EW SYSTEMS MANAGEMENT. A CRITICAL REVIEW IN THE ACTUAL CONTEXT OF MULTIPLE CRISIS AND TURBULENCES

Mihai-Alin MECLEA, Eugen Silviu VRĂJITORU, Mircea BOȘCOIANU

”Transilvania” University of Brașov, Romania (mihai.meclea@unitbv.ro, eugen.vrajitoru@unitbv.ro, boscoianu.mircea@yahoo.com)

DOI: 10.19062/2247-3173.2023.24.4

Abstract: *The paper refers to the management of electronic warfare systems and the latest approaches in this field. Also, some important main historical milestones and new development trends in the field of EW (Electronic Warfare) are being discussed. Finally, after identifying the relationship between ECM (electronic counter measures) and ES (electronic support) and the gaps in the current research of electronic warfare systems, it has been shown how is this domain influenced in the current context of multiple turbulences and crises.*

Keywords: *Electronic Warfare, systems management*

1. INTRODUCTION

For this article we have formulated the following research questions:

• What are the main historical milestones and new development trends in the field of EW (electronic warfare)?

• What are the latest approaches in the management of electronic warfare systems and the relationship between ECM (electronic counter measures) and ES (electronic support)?

• What are the gaps in the current research of electronic warfare systems?

• How is the EW domain influenced in the current context of multiple turbulences and crises?

To answer the study questions formulated, we applied a widely used methodology to conduct a systematic review of the literature based on the preferred reporting elements for systematic reviews and meta-analyses (PRISMA 2020) [1]. We conducted a search in scientific databases that include important journals and conferences in the field studied such as IEEE Xplore, the ACM digital library, ScienceDirect, SAGE Journals Online and Springer Link, to discover relevant articles in the field of electronic warfare. We used the following search string to discover the publications and papers relevant to this research: ("Electronic Warfare" OR "Electronic Surveillance") in the fields of electrical engineering, applied physics, telecommunications, defense, and information systems, for the last six years (2018-2023). In total, we have gathered a set of about 7500 potentially relevant publications, except for gray literature and preprints.

I further analyzed the titles, keywords, and summaries of publications to find documents and articles that fit my area of interest, and I selected a total of eighty-nine relevant publications. We have also studied the bibliographic resources of the selected publications with the aim of expanding our own database.

2. HISTORICAL LANDMARKS AND NEW DEVELOPMENT TRENDS IN THE FIELD OF EW

In the conflicts conducted after the Second World War, all known means and methods of electronic warfare are referring to electronic jamming to the destruction with fire of the opponent's electronic means.

The means of neutralization by electronic jamming arranged on board the means of air attack are for the creation of jamming against the electronic missile and anti-aircraft artillery control systems, the fighter aviation and for preventing the work or misleading the electronic means of radiolocation research from the equipment of the anti-aircraft defense forces. For this purpose, the military used electronic means of attack installed on impactors and aircraft specially designed for electronic warfare, false radar targets and infrared traps. The Air forces launched bombs and air-to-ground guided missiles against the radar stations and the positions of the anti-aircraft missile control stations.

The tactical procedures of electronic warfare execution have changed and have evaluated as the characteristics of the armaments and the technique of electronic surveillance and attack evolved.

In the Korean War, the U.S. Air Force used B-26 aircraft equipped with electronic attack means that usually evolved before the strike group.

In the Vietnam War, the electronic research was executed by the USA with strategic bombing aircrafts of type B-52 and research planes RF-101 A that operated from heights of up to 11000 m, constituted in formations of 16-20 aircrafts, in the composition of the hit groups or outside them, with the evolution in one direction. The RF-101 A research aircrafts were taking pictures of the terrain, with an accuracy of 0.5 m, after which the pilots received the photos to prepare for the execution of the radar jamming and the air attack, after about 15 minutes from the landing of the research planes. To create false aerial situations on the screens of the radiolocation stations, metallic cardboard reflectors launched with a parachute were used, as well as special anti-radiation cartridges that were fired in the anterior hemisphere of the planes' flight direction. There were also used trap missiles (of type MQM-74 A) equipped with equipment for creating active and passive jamming and ground jamming transmitters arranged on dominant heights close to the contact line.

