LÁSZLÓ KOVÁCS

ELECTRONIC WARFARE AND THE ASYMMETRIC CHALLENGES

AZ ELEKTRONIKAI HADVISELÉS ÉS AZ ASZIMMETRIKUS KIHÍVÁSOK

This paper highlights the main roles of electronic warfare in today's new military operations. The modern armed forces have to execute these operations in asymmetric circumstances. Electronic warfare as a part of the information operations has a major function to achieve information dominance as the main goal of these kinds of activities. However, electronic warfare usually belongs to conventional warfare, not unconventional wars. That's why in this paper will examine which kind of unconventional military missions and tasks could be supported by electronic warfare on such fields as Iraq or Afghanistan. Key words: information operations, electronic warfare, improvised explosive device

Jelen írás az elektronikai hadviselés főbb céljait kívánja bemutatni napjaink katonai műveleteiben. Ezekre a katonai műveletekre ma elsősorban az aszimmetrikus jelző illik. Az elektronikai hadviselés része az információs műveleteknek, melynek célja elősegíteni az információs fölény elérését. Ugyanakkor az elektronikai hadviselés a hagyományos katonai műveletek, és nem az új típusú katonai műveletek támogatására szolgált eredetileg. Ennek megfelelően ebben az írásban bemutatásra kerül, hogy melyek azok a területek, amelyeket az elektronikai hadviselés támogatni tud az olyan műveleti területeken, mint Irak vagy Afganisztán. Kulcsszavak: információs műveletek, elektronikai hadviselés, házi készítésű robbanó szerkezetek.

Introduction

History of electronic warfare goes back to more than one hundred years. It started when the first electronic asset — the radio — appeared on the battlefield. The radio and radio communication has changed the information flow of the military forces.

Nowadays thousands of electronic devices are used by military units. Modern warfare based on these electronic and computerized systems. However, the opposite side always wants to know what the enemy talking about and especially what they plan for the next period of time. If the enemy uses electronic assets and systems in his decision circle we need to virtually get into these systems to get information. One of the main tools to perform this kind of job is the Electronic Warfare (EW). EW supports own troops with different kind of information about the enemy's electronic systems. Based on this information the commander is able to realize adversary organization and possible activities in the close future. In addition, the electronic warfare has methods, activities and devices to reduce the enemy's capabilities in the full electromagnetic spectrum. This is the electronic countermeasures that are able to jam or destruct electronic assets or systems with electromagnetic or directed energy.

Beside these activities the electronic warfare has to protect our electronic systems as well our troops. This protection particularly important in fight against Improvised Explosive Devices (IEDs) or against Radio Controlled IEDs (RCIEDs). The IEDs and RCIEDs are the most dangerous challenges on recent battlefields. Electronic warfare as a part of the information operations has a major function to achieve information dominance as the main goal of these kinds of activities, so this paper will start with the examination of information warfare and information operation principles.

Electronic Warfare as the Essential Part of Information Operations

Information Warfare

Information warfare as a term was used in military doctrines until the end of '90s. Information warfare was the use and management of information in pursuit of a competitive advantage over an opponent. Information warfare could involve collection of tactical information, assurance that one's own information was valid, spreading of propaganda or disinformation to demoralize the enemy and the public, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces. [1]

Martin C. Libicki, the famous American mathematician has divided into five subparts the information warfare in 1995. These were the following:

- Command and Control Warfare (C2W);
- Intelligence Based Warfare (IBW);
- Electronic Warfare (EW);
- Psychological Warfare (PSYOP);
- Hacker Warfare;
- Economic Information Warfare (EIW);
- Cyber warfare. [2]

As we can see it is a very special classification that not necessarily reflects any military approaches. According to Joint Publication 3-13 Information Warfare is Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. [3]

However, information warfare as a term was removed from doctrines in the US and from NATO's documents as well in early 2000.

