones are communications intelligence (COMINT) and electronic intelligence (ELINT).

## Disciplines shared across the branches

---

### Targeting

A collection system has to know to look for a particular signal. "System", in this context, has several nuances. Targeting is the process of developing *collection requirements*:

- "1. An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency.
- "2. An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer."<sup>[17]</sup>

### Need for multiple, coordinated receivers

First, atmospheric conditions, sunspots, the target's transmission schedule and antenna characteristics, and other factors create uncertainty that a given signal intercept sensor will be able to "hear" the signal of interest, even with a geographically fixed target and an opponent making no attempt to evade interception. Basic countermeasures against interception include frequent changing of radio frequency, polarization, and other transmission characteristics. An intercept aircraft could not get off the ground if it had to carry antennas and receivers for every possible frequency and signal type to deal with such countermeasures.

Second, locating the transmitter's position is usually part of SIGINT. Triangulation and more sophisticated radio location techniques, such as time of arrival methods, require multiple receiving points at different locations. These receivers send location-relevant information to a central point, or perhaps to a distributed system in which all participate, such that the information can be correlated and a location computed.

### Intercept management

Modern SIGINT systems, therefore, have substantial communications among intercept platforms. Even if some platforms are clandestine, there is still a broadcast of information telling them where and how to look for signals.<sup>[18]</sup> A United States targeting system under development in the late 1990s, PSTS, constantly sends out information that helps the interceptors properly aim their antennas and



A52 *Oste*, an Oste class ELINT (Electronic signals intelligence) and reconnaissance ship, of the German Navy



Satellite ground station of the Dutch Nationale SIGINT Organisatie (NSO) (2012)



tune their receivers. Larger intercept aircraft, such as the EP-3 or RC-135, have the on-board capability to do some target analysis and planning, but others, such as the RC-12 GUARDRAIL, are completely under ground direction. GUARDRAIL aircraft are fairly small and usually work in units of three to cover a tactical SIGINT requirement, whereas the larger aircraft tend to be assigned strategic/national missions.

Before the detailed process of targeting begins, someone has to decide there is a value in collecting information about something. While it would be possible to direct signals intelligence collection at a major sports event, the systems would capture a great deal of noise, news signals, and perhaps announcements in the stadium. If, however, an anti-terrorist organization believed that a small group would be trying to coordinate their efforts using short-range unlicensed radios at the event, SIGINT targeting of radios of that type would be reasonable. Targeting would not know where in the stadium the radios might be located or the exact frequency they are using; those are the functions of subsequent steps such as signal detection and direction finding.

Once the decision to target is made, the various interception points need to cooperate, since resources are limited.

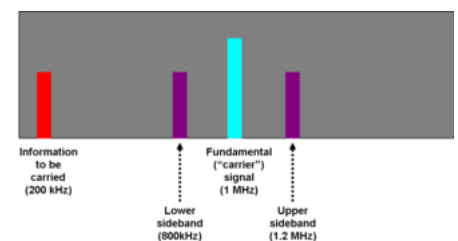
Knowing what interception equipment to use becomes easier when a target country buys its radars and radios from known manufacturers, or is given them as military aid. National intelligence services keep libraries of devices manufactured by their own country and others, and then use a variety of techniques to learn what equipment is acquired by a given country.

Knowledge of physics and electronic engineering further narrows the problem of what types of equipment might be in use. An intelligence aircraft flying well outside the borders of another country will listen for long-range search radars, not short-range fire control radars that would be used by a mobile air defense. Soldiers scouting the front lines of another army know that the other side will be using radios that must be portable and not have huge antennas.

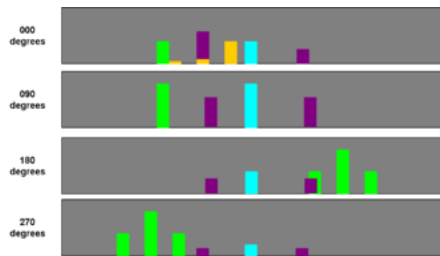
## Signal detection

Even if a signal is human communications (e.g., a radio), the intelligence collection specialists have to know it exists. If the targeting function described above learns that a country has a radar that operates in a certain frequency range, the first step is to use a sensitive receiver, with one or more antennas that listen in every direction, to find an area where such a radar is operating. Once the radar is known to be in the area, the next step is to find its location.

If operators know the probable frequencies of transmissions of interest, they may use a set of receivers, preset to the frequencies of interest. These are the frequency (horizontal axis) versus power (vertical axis) produced at the transmitter, before any filtering of signals that do not add to the information being transmitted. Received energy on a particular frequency may start a recorder, and alert a human to listen to the signals if they are intelligible (i.e., COMINT). If the frequency is not known, the operators may look for power on primary or sideband frequencies using a spectrum analyzer. Information from the spectrum analyzer is then used to tune receivers to signals of interest. For example, in this simplified spectrum, the actual information is at 800 kHz and 1.2 MHz.



