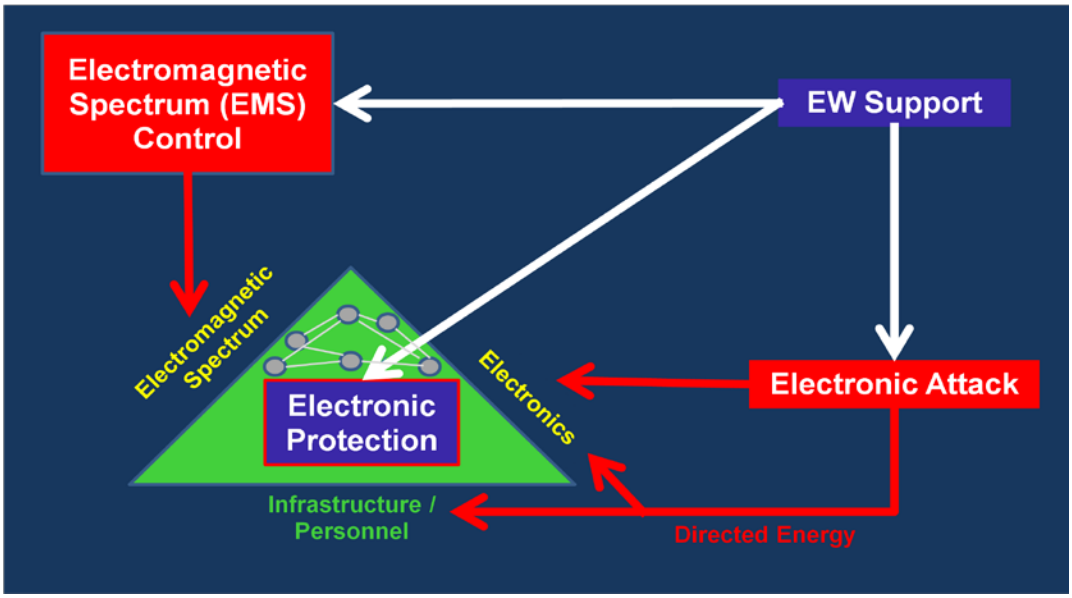

Figure 7: EW Physical Effects.

Electronic Protection (EP): Electronic Protection (previously referred to as Electronic Counter Countermeasures or ECCM) involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralise, or destroy friendly combat capability. In practice, EP allows mission capabilities and processes to continue effectively under challenge of denied or otherwise complex EM environments. Examples include anti-jam features, Joint Restricted Frequency Lists (JRFL), multi-spectral "low observable" technologies and applications.

Electronic Warfare Support (ES): Electronic Warfare Support (previously referred to as Electronic Support Measures or ESM) 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 localise sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

ES receivers are mainly utilized in the Signals Intelligence or the EA systems control roles.

- Signals Intelligence (SIGINT) is intelligence-gathering by interception of signals, whether between people (Communications Intelligence - COMINT), whether involving electronic signals not directly used in communication (Electronic Intelligence - ELINT), or combinations of the two.
- Communications Intelligence (COMINT) is a sub-category of signals intelligence that engages in dealing with both the technical information as well as messages or voice information derived from the interception of communications. As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalysis. Also, traffic analysis - the study of who is signalling whom and in what quantity - can often produce valuable information, even when the messages themselves cannot be decrypted.
- Electronic Intelligence (ELINT) refers to intelligence-gathering by use of electronic sensors. Its primary focus lies on non-communications signals intelligence. ELINT is normally seen as a non-time critical gathering of data – more strategic in nature. The data can be captured and analyzed off-line. Whenever the data is time critical, for example to warn of an incoming missile, or to control an EA system, the system required is an Electronic Support Measures (ESM) system – not to be confused with the old EW definition as shown in Figure 6.