Information Operations

Information Operations is an evolving discipline within the military affairs. It has emerged from earlier concepts such as Command and Control Warfare (C2W) and Information Warfare. [1] As we mentioned before, the Information Warfare appears less frequently in Joint Publications and Allied Joint Publication, but still is a common term. n official definition the Information Operations are:

„Information operations (IO) are integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies. Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior decisions. IO are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own." [4]

Command and control warfare incorporates five activities which are pursued to achieve tactical objectives. These five activities are OPSEC, military deception, PSYOPS, EW, and physical destruction. The main objective of command and control warfare is to influence the adversary decision chain. In definition: „*Command and Control Warfare the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions…in military operations.*" [3]

Nowadays the C2W as a term is used less frequently as well as Information Warfare. The main goal of Information Operations is to achieve information superiority. The information superiority means the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. [5] Information superiority is shown in Figure 1.

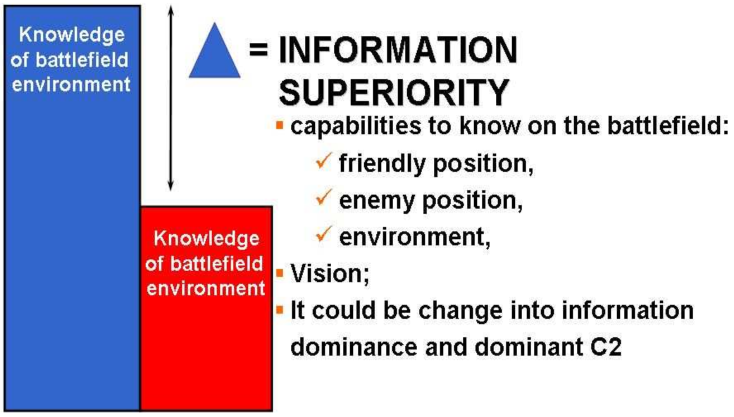

Knowledge of battlefield environment
Knowledge of battlefield environment
= INFORMATION SUPERIORITY
▪ capabilities to know on the battlefield:
✓ friendly position,
✓ enemy position,
✓ environment,
▪ Vision;
▪ It could be change into information dominance and dominant C2

Figure 1.
Information Superiority as the main goal of Information Operation

According to the Joint Publications and the NATO terminology, Information Operations have six1 main core elements (capabilities), and many others as supporting and relating capabilities.[2]

[1] There are five core elements in US Joint Publications.

[2] If we compare Libicki's information warfare subdivisions with this one we can observe an evaluation process during the time. This evaluation has happened during the last years or

The core capabilities are the following:

- operational security (OPSEC);
- military deception (MD);
- psychological operations (PSYOPS);
- physical destruction[3] (PD);
- electronic warfare (EW);
- computer network operations (CNO).

The Information Operations have some supporting and relating elements as mentioned before, which are the following:

- public information (PI);
- civil and military cooperation (CIMIC).

All of the elements are supported by All Source Intelligence[4] (ASI) and Command and Control, Communication, Computer and Intelligence (C4I)[5].

The Information Operations are executed in a special environment. This is the information environment „where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. Even though the information environment is considered distinct, it resides within each of the four domains. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.“ [4] These dimensions are shown in Figure 2.

The physical dimension is composed of the command and control (C2) systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside.

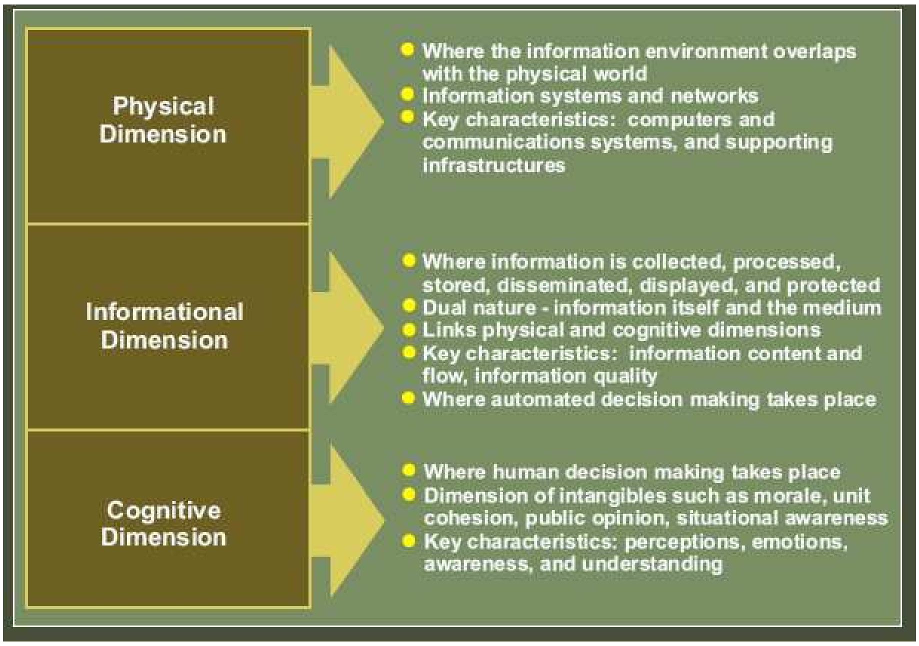
This includes the means of transmission, infrastructure, technologies, groups, and populations. Comparatively, the elements of this dimension are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this dimension.

decade. Further more, the second partition is reflects a special military point of view opposite Libicki's "civilian" structure was mentioned above.

[3] It is important to note that the PD is already not necessarily part of IO neither in US joint publications nor in NATO allied joint publications.

[4] ASI: Intelligence produced using all available sources and agencies. [7]

[5] It is called Communication and Information Systems (CIS) in NATO.



Physical Dimension

- Where the information environment overlaps with the physical world
- Information systems and networks
- Key characteristics: computers and communications systems, and supporting infrastructures

Informational Dimension

- Where information is collected, processed, stored, disseminated, displayed, and protected
- Dual nature - information itself and the medium
- Links physical and cognitive dimensions
- Key characteristics: information content and flow, information quality
- Where automated decision making takes place

Cognitive Dimension

- Where human decision making takes place
- Dimension of intangibles such as morale, unit cohesion, public opinion, situational awareness
- Key characteristics: perceptions, emotions, awareness, and understanding

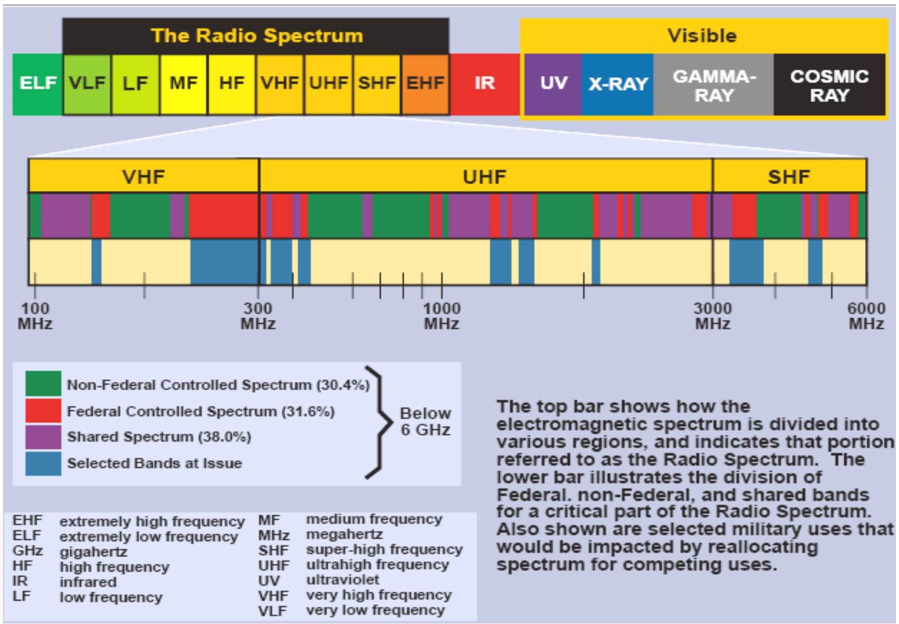
Figure 2
Three dimensions of information environment [4]

The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. It is the dimension where the C2 of our modern military forces is communicated, and where commander's intent is conveyed. It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected.

The cognitive dimension includes the mind of the decision maker and the target audience. This is the dimension in which people think, perceive, visualize, and decide. Sometimes — i.e. during psychological operations — it is the most important of the three dimensions. This dimension is also affected by a commander's orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension.

