**Advanced Engineering Days**

aed.mersin.edu.tr

# Electronic interference and protection from it

**Fatmir Basholli** *[1]

[1]*Albanian University, Department of Engineering, Tirana, Albania, e-mail: fatmir.basholli@albanianuniversity.edu.al/ fbasholli@yahoo.com*

Cite this study: Basholli, F. (2022). Electronic interference and protection from it. 5th Advanced Engineering Days, 74-76

**Keywords**
Electronic interference
Systems
Spectrum
Electronic protection
Frequencies

**Abstract**

The main purpose of this article is to present the importance of complex protection from this advanced electronic technology which is an important part to achieve objectives at different levels of a conflict or a military operation. Electronic interference is used to enhance capability and ensure superiority over the adversary. Control of the electromagnetic spectrum has a major impact on the success of military operations. Modern weapons and support systems utilize radio, radar, infrared, optical, laser and ultraviolet technologies. Electronic interference has a major role in ensuring and maintaining the independence of action in an electromagnetic environment, it is vital in the formation, content, dominance, stabilization and capabilities in the various phases of an operation. The level of electronic intervention helps the leaders of the operation to understand the battlefield, to organize, structure and harmonize the actions with the various civil authorities, etc. Electronic interference applications are important to restrain, detect, prevent various threats such as missiles, aircraft, ships, terrorist groups, cyber threats, etc. The experience from the applications of electronic intervention allows to ensure the normal functioning of communication and information systems as well as the independence of the work of different systems, which makes it interesting to study and include different security structures of a country.

## Introduction

*Electronic interference* is the totality of measures and efforts that are carried out for the use of directed electromagnetic energy, ie to control the electromagnetic spectrum. Nowadays, the use of this spectrum for directing weapon systems, for observation and detection, etc. is increasing. The use of the electromagnetic spectrum is an integral part of military and civilian operations [1].

The electromagnetic spectrum is a composite of oscillating electric and magnetic fields that propagate at the speed of light. It includes radio frequencies, infrared rays, light rays, ultraviolet rays, gamma rays and X-rays. Radio frequencies, as part of the electromagnetic spectrum, include the radio wave and microwave band from 3 kHz to 3000 GHz. *Show fig. 1*

The purpose of electronic interference is to provide complete information on the adversary, damage its electromagnetic spectrum during the entire time of the operation and protect our electromagnetic spectrum from the attacks of the adversary [2].

The main purpose of this article is to present the importance of background control and surveillance of this spectrum with the aim of increasing the detection capacity of electronic intrusions and focusing on effective protective measures. The main components of electronic intervention are:

*Electronic attack* that includes actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum or of weapons that use electromagnetic energy; Electronic defense includes actions taken to protect personnel, facilities and equipment from the effects of the use of electronic warfare by adversary forces; *Electronic support* that includes actions to capture, identify and locate sources of electromagnetic energy radiated intentionally or not, for immediate hazard determination. It includes actions determined to seek, capture, identify and locate sources of electromagnetic energy radiated intentionally or unintentionally with the aim of immediate recognition of threats, of targets, planning and implementation of future actions; *Electromagnetic*

*interference* encompasses any electromagnetic disturbance that interrupts, impedes or reduces and limits the normal operation of electrical and electronic equipment. Electromagnetic interference is the intentional introduction of electromagnetic energy into transmission paths to cause confusion; *Electromagnetic stability* consists of the actions taken to protect personnel, objects and equipment by means of transmission, attenuation, burial, limitation and protection against the unwanted effects of electromagnetic energy; *Electromagnetic jamming* is the intentional radiation, re-radiation or reflection of electromagnetic energy to prevent or reduce the effective use of electromagnetic energy and damage an adversary's combat power; *The electromagnetic impulse* is a powerful electronic impulse, with a short duration, that with the electric and electronic fields it creates, can completely or temporarily damage the electrical and electronic systems; *Electronic masking* is the controlled radiation of electromagnetic energy at our frequencies ensuring the protection of transmission and electronic systems from supporting measures of electronic interference; *Electronic recording* is intentional radiation, determined to be introduced into the equipment or systems of the adversary, with the aim of learning about the operation and operational capabilities of the equipment and systems; *Electronic reconnaissance* is the detection, location, identification and evaluation of electromagnetic radiation. Electronic discovery is a technical and multifaceted discovery that benefits from external electromagnetic radiation; *Electronic security* is the protection resulting from all the measures established to deny unauthorized persons valuable information that could have benefited from their capture and study of non-communicating electromagnetic radiation; *Emissions control* means the selected and controlled use of electromagnetic energy transmitters to make the best use of command and control capabilities and minimize adversary detection and interception and mutual interference; *Spectrum management* involves the planning, coordination and administration of the use of the electromagnetic spectrum through operational, technical and administrative procedures [3-6].

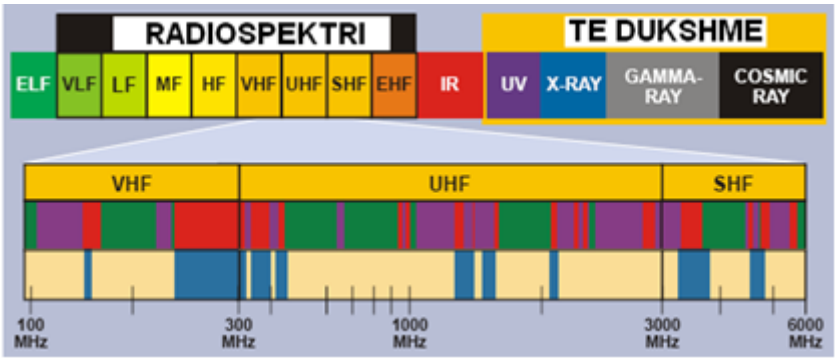


**Figure 1.** View of the breakdown of the electromagnetic spectrum

## Material and Method

Electronic attack has two main sub-components, jamming and electronic spoofing.

