CONVERGENCE BETWEEN SIGNALS INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT MEASURES

Zsolt HAIG
haig.zsolt@uni-nke.hu
National University of Public Service, Budapest, Hungary

ABSTRACT

In this paper the author introduces the common and different features of signals intelligence and electronic warfare support measures, as well as interprets the content of intelligence and combat information. The paper shows the role of low probability of intercept transmission modes in the modern tactical communications. It focuses on the challenges to signals intelligence and electronic warfare support measures. Finally the author emphasizes the necessity of integration of signals intelligence and electronic warfare including electronic warfare support measures.

KEYWORDS: *SIGINT, ESM, LPI transmission modes, intelligence, combat information*

1. Introduction

Today, the effectiveness of modern armed forces is significantly based on the usage of electromagnetic spectrum. Electromagnetic spectrum has a significant role in functioning of command and control systems and weapon guidance systems. The electromagnetic spectrum is used in a wide range for communication, weapon guidance, intelligence, surveillance, reconnaissance, target acquisition, navigation etc. Numerous electronic assets are applied for these functions on the battlefield.

New digital devices and systems - have been developed by the information technology revolution – appear on the battlefield. The advanced civilian technology is becoming more frequently used by armed forces and by non regular military actors like insurgents. In the military operations, the new technologies have been used to extend system ranges, improve security and to provide information throughout the battlespace. Among these the new digital technologies, the low probability of intercept (LPI) transmission modes are a significant challenge to the signals intelligence (SIGINT) and electronic warfare (EW). So, as the battlefield becomes more technologically sophisticated, military forces execute operations in an increasingly complex electromagnetic environment. Therefore coordination is important between SIGINT and electronic warfare including electronic warfare support measures (ESM).

2. Signals Intelligence

There are myriad of electronic devices with different types and purposes on the battlefield. This area of military operations – regarding the operations in the electromagnetic spectrum – could be

described as electronic battlefield. According to a type of classification these devices could be the following:

- non-communications devices:
  - intelligence, surveillance and reconnaissance devices that ensure data collection from all source on the battlefield;
  - air defense devices ensuring air surveillance, targeting and missile guidance;
  - air traffic control and navigation devices;
  - electronic warfare devices that are used to intercept, disrupt, degrade and deceive the adversary's electronic systems;
- communications devices that are a group of electronic assets, which is applied in the greatest number in the battlespace, and they ensure connection between superiors, subordinates and neighbors.

These devices operate in the same electromagnetic environment that is: *"the totality of electromagnetic phenomena existing at a given location"* [1]. It is the electronic theatre of military affairs, when simultaneous electronic activities are carried out by both friendly and enemy forces. Due to the above listed numerous electronic emitters and the finiteness of electromagnetic spectrum, this environment is very crowded. Consequently, electronic equipment must be able to operate in this crowded electromagnetic environment. Moreover activities in this crowded electromagnetic environment are becoming further complicated by SIGINT and electronic warfare.

SIGINT is *"the generic term used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two"* [2]. Communications intelligence provides *"intelligence derived from electromagnetic communications and communication systems by other than intended recipients or users"* [3]. Electronic intelligence provides *"intelligence derived from electromagnetic non-communications transmissions by other than intended recipients or users"* [4].

SIGINT may be either strategic or tactical. Strategic SIGINT intercepts and monitors the overall equipment, systems and deployment of opponent's forces and may give warning of new techniques, tactics and procedures. Tactical SIGINT intercepts, locates and identifies the enemy's military forces, their communications and other electronic systems as well as application of them on the battlefield. In this essay we focus on the tactical one.

SIGINT consists of these below listed data collection methods:

- search;
- interception;
- direction finding.