In the 1967 conflict between Israel, on the one hand, and Egypt, Syria and Jordan, on the other hand, electronic warfare was carried out by all categories of armed forces, with the aim of disorganizing the radio links of troop management and neutralizing the electronic means of discovering the means of air attack and of directing anti-aircraft missiles and fighter aviation. During the execution of the first strike, Israeli forces disorganized by jamming the radio connections of the opponents, neutralized the radar stations of the anti-aircraft defense and on board the planes. The execution of electronic warfare measures and disinformation have negatively affected the conduct and coordination of electronic warfare actions of the ground forces, aviation and anti-aircraft defense means of Arab countries.

In the War in the Middle East since 1973, electronic warfare has been used based on experience gained in previous wars in Vietnam and the Near East. On the one hand, it was aimed at neutralizing the electronic means and systems of aviation, anti-aircraft defense, tank units and subunits of the adversary and on the other hand, on the protection of own forces. About 30% of the Israeli strikers were equipped with electronic jamming means, of American origin, and some of them with anti-radar missiles of SHRIKE type. The electronic jamming means were installed on fighter-bomber aircrafts of type F-4 E "PHANTON- II", A-4 E "SKYHAWK" and MIRAGE-III-C, on unmanned aircrafts and

on other special jamming creation installations. The F-4 E and A-4 E aircrafts had snapped containers with radar irradiation equipment of the aircraft (RWR) and active jamming stations of type AN/ALQ-71 (87) and AN/ALQ -19 (55, 100) respectively. Passive jamming made using AN/ALE-29 systems (on A-4E aircrafts) equipped with thirty-two cartridges with dipole reflectors, as well as aviation bombs with dipole reflectors, was also used.

The Arab Israeli conflict in Lebanon since 1982 it has been distinguished by the scale of electronic warfare actions. Active and passive jamming was widely used, which led to air targets being discovered extremely late by Syrian air defense systems.

Before the air attacks were carried out, Israeli forces acted on the Syrian anti-aircraft defense system, with unmanned aircraft and missiles that created clouds of dipole reflectors above the anti-aircraft defense system and mimicked a large number of targets, resulting in the complete "flooding" of the radiolocation station screens, on which it was very difficult to distinguish the real targets from the false ones. For the diversion of infrared-guided missiles, the Israeli air force effectively used overheated balloons for the first time.

In the Anglo-Argentine conflict concerning the Malvin Islands (Falkland), the electronic countermeasures of the English consisted in the use of passive and active jamming in naval warfare. The success of the EXOCET-type missiles used by the Argentine forces was 50% (three out of six missiles hit the targets), and that of the ground-ship ones was 25% (one missile out of four hit the targets). To repel the attack of the aerial means provided with modern anti-ship missiles, the English used the unguided missile projectiles KORVUS, SEAFAN, STOCKADE, loaded with antiradar dipole made of metallized glass wool, aluminum foils and other materials. Due to the opportune use of passive jamming, but also of the active one, no SEA HARRIER aircraft was hit by missiles with radar self-routing heads, launched from the ground.