Simplified spectrum analyzer display of superheterodyned, amplitude modulated signals.



Hypothetical displays from four spectrum analyzers connected to directional antennas. The transmitter is at bearing 090 degrees.

Real-world transmitters and receivers usually are directional. In the figure to the left, assume that each display is connected to a spectrum analyzer connected to a directional antenna aimed in the indicated direction.

## Countermeasures to interception

Spread-spectrum communications is an electronic counter-countermeasures (ECCM) technique to defeat looking for particular frequencies. Spectrum analysis can be used in a different ECCM way to identify frequencies not being jammed or not in use.

## Direction-finding

The earliest, and still common, means of direction finding is to use directional antennas as goniometers, so that a line can be drawn from the receiver through the position of the signal of interest. (See HF/DF.) Knowing the compass bearing, from a single point, to the transmitter does not locate it. Where the bearings from multiple points, using goniometry, are plotted on a map, the transmitter will be located at the point where the bearings intersect. This is the simplest case; a target may try to confuse listeners by having multiple transmitters, giving the same signal from different locations, switching on and off in a pattern known to their user but apparently random to the listener.

Individual directional antennas have to be manually or automatically turned to find the signal direction, which may be too slow when the signal is of short duration. One alternative is the Wullenweber array technique. In this method, several concentric rings of antenna elements simultaneously receive the signal, so that the best bearing will ideally be clearly on a single antenna or a small set. Wullenweber arrays for high-frequency signals are enormous, referred to as "elephant cages" by their users.

An alternative to tunable directional antennas or large omnidirectional arrays such as the Wullenweber is to measure the time of arrival of the signal at multiple points, using GPS or a similar method to have precise time synchronization. Receivers can be on ground stations, ships, aircraft, or satellites, giving great flexibility.

Modern anti-radiation missiles can home in on and attack transmitters; military antennas are rarely a safe distance from the user of the transmitter.

## Traffic analysis

When locations are known, usage patterns may emerge, from which inferences may be drawn. Traffic analysis is the discipline of drawing patterns from information flow among a set of senders and receivers, whether those senders and receivers are designated by location determined through direction finding, by addressee and sender identifications in the message, or even MASINT techniques for "fingerprinting" transmitters or operators. Message content other than the sender and receiver is not necessary to do traffic analysis, although more information can be helpful.

For example, if a certain type of radio is known to be used only by tank units, even if the position is not precisely determined by direction finding, it may be assumed that a tank unit is in the general area of the signal. The owner of the transmitter can assume someone is listening, so might set up tank

radios in an area where he wants the other side to believe he has actual tanks. As part of Operation Quicksilver, part of the deception plan for the invasion of Europe at the Battle of Normandy, radio transmissions simulated the headquarters and subordinate units of the fictitious First United States Army Group (FUSAG), commanded by George S. Patton, to make the German defense think that the main invasion was to come at another location. In like manner, fake radio transmissions from Japanese aircraft carriers, before the Battle of Pearl Harbor, were made from Japanese local waters, while the attacking ships moved under strict radio silence.

Traffic analysis need not focus on human communications. For example, if the sequence of a radar signal, followed by an exchange of targeting data and a confirmation, followed by observation of artillery fire, this may identify an automated counterbattery system. A radio signal that triggers navigational beacons could be a landing aid system for an airstrip or helicopter pad that is intended to be low-profile.

Patterns do emerge. Knowing a radio signal, with certain characteristics, originating from a fixed headquarters may be strongly suggestive that a particular unit will soon move out of its regular base. The contents of the message need not be known to infer the movement.

There is an art as well as science of traffic analysis. Expert analysts develop a sense for what is real and what is deceptive. Harry Kidder,<sup>[19]</sup> for example, was one of the star cryptanalysts of World War II, a star hidden behind the secret curtain of SIGINT.<sup>[20]</sup>

## Electronic order of battle

Generating an **electronic order of battle** (EOB) requires identifying SIGINT emitters in an area of interest, determining their geographic location or range of mobility, characterizing their signals, and, where possible, determining their role in the broader organizational order of battle. EOB covers both COMINT and ELINT.<sup>[21]</sup> The Defense Intelligence Agency maintains an EOB by location. The Joint Spectrum Center (JSC) of the Defense Information Systems Agency supplements this location database with five more technical databases:

1. FRRS: Frequency Resource Record System
2. BEI: Background Environment Information
3. SCS: Spectrum Certification System
4. EC/S: Equipment Characteristics/Space
5. TACDB: platform lists, sorted by nomenclature, which contain links to the C-E equipment complement of each platform, with links to the parametric data for each piece of equipment, military unit lists and their subordinate units with equipment used by each unit.

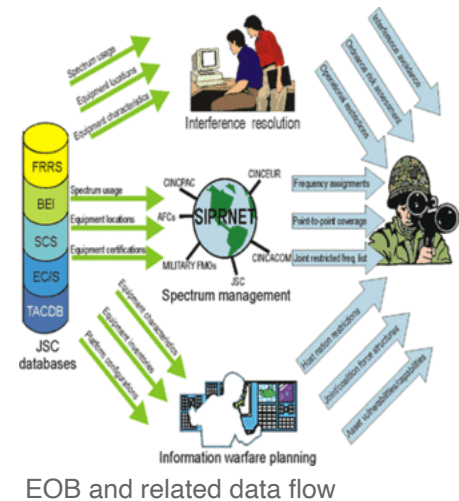
For example, several voice transmitters might be identified as the command net (i.e., top commander and direct reports) in a tank battalion or tank-heavy task force. Another set of transmitters might identify the logistic net for that same unit. An inventory of ELINT sources might identify the medium- and long-range counter-artillery radars in a given area.

Signals intelligence units will identify changes in the EOB, which might indicate enemy unit movement, changes in command relationships, and increases or decreases in capability.

Using the COMINT gathering method enables the intelligence officer to produce an electronic order of battle by traffic analysis and content analysis among several enemy units. For example, if the following messages were intercepted:

1. U1 to U2, requesting permission to proceed to checkpoint X.
2. U2 to U1, approved. please report at arrival.
3. (20 minutes later) U1 to U2, all vehicles have arrived to checkpoint X.

This sequence shows that there are two units in the battlefield, unit 1 is mobile, while unit 2 is in a higher hierarchical level, perhaps a command post. One can also understand that unit 1 moved from one point to another which are distant from each 20 minutes with a vehicle. If these are regular reports over a period of time, they might reveal a patrol pattern. Direction-finding and radio frequency MASINT could help confirm that the traffic is not deception.



The EOB buildup process is divided as following:

- Signal separation
- Measurements optimization
- Data fusion
- Networks build-up

Separation of the intercepted spectrum and the signals intercepted from each sensor must take place in an extremely small period of time, in order to separate the different signals to different transmitters in the battlefield. The complexity of the separation process depends on the complexity of the transmission methods (e.g., hopping or time-division multiple access (TDMA)).

By gathering and clustering data from each sensor, the measurements of the direction of signals can be optimized and get much more accurate than the basic measurements of a standard direction finding sensor.<sup>[22]</sup> By calculating larger samples of the sensor's output data in near real-time, together with historical information of signals, better results are achieved.

Data fusion correlates data samples from different frequencies from the same sensor, "same" being confirmed by direction finding or radiofrequency MASINT. If an emitter is mobile, direction finding, other than discovering a repetitive pattern of movement, is of limited value in determining if a sensor is unique. MASINT then becomes more informative, as individual transmitters and antennas may have unique side lobes, unintentional radiation, pulse timing, etc.

**Network build-up**, or analysis of emitters (communication transmitters) in a target region over a sufficient period of time, enables creation of the communications flows of a battlefield.<sup>[23]</sup>

## Communications intelligence

COMINT (**communications intelligence**) is a sub-category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. COMINT is commonly referred to as SIGINT, which can cause confusion when talking about the broader intelligence disciplines. The US Joint Chiefs of Staff defines it as "Technical information and intelligence derived from foreign communications by other than the intended recipients".<sup>[17]</sup>



COMINT, which is defined to be communications among people, will reveal some or all of the following:

1. Who is transmitting
2. Where they are located, and, if the transmitter is moving, the report may give a plot of the signal against location
3. If known, the organizational function of the transmitter
4. The time and duration of transmission, and the schedule if it is a periodic transmission
5. The frequencies and other technical characteristics of their transmission
6. If the transmission is encrypted or not, and if it can be decrypted. If it is possible to intercept either an originally transmitted plaintext or obtain it through cryptanalysis, the language of the communication and a translation (when needed).
7. The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message. These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both. Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

## Voice interception

A basic COMINT technique is to listen for voice communications, usually over radio but possibly "leaking" from telephones or from wiretaps. If the voice communications are encrypted, traffic analysis may still give information.

In the Second World War, for security the United States used Native American volunteer communicators known as code talkers, who used languages such as Navajo, Comanche and Choctaw, which would be understood by few people, even in the U.S. Even within these uncommon languages, the code talkers used specialized codes, so a "butterfly" might be a specific Japanese aircraft. British forces made limited use of Welsh speakers for the same reason.

While modern electronic encryption does away with the need for armies to use obscure languages, it is likely that some groups might use rare dialects that few outside their ethnic group would understand.

## Text interception

Morse code interception was once very important, but Morse code telegraphy is now obsolete in the western world, although possibly used by special operations forces. Such forces, however, now have portable cryptographic equipment.

Specialists scan radio frequencies for character sequences (e.g., electronic mail) and fax.

## Signaling channel interception

A given digital communications link can carry thousands or millions of voice communications, especially in developed countries. Without addressing the legality of such actions, the problem of identifying which channel contains which conversation becomes much simpler when the first thing intercepted is the *signaling channel* that carries information to set up telephone calls. In civilian and many military use, this channel will carry messages in Signaling System 7 protocols.

Retrospective analysis of telephone calls can be made from Call detail record (CDR) used for billing the calls.

## Monitoring friendly communications

More a part of communications security than true intelligence collection, SIGINT units still may have the responsibility of monitoring one's own communications or other electronic emissions, to avoid providing intelligence to the enemy. For example, a security monitor may hear an individual transmitting inappropriate information over an unencrypted radio network, or simply one that is not authorized for the type of information being given. If immediately calling attention to the violation would not create an even greater security risk, the monitor will call out one of the BEADWINDOW codes<sup>[24]</sup> used by Australia, Canada, New Zealand, the United Kingdom, the United States, and other nations working under their procedures. Standard BEADWINDOW codes (e.g., "BEADWINDOW 2") include:

1. **Position:** (e.g., disclosing, in an insecure or inappropriate way), "Friendly or enemy position, movement or intended movement, position, course, speed, altitude or destination or any air, sea or ground element, unit or force."
2. **Capabilities:** "Friendly or enemy capabilities or limitations. Force compositions or significant casualties to special equipment, weapons systems, sensors, units or personnel. Percentages of fuel or ammunition remaining."
3. **Operations:** "Friendly or enemy operation – intentions progress, or results. Operational or logistic intentions; mission participants flying programmes; mission situation reports; results of friendly or enemy operations; assault objectives."
4. **Electronic warfare (EW):** "Friendly or enemy electronic warfare (EW) or emanations control (EMCON) intentions, progress, or results. Intention to employ electronic countermeasures (ECM); results of friendly or enemy ECM; ECM objectives; results of friendly or enemy electronic counter-countermeasures (ECCM); results of electronic support measures/tactical SIGINT (ESM); present or intended EMCON policy; equipment affected by EMCON policy."
5. **Friendly or enemy key personnel:** "Movement or identity of friendly or enemy officers, visitors, commanders; movement of key maintenance personnel indicating equipment limitations."
6. **Communications security (COMSEC):** "Friendly or enemy COMSEC breaches. Linkage of codes or codewords with plain language; compromise of changing frequencies or linkage with line number/circuit designators; linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure."
7. **Wrong circuit:** "Inappropriate transmission. Information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or it is not appropriate to the purpose for which the circuit is provided."
8. Other codes as appropriate for the situation may be defined by the commander.

In WWII, for example, the Japanese Navy, by poor practice, identified a key person's movement over a low-security cryptosystem. This made possible Operation Vengeance, the interception and death of the Combined Fleet commander, Admiral Isoroku Yamamoto.

## Electronic signals intelligence

---

Electronic signals intelligence (ELINT) refers to intelligence-gathering by use of electronic sensors. Its primary focus lies on non-communications signals intelligence. The Joint Chiefs of Staff define it as "Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from sources other than nuclear detonations or radioactive sources."<sup>[17]</sup>

Signal identification is performed by analyzing the collected parameters of a specific signal, and either matching it to known criteria, or recording it as a possible new emitter. ELINT data are usually highly classified, and are protected as such.

The data gathered are typically pertinent to the electronics of an opponent's defense network, especially the electronic parts such as radars, surface-to-air missile systems, aircraft, etc. ELINT can be used to detect ships and aircraft by their radar and other electromagnetic radiation; commanders have to make choices between not using radar (EMCON), intermittently using it, or using it and expecting to avoid defenses. ELINT can be collected from ground stations near the opponent's territory, ships off their coast, aircraft near or in their airspace, or by satellite.

## Complementary relationship to COMINT

Combining other sources of information and ELINT allows traffic analysis to be performed on electronic emissions which contain human encoded messages. The method of analysis differs from SIGINT in that any human encoded message which is in the electronic transmission is not analyzed during ELINT. What is of interest is the type of electronic transmission and its location. For example, during the Battle of the Atlantic in World War II, Ultra COMINT was not always available because Bletchley Park was not always able to read the U-boat Enigma traffic. But high-frequency direction finding ("huff-duff") was still able to detect U-boats by analysis of radio transmissions and the positions through triangulation from the direction located by two or more huff-duff systems. The Admiralty was able to use this information to plot courses which took convoys away from high concentrations of U-boats.

