THE CURRENT STATE OF RESEARCH IN ELECTRONIC SURVEILLANCE SYSTEMS MANAGEMENT; JAMMING AND COUNTER JAMMING

Mihai-Alin MECLEA, Liviu GĂINĂ, Mircea BOȘCOIANU

”Transilvania University”, Brașov, Romania (mihai.meclea@unitbv.ro,
liviu.gaina@unitbv.ro, boscoianu.mircea@yahoo.com)

DOI: 10.19062/2247-3173.2021.22.6

Abstract: *We all saw an important development of weapons containing electronic devices and systems. Not so many years ago, military specialists were considering that precision will make the difference in combat and that precision must be increased using electronics. First, it was stated that augmenting the explosive charge ten times, will increase the effectiveness of the hit only five times. On the other hand, the precision of weapons systems increased 10 times will increase the effectiveness of the hit 100 times. A single surgical shot will be enough to annihilate the target.*

In the same time, when considering a defensive approach, a very sensitive issue has become the management of electronic surveillance (ES) systems, not only in the military, but also in civilian use. Those ES systems must work properly, at full capacity and in a secured and private environment.

In jamming area, new techniques are developed constantly. We witness the integration of AI (artificial intelligence) in ECM (electronic counter measures) systems and the solution to bring the EW (electronic warfare) payload on UCAVs (unmanned combat aerial vehicle). Also new techniques to counter jamming are emerging.

Keywords: *electronic surveillance, jamming, electronic counter measures*

1. INTRODUCTION

We all acknowledge important developments of weapons containing electronic devices and systems. Not so many years ago, military specialists were considering that precision will make the difference in combat and that precision must be increased using electronics. First, it was stated that augmenting the explosive charge ten times, will increase the effectiveness of the hit only five times. On the other hand, the precision of weapons systems increased 10 times will increase the effectiveness of the hit 100 times. A single surgical shot will be enough to annihilate the target.

In EW (electronic warfare) domain, first you should choose correctly your target and also use a single electronic attack action against it, with one hundred percent efficiency, if possible. This should be done in order to avoid being exposed on your next possible second „shot”, to annihilate or disable the target and accomplish the mission received.

In the same time, when considering a defensive approach, a very sensitive issue has become the management of electronic surveillance (ES) systems, not only in the military, but also in civilian use. Those ES systems must work properly, at full capacity and in a secured and private environment.

We also witness the integration of AI (artificial intelligence) in ECM (electronic counter measures) systems and the solution to bring the EW payload on UCAVs (unmanned combat aerial vehicle).

2. THE MANAGEMENT OF ELECTRONIC SURVEILLANCE SYSTEMS

Very recently, Russian Federation military forces have brought to Kazakhstan, along with other tracked and wheeled light armored vehicles, an electronic warfare system that includes small drones equipped with jammers. The LEER-3 system, which consists of the KAMAZ truck and between two and three specially configured ORLAN-10 drones, is primarily intended to scramble cell phone communications. The truck serves as the ground control center for these small unmanned aircraft, which carry small electronic warfare jammers. ORLAN-10 drones also carry full-motion video cameras and, while their range is relatively limited, could be used to help monitor continued protests and otherwise provide improved situational awareness to military commanders [1].

We see here the use of both electronic surveillance (ES) systems and jamming capabilities in a crisis situation. ES systems are effective in a common Electromagnetic Environment (EME), which is not too complex or too dense and is able to produce a good electromagnetic scenario translated into a very useful EOB (electronic order of battle) for the decision making process.

In the situation described above, jamming capabilities were used to bring advantage or to precisely solve a problem in a small range (the protest area in Almaty, the country's former capital). Usually, this type of action is well hidden and covers large areas in the batlefield or the operation theatre.

The target of the jamming is also different. Those ORLAN-10 drones, a relatively new capability of the russian arsenal, were targeting cell phone communications, which is modern technology, a very powerful weapon nowadays. In the past, the common targets of the jammers were HVT s (high value targets) as command and control centers, strategic communications, information centers, EW systems, surface-based air defence systems or fighter bombers.

But ES systems are very common today also in civilian things. We talk more and more about IoT (Internet of Things), integration of AI (artificial intelligence) in everyday life and smarter and greener means of transportation. Many activities have quickly moved online, forced in some cases by the pandemic started in 2019. We study online, we use the Internet to pay bills or to protect our goods and our gadgets and smart devices ”talk” to us or with each other. In all cases, these devices must be secured and protected in order to make our life easier.

3. JAMMING AND COUNTER JAMMING TECHNIQUES

The jamming can be passive or active. The active jamming is intended against air-borne radar systems, radio networks and directions for fire command and control or HF (high frequency) or UHF (ultra high frequency) communication signals. The active jamming emitters, including those of single use, can be placed or parachuted on the ground, but they are also common on aerial vehicles (piloted or unmanned) and on naval platforms.

In communication jamming area, new techniques are developed constantly. Also new improved techniques to counter jamming are emerging. The weapon-counter weapon concept is again well applied and validated.