In the Gulf War , electronic research began intensively as early as August 1990 with Key Hales 11, 12, Lacrosse, TRDS, SDS satellites to obtain the data and information necessary to conduct military operations. The data obtained was entered in the memoirs of cruise missiles Cruise and Tomahawk from ships and submarines. Subsequently, the distant electronic research aircraft AWACS, U-2 and TR-1 were used. The laser marking of some targets (the SCUD Iraqi missile launch facilities), in the depth of Iraqi territory by diversionary scouts, was constituted in support measures for further e-warfare actions. 24 hours before the conflict began, the Allies used SKY SHADOW systems to execute ECM against Iraqi systems. Electronic countermeasures were executed against radar, radio, radio navigation and radio relay means. The "electronic shield" has designated all electronic protection measures used by the Allies. Ef-111 aircraft flew in front of the hit formations and executed active barrage jamming and target imitation (with AN/ALQ-99E systems). In all the air raids conducted, the formations of aircraft had in their composition electronic warplanes: EA-6B, F-4G, Wild Weasel, for group protection, which determined that the reaction of the Iraqi anti-aircraft defense to be weak, conducted with classical means of fire. "STEALTH" planes were also used.

The factors that contributed to the victory in this conflict are:

-the application of electronic warfare measures in the preparation and conduct of military actions had a primary role in achieving success;

- the rapid obtaining of the air and maritime supremacy allowed the combat aircrafts equipped with the most modern air-to-air, air-to-ground missile systems, laser, or video guided bombs, to execute unbroken bombings, these being intensified during the offensive of the ground forces;

- the use of state-of-the-art weapons at that time, with a high impact accuracy (cruise missiles, anti-radar missiles, anti-aircraft missiles, laser-directed artillery shells, research-impact systems, helicopters equipped with guided anti-tank missiles, airplanes equipped with "STEALTH" technology)
- the rapid achievement of victory by the infantry troops, permanently supported by "APACHE" helicopters carrying directed anti-tank missiles and armored aircrafts of the "A-10" type, equipped with projectiles capable of penetrating the armor of the Iraqi tanks;
- logistical organization and coordination throughout the operation;
- high morale of allied forces.

In the events of December 1989 in Romania, through electronic diversion, the aim was to achieve a large consumption of aviation resources and ammunition of artillery and anti-aircraft missiles. At the same time with the imitated aerial targets, in the Romanian airspace, real targets also evolved, which flew under the protection of a strong active radiolocation jamming.

In the events of the former Yugoslavia (90s), the actions of electronic warfare supported an intense confrontation in the electromagnetic environment between the Serbian anti-aircraft defense troops and the Air Force of the Alliance.

3. APPROACHES TO ELECTRONIC WARFARE SYSTEMS MANAGEMENT

3.1 Intelligence Push Technology

The advantages of information superiority exceed those of technological superiority.

Informational superiority generates advantage in the decision-making process in a dynamic space, permanently changing but especially in an armed confrontation, a fact recently demonstrated including in the war in Ukraine. The process of its own "intelligence" (processing and analyzing data and information obtained in diverse ways) must always be doubled by the prohibition of the same process executed by the adversary.

Among the technologies still used, we list the "distribution "on request" to combatants of the information processed that raises the following issues:

- lack of radar data about air targets at any given time;
- the low level of scalability of the collaborative filtering algorithms of this data;
- currently, the collection, processing and analysis of radar data is conducted manually;
- the information technology does not consider the type/need for information requested;
- the personalization of the transmitted information is strictly based on the subjective requirements of the military and does not consider the combat environment;
- "Information overload" - too much information received at a time, or "information lack" - total lack of information.

The modern technologies currently used are:

- IPT ("Intelligence Push Technology"): which involves the generation of three models: user model, Intel model (type of information) and model "Push" (mode of transmission of information), selected with the support of artificial intelligence. This eliminates the flow of information on demand and automates the transfer of information. Information resources become dynamic, are transmitted in real time and information needs are automatically changed according to the transformations in the battle space [2];
- "Service discovery": automatic identification of services and devices in a computer network;
- „Information mining;”

- HUMINT (Human Intelligence): information provision services (obtained by human operators) adapted to the needs of combatants;

- Machine Learning, managing "Big data" and the widespread use of artificial intelligence.

3.2 Agent-Principal theory

The application of the problem Main agent involves the designation of the radar system in the role of "Principal", that is, the owner of the company, the role of the "agent" (manager hired on the basis of a contract) being the responsibility of the equipment with which the jamming is performed (jammer or ECM system- electronic counter measures) [3] .