Other ELINT disciplines include intercepting and analyzing enemy weapons control signals, or the identification, friend or foe responses from transponders in aircraft used to distinguish enemy craft from friendly ones.

## Role in air warfare

A very common area of ELINT is intercepting radars and learning their locations and operating procedures. Attacking forces may be able to avoid the coverage of certain radars, or, knowing their characteristics, electronic warfare units may jam radars or send them deceptive signals. Confusing a radar electronically is called a "soft kill", but military units will also send specialized missiles at radars, or bomb them, to get a "hard kill". Some modern air-to-air missiles also have radar homing guidance systems, particularly for use against large airborne radars.

Knowing where each surface-to-air missile and anti-aircraft artillery system is and its type means that air raids can be plotted to avoid the most heavily defended areas and to fly on a flight profile which will give the aircraft the best chance of evading ground fire and fighter patrols. It also allows for the jamming or spoofing of the enemy's defense network (see electronic warfare). Good electronic intelligence can be very important to stealth operations; stealth aircraft are not totally undetectable and need to know which areas to avoid. Similarly, conventional aircraft need to know where fixed or semi-mobile air defense systems are so that they can shut them down or fly around them.

## ELINT and ESM

**Electronic support measures (ESM)** or **electronic surveillance measures** are ELINT techniques using various *electronic surveillance systems*, but the term is used in the specific context of tactical warfare. ESM give the information needed for **electronic attack (EA)** such as jamming, or directional bearings (compass angle) to a target in *signals intercept* such as in the huff-duff radio direction finding (RDF) systems so critically important during the World War II Battle of the Atlantic. After WWII, the RDF, originally applied only in communications, was broadened into systems to also take in ELINT from radar bandwidths and lower frequency communications systems, giving birth to a family of NATO ESM systems, such as the shipboard US AN/WLR-1<sup>[25]</sup>—AN/WLR-6 systems and comparable airborne units. EA is also called **electronic counter-measures (ECM)**. ESM provides information needed for **electronic counter-counter measures (ECCM)**, such as understanding a spoofing or jamming mode so one can change one's radar characteristics to avoid them.

## ELINT for meaconing

Meaconing<sup>[26]</sup> is the combined intelligence and electronic warfare of learning the characteristics of enemy navigation aids, such as radio beacons, and retransmitting them with incorrect information.

## Foreign instrumentation signals intelligence

FISINT (Foreign instrumentation signals intelligence) is a sub-category of SIGINT, monitoring primarily non-human communication. Foreign instrumentation signals include (but not limited to) telemetry (TELINT), tracking systems, and video data links. TELINT is an important part of national means of technical verification for arms control.

## Counter-ELINT

Still at the research level are techniques that can only be described as counter-ELINT, which would be part of a SEAD campaign. It may be informative to compare and contrast counter-ELINT with ECCM.

## SIGINT versus MASINT

---

Signals intelligence and measurement and signature intelligence (MASINT) are closely, and sometimes confusingly, related.<sup>[27]</sup> The signals intelligence disciplines of communications and electronic intelligence focus on the information in those signals themselves, as with COMINT detecting the speech in a voice communication or ELINT measuring the frequency, pulse repetition rate, and other characteristics of a radar.

MASINT also works with collected signals, but is more of an analysis discipline. There are, however, unique MASINT sensors, typically working in different regions or domains of the electromagnetic spectrum, such as infrared or magnetic fields. While NSA and other agencies have MASINT groups, the Central MASINT Office is in the Defense Intelligence Agency (DIA).

Where COMINT and ELINT focus on the intentionally transmitted part of the signal, MASINT focuses on unintentionally transmitted information. For example, a given radar antenna will have sidelobes emanating from a direction other than that in which the main antenna is aimed. The RADINT (radar intelligence) discipline involves learning to recognize a radar both by its primary signal, captured by ELINT, and its sidelobes, perhaps captured by the main ELINT sensor, or, more likely, a sensor aimed at the sides of the radio antenna.

MASINT associated with COMINT might involve the detection of common background sounds expected with human voice communications. For example, if a given radio signal comes from a radio used in a tank, if the interceptor does not hear engine noise or higher voice frequency than the voice modulation usually uses, even though the voice conversation is meaningful, MASINT might suggest it is a deception, not coming from a real tank.