(a) Jamming is the interruption of the signal before it reaches the intended receiver. Blocking radiation by means of blocking includes equipment that radiates: for example, the transmission of electromagnetic energy in order to disrupt radio and radar transmissions.
(b) Re-radiation jamming, uses the collected transceiver signal to receive the adversary's transmissions, alters them in some way, and re-radiates the signal back to him. The two devices used are repeaters and transponders.
(c) Reflection blocking confuses opposing electronic systems, thus degrading their effectiveness. The three effective jammers are exciter, loop and corner reflectors. Examples include government treaty frequencies as well as RADAR frequencies used for missile control and rapid air defense alerting.

Likewise, electronic fraud with the creation of the list of necessary frequencies is of particular importance. This list summarizes all the necessary electromagnetic spectrum within an operation area and is the basis for frequency support during all phases of operation planning. It is vital to prevent tampering and helps optimize the use of limited electronic tampering resources [7,8].

## Results and Discussion

The implementation of electronic protection, is carried out following several main methods such as: Avoiding the use of transmissions perpendicularly, in contrast to our communication signals. By eliminating perpendicularity, we reduce the chance of an adversary successfully using electronic interference to disrupt our communications. The use of terrain camouflage consists of placing communication antennas in positions that give

advantages in the protection of the apparatus using the features of the terrain and also the buildings and fortified facilities built for this purpose. The use of directional systems such as microwave and satellite, or other systems such as frequency modulation (FM) and encrypted radios, the use of directional antennas oriented parallel to the front. The use of terrain cover and the remote placement of the power emitting antenna system create real impossibility for the adversary to identify the object from which it is being transmitted. The increase in false transmissions and especially the most effective way to protect our communication is to limit the emission to the greatest possible distances and to use radio silence whenever possible [9].

Secondary communication is envisaged and provided as an alternative route and means communications during non-critical moments. This will prevent the adversary from collecting and analyzing information on our primary system beforehand. As a result, the collected information is often useless, due to the greater time required to analyze and process it for decryption, especially in cases of the alphanumeric encoding system.

Primary communication systems use advanced technological equipment and are protected from visual and satellite surveillance. This can be accomplished by careful use of camouflage and by installing antennas on the opposite side of slopes, behind natural obstacles, and by using encrypted electronic systems [10].

Highly directional antennae. These antennas are used to cover a sector where jamming is present, thus nullifying the effects of useless signals. Multi-function antenna. Multi-functionality allows multiple radios to work on the same antenna, making it possible to reduce and physically display multiple antennas without compromising communication quality. Systems of a wide spectrum. These systems spread the transmitted signal over a very wide frequency band, so it becomes difficult to detect and separate the signal in the noise environment. Automatic frequency adjustment. Systems that have this feature reduce the output power to the minimum required to maintain stable communication. This reduces the range at which the signal can be captured and analyzed [11].

## Conclusion

Nowadays, referring also to the Russia-Ukraine war, electronic interference is a reality and an important element of command-and-control operations. In the planning, organization and development of electronic interference, different structures, detection, communication and radio detection are included in an integrated manner. The provision of communication and information systems depends directly on electronic intervention. A successful electronic intervention is dependent on personnel training in the use of electromagnetic energy, and the appropriate amount of frequency band.

Electronic warfare must be evaluated in the complex with all elements of the communication and information system, whether they are communication, non-communication or electro-optical systems.

An important role in the implementation of protection measures against electronic interference is the use of new technologies and the advantages of technology must be recognized when dealing with the electronic interference of the adversary.

## References


1. Allan, C. T. (1998). Electronic Warfare: Foundation of Information Operations. *Journal of Electronic Defense*, *21*(10), 59-66.
2. Bowen, A. (2022). Russia's war in Ukraine: Military and intelligence aspects. *Congressional Research Service*, *47068*.
3. Ogunsola, A. (2008). EMC and functional safety requirements for integrated electronics systems. In Electronics system-integration technology conference, ESTC 2008, Sept.2008 (pp. 69–74).
4. Nelson, J. J., Taylor, W., & Kado, R. (2012, March). Impact on EMC for electrical powertrains with respect to functional safety: ISO 26262. In *2012 IEEE international electric vehicle conference* (pp. 1-7). IEEE.
5. Jaekel, B. W. (2007, July). Recent developments in standardization related to EMC and Functional Safety. In *2007 IEEE International Symposium on Electromagnetic Compatibility* (pp. 1-6). IEEE.
6. Fiore, N. J. (2017). Defeating the Russian battalion tactical group. *Armor: Mounted Maneuver Journal*, 9-17.
7. Fernandez-Garcia, R., Gil, I. (2012). Impact of temperature on the electromagnetic susceptibility of operational amplifiers. In Progress in electromagnetics research symposium proceedings Moscow, Russia, August 19–23, 2012 (pp. 1063–1065).
8. Boyer, A., Sentis, M. G., Ghfiri, C., & Durier, A. (2017, July). Study of the thermal aging effect on the conducted emission of a synchronous buck converter. In *2017 11th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMCCompo)* (pp. 79-84). IEEE.
9. Lavarda, A., & Deutschmann, B. (2015, August). Effects of single tone RF interferences on chopped operational amplifiers. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)* (pp. 96-101). IEEE.
10. ISO 26262 (2011). Road vehicles—functional safety. 1st ed. International Electrotechnical Commission, November 2011.
11. Glantz, D. M. (2018). The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces.