MILITARY COMMUNICATIONS AND INTELLIGENCE

Harry Obi - Nwosu Ph.D
Dept. of Psychology,
Nnamdi Azikiwe University, Awka.

Abstract

Military communications represent all activities, equipment, techniques and tactics used by the military in hostile areas of the world to generate, gather, transmit and interpret information on land, in the sea or on air. The importance cannot be over emphasized since communication and intelligence not only aid countries to execute wars at least costs, but also prevent wars. Signals interpretation and analysis often depend on sophistication of a country's military technology, indeed, modern forms of warfare revolve around military communications and intelligence.

Key Words: Military, Communications, Intelligence.

INTRODUCTION

Military communications(mil comms) are activities, equipment, techniques and tactics used by the Military in some of the most hostile areas of the earth not only geographically but also from the point of view of the conditions of operations and equipment functionality like in battle fields, on land, underwater, air and whatever other conditions one can encounter. Military comms includes Command, Control, Communications and Intelligence which is also known as the C3I model. The Command here refers to the communication with the Highest Command in the country. The first military communications had the form of sending/receiving simple signals (often hidden or encoded to be unrecognizable for the enemy). Respectively, the first distinctive tactics of military communications were called Signals, while units specializing in those tactics received the Signal Corps name. Later, Signals and Signaller became a highly-distinct military occupation dealing rather with general communications methods (similar to those in civil uses) than with weapons. Present-day militaries of an informational society conduct very intense and complicated communicating activities on a daily basis, using modem high-tech telecommunications and computing methods. Only a small part of these activities is immediately related to the combat actions. That's why some prefer the term "military communications". As earlier mentioned, in 1934, the USSR invented the first military based equipment inside an automotive vehicle. Many pieces of military communications equipment are built to encrypt and decode transmissions and survive rough treatment in hostile climates. They use many frequencies to send signals to other radios and to satellites. http://en.wiktionary.org/wiki/signal. With the prevalent global orientation, which favours the avoidance of war at all costs, the role of the military comms is more intense, complicated, hi-tech, bordering on futuristic with the communication satellites, reconnaissance drones and aircraft. Computers and their varied uses have revolutionised military comms. Fortunately these activities are not only related to action in combat but also gathering intelligence to prevent war.

The following are categories of military comms: the alert measurement systems, cryptography, military radio systems, nuclear command control, and the signal corps. Another new concept is network-centric warfare. The alert measurement systems are various states of alert or readiness for the armed forces used world over - be it a state of war, terrorism or military attack against a state. They are known by different acronyms such as - DEFCON, INFOCON and REDCON in the US military comms, and BIKINI states in the British protocol. Cryptography is the study of methods of converting readable messages into guised unreadable information, unless one knows the methods of decryption. This

military comms method ensured that the messages reached the correct hands and eyes or ears. Nowadays digital cash, signatures, digital rights management and intellectual property rights and secure electronic commerce are its new purviews. It is also being used in computing, telecommunications and infrastructure.

There are close to 97 different categories of military comms by radio. To name a few are ACP-131, AN/ARC-164, AN/ARC-5, HWU transmitter, Hallicrafters SX-28, SCR-197, SCR-203, SCR-270 radar, etc.

COMMAND AND CONTROL

Command and control, (C2) in a military organization can be defined as the exercise of authority and direction by a properly designated commanding officer over assigned and attached forces in the accomplishment of the mission. The term may also refer to command and control systems within a military system. The DOD Dictionary of Military and Associated Terms defines it as the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (US Department of Defense).

Commanding officers are assisted in executing these tasks by specialized staff officers and enlisted personnel. These military staff are a group of officers and enlisted personnel that provides a bi-directional flow of information between a commanding officer and subordinate military units. The purpose of a military staff is mainly that of providing accurate, timely information which by category represents information on which command decisions are based. The key application is that of decisions that effectively manage unit resources. While information flow toward the commander is a priority, information that is useful or contingent in nature is communicated to lower staff and units.