See HF/DF for a discussion of SIGINT-captured information with a MASINT flavor, such as determining the frequency to which a *receiver* is tuned, from detecting the frequency of the beat frequency oscillator of the superheterodyne receiver.



A model of a German SAR-Lupe reconnaissance satellite inside a Soviet Cosmos-3M rocket.

## Legality

Since the invention of the radio, the international consensus has been that the radio-waves are no one's property, and thus the interception itself is not illegal.<sup>[28]</sup> There can, however, be national laws on who is allowed to collect, store, and process radio traffic, and for what purposes. Monitoring traffic in cables (i.e. telephone and Internet) is far more controversial, since it most of the time requires physical access to the cable and thereby violating ownership and expected privacy.

## See also

- Central Intelligence Agency Directorate of Science & Technology
- COINTELPRO
- ECHELON
- Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008
- Geospatial intelligence
- Human intelligence (espionage)
- Imagery intelligence
- Intelligence Branch (Canadian Forces)
- List of intelligence gathering disciplines
- Listening station
- Open-source intelligence
- Radio Reconnaissance Platoon
- RAF Intelligence
- Signals intelligence by alliances, nations and industries
- Signals intelligence operational platforms by nation for current collection systems



- SOT-A
- TEMPEST
- US signals intelligence in the Cold War
- Venona
- Zircon satellite
- Vulkan files leak

## References

1. "Signals Intelligence (SIGINT) Overview" (<https://www.nsa.gov/Signals-Intelligence/Overview/>). *nsa.gov*. HOME > SIGNALS INTELLIGENCE > OVERVIEW. Retrieved 3 December 2022. "National Security Agency/Central Security Service > Signals Intelligence > Overview"
2. Chapman, J.W.M. (2002). "British Use of 'Dirty Tricks' in External Policy Prior to 1914" (<https://www.jstor.org/stable/26014122>). *War in History*. **9** (1): 60–81. doi:10.1191/0968344502wh244oa ([http s://doi.org/10.1191%2F0968344502wh244oa](http://s://doi.org/10.1191%2F0968344502wh244oa)). ISSN 0968-3445 (<https://www.worldcat.org/issn/0968-3445>). JSTOR 26014122 (<https://www.jstor.org/stable/26014122>). S2CID 159777408 (<https://api.semanticscholar.org/CorpusID:159777408>).
3. Compare: Lee, Bartholomew. "Radio Spies – Episodes in the Ether Wars" (<https://web.archive.org/web/20080227075207/http://www.trft.org/TRFTPix/spies9eR2006.pdf>) (PDF). Archived from the original (<http://www.trft.org/TRFTPix/spies9eR2006.pdf>) (PDF) on 27 February 2008. Retrieved 8 October 2007. "As early as 1900 in the Boer War, the Royal Navy in South Africa appears to have used wireless sets inherited from the Royal Engineers to signal from the neutral port of Lourenco Marques 'information relative to the enemy' albeit in violation of international law. [...] This first use of radio for intelligence purposes depended, of course, on the inability of others to intercept the signals, but in 1900, only the British in that part of the world had any wireless capability."
4. *Report from HMS Diana on Russian Signals intercepted at Suez*, 28 January 1904, Naval library, Ministry of Defence, London.
5. Douglas L. Wheeler. "A Guide to the History of Intelligence 1800–1918" ([http://www.afio.com/publications/Wheeler\\_Hist\\_of\\_Intel\\_1800-1918\\_in\\_AFIO\\_INTEL\\_WinterSprg2012.pdf](http://www.afio.com/publications/Wheeler_Hist_of_Intel_1800-1918_in_AFIO_INTEL_WinterSprg2012.pdf)) (PDF). *Journal of U.S. Intelligence Studies*.
6. Winkler, Jonathan Reed (July 2009). "Information Warfare in World War I". *The Journal of Military History*. **73** (3): 845–867. doi:10.1353/jmh.0.0324 (<https://doi.org/10.1353%2Fjmh.0.0324>). S2CID 201749182 (<https://api.semanticscholar.org/CorpusID:201749182>).
7. Beesly, Patrick (1982). *Room 40: British Naval Intelligence, 1914–1918*. Long Acre, London: Hamish Hamilton Ltd. ISBN 0-241-10864-0.
8. Livesey, Anthony, *Historical Atlas of World War One*, Holt; New York, 1994 p. 64
9. "Code Breaking and Wireless Intercepts" (<http://marconiheritage.org/ww1-intel.html>).
10. Johnson, John (1997). *The Evolution of British Sigint: 1653–1939*. HMSO. p. 44. ASIN B002ALSXTC (<https://www.amazon.com/dp/B002ALSXTC>).
11. Smith, Michael (2001). "GC&CS and the First Cold War". In Smith, Michael; Erskine, Ralph (eds.). *Action This Day: Bletchley Park from the Breaking of the Enigma Code to the Birth of the Modern Computer*. Bantam Press. pp. 16–17. ISBN 978-0-593-04910-5.
12. Gannon, Paul (2011). *Inside Room 40: The Codebreakers of World War I*. Ian Allan Publishing. ISBN 978-0-7110-3408-2.
13. David Alvarez, GC&CS and American Diplomatic Cryptanalysis