The communications have evolved from Morse code to wired telephony and GSM technology to the large scale use of satellites. The amount of information transmitted has grown exponentially against limitation of time needed to search and collection, analysis, processing and dissemination processes. More secured, encrypted and permanent channels are required in order to enhance the C2 (command and control) process and satellite communications bring obvious advantage. These transmissions are not time and weather affected, are hard to be jammed, covers large areas, are quick and quite discreet.

Communication jamming techniques are classified as follows [2]:

- **Noise jamming** is when jamming signal is modulated with a common noise signal. It could be **Broadband Noise** jamming or full band jamming or **Partial-Band Noise** jamming – in this case the noise energy is spread across a number of channels, but not all channels of our target. These channels could be in sequence or apart. The **Narrowband Noise** jamming uses all energy directed on a particular channel. It can affect all width of that channel or just a specific portion carrying data.

- **Pulse jamming**: the signal of jamming consists in a broadband noise for a limited portion of time. For the rest of time that signal is off. It is considered that this type of jamming is more effective than partial-band noise jamming against Direct Sequence Spread Spectrum (DSSS) targets.

- **Tone jamming:** in this case, a single tone or more are placed in the frequency spectrum. The single tone jamming (or spot jamming) is also effective against DSSS targets because it can overcome the processing gains and may cause bad effects at dispreading. Comb jamming uses tones in consecutive channels, gaining more flexibility comparing to spot jamming.

- **Swept jamming** uses a narrowband signal, similar to a tone. But in most cases, this jamming signal is a partial-band noise signal that sweeps in time across the frequency band of the target. This type of jamming is similar to barrage jamming. The difference between those two is that the power of swept jamming signal is focused in each dwell bandwidth. The speed of the sweeping process is also very important because the entire band of the signal jammed must be covered in a very short period of time.

- **Follower jamming**: in this jamming technique, also known as responsive jamming, repeater jamming, and repeat-back jamming, the jammer tries to detect the RF (radio frequency) signal to be damaged and tunes to that frequency. The time is very important here as well, as the jammer must act in limited portions of time related to the propagation and processing sequences of the signal of interest.

- **Adaptive jamming** is also a follower jamming technique used to counter more than one target at the same time. The effects of this type of jamming are similar to those of barrage jamming, but in this case, the energy radiated is more concentrated on specific targets well chosen.

- **Smart jamming,** a relatively new technique, is targeting portions of digital signals in order to deny communications. In many cases, the jamming signal is affecting paging channels, pilot channels or synchronization channels. In order to be successful, the jammer must obtain the Channel State Information (CSI) of the attacked channel.

According to the Allied Joint Doctrine for Cyberspace Operations ,,the Alliance finds itself operating in increasingly interconnected environments, in particular, cyberspace and the information environment (IE)"[3]. The free flow of data and continuous functioning of information networks have become critical for the civil society and for military forces. State or non-state entities seek to exploit vulnerabilities in military and non-military information systems to exfiltrate, corrupt or destroy data or to gain prestige, political or military advantage or profit.

Digital networks and systems, therefore, need to be safeguarded against information denial by disruption, degradation or destruction, and manipulation and exfiltration. In an interconnected world where military success may depend as much on the ability to control one's narrative as the ability to create physical effects, freedom of action in cyberspace may be as important as control over land, air and space, or sea.

In order to counter jamming, two types of actions are taking into consideration: Low Probability of Intercept (LPI) and Low Probability of Detection (LPD) techniques, which are applied when we want to avoid interception and detection, and anti-jamming (AJ) techniques, when maintaining our line of communication is needed, even while jamming is still active.

The LPI/LPD waveform design is chosen to attenuate the RFI (Radio Frequency Interference) problem with minimal distortion when RFI information is available, while providing signal security. When information is unavailable, RFI is detected, notched, and autoregressive filtering applied to recover the target signals.

Usually, some organizational and technical measures are taken to avoid being jammed: use of terrain and clutter shielding, power management, frequent changes of frequency, intermittent use of your systems, use of antennas with nulls or low energy output in the direction of jammers or highly directional ones and spoofing.

One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done through a specific frequency, the frequency can be changed if necessary. Another solution consists in engaging the jammer on the jammed channel and continuing communication in another clean channel.

4. CONCLUSIONS

The management of electronic surveillance systems has an increasingly important role in a complex information environment. Tendencies in jamming are the introduction of cross-eye jamming, new LPI/LPD techniques or more efficient single use jamming emitter and expandable decoys (chaff and flare). Emerging and innovative technologies are widely intensively integrated in Electronic Warfare.

5. REFERENCES

[1] https://www.thedrive.com/the-war-zone/43785/russian-sent-electronic-warfare-systems-and-armored-vehicles-to-kazakhstan-for-peacekeeping-mission, accesat la 20.01.2022;

[2] Jasmin A. Mahal, *Analysis of Jamming-Vulnerabilities of Modern Multi-carrier Communication Systems,* Arlington, 2018;

[3] NATO STANDARD AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations,* Edition A Version 1, 2020.