Generating an Electronic Order of Battle (EOB) requires identifying emitters in an area of interest, determining their geographic location or range of mobility, characterizing their signals, and, where possible, determining their role in the broader organizational order of battle. EOB covers both COMINT and ELINT

Electromagnetic Control (EMC): EW can and must be used in all phases of conflict in conjunction with or as an alternative to kinetic fires. From radio-controlled roadside bombs to integrated air defenses. EW has become the face of combat in the Information Age. Efficient use, management, and control of the EMS are critical to national security in terms of Strategic Communication (SC), information operations (IO), and Electronic Warfare. Effective spectrum management is essential to sound defensive Information Operations, Command & Control (C^2) protection and EA, which ensures operations can be conducted with minimal unintentional interference and without negative Electromagnetic Environmental Effects (E^3). The rapid growth of sophisticated weapons systems, as well as intelligence, operations and communications systems. greatly

increases demand for frequencies. Lack of proper frequency coordination will have an adverse effect upon friendly users (joint and coalition forces as well as civilians).

Spectrum availability is further constrained by national legislation designed to protect the rights of sovereign governments by requiring approval prior to transmission in any portion of the spectrum that lies within a particular country's national borders. Furthermore, unacceptable Electromagnetic Interference (EMI) among all emitters and receivers (for example E^3 issues such as Hazards of Electromagnetic Radiation to Ordnance (HERO) in joint operations) must be minimized. Another challenge is the orchestration and synchronization of competing systems of receivers and jammers, how and when to use them, and whether they could counteract each other. causing EW fratricide.

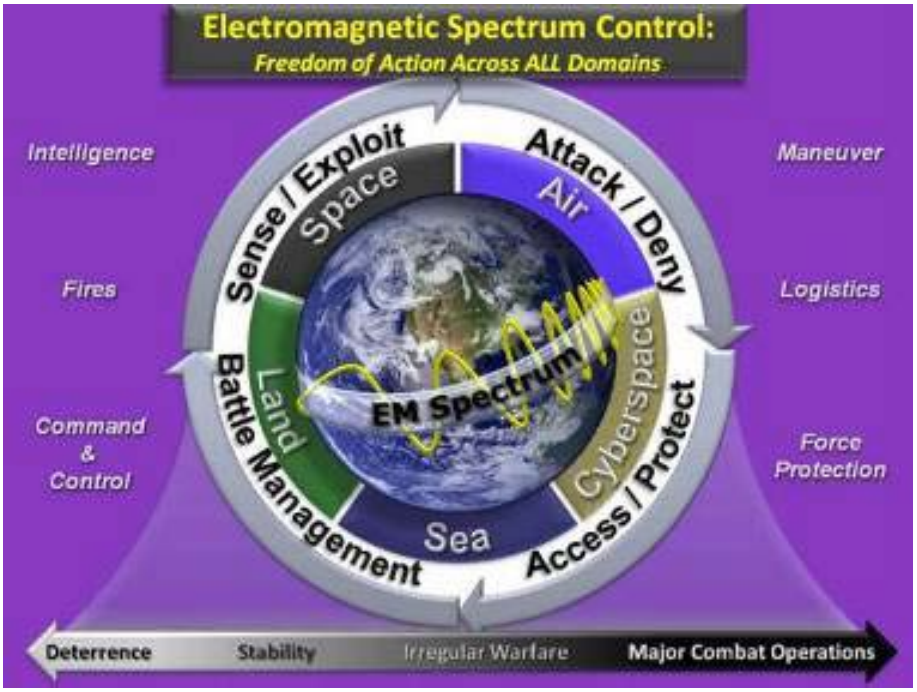

Figure 8: Electromagnetic Spectrum Control.

EMS Control (EMC): Control of the EMS is achieved by effective management and coordination of friendly systems while countering adversary systems. EA limits adversary use of the EMS; EP secures use of the EMS for friendly forces; and ES enables the commanders' accurate estimate of the situation in the operational area. All three must be carefully integrated to be effective. Additionally, commanders should ensure maximum integration among EW, communications, ISR, and other IO capabilities. EMS control consists of EW Battle Management (EWBM) and EM Spectrum Management.