Search is the first phase of data collection process of SIGINT that involves reconnaissance of the adversary's electronic activity in the electromagnetic spectrum to detect and classify radiated electromagnetic signals of interest. In case of signals of interest are identified in the search process, they are examined for their external technical characteristics, such as frequency, modulation, and bandwidth. This is the interception phase of data collection, when we can determine fingerprint of signals. Fingerprinting refers to the process of identifying an emitter by the unique characteristics of its spectrum. In some cases, it may be possible to identify not only the type of emitter but also an individual item of equipment. In addition beside detection and interception the location of emitters is necessary too, so different direction finding and location techniques must be applied. Direction finding can be used to provide information on the approximate location of emitters. The purpose of radio direction finding to determine line of bearing (LOB) of any source of electromagnetic radiation using

nature of radio waves propagation. It is predicated on the basic principle of triangulation to find the right position of an emitter. Finally one of the main goals of SIGINT including COMINT is gathering information content. The course of interception the determination of information content of communication is important too if it is possible at tactical level. To obtain the internal information content, often referred to as monitoring [5].

The final result of SIGINT is the intelligence as the product. The intelligence is *"the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity"* [6].

3. Electronic Warfare Support Measures in the Electronic Warfare

Electronic warfare is defined as: *"military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects"* [7]. Electronic warfare is an integral part of every kind of military operations and it is a capability of information operations. Electronic warfare consists of three complementary and partly overlapping areas, such as:

- electronic counter measures (ECM);
- electronic protective measures (EPM) and
- electronic warfare support measures (ESM) (see Figure no. 1).

The three areas are defined in the AAP-6 NATO Glossary of Terms and Definitions. According to this, electronic countermeasures: *„That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are three subdivisions of electronic countermeasures: electronic jamming, electronic deception and electronic neutralization"* [8].

Electronic protective measures: *„That division of electronic warfare involving actions taken to ensure effective friendly use of the electromagnetic spectrum despite the enemy's use of electromagnetic energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures"* [9].

Electronic warfare support measures: *„That division of electronic warfare involving actions taken to search for, intercept and identify electromagnetic emissions and to locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving electronic countermeasures, electronic protective measures and other tactical actions"* [10].

Electronic warfare employs many tactics, techniques and procedures to reach its aim. These are illustrated in Figure no. 1.

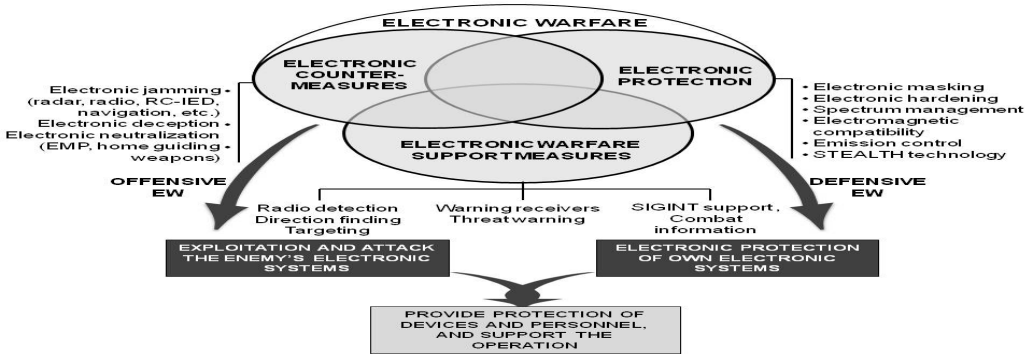

Fig. no. 1 Areas and Capabilities of Electronic Warfare

Source: edited by the author

The main goal of electronic warfare is to exploit and attack the enemy's electronic systems as well as to ensure the functioning of own similar systems, thereby to provide protection of devices and personnel and to support military operations. According to this, electronic warfare has an offensive and a defensive side (see Figure no. 1).

There is a close connection between the three elements of electronic warfare. An ESM system usually operates together with electronic countermeasures and electronic protective measures systems to form a unified electronic warfare capability. It provides target and threat warning information for the other two.

Regarding to the definition, the ESM obtains information about electromagnetic spectrum used by an adversary. In other words these activities detect, identify and exploit the enemy's radiated signals. These radiated signals can be from any type of deliberate transmitter such as from radios in communication networks, radars, telemetry transmitters, and other unintentional transmitters e.g. infra-red radiations of a jet engine.

Important information can be gained from the measurement of a few so called external parameters associated with a transmission. These parameters could be the frequency, the modulation type, the bit rate, the location of the transmitter or other spectral features. In some cases it is also possible to intercept the so called internals of a transmission, namely the information content. In this case we talk about SIGINT, where the goal is to generate intelligence products about an adversary. ESM is usually restricted to collection of external parameters [11].

ESM provides combat information. The combat information is *"that frequently perishable data gathered in combat by, or reported directly to, units which may be immediately used in battle or in assessing the situation. Relevant data will simultaneously enter intelligence reporting channels"* [12].

Combat information collected by the ESM is primarily used to immediate threat recognition and warning, targeting for electronic or destructive attack as well as contribute to construction of an electronic order of battle (EOB). Combat information is necessary to:

- electronic countermeasures;
- electronic protective measures;
- self-protection;
- create and update electronic warfare database;
- confirm information deriving from other sources, as well as
- support information operations.

4. Challenges to Signals Intelligence and Elctronic Warfare Support Measures

Thanks to the development and proliferation of digital technology, many new modulation and transmission methods appeared on the field of communications technology during the last decades. Mobile cell phone systems, mobile internet, WiMax, worldwide navigation via GPS and different spread spectrum technologies are some examples that represent the new technological development. In the military sphere, many of these new technologies have been used to improve security and to provide information on the battlefield. These commercial systems are used by the armed forces because they are in some cases better than their own systems and they can be fielded more quickly than new military systems [13].

These new technologies complemented with encryption techniques pose a serious challenge to SIGINT and ESM. The new digital wireless communication systems have made it clear the traditional analog communications intelligence equipments and systems are unusable to intercept them. Today on the battlefield the spread spectrum techniques represent very high challenge to SIGINT and ESM at tactical level.

Resistance to jamming, LPI and multiple access are the major motivations for the use of spread spectrum transmission mode in military communications systems. The spread spectrum techniques are the best example of LPI, because interception and jamming of these transmission modes is not possible or greatly difficult. Spread spectrum signals have special modulations which spread their spectrum over a very wide bandwidth and are used for selective addressing, hiding transmitted signals, and rejecting interfering signals. Spread spectrum techniques provide transmission security, so they make it difficult to detect the presence of a signal in the spectrum. If message security is required, encryption must be added to the spread spectrum transmission mode [14].

There are several types of spread spectrum techniques. The most frequently used types are:

- frequency hopping spread spectrum (FHSS);
- direct sequence spread spectrum (DSSS).

Chirp spread spectrum (CSS) should be mentioned also. It is mostly used in radar systems but is not common in communications systems, so we do not deal with it further in this essay.

The common features of spread spectrum techniques are the following:

- bandwidth of the spread spectrum signal is greater than the information bandwidth and
- the spreading sequence is independent from the information, so to calculate the information is impossible if the sequence is known and vice versa.

3.1. Frequency Hopping Spread Spectrum

Frequency hopping technique is widely used in military communications systems because the conventional interception, direction finding, and jamming techniques are not effective against them. In this mode the transmitter periodically changes the frequency of transmission and by knowing the hopping sequence, the receiver follows the changes in frequency and is able to receive the transmission (see Figure no. 2). In order to provide protection against interception and resistance to jamming, it is necessary to use a pseudo-random hop sequence [15].

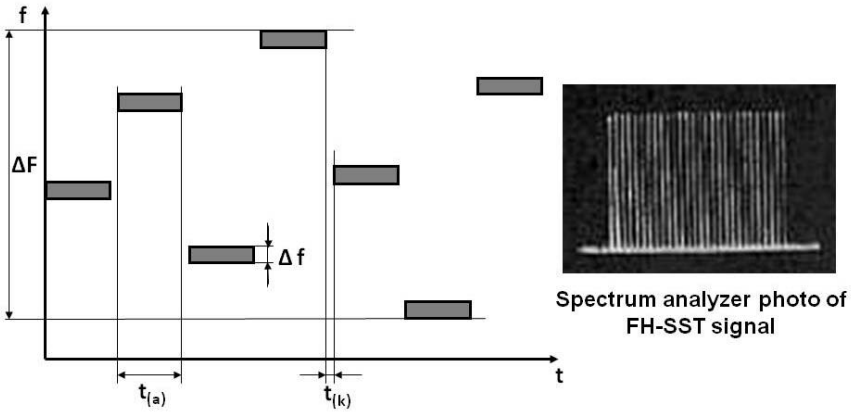

Fig. no. 2 Frequency Hopping Spread Spectrum
Source: based on [16] edited by the author

The receiver must synchronize itself to the transmitter. It can be realized by transmitting synchronization code, or using an accurate time reference (e.g. GPS) known to both transmitter and receiver. The hopping frequencies are selected by a pseudo-random code generator and normally spaced at regular intervals (e.g. 25

kHz) and cover a very wide frequency range (e.g. 30-88 MHz). Frequency hopping could be slow or fast hopping. Slow hopping means that hop rate slower than the data rate (e.g. some 10-100 hop/ sec). Fast hopping refers to the hop rate faster than the data rate (e.g. approx. 1000 hop/sec).

Frequency hopping transmissions are relatively difficult to detect using narrowband search receivers. The detection only takes place when the frequency of the hopping transmission coincides with the frequency of the scanning receiver. The probability of this is very low, because the presence of a frequency hopping signal is too short. A digital wideband receiver is more suitable for the detection of frequency hopping transmissions because it can effectively monitor a number of channels simultaneously. Direction finding of a frequency hopping transmitter requires detection and direction finding to carry out within the dwell time. This is the reason that integration is needed between search, detection and direction finding [17]. However without knowing the synchronization code to get the information content out of transmission is very complicated, in a short time it is not possible.

3.2. Direct Sequence Spread Spectrum

Direct sequence spread spectrum signal is actually spread in frequency rather than being rapidly tuned across a wide frequency range. This technique is used in many military and civil applications because it is extremely hard to detect and intercept, it has a good interference protection and can also provide multiple use of a frequency band.

In direct sequence spread spectrum data signal is multiplied by a binary pseudo-random sequence. The frequency of this is much higher than the data signal. The transmitted signal is similar to white noise. At the receiver, the original data signal is restored from this white noise type signal by multiplying it with the same binary pseudo-random sequence (see Figure no. 3). A direct sequence signal continuously occupies a wide frequency range. This signal power is distributed over this extended range, the amount of power transmitted within the information bandwidth of the signal is reduced by the spreading factor.

In a typical application, the amount of signal power from a direct sequence spectrum signal will be much less than this amount of noise power [18].

