

Electronic warfare

From Wikipedia, the free encyclopedia

Electronic warfare (EW) is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack of an enemy, or impede enemy assaults via the spectrum. The purpose of electronic warfare is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the EM spectrum. EW can be applied from air, sea, land, and space by manned and unmanned systems, and can target humans, communications, radar, or other assets.^[1]

Contents

- 1 The electromagnetic environment
 - 1.1 Electronic warfare applications
- 2 Subdivisions
 - 2.1 Electronic attack (EA)
 - 2.2 Electronic Protection (EP)
 - 2.3 Electronic warfare support (ES)
- 3 Relevant EW History
- 4 See also
- 5 Further reading
- 6 References
- 7 General references

The electromagnetic environment

Military operations are executed in an information environment increasingly complicated by the electromagnetic (EM) spectrum. The electromagnetic spectrum portion of the information environment is referred to as the electromagnetic environment (EME). The recognized need for military forces to have unimpeded access to and use of the electromagnetic environment creates vulnerabilities and opportunities for electronic warfare (EW) in support of military operations.^[1]

Within the information operations construct, EW is an element of information warfare; more specifically, it is an element of offensive and defensive counterinformation.^[2]

NATO has a different and arguably more encompassing and comprehensive approach to EW. A Military Committee conceptual document from 2007 (MCM_0142 Nov 2007 Military Committee Transformation Concept for Future NATO Electronic Warfare) recognised the EME as an operational manoeuvre space and warfighting environment/domain. In NATO, EW is considered to be warfare in the EME. NATO has adopted simplified language which parallel those used in the other warfighting environments like maritime, land and air/space. For example, Electronic Attack is offensive use of EM energy. ED is electronic defence and ES electronic surveillance. The use of the traditional NATO EW measures (ECM, EPM and ESM) has been retained as they contribute to and support EA, ED and ES. Besides EW, other EM operations include ISTAR and SIGINT. Subsequently NATO has issued EW Policy and Doctrine and is addressing the other NATO defence lines of development.

Electronic warfare applications

Electronic warfare is any military action involving the use of the EM spectrum to include directed energy (DE) to control the EM spectrum or to attack an enemy. This is not limited to radio or radar frequencies but includes IR, visible, ultraviolet, and other less used portions of the EM spectrum. This includes self-protection, standoff, and escort jamming, and antiradiation attacks. EW is a specialized tool that enhances many air and space functions at multiple levels of conflict.^[2]

The purpose of EW is to deny the opponent an advantage in the EM spectrum and ensure friendly unimpeded access to the EM spectrum portion of the information environment. EW can be applied from air, sea, land, and space by manned and unmanned systems. EW is employed to support military operations involving various levels of detection, denial, deception, disruption, degradation, protection, and destruction.^[1]

EW contributes to the success of information operations (IO) by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. Expanding reliance on the EM spectrum increases both the potential and the challenges of EW in information operations. All of the core, supporting, and related information operations capabilities either directly use EW or indirectly benefit from EW.^[2]

The principal EW activities have been developed over time to exploit the opportunities and vulnerabilities that are inherent in the physics of EM energy. Activities used in EW include: electro-optical, infrared and radio frequency countermeasures; EM compatibility and deception; communications jamming, radar jamming and anti-jamming; electronic masking, probing, reconnaissance, and intelligence; electronics security; EW reprogramming; emission control; spectrum management; and wartime reserve modes.^{[1][2]}

Subdivisions

Electronic warfare includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).^[1]

Electronic attack (EA)

Electronic attack (EA) (previously known as Electronic Counter Measures (ECM)) involves the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability including human life. In the case of EM energy, this action is referred to as jamming and can be performed on communications systems (see Radio jamming) or radar systems (see Radar jamming and deception).

Electronic Protection (EP)

Electronic Protection (EP) (previously known as electronic protective measures (EPM) or electronic counter countermeasures (ECCM)) involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Jamming is not part of EP, it is an EA measure.

The use of flare rejection logic on an Infrared homing missile to counter an adversary's use of flares is EP. While defensive EA actions and EP both protect personnel, facilities, capabilities, and equipment, EP protects from the *effects* of EA (friendly and/or adversary). Other examples of EP include spread spectrum technologies, use of Joint Restricted Frequency List (JRFL), emissions control (EMCON), and low observability or "stealth".^[1]



RAF Menwith Hill, a large ECHELON site in the United Kingdom, and part of the UK-USA Security Agreement

An Electronic Warfare Self Protection (EWSP) is a suite of countermeasure systems fitted primarily to aircraft for the purpose of protecting the aircraft from weapons fire and can include among others: DIRCM (protects against IR missiles), Infrared countermeasures (protects against IR missiles), Chaff (protects against RADAR guided missiles), DRFM Decoys (Protects against Radar guided missiles), Flare (protects against IR missiles).

An Electronic Warfare Tactics Range (EWTR) is a practice range which provides for the training of aircrew in electronic warfare. There are two such ranges in Europe; one at RAF Spadeadam in the United Kingdom and the POLYGON range in Germany and France. EWTRs are equipped with ground-based equipment to simulate electronic warfare threats that aircrew might encounter on missions.

Antifragile EW is a step beyond standard EP, occurring when a communications link being jammed actually increases in capability as a result of a jamming attack, although this is only possible under certain circumstances such as reactive forms of jamming.^[3]

Electronic warfare support (ES)

Electronic Warfare Support (ES), is the subdivision of EW involving 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 (EM) energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.^[1] These measures begin with systems designed and operators trained to make Electronic Intercepts (ELINT) and then classification and analysis broadly known as Signals intelligence from such detection to return information and perhaps actionable intelligence (e.g. a ship's identification from unique characteristics of a specific radar) to the commander.

The overlapping discipline, signals intelligence (SIGINT) is the related process of analyzing and identifying the intercepted frequencies (e.g. as a mobile phone or radar). SIGINT is broken into three categories: ELINT, COMINT, and FISINT. the parameters of intercepted txn are-: communication equipment-: freq, bandwidth, modulation, polarisation etc. The distinction between intelligence and electronic warfare support (ES) is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. Electronic warfare support is achieved by assets tasked or controlled by an operational commander. The purpose of ES tasking is immediate threat recognition, targeting, planning and conduct of future operations, and other tactical actions such as threat avoidance and homing. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements.^[1]

Where these activities are under the control of an operational commander and being applied for the purpose of situational awareness, threat recognition, or EM targeting, they also serve the purpose of Electronic Warfare surveillance (ES).

Relevant EW History

In the 2007 Operation Orchard Israeli attack on a suspected Syrian nuclear weapons site, the Israel Air Force used electronic warfare to take control of Syrian airspace prior to the attack.^[4] Israeli electronic warfare (EW) systems took over Syria's air defense systems, feeding them a false sky-picture while Israel Air Force jets crossed much of Syria, bombed their targets and returned.^[5]



A right front view of a USAF Boeing E-4 advanced airborne command post (AABNCP) on the electromagnetic pulse (EMP) simulator (HAGII-C) for testing.

In February 2015 the Russian army received their first set of the multifunctional electronic warfare system, known as Borisoglebsk 2.^{[6][7][8]} Svenska Dagbladet claimed its initial usage caused concern within NATO.^[9] A Russian blog describes Borisoglebsk 2 as *"The 'Borisoglebsk-2' when compared to its predecessors has better technical characteristics: wider frequency bandwidth for conducting radar collection and jamming, faster scanning times of the frequency spectrum, and higher precision when identifying the location and source of radar emissions, and increased capacity for suppression."*^[10]

See also

- Directed-energy weapon
- Electromagnetic pulse
- Electromagnetic interference
- Electronic harassment
- Electronic warfare support measures
- Radar jamming and deception
- Radio jamming

Electronic Warfare Systems:

- Chaff
- Digital Radio Frequency Memory (DRFM)
- Electronic Intelligence (ELINT)
- Radar Warning Receiver (RWR)
- Borisoglebsk 2

Historic:

- Battle of Latakia: the first use of deception EW in a naval battle
- Battle of the Beams
- No. 100 Group RAF
- 36th Bombardment Squadron

US specific:

- Association of Old Crows
- Electronic Warfare Officer
- Fleet Electronic Warfare Center
- Joint Functional Component Command for Network Warfare
- U.S. Marine Corps Radio Reconnaissance
- Historical Electronics Museum
- USACEWP (United States Army Computer Network Operations-Electronic Warfare Proponents)
- Cyber Operations

Further reading

- FM 3-36: Electronic Warfare In Operations. Safeguarding Soldiers Through Technology (<http://usacac.army.mil/cac2/Repository/FM336/FM336.pdf>). Fort Leavenworth, U.S. Army Combined Arms Center (<http://usacac.army.mil/cac2/index.asp>) (CAC), 26 February 2009 – PDF, 114 p., 4,5 MB. – *See also*: John Milburn: Army manual raises emphasis on electronic warfare (http://www.washingtonpost.com/wp-dyn/content/article/2009/02/25/AR2009022502250_pf.html). Washington Post, 26 February 2009.
- Jon Latimer, *Deception in War*, London: John Murray, 2001
- David Adamy EW 101: A First Course in Electronic Warfare

- David Adamy EW 102: A Second Course in Electronic Warfare
- Joint Publication 3-13.1: Electronic Warfare^[1]
- Jogiaas, Aadu. "Disturbing soviet transmissions in August 1991". Archived from the original on 14 November 2011.
- Bolton, Matt; Munro, Matt (2011). "The Tallinn Cables" (PDF). *Lonely Planet Magazine* (December): 48–55.