Electronic Warfare

Electronic warfare refers to any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary. This electromagnetic spectrum is shown in Figure 3.



EHF	extremely high frequency	MF	medium frequency
ELF	extremely low frequency	MHz	megahertz
GHz	gigahertz	SHF	super-high frequency
HF	high frequency	UHF	ultrahigh frequency
IR	infrared	UV	ultraviolet
LF	low frequency	VHF	very high frequency
		VLF	very low frequency

The top bar shows how the electromagnetic spectrum is divided into various regions, and indicates that portion referred to as the Radio Spectrum. The lower bar illustrates the division of Federal. non-Federal, and shared bands for a critical part of the Radio Spectrum. Also shown are selected military uses that would be impacted by reallocating spectrum for competing uses.

Figure 3
The electromagnetic spectrum[6] [6]

Electronic warfare includes three major subdivisions (as shown in Figure 4.): electronic warfare support (ES), electronic attack (EA) and electronic protection (EP). These are the common terms of these subparts in US joint doctrines. The NATO and Hungarian doctrines use the terms of electronic support measures instead of ES, electronic counter measures (ECM) instead of EA. The electronic protection term is also common use in the NATO instead of electronic counter-counter measures (ECCM) that was used earlier.

[6] In this figure US electromagnetic spectrum division is shown.

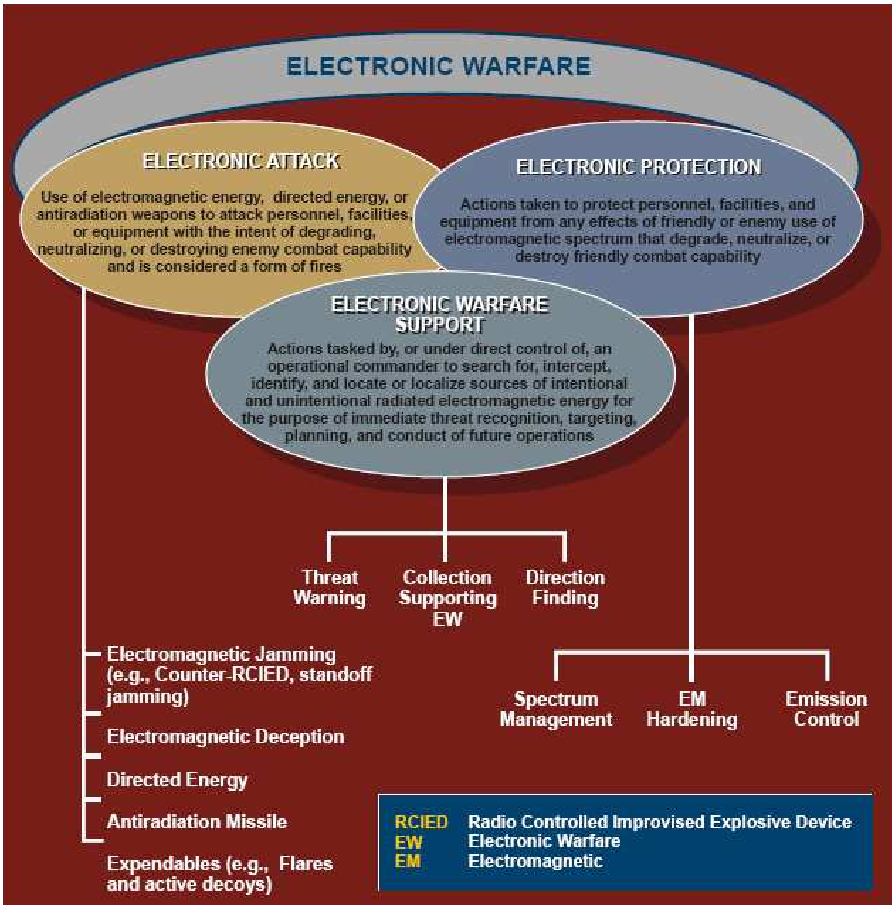

ELECTRONIC WARFARE
ELECTRONIC ATTACK
Use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires
ELECTRONIC PROTECTION
Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability
ELECTRONIC WARFARE SUPPORT
Actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations
Threat Warning
Collection Supporting EW
Direction Finding
Electromagnetic Jamming (e.g., Counter-RCIED, standoff jamming)
Electromagnetic Deception
Directed Energy
Antiradiation Missile
Expendables (e.g., Flares and active decoys)
Spectrum Management
EM Hardening
Emission Control
RCIED Radio Controlled Improvised Explosive Device
EW Electronic Warfare
EM Electromagnetic

Figure 4
Main parts of electronic warfare [6]

Electronic Warfare Support consists of actions tasked by, or under direct control of an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

Electronic Warfare Support provides information required for decisions involving Electronic Warfare operations and other tactical actions such as threat avoidance and targeting. There is a close connection between the Electronic Warfare Support and the Signal Intelligence

(SIGINT), so ES data can be used to produce SIGINT, provide targeting for electronic or other forms of attack, and produce measurement and signature intelligence (MASINT).

Electronic Attack involves the use of electromagnetic energy, directed energy, or homing guidance weapons (active, semi-active, passive) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability.

Electronic Protection ensures the friendly use of the electromagnetic spectrum with special measures, techniques and activities.

Electronic Warfare contributes to the success of Information Operations by using offensive and defensive tactics and techniques in a variety of combinations to form, disrupt, and exploit adversarial use of the electromagnetic spectrum while protecting friendly smooth use of action in spectrum. Since the use of the electromagnetic spectrum has become common in military operations, so Electronic Warfare has become involved in all aspects of Information Operations. All of the core, supporting, and related Information Operations capabilities are directly or indirectly supporting by Electronic Warfare. These connections are shown in Figure 5.

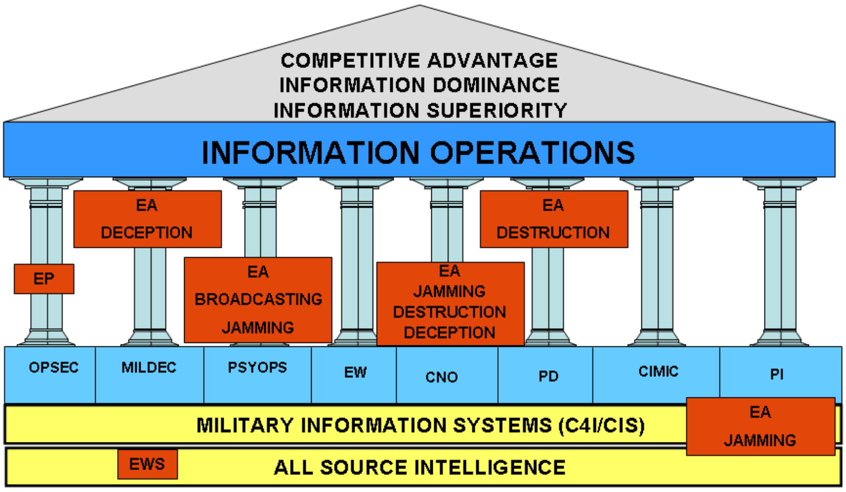


Figure 5
Information Operations supported
by Electronic Warfare subdivisions and activities

Electronic Warfare has major role in the ground forces activities as well air force operations. Airborne integrated electronic warfare systems are vital to survive any missions in case of fighter airplanes as well as transport aircrafts. These onboard and integrated EW systems provide functions for:

- detection and localization of threat signals;
- signal processing for threat identification;
- automatic selection of appropriate countermeasures reaction.

Other Electronic Warfare function in the air force is the SEAD (Suppression of Enemy Air Defenses). SEAD is *„That activity which neutralizes, temporarily degrades or destroys enemy air defences by a destructive and/or disruptive means."* [7]

SEAD *„has long been in critical mission essential to US and allied air superiority and all that springs from it. … Non-lethal means of SEAD have included the use of support jamming aircraft, such as the Navy's EA-6B Prowler, to protect packages of strike aircraft by temporarily blinding* enemy early-warning, SAM and anti aircraft artillery (AAA) radars." [8]

New Challenges of Electronic Warfare and the Possible Answers

Heavy and expanding reliance on the electromagnetic spectrum for informational purposes increases both the potential and the challenges of Electronic Warfare in Information Operations.