C2 consists of several aspects and sub-domains, which are represented by derivative terms hereunder explained:

- C2I - Command, Control & Intelligence
- C2I - Command, Control & Information (A less common usage) C2ISR - C2I plus Surveillance
- C2ISTAR - C2 plus ISTAR : Intelligence , Surveillance, Target Acquisition , and Reconnaissance
- C3 - Command, Control & Communication (Human activity focus) C3 - Command, Control & Communications (Technology focus)
- C3I - 4 possibilities; the most common is Command, Control, Communications & Intelligence
- C3ISTAR - C3 plus ISTAR
- C3ISREW - C2ISR plus Communications plus Electronic Warfare (Technology focus) C4, C4I, C4ISR, C4ISTAR, C4ISREW - plus Computer (Technology focus) or computing (Human activity focus)
- C5I - Command, Control, Communications, Computers, Combat systems and Intelligence, and others.

In this context, Command is the exercise of authority based upon certain knowledge to attain an objective, while Control is the process of verifying and correcting activity such that the objective or goal of command is accomplished. Communication here is the ability to exercise the necessary liaison to exercise effective command between tactical or strategic units to command. Computers mean the computer systems and compatibility of computer systems as well as data processing while intelligence includes collection as well as analysis and distribution of information.

COMMAND AND CONTROL CENTERS

A Command and Control Center is typically a secure room or building in a government, military or prison facility that operates as the agency's dispatch center, surveillance monitoring center, coordination office and alarm monitoring center all in one. Command and control centers are operated by a government (at any level) agency. Various branches of the V.S Military such as the V.S Coast Guard have command and control centers. They are also common in many large correctional facilities. A command and control center that is used by a military unit in a deployed location is usually called a command post.

A warship has a Combat Information Center for tactical control of the ship's resources, but commanding a fleet or joint operation requires additional space for commanders and staff, plus C4I facilities provided on a Flagship (e.g. Aircraft Carriers), sometimes a Command ship or upgraded logistics ship such as USS Coronado (AGF-ll). There are other derivative terms especially in connection to control centers. It should be noted that some advanced forces like NATO have their specific terminologies or derivatives connected with control.

SIGNALS INTELLIGENCE

Signals intelligence often contracted to SIGINT is intelligence-gathering by interception of Signals, whether between people (communications intelligence - COMINT), whether involving electronic signals not directly used in communication (electronic intelligence _ ELINT), or combinations of the two. As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalys. Also, traffic analysis - the study of who is signaling whom and in what quantity - can often produce valuable information, even when the messages themselves cannot be decrypted. As a means of collecting intelligence, signals intelligence is a subset of intelligence collection management, which, in turn, is a subset of intelligence cycle management.

History

Intercepting written but encrypted communications, and extracting information, probably did not wait long after the development of writing. A simple encryption system, for example, is the Caesar cipher. Electronic interception appeared as early as 1900, during the Boer War. The Boers had captured some British radios, and, since the British were the only people transmitting at the time, no special interpretation of the signals was necessary (Batholomew, 2006).

More technical definitions of SIGINT and its branches

In the United States and other nations involved with NATO, signals intelligence is defined as: A category of intelligence comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and Foreign instrumentation signals intelligence, however transmitted. It is also Intelligence derived from communications, electronic, and foreign instrumentation signals (US Department of Defence, 2007).

The JCS definition may overemphasize "foreign instrumentation signals". That part should be considered in combination with measurement and signature intelligence (MASINT), which is closely linked to foreign instrumentation such as telemetry or radionavigation. An ELINT sensor may find a radar, and then cue (i.e., guide) a COMINT sensor for listening in on the talk between the radar and its remote users. A nonspecific SIGINT sensor can cue a Frequency Domain MASINT sensor that can help identify the purpose of the signal. If MASINT cannot identify the signal, then the intelligence

organization may task an IMINT aircraft or satellite to take a picture of the source, so photo interpreters can try to understand its functions.

Being a broad field, SIGINT has many sub-disciplines. The two main ones are communications intelligence (COMINT) and electronic intelligence (ELINT). There are, however, some techniques that can apply to either branch, as well as to assist FISINT.