References

1. EW contributes to the success of information operations (IO) by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. "Joint Publication 3-13.1 Electronic Warfare" (Online PDF available for download). Chairman of the Joint Chiefs of Staff (CJCS) - Armed Forces of the United States of America. 25 January 2007. pp. i, v – x. Retrieved 2011-05-01. "This publication provides...doctrine for electronic warfare planning, preparation, execution, and assessment in support of joint operations across the range of military operations."
 2. "Electronic Warfare; Air Force Doctrine Document 2-5.1" (PDF). Secretary of the Air Force. 5 November 2002. pp. i, v – x. Archived from the original (Online PDF available for download) on August 12, 2011. Retrieved 2011-05-01. "This AFDD establishes operational doctrine for United States Air Force EW operations. This doctrine provides guidance for planning and conducting electronic warfare operations in support of national and joint force commander (JFC) campaign objectives."
 3. Lichtman, Marc; Vondal, Matthew; Clancy, Charles; Reed, Jeffrey (Feb 2016). "Antifragile Communications". *IEEE Systems Journal*. doi:10.1109/JSYST.2016.2517164.
 4. [1] (<http://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness>) By YAAKOV KATZ, 09/29/2010, Jerusalem Post
 5. Israel Shows Electronic Prowess (<http://aviationweek.com/awin/israel-shows-electronic-prowess>) Nov 26, 2007, David A. Fulghum and Robert Wall, Aviation Week & Space Technology
 6. "Borisoglebsk-2". *Deagel.com*.
 7. Administrator. "Russian army units of Eastern District have received new Borisoglebsk-2 electronic warfare vehicles - February 2015 Global Defense Security news UK - Defense Security global news industry army 2015". *armyrecognition.com*.
 8. "Russia surges ahead in radio-electronic warfare". *rbth.com*.
 9. "Translation: "Putin's new super weapon frightens NATO"". *Svenska Dagbladet*. 16 August 2015.
 10. Shoki Driver. "Russian Military News in English". *shokidriver.blogspot.se*.
- ⓘ This article incorporates public domain material (<http://www.af.mil/Disclaimer.aspx>) from the United States Air Force website <http://www.af.mil>.
 - ⓘ This article incorporates public domain material from websites or documents of the United States Government.

General references

- The Changing Capability of Manpack Electronic Warfare Systems (http://www.rusi.org/publications/defence_systems/ref:A4B8E7E2F3AFDB/)
- Carlo Kopp "Electronic Warfare in Operation Desert Storm (<http://www.sci.fi/~fta/storm-01.htm>)", Australian Aviation, June/July/August, 1993
- Association of Old Crows (<http://www.crows.org>)
- Electronic Warfare Jamming Systems (http://www.stratign.com/electronic_warfare.htm)
- Information Warfare, Information Operations and Electronic Attack on APA (<http://www.ausairpower.net/iw.html>)
- Electronic Warfare Products (https://web.archive.org/web/20160208190823/http://www.tmd.co.uk/markets/electronic_warfare.asp)
- Joint Publication 3-13.1 Electronic Warfare (<http://www.dtic.mil/dtic/tr/fulltext/u2/a464647.pdf>); PDF-674k (text version (http://dsearch.dtic.mil/search?q=cache:9Es7dI9gqCIJ:www.dtic.mil/dtic/tr/fulltext/u2/a464647.pdf+%22Joint+Publication+3-13.1%22+Electronic+Warfare&site=default_collection&client=dticol_frontend&proxystylesheet=dticol_frontend&ie=UTF-8&access=p&oe=UTF-8))

- Air Force Instruction on Electronic Warfare (EW) Operations (<http://www.e-publishing.af.mil/shared/media/epubs/AFI10-706.pdf>) PDF

Retrieved from "https://en.wikipedia.org/w/index.php?title=Electronic_warfare&oldid=756145956"

Categories: [Electronic warfare](#) | [Information operations and warfare](#)

- This page was last edited on 22 December 2016, at 08:22.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.