The increasing dominance of software defined radios[7,] wireless techniques and computer networks extends both the utility and threat of Electronic Warfare, offering opportunities to exploit an adversary's electronic vulnerabilities and a requirement to identify and protect our own from similar exploitation. Many new modulation and transmission mode and methods appeared on the field of military communications during the last

[7] Software Defined Radio (SDR): Radio in which some or all of the physical layer functions are software defined. Traditional hardware based radio devices limit cross-functionality and can only be modified through physical intervention. This results in higher production costs and minimal flexibility in supporting multiple waveform standards. By contrast, software defined radio technology provides an efficient and comparatively inexpensive solution to this problem, allowing multi-mode, multi-band and/or multi-functional wireless devices that can be enhanced using software upgrades. [9]

decades. These represent very high challenges for Electronic Warfare. Some examples:

- New modulation techniques:
  - Direct-sequence Spread Spectrum Technique (DS-SST);
  - Frequency-hopping Spread Spectrum Technique (FH SST);
  - Time-hopping Spread Spectrum Technique – TH-SST;
  - Chirp Spread Spectrum Technique (Chirp-SST).
- Automatic Link Establishment (ALE);
- Link Quality Analysis (LQA);
- Other technologies:
  - electromagnetic waves absorbing paints;
  - other STEALTH technology (i.e. dispersive shape)
  - camouflage fog with special materials;
  - blinding projectiles against night and infra goggles;
  - multi spectral camouflage net etc.

Figure 6
Joint Tactical Radio System, Ground Mobile Radios (JTRS GMR)[8]
as a representative of SDR technology [10]

[8] The Joint Tactical Radio System, Ground Mobile Radios, is a software-programmable radio system providing secure, reliable, multi-channel voice, data, imagery and video communications for mobile military users. The system delivers networked communications on-the-move at the tactical edge supporting information sharing and combat readiness between service branches. JTRS GMR enables commanders to view and understand the battle space, communicate their intent, lead their forces and disseminate real-time information. It puts the full power of the Global Information Grid into the hands of the warfighter. [10]

New threat has come out on recent battlefields such as Iraq or Afghanistan. This is the Improvised Explosive Device (IED). IED is a homemade bomb which is constructed and deployed in other ways than in conventional military action. This device may be constructed of conventional military explosives, such as an artillery round (that was found on the field), attached to a detonating mechanism. These IEDs may be used in terrorist actions or in unconventional warfare by guerrillas. In case of remote-controlled IED the trigger is controlled by radio link. The receiver is connected to an electrical firing circuit and the transmitter operated by the perpetrator at a distance, signal from the transmitter causes the receiver to trigger a firing pulse which operates the switch. The radio link as a controller could be:

- High Powered Cordless Phone (HPCP);
- GSM phone;
- wireless door bell;
- garage door opener;
- car central door controller;
- enhanced distance walkie-talkie.

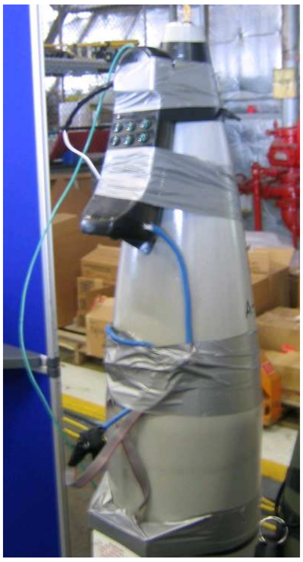


Figure 7.
Wireless phone-controlled artillery ammunition as an RCIED. [11]

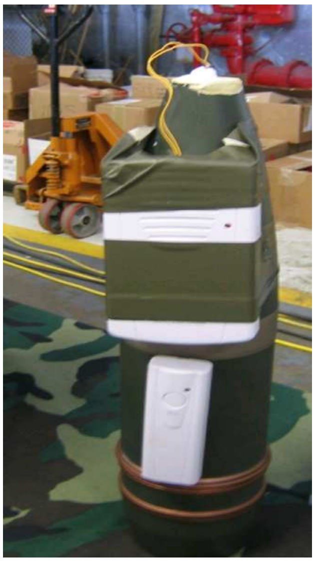


Figure 8.
Wireless door bell as a controller for RCIED. [12]