Between the two there is a clear information asymmetry, as follows:

- The objectives of the main (radar) are to discover as many air targets as possible, with the best possible accuracy, to identify the destructive ECM actions of the agent (jamming) and to apply countermeasures – ECCM against it, allowing it to continue the basic mission – airspace surveillance;

- The agent seeks to decrease the accuracy with which the principal discovers air targets, or even missing some of them by applying the ECM. The jamming applied has certain costs and, to increase efficiency, it should be continuous.

This creates an ECM-ECCM covariance, the independent variable being the air target.

The subject untreated in the literature involves the reversal of roles: the main one to be a system or an assembly of mobile terrestrial RE systems and the agent – the radar system on board the opponent's aviation.

Information asymmetry in this situation it is explained as follows:

- The main (offensive electronic warfare system) aims to affect as many opposing on-board radars as possible, with the means at their disposal, to hinder or prevent the actions of the opponent. The aim is to limit the operating costs and to avoid discovering the location of the RE technique in order not to be destroyed;

- The agent aims to discover with the best possible accuracy the elements to be destroyed on the Earth's surface by reducing the effects of the soil jamming performed by the principal.

An ECM-ECCM covariance is also created here, the independent variable being the terrestrial objective to be destroyed by the adversary.

On the other hand, a direction of research involves the designation of many "agents" with several distinct roles and redefining the objectives pursued by the "principal".

3.3. Game theory

The strategy of dynamic allocation of jamming resources simultaneously on-air targets (air raid) can be approached through Game Theory. The novelty is the simulation of dynamic scenarios because approaches with static scenarios have been conducted in the past.

The final stable solution of the stated problem involves identifying the "Nash equilibrium" (NE – Nash Equilibrium) and subsequently choosing the most effective algorithm for learning the response.

It is obvious that the role of the RE executed by one's own forces involves collecting information about the opponent and influencing his actions. The means of jamming are always limited, and this directly influences the effectiveness of one's own jamming actions.

To date, various methods have been identified to optimize the allocation of jamming resources, for example: "Genetically Adapted Immune Allocation Algorithm", "Simulated Annealing Algorithm" [6] or "Hungarian Algorithm [7].

The formulation of the problem of dynamic allocation of jamming resources simultaneously, on several targets, using Game Theory, starts from the initial assumption that in this case we are talking about a potential game, with at least one Nash balance. It aims to identify a final solution / stable strategy with a reduced complexity of processing input data.

The initial data are as follows:

The letter M denotes the number of jamming systems and N, the number of targets to be combated at a given time. It follows that:

M = set of jamming systems, N = set of targets

M = {1,2.... M}, N = {1.2.... N}

According to [9], because there is a certain distance between targets, a jamming signal is considered to cover/hit a single aircraft.

It is known that the opponent is moving information, using a "COMAO" type of force pack (Combined Air Operation) intended for the execution of a specific mission consisting of between eight and over one hundred aircraft of diverse types. [10]

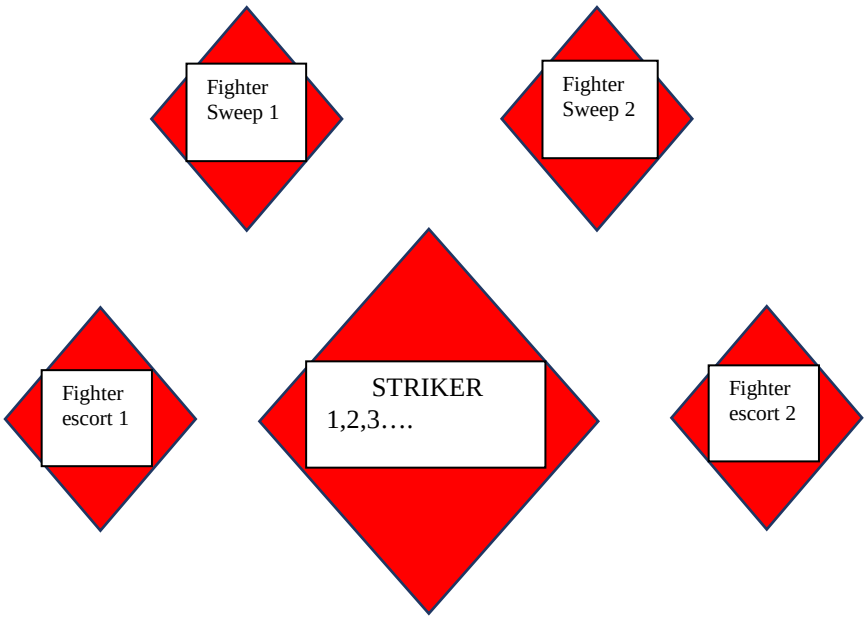

FIG. 3 Diagram of a COMAO package

Denoted by Cm = {Cm1,Cm2... CmN} jamming strategy and as follows:

If Cmn = 1 it follows that the system "m" is assigned to jam the target "n"

If Cmn = 0 it follows that the system "m" does not perform jamming on the target "n".

The following assumptions are made below:

1. When a target is detected, it can be jammed by any jamming system and each target is enough to be jammed by a single jamming system (It happens differently)
2. The jamming signal covers the work lane of the targets and can jam all types of radar signal modulation on board the air target; the effectiveness of the action depends on the strength of the jamming signal received by the target.
3. There are no attenuations in the transmitting antenna.
4. Since M < N (the number of N targets is greater than the number of M jamming systems), when one target changes its strategy, automatically another does the same.

The problem identified here is that we will have a limited set of jamming avoidance strategies borrowed from one target to another. A target can independently change its strategy, or several targets can change their strategies simultaneously, or a different strategy change may be the "exit from the game" (decoupling the radio locator, changing the way of working or the frequencies used).

For the development of electronic warfare systems, it is aimed at:

- improvement of the characteristics of unmanned aerial offensive aircraft and electronic research;
- ensuring the distant discovery by radar with the help of aerostats and airships, as well as using dispersed radiolocation stations and systems;
- increasing the sensitivity of radiolocation research equipment and the accuracy of measurements;
- increasing the power of jamming transmitters and expanding the working range;
- creating jamming with rapid re-tuning on several frequencies by using several magnetrons to generate jamming;
- elaboration of combined jamming systems and simultaneous launch of different undirected reactive projectiles (passive jamming with dipole reflectors, infrared traps, and active jamming transmitters with a sole use);
- making self-guided heads of missiles to be able to distinguish the real target that usually moves in a horizontal direction from the trap created with a dipole reflector cloud that is stationary or moves vertically;
- achieving electromagnetic compatibility of land, air, and naval electronic systems;
- upgrading and modernization of methods of training users of electronic warfare systems, including VR (virtual reality) and AR (augmented reality) [11].

CONCLUSIONS

Based on the analysis and experience gained in conducting electronic warfare actions in previous conflicts, the following conclusions can be drawn:

- the role of electronic warfare has become increasingly important, for all categories of armed forces, but especially for the air force;
- there are increasing use of state-of-the-art electronic surveillance and electronic attack systems, electronic countermeasures (thermal traps and electromagnetic dipoles), aerial research and unmanned combat aircraft, as well as active jamming transmitters with a sole use, car missiles directed on the electromagnetic beam of the opponent's electronic means;
- support with information about the adversary (especially about aviation and air defense) in real time has a primary role in achieving success in the operation;
- while the placement of noise jamming transmitters aboard combat aircraft proved ineffective, the use of "stealth" technology contributed decisively to the success of the operation.

By analyzing the elements in the field of EW present in the war triggered by the Russian Federation on Ukraine, a number of conclusions can be drawn:

- the high technological level of the Russian EW technique unsupported by an optimal level of training of the operators of those systems did not bring significant benefits to the Russian Federation;
- electronic attack systems against GPS systems and satellite communications with a range of up to one hundred kilometers are increasingly used;
- the means of electronic surveillance are used to identify future "jamming targets" or to accurately locate these targets and destroy them with artillery and missile systems;

- with the widespread use in this conflict of UAVs, including combat ones, a counter-weapon has also been developed – anti-drone systems, which jam GPS signals (for example, the Russian production system "Repellent-1");

- the Ukrainian ground forces use portable radio stations with frequency jump broadcasting, with encrypted transmission with over 2000 channels of work, "SINCGARS" (NATO Single-Channel Ground and Airborne Radio System), difficult to intercept by the adversary; however, in the event that SINCGARS stations are unavailable, mobile phones or classic radio stations with unprotected, vulnerable transmissions shall be used alternatively.

Innovative technologies create new risks that affect the armed forces entirely, or punctually, on the operators of the new combat systems. It is precisely this operator that represents the first threshold of defense against threats in cyberspace, a solution in its support being the use of encrypted data transmissions and the implementation of an efficient information management system that does not allow the interception by the adversary of sensitive information [12].

In the current macroeconomic context marked by multiple turbulences and crises, the field of electronic warfare is also significantly influenced. On the one hand, we are considering the increase in inflation amid a global energy crisis, the negative effects being doubled in SCM (supply chain management) through the semiconductor crisis.

REFERENCES

[1] https://www.bmj.com/content/372/bmj.n160, accessed on 08.01.2023, 10.54;

[2] B. Niu, Z. Huang, *Demand analysis of the application of intelligence push based on AI in the military field*, ICETIS 2022, Harbin, China;

[3] G. J. Miller, S*olutions to Principal-Agent Problems in Firms*, Boston, MA, USA: Springer, 2005;

[4] N. Min-Allah, M.B. Qureshi, S. Alrashed, et al, *Cost Efficient Resource Allocation for Real-Time Tasks in Embedded Systems*, Sustainable Cities and Society, 2019;

[5] X. -F. Zhai and Z. Yi, *IIGA based algorithm for cooperative jamming resource allocation*, 2009 Asia Pacific Conference on Postgraduate Research in Microelectronics Electronics (PrimeAsia), 2009, pp. 368-371;

[6] C. Liu, Y.A. Liu, X. Song. *Research of Radar Jamming Resources Optimization Allocation Model and Algorithm*, Computer Simulation, 2016;

[7] G. Yangyang, et al, *Research on the Method of Unbalanced Target Allocation in Multi-aircraft Air Combat Command and Guidance*, Advances in Aeronautical Science and Engineering, vol. 9, no. 4, pp. 523-529, 2018;

[8] Principal–Agent Problem as a Principled Approach to Electronic Counter-Countermeasures in Radar disponibil la https://ieeexplore-ieee-org.am.e-nformation.ro/document/9698992;

[10] https://www.keymilitary.com/article/composite-air-operations-little-help-your-friends accessed on 08.04.2023, 10.56;

[11] E..L. Miron, L. Gherman, *A New age in the Air force: the digitalization of military higher education*, AFASES 2022 conference, pp. 99-102, https://www.afahc.ro/ro/afases/2022/lucrari/14-EcaterinaLilianaMIRON, LaurianGHERMAN.pdf;

[12]C. Cârstea., L. Sângeorzan., N. David-Enache, L. Hen, *Security and encryption of classified information Shamir data sharing system*, 35th IBIMA (International-Business-Information-Management-Association) Conference Pp:16623-16630, WOS:000661489807058, ISBN: 978-0-9998551-4-0, IDS Number: BR6JR, https://ibima.org/accepted-paper/security-and-encryption-of-classified-information-shamir-da ta-sharing-system/ https://www-webofscience-com.am.e-nformation.ro/wos/woscc/full-record/WOS:000661489807058.