Electromagnetic Spectrum Management:

Electromagnetic Spectrum Management involves planning, coordinating, and managing use of the EMS through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. To this end, frequency assignments must be made so they do not conflict or cause interference with other frequency assignments. The EMS is a resource that is finite and has to be managed to provide the user with acceptable service.

EMS Operational Environment:

The EMS operational environment goes further than that of the military. Spectrum management, frequency allocation and the creation of policies are an integral part of EMC.

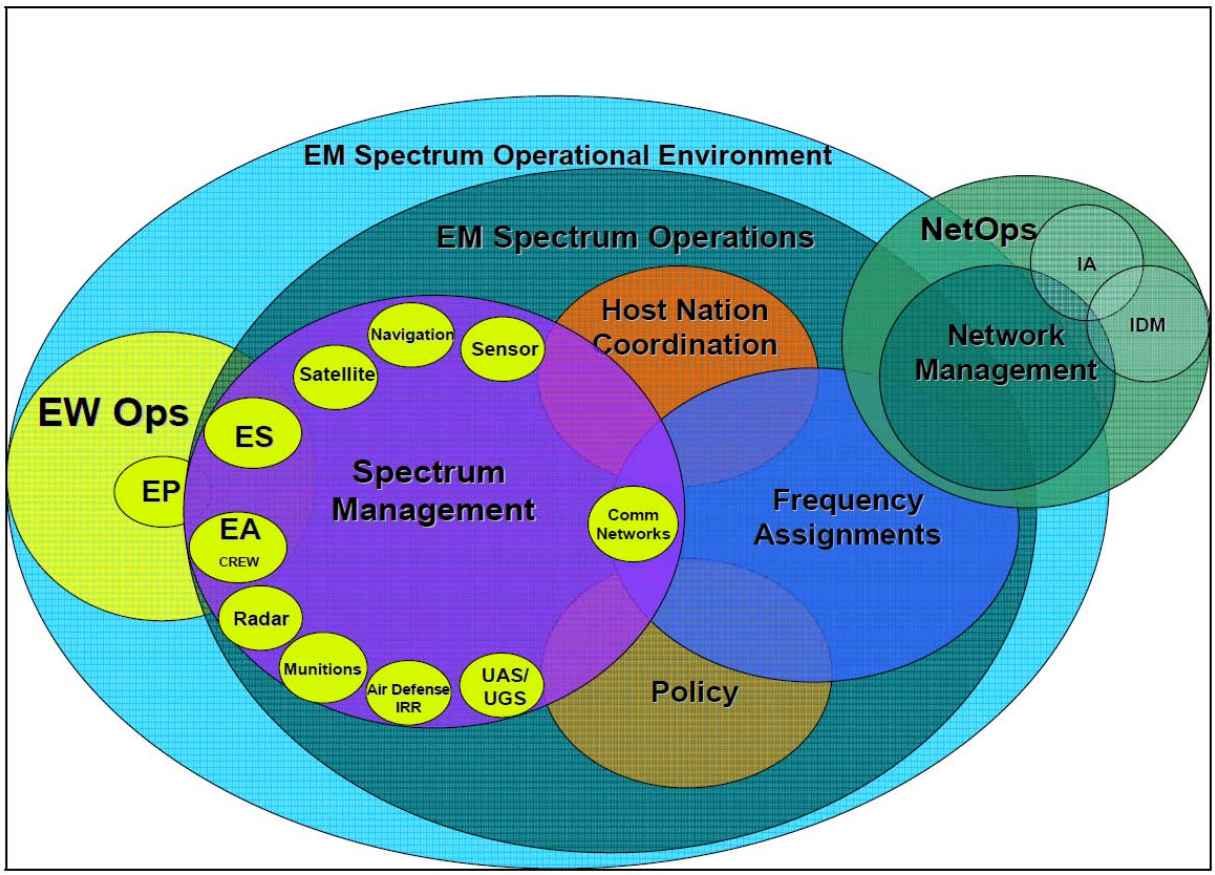

Figure 9: The EMS Operational Environment.