However, when the remote-controlled IEDs appeared in Iraq in 2003-2004, the Electronic Warfare was not well prepared to deal with this threat and challenge. Until that time jamming techniques and assets used high energy, mainly communication frequencies, and large and dedicated EW platforms. Fighting against RCIED required smaller, mobile jammers with higher frequency and relatively lower power. “As urgent requirements for IED jammers began to emerge in 2004 and 2005, it created a wide open market for the US defense industry. No US company manufacturing IED jammers before Operation Iraqi Freedom in 2003. Over the next five years, more than 40 companies (most of them from outside the traditional EW market) would offer IED jammer solutions.” [13]

Today IED jammers (as an example shown in Figure 9.) are build in or just transported on military vehicles. In a convoy one or more jammers emit a jamming signal; the troops have an electronic “bubble” that made them safe from an IED they had not spotted. It's not uncommon for vehicles to have had an IED go off behind them, the result of the IED detonation crew continuing to send the signal, believing that there might be something wrong with their equipment. In those cases, the patrol often turns around and goes looking for the enemy team. [14]

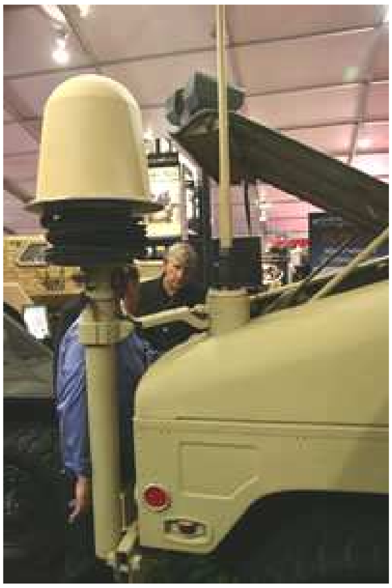


Figure 9
Vehicle based IED jammer [15]

Summary

During the last decades a new discipline appeared in the military affairs. This is the Information Operations which includes actions taken to affect adversary information and information systems while defending own information and information systems. Electronic Warfare has become essential subdivision of Information Operation. Electronic Warfare supports the entire core, supporting, and related Information Operations capabilities in the full electromagnetic spectrum. However, today the Electronic Warfare has to prepare itself new threats and challenges such as Improvised Explosive Devices.

References

1. Information warfare. http://en.wikipedia.org/wiki/Information_warfare (downloaded: 05 July 2009)
2. Martin Libicki: What is information warfare? National Defense University, ACIS Paper 3, August 1995. http://www.ndu.edu/inss/actpubs/act003/a003.html (downloaded: 12 September 2002)
3. Joint Publication 3-13. Joint Doctrine for Information Operation. 9 October1998
4. Joint Publication 3-13. Information Operation. 13 February 2006
5. Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.
6. Joint Publication 3-13.1 Electronic Warfare. 25 January 2007
7. AAP-6 (2007) NATO glossary of terms and definitions.
8. Glenn Goodman: Lethal SEAD. in Journal of Electronic Defense. April 2009, Vol. 32 No. 4. p.: 26
9. What is Software Defined Radio? http://www.sdrforum.org/pages/aboutSdrTech/whatIsSdr.asp (downloaded: 05 July 2009)
10. Joint Tactical Radio System, Ground Mobile Radios (JTRS GMR). http://www.boeing.com/defense-space/ic/jtrs/index.html (downloaded: 05 July 2009)
11. RCIED http://www.globalsecurity.org/military/intro/images/ied-artillery_mock-model02.jpg (downloaded: 05 July 2009)
12. RCIED http://www.globalsecurity.org/military/intro/images/ied-artillery_mock-model01.jpg (downloaded: 05 July 2009)
13. John Knowles: GaN Amplifiers: Boosting the Power behind Communications Jammers. in Journal of Electronic Defense. April 2009, Vol. 32 No. 4. p.: 43

14. New Generation IED Jammer Arrives. http://www.strategypage.com/htmw/htecm/20070418.aspx (downloaded: 05 July 2009)

15. Counter IED Technologies at the Modern Day Marine Expo. http://defense-update.com/events/2007/summary/mdm07_ ied. htm (downloaded: 05 July 2009)