Disciplines shared across the branches

Targeting: A collection system has to know how to look for a particular signal. "System", in this context, has several nuances. Targeting is an output of the process of developing /collection requirements/: "1. An intelligence need considered in the allocation of intelligence resources. Within the Department of De fen se, 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 (U.S. Department of De fen se (July 2007).

http://www.dtic.milldoctrine/jellnew_pubs/jpl_02.pdf.Retrieved2007-10-01]

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

Modem SIGINT systems, therefore, have substantial communications among intercept platforms. Even if some platforms are clandestine, there is a broadcast of information telling them where and how to look for signals (Federation of American Scientists). A U.S. targeting system under development in the late 1990s, PSTS, constantly sends out information that helps the interceptors properly aim their antennas and 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 underground direction. GUARDRAIL aircraft are fairly small, and usually work in units of three to cover a tactical SIGINT requirement, where 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, 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 part of foreign 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 (Wikipedia 20 11).

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. 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. Modem 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. Of course, 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 Kidde, for example, was one of the star cryptanalysts of World War II, a star hidden behind the secret curtain of SIGINT (Whitlock,1995).

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. Wikipaedia (2011(b). In the US, 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.   BEl: 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.

EOB and related data flow

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. U 1 from U2, requesting permission to proceed to checkpoint x.
2. U2 from U 1, approved. please report at arrival.
3. (20 minutes later) U 1 from 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 radiofrequency MASINT could help confirm that the traffic is not deception.

The EOB buildup process is divided as following: Signal, separation, Measurements optimization and Data Fusion Networks build-up. It is important that 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 deferent signals to different transmitters in the battlefield. The complexity of the separation process depends on the complexity of the transmission methods (e.g., hopping; 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 then the basic measurements of a standard direction finding sensor (Otto, 2000).

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 or radio frequency 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.

COMINT

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. It should be noted that 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 (US Department of Defense)

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 clear text 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, the encryption first must be solved through a process of introelectric diagram in order to listen to the conversation, although traffic analysis may give information simply because one station is sending to another in a radial pattern. It is important to check for various cross sections of conversation. It is equally important to mark the correct movement pattern in case the 'source changes position. Obviously, the interceptor must understand the language being spoken.

In the Second World War, the United States used 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., who did not grow up speaking the language. Even within these uncommon languages, the code talkers used specialized codes, so a "butterfly" might be a specific Japanese aircraft. British forces made more limited use of Welsh speakers for the additional protection. While modem electronic encryption does away with the need for armies to use obscure languages, it is certainly possible that guerrilla groups might use rare dialects that few outside their ethnic group would understand.

TEXT INTERCEPTION

Not all communication is in voice. Morse code interception was once very important, but Morse code telegraphy is now obsolescent in the western world, although possibly used by special operations forces. Such forces, however, now have portable cryptographic equipment. Morse code is still used by military forces of former Soviet Union countries. Specialists scan radio frequencies for character sequences (e.g., electronic mail) and facsimile.

SIGNALING CHANNEL INTERCEPTION AND MONITORING FRIENDLY COMMUNICATIONS

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 uses, this channel will carry messages in Signaling System 7 protocols. Retrospective analysis of telephone calls can be made from call detail records (CDR) used for billing the calls.

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 BEAD WINDOW codes. Standard BEAD WINDOW codes (e.g., "BEAD WINDOW 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 offriendly 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 World War II, for example, the Japanese Navy made possible the interception and death of the Combined Fleet commander, Admiral Isoroku Yamamoto, by BEADWINDOW 5 and 7 violations. They identified a key person's movement over a low-security cryptosystem (Wikipedia, 20 11 (b).

ELINT

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 other than nuclear detonations or radioactive sources (US Department of Defense). 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, 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 CO MINT

The combination of ELINT and other sources of information 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 COMINT was not always available because Bletchley Park was not always able to read the U-Boat Enigma traffic. But "Huff-Duff' (High Frequency Direction Finder) was still able to find where the U-Boats were 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. Yet 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 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 modem 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) are really ELINT techniques, but the term is used in the specific context of tactical warfare. ESM give the information needed for Electronic Attack (EA) such as

jamming. EA is also called Electronic Counter-Measures. 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 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. There are tales, perhaps apocryphal, that the meaconing was so confusing that an enemy aircraft landed, quite smoothly, at an airport of the other side (US Army FM 23-33, 1990).