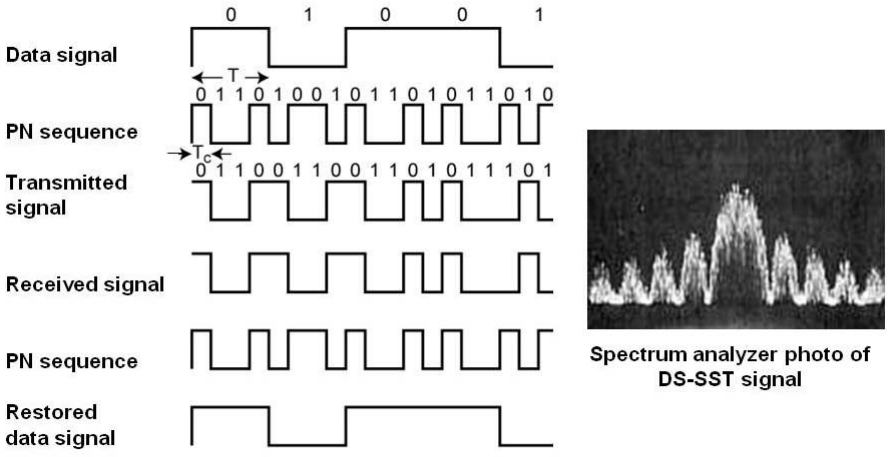

Fig. no. 3 Direct Sequence Spread Spectrum

Source: based on [19], [20] edited by the author

A principal advantage of direct sequence spread spectrum that the spreading of transmitted signal reduces the power in any one channel below the noise floor of conventional receiver, so detection and interception with analog receivers is impossible.

5. Integrated Signals Intelligence and Electronic Warfare Support Measures

ESM and SIGINT also operate in the electromagnetic spectrum and use the same electromagnetic resources. The difference between them is the type and using of collected information, the depth of signal analysis and the time lines required. As we mentioned earlier, while SIGINT obtains intelligence (as product), ESM provide combat information that can be used to real-time threat warning and targeting for electronic countermeasures, e.g. communications jamming.

Intelligence – provided by SIGINT – is resulted from the detailed signal processing and it has relatively longer validity time. The ultimate result of data processing of SIGINT is to produce internal information content that is used in commander's decision making process. Considering the LPI techniques producing information content is extremely difficult.

On the other hand the combat information can be reached by the fast and not detailed analyzing and processing of the interested signals and it has a short validity time. In this aspect SIGINT differs to ESM also, because this latter does not require any information content, but it provides time critical, so called external information (e.g. frequency using, modulation, location, etc.) about operation of adversary's emitters.

However from the beginning there are many common features of ESM and SIGINT in an operational environment. Data collection techniques, namely the search, detection, interception and location are common to both ESM and SIGINT operations. Therefore they use the same or very similar data collection methods and means for these functions.

Detection, interception and direction finding of the LPI transmission methods are a serious challenge to the SIGINT and ESM. Among the LPI techniques, the frequency hopping systems are becoming the most widely used in the military operations at tactical level. The main missions of the data collection process of a frequency hopping transmission are:

- to detect the radiated signal;
- to ascertain the transmission comes from a frequency hopping radio;
- to determine whether one or more frequency hopping transmission are received;
- to select the target signal;
- to determine the main technical parameters of transmission, such as total hopping frequency range, hop time, hop rate, modulation type, etc.;
- to locate transmitter;
- to produce information content of transmission (if it is possible).

To accomplish these missions is almost impossible with analog techniques. Traditional sweeping and panoramic narrowband receivers are not suitable for detection because they should be capable to sweep the total bandwidth during a hop time (i.e. a few ms) to catch a frequency hopping signal. In addition they should separate this signal from other transmissions. Therefore digital receivers provide greater opportunities for detection and interception instead of analog narrowband receiver. Channelized receiver, Bragg cell receiver, compressive receiver and receiver using software defined radio (SDR) technology are some examples to use in this mission.

Of course at tactical level there is no possibility to get the information content out of the LPI transmission by the above mentioned systems. It requires high performance computing and it is a time

consuming process that cannot be carried out on the battlefield. Therefore SIGINT including COMINT activities must be reinterpreted.

As a result of the widespread emergence of LPI techniques the upshot of SIGINT is not the information content but the radiofrequency fingerprint radiated by the emitter. This means that the COMINT becomes ELINT type, in other words it can define only the detailed parameters of the signals of interest and the location of the emission. As we explained earlier the function of ESM is the same namely the analyzing of the received signal parameters in order to targeting. Thus at tactical level the differences seem to be disappearing between the SIGINT and the ESM.