14. Gross, Kuno, Michael Rolke and András Zboray, *Operation SALAM* ([http://fjexpeditions.com/resources/salam/operation\\_salam.htm](http://fjexpeditions.com/resources/salam/operation_salam.htm)) – László Almásy's most daring Mission in the Desert War, Belleville, München, 2013
15. Winterbotham, F. W. (1974), *The Ultra Secret*, New York: Harper & Row, pp. 154, 191, ISBN 0-06-014678-8
16. Hinsley, Sir Harry (1996) [1993], *The Influence of ULTRA in the Second World War* ([http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC\\_08e.PDF](http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF)) (PDF), retrieved 23 July 2012
17. US Department of Defense (12 July 2007). "Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms" ([https://web.archive.org/web/20091108082044/http://www.dtic.mil/doctrine/jel/new\\_pubs/jp1\\_02.pdf](https://web.archive.org/web/20091108082044/http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf)) (PDF). Archived from the original ([http://www.dtic.mil/doctrine/jel/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf)) (PDF) on 8 November 2009. Retrieved 1 October 2007.
18. "Precision SIGINT Targeting System (PSTS)" (<https://web.archive.org/web/20160314031126/http://fas.org/irp/program/process/psts.htm>). *Intelligence Research Program*. Federation of American Scientists. Archived from the original (<https://fas.org/irp/program/process/psts.htm>) on 14 March 2016. Retrieved 29 October 2015.
19. "About" (<https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/hall-of-honor/Article/2014217/chief-harry-kidder-usn/>). *nsa.gov*.
20. Whitlock, Duane (Autumn 1995). "The Silent War against the Japanese Navy" (<http://www.ibiblio.org/pha/ultra/nwc-01.html>). *Naval War College Review*. **48** (4): 43–52. Retrieved 30 September 2007.
21. 743d Military Intelligence (MI) Battalion (August 1999). "Warfighter Guide to Intelligence 2000" (<https://web.archive.org/web/20070814165342/http://www.gordon.army.mil/AC/Fall/Fall%2001/JSCmtrc.htm>). Joint Spectrum Center, (US) Defense Information Services Agency. Archived from the original (<http://www.gordon.army.mil/AC/Fall/Fall%2001/JSCmtrc.htm>) on 14 August 2007. Retrieved 26 October 2007.
22. Kessler, Otto. "SIGINT Change Detection Approach" ([https://web.archive.org/web/20080227075206/http://www.darpa.mil/DARPAtech2000/Presentations/tto\\_pdf/6KesslerDDBB%26WRev1.pdf](https://web.archive.org/web/20080227075206/http://www.darpa.mil/DARPAtech2000/Presentations/tto_pdf/6KesslerDDBB%26WRev1.pdf)) (PDF). *Dynamic Database: Efficiently Convert Massive Quantities of Sensor Data into Actionable Information for Tactical Commanders*. Defense Advanced Research Projects Agency. Archived from the original ([https://www.darpa.mil/DARPAtech2000/Presentations/tto\\_pdf/6KesslerDDBB&WRev1.pdf](https://www.darpa.mil/DARPAtech2000/Presentations/tto_pdf/6KesslerDDBB&WRev1.pdf)) (PDF) on 27 February 2008.
23. Terry, I. (2003). "US Naval Research Laboratory – Networked Specific Emitter Identification in Fleet Battle Experiment Juliet" (<https://web.archive.org/web/20071126144234/http://www.nrl.navy.mil/content.php?P=03REVIEW207>). *NRL Review*. Archived from the original (<http://www.nrl.navy.mil/content.php?P=03REVIEW207>) on 26 November 2007. Retrieved 26 October 2007.
24. Combined Communications-Electronics Board (CCEB) (January 1987). "ACP 124(D) Communications Instructions: Radio Telegraph Procedure" (<https://web.archive.org/web/20070901131123/http://www.nor.com.au/community/sarc/acp124~1.pdf>) (PDF). ACP 224(D). Archived from the original (<http://www.nor.com.au/community/sarc/acp124~1.pdf>) (PDF) on 1 September 2007. Retrieved 2 October 2007.
25. "AN/WLR-1" (<https://fas.org/man/dod-101/sys/ship/weaps/an-wlr-1.htm>). 1 January 1999. Retrieved 27 September 2015.
26. US Army (17 July 1990). "Chapter 4: Meaconing, Intrusion, Jamming, and Interference Reporting" ([https://fas.org/irp/doddir/army/fm24-33/fm243\\_5.htm](https://fas.org/irp/doddir/army/fm24-33/fm243_5.htm)). *Field Manual 23–33, Communications Techniques: Electronic Counter-Countermeasures*. FM 23–33. Retrieved 1 October 2007.
27. Interagency OPSEC Support Staff (IOSS) (May 1996). "Operations Security Intelligence Threat Handbook: Section 2, Intelligence Collection Activities and Disciplines" (<https://fas.org/irp/nsa/iOSS/threat96/part03.htm>). IOSS Section 2. Retrieved 3 October 2007.