FISINT

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.

SIGINT versus MASINT

A model of a German SAR-Lupe - reconnaissance satellite inside a Russian Cosmos-3M rocket. Signals intelligence, and measurement and signature intelligence (MASINT) are closely, and sometimes confusingly, related. 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) (Interagency OPSEC Support Staff (IOSS) (May 1996).

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 other than the direction in which the main antenna is aimed. The RADINT (radar intelligence) discipline involves learning to recognize 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.

Defensive signals intelligence

There are a number of ways that a person or organization can defend against signals intelligence. There is a delicate balance between the level of protection and the actual threat. One must begin by defining the threat. It is considerably more difficult to defend against detection that one is signaling, as opposed to defending against an opponent discovering the content of the transmitted message. Appropriate encryption can protect against content interception, but protecting against signal detection, especially with a capable opponent, requires measures to make the signal hard to detect - which can also make it difficult for the intended recipient to receive the signal. Any defensive program needs to consider the nature of the threat and the capabilities of the opponent.

Strong and well-managed encryption

Encryption is central to the defense. The encryption process is vulnerable if the cryptographic keys are not strong and protected, and, on computers, if the clear text is not j~kted when not needed.

Appropriate transmission security

When using radio transmitters, use directional antennas that have as little "spillover" into sidelobes as possible. If it is most important to hide the location of a transmitter, the rninimum is to cable the antennas as far as possible away from the transmitter proper. In many circumstances, aiming the antenna upward to a satellite will help hide its location. The amount of total transmission power needs to be minimized, and the power preferably should be split into multiple and changing frequencies using spread spectrum techniques. If possible, avoid transmitting when hostile SIGINT satellites or monitoring aircraft are overhead. If in an urban area, avoid using regular commercial power to transmit. There are ways in which the signal can "leak" into power and ground lines. The adversary may turn off power to an area, which will tell him there is a line-operated transmitter if the transmission stops, and that there is a battery-powered transmitter if it continues. Use highly variable transmission schedules and vary frequencies if technically possible (Wikipedia).

Appropriate receiving security

If Operation RAFTER -style intercept is a threat, protect against this form of unintentional radiation MASINT by using optoisolators or other shielded techniques (e. g., waveguides) to bring in the radio frequency received signal, and shield the local oscillator and intermediate frequency stages in the superheterodyne receiver. This technique should be far less effective against the new generation of software-defined radio. Unintentional radiation on power or ground circuits is a threat here as well; use appropriate TEMPEST or other techniques.

Protection against compromising emanations

There are risks that electronic, acoustic, or other information could "leak" from a computer system or other electronic communications devices. Understanding details of the risks requires a substantial knowledge of electronics, but a simple example might serve. Many people have put a radio receiver near a computer, to listen to music as they work, and discovered that the radio suffered clicks, squeals, and other interference. These interfering signals are radiating from various parts of the computer, especially its display but often also from the power and grounding system. TEMPEST is the name for one family of protective measures against an opponent intercepting these emanations and extracnng sensitive information from them.

While not strictly within the scope of protecting against "leakage" a place where sensitive information is processed or discussed needs protection against hidden microphones, wiretaps, and other "bugging". Sometimes, an electronic sweep to verify TEMPEST compliance reveals the presence of hidden transmitters. Again, there is probably more suspicion than reality in most cases. A member of a crime organization in the middle of a nasty divorce, or a foreign intelligence agent might have reason to worry, but, even with the serious questions about warrantless surveillance in the US and other countries, there is little reason for someone to go to the risk and expense of illegal Surveillance on an ordinary citizen. TEMPEST is usually associated with direct electromagnetic r3d:3tion from the device, either free-space or through power and ground lines. TEMPEST generically talks about acoustic isolation, but that is fairly easily solved through physical security and noise damping, as well as searches for microphones. There are several threats that have not been officially defined in the unclassified literature. Nevertheless, there are some informed guesses (McNamara, 2002).

NONSTOP is a threat that involves some type of coupling of compromising RF energy from a classified system, which "leaks" into an independent RF-transmitting or -recording device such as cell phones, PDAs, pager, alarm systems. Commercial AM/FM radios are not considered a risk.

HIJACK is a similar threat of coupling, but to some type of digital computer or related equipment.

TEAPOT is a very different vulnerability, which appears to apply to incidental audio modulation of the backscatter from an RF, typically microwave, directed into the secure area. A passive resonant cavity bug of this type was discovered in a Great Seal of the United States presented by the USSR, but containing a resonant cavity with a wall that moved with sound in the room, thus imposing frequency modulation onto the backscattered signal.

Mitigation and countermeasures.

The word TEMPEST itself, and its meaning, are unclassified. Some of the techniques for measuring the compliance of a piece of equipment, or whether it is actually emitting compromising emanations, are classified. A good deal of the information has come into public view either through Freedom of Information Act queries, books talking about interception techniques, inferences drawn from partially released documents, and straightforward thinking by electronic engineers (Wikipedia)

Protection against side channel attacks and covert channels: A side channel attack is an unintentional vulnerability of an encryption device, not related to the encryption algorithm I http://www.scientificamerican.com/article.cfm?id=hackers-can-steal-from-reflections) Potential vulnerabilities include different processing and thus transmission speeds for blocks of plaintext with certain statistical characteristics, changes in power consumption, or compromising emanations. Covert channels are deliberate means to elude communications security (National Computer Security Center 1993). They send out an unauthorized signal by stealing bandwidth from a legitimate, often encrypted channel. One low-bandwidth method would be to send information by varying the inter-block transmission times. A steganographic covert channel might use the low-order bit of pixels in a graphic image, perhaps not even consecutive pixels, in a manner that would not be obvious to a person looking at the graphic.

REFFERENCES

Federation of American Scientists, (?). Precision SIGINT Targeting System (PSTS). http://www.fas.org/irp/prograrnlprocess/psts.htm

lnteragency OPSEC Support Staff (IOSS), (1996). Operations Security Intelligence Threat Handbook: Section 2, Intelligence Collection Activities and Disciplines. http://www.fas.org/irp/nsalioss/threat96/part03.htm. Retrieved 2007 -10-03.

Kessler, O. (2000). SIGINT Change Detection Approach.

http://www.darpa.milIDARPATech2000IPresentations/tto_pdf/6KesslerDDBB& WRev 1. p dfRetrieved Through Wikipedia 20 11- 07 - 19.

Lee, B. (2006). Radio Spies - Episodes in the Ether Wars. http://www.trft.orglTRFTPixlspies9eR2006.pdf. Retrieved 2007 -10-08.

McNamara, J. (2002). (1990). The Complete Unofficial TEMPEST Information Page. http://www.eskimo.com/~joelm/tempest.html. http://www.scientificamerican.com/artic1e.cfm?id=hackers-can-steal-from-reflections

National Computer Security Center (1993). "NCSC-TG-030 VERSION-l A Guide to

Understanding Covert Channel Analysis of Trusted Systems ("Light Pink Book")"

http://www.fas.orglirp/nsalrainbow/tg030.htm

US Department of Defense, (2007). Joint publication 1-02 Deparmlent of Defense Dictionary of Military and Associated Terms.

http://www.dtic.milldoctrine/jel/ new _pubs/jp 1_02. pdfRetrieved 2007 -10-01

US Army Field Manual 24 - 33, (1990). Communications Techniques: Electronic Counter-Countermeasures. http://www.fas.org/irp/doddir/army/fm2.f-33fm243_5.htm.

Retrieved Through Wikipedia 2011-07 -09

Whitlock, D. (1995). "The Silent War against the Japanese Navy" Naval War College Review: XLVIII (4).