Considering the above in order to better mission coordination, the SIGINT and ESM activities should be carried out in an integrated structure at tactical level. The integrated COMINT-ESM system enables search, detection and interception, direction finding, emitter location and detailed signal analysis (radiofrequency fingerprints) under a unified command and control. The integrated SIGINT-ESM system provides:

- elimination of the parallel activities;
- better exploitation of assets and troops;
- better mission distribution;
- coordinated mission execution;
- generating and visualizing of the equally interpreted electronic order of battle.

On one hand in the integrated SIGINT-ESM system the collected and analyzed information provides the necessary target information for the electronic warfare including electronic countermeasures (e.g. communications jamming), on the other hand this information is integrated in the all-source intelligence system to contribute the commander's decision making process.

Recognizing the challenge discussed earlier, several countries have begun to develop integrated SIGINT-ESM systems [21], [22]. These systems provide near real-time tactical SIGINT and ESM capability including high probability of interception with extended interception ranges and close support to tactical forces on the battlefield, as well as relevant intelligence reports to commander's decision. A jamming capability is integrated in these systems also, so if it is necessary they can disrupt the enemy's communications.

6. Conclusions

There are many new digital info-communications technologies on the battlefield, which increase the commander's command and control capabilities. These technologies could be found among the command, control, communications, computer and intelligence (C4I) systems. In the field of tactical communications the LPI transmission modes are a significant challenge to the SIGINT and ESM, because the spread spectrum techniques (as LPI transmission modes) have extreme protection against interception and jamming.

In case of LPI transmission methods the detection, interception and direction finding of the signals of interest are achievable by digital receivers, but in a short time there is no possibility to produce the information content. It is a serious problem for SIGINT because it has to produce intelligence but during its activities the information content cannot be deciphered. Therefore SIGINT can produce only the signal parameters of the transmission and locate the emitter, and these are matched with functions of the ESM.

In order to have better mission coordination, the SIGINT and the electronic warfare including ESM activities are planned and accomplished in an integrated intelligence and electronic warfare structure based on unified command and control. In this structure the collected and analyzed information can be used more efficiently both to targeting and decision making

REFERENCES

1. AAP-6 *NATO Glossary of Terms and Definitions*, (NATO Standardization Agency, 2014) 2-E-2.
2. *Ibidem,* 2-S-5.
3. *Ibidem,* 2-C-10.
4. *Ibidem,* 2-E-2.
5. Michael R. Frater and Michael Ryan, *Electronic Warfare for the Digitized Battlefield*, (Norwood: Artech House, 2001), 112.
6. AAP-6, *cit.ed.,* 2-I-6.
7. *Ibidem,* 2-E-2.
8. *Ibidem*.
9. *Ibidem*.
10. *Ibidem,* 2-E-3.
11. Richard A. Poisel, *Introduction to Communication Electronic Warfare Systems* (Norwood: Artech House, Inc. 2008), 5.
12. *Ibidem,* 2-C-7.
13. Adrian Graham, *Communications, Radar and Electronic Warfare,* (Chichester: John Wiley and Sons Ltd. Publication, 2011), 4.
14. David L. Adamy, *EW 103 Tactical Battlefield Communications Electronic Warfare,* (Norwood: Artech House, 2009), 31.
15. Michael R. Frater and Michael Ryan, *cit.ed.*, 79.
16. Randy Roberts, *Introduction to Spread Spectrum,* http://www.sss-mag.com/ss.html (accessed June 30, 2014).
17. Michael R. Frater and Michael Ryan, *cit.ed.*, 83.
18. David L. Adamy, *cit.ed.*, 44.
19. *Wireless Networking*, http://ironbark.xtelco.com.au/subjects/DC/lectures/22 (accessed June 30, 2014).
20. Randy Roberts, *cit.ed.*
21. Prophet, http://fas.org/man/dod-101/sys/land/wsh2013/272.pdf (accessed June 30, 2014).
22. EL/I-6063 Integrated Mobile Ground-based SIGINT & EW System, http://www.iai.co.il/sip_storage/FILES/4/37544.pdf (accessed June 30, 2014).