28. "Radio Regulations Board of the ITU" (<http://www.itu.int/en/ITU-R/conferences/RRB/Pages/default.aspx>). *www.itu.int*.

## Further reading

- Bamford, James, *Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World* (Century, London, 2001) ISBN 978-0-7126-7598-7
- Bolton, Matt (December 2011). "The Tallinn Cables: A Glimpse into Tallinn's Secret History of Espionage" ([https://web.archive.org/web/20131113200915/http://www.hot.ee/aasa/LPL\\_1211.pdf](https://web.archive.org/web/20131113200915/http://www.hot.ee/aasa/LPL_1211.pdf)) (PDF). *Lonely Planet Magazine*. ISSN 1758-6526 (<https://www.worldcat.org/issn/1758-6526>). Archived from the original ([http://www.hot.ee/aasa/LPL\\_1211.pdf](http://www.hot.ee/aasa/LPL_1211.pdf)) (PDF) on 13 November 2013. Retrieved 25 June 2013.
- Biyd, J. A.; Harris, D. B.; King, D. D. Jr.; Welch, H. W., eds. (1979) [1961]. *Electronic Countermeasures*. Los Altos, CA: Peninsula. ISBN 0-932146-00-7.
- Gannon, Paul (2007) [2006]. *Colossus: Bletchley Park's Greatest Secret*. London: Atlantic Books. ISBN 978-1-84354-331-2.
- Jõgiaas, Aadu. "Disturbing Soviet Transmissions in August 1991" (<https://web.archive.org/web/201114094618/http://www.okupatsioon.ee/en/lists/47-aadu-jogisoo>). Museum of Occupations. Archived from the original (<http://www.okupatsioon.ee/en/lists/47-aadu-jogisoo>) on 14 November 2011. Retrieved 25 June 2013.
- West, Nigel, *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today* (William Morrow, New York, 1988)

## External links

-  Media related to SIGINT at Wikimedia Commons
- Part I of IV Articles On Evolution of Army Signal Corps COMINT and SIGINT into NSA ([http://www.armysignalocs.com/index\\_jan\\_14.html](http://www.armysignalocs.com/index_jan_14.html)) Archived ([https://web.archive.org/web/20140203201852/http://www.armysignalocs.com/index\\_jan\\_14.html](https://web.archive.org/web/20140203201852/http://www.armysignalocs.com/index_jan_14.html)) 3 February 2014 at the Wayback Machine
- NSA's overview of SIGINT (<https://www.nsa.gov/what-we-do/signals-intelligence/>) Archived (<https://web.archive.org/web/20160801024348/https://www.nsa.gov/what-we-do/signals-intelligence/>) 1 August 2016 at the Wayback Machine
- USAF Pamphlet on sources of intelligence (<https://fas.org/irp/doddir/usaf/afpam14-210/part16.htm>)
- German WWII SIGINT/COMINT ([https://web.archive.org/web/20110710143344/http://fykse.dnsalias.com/radio/dok/german\\_sigint.pdf](https://web.archive.org/web/20110710143344/http://fykse.dnsalias.com/radio/dok/german_sigint.pdf)) (PDF)
- Intelligence Programs and Systems (<https://fas.org/irp/program/index.html>)
- *The U.S. Intelligence Community* by Jeffrey T. Richelson (<https://books.google.com/books?id=BaeJNdRySPoC>)
- *Secrets of Signals Intelligence During the Cold War and Beyond* by Matthew Aid et al. (<https://books.google.com/books?id=KaR5O4PKNAoC>)
- Maritime SIGINT Architecture Technical Standards Handbook ([http://www.tscm.com/sigintarchms\\_h.pdf](http://www.tscm.com/sigintarchms_h.pdf)) (PDF)

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Signals\\_intelligence&oldid=1182698321](https://en.wikipedia.org/w/index.php?title=Signals_intelligence&oldid=1182698321)"

▪