EW Activities

The purpose of EW is to deny the opponent an advantage in the EM ops domain and ensure friendly use of the EM ops domain. The main activities to enable the control, attack and protection of the EMS are listed here:

- EM countermeasures
- EM compatibility
- EM deception
- EM hardening
- EM interference
- EM intrusion
- EM jamming
- Electronic masking
- Directed Energy
- EM threat avoidance
- Electronic probing
- Electronic reconnaissance
- Electronic intelligence
- Electronic security
- EW reprogramming
- Emission Control
- Spectrum management
- War reserve modes

EA includes actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and employment of weapons that use either

electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

Information Operations (IO)

Information Operations require a new analytical paradigm, one that requires close synchronization between the EW and Intelligence, Surveillance and Recognisance (ISR) communities. Furthermore, interoperability between own and coalition systems requires a level of joint electronic warfare advocacy previously not required. To achieve this sharing of information has become crucial - the need to know has been outweighed by the need to share - previously everything that had something to do with EW was classified.

In order to achieve the desired effect, defence forces have to move away from being reactive to being proactive. This requires sensing the right data ahead of need, and paves the way for modern information theory and systems, where understanding the adversary (wisdom) is the only way to pre-emptively predict his intent so that the right action can be taken ahead of time (as shown in Figure 10). For example, it is useless to jam the RF-IED after the trigger signal has been transmitted (and it has exploded).

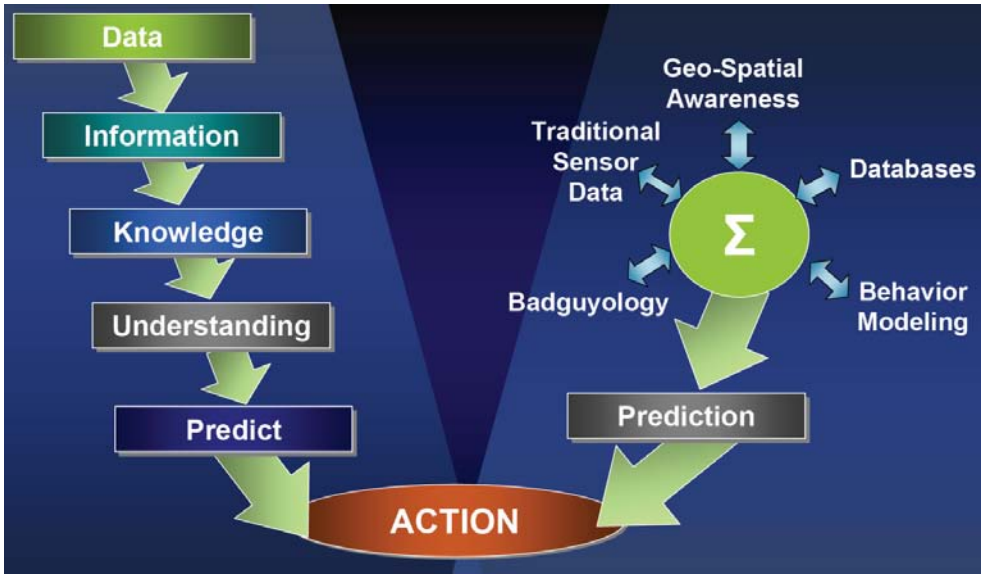

Figure 10: The Information Operations paradigm.

Electronic Warfare can be employed in support of Information Operations to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

Electronic Warfare Support and Intelligence: The distinction between intelligence and ES is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. ES is achieved by assets tasked or controlled by an operational commander. The purpose of ES tasking is immediate threat recognition, targeting, planning and conducting 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.

EW, IO and Cyberspace: EW. in its most basic form, seeks to shape, disrupt and exploit adversarial use of the EMS while protecting friendly freedom of action in that spectrum.

Information Operations (IO) are activities conducted in or via the information environment with the intent to affect and protect cognition, cognitive processes, information, and the connectivity and processing systems necessary to create and exchange information. IO uses any or all means, in integrated and coordinated means, to create cognitive effects. IO span the full range of activities in human interaction from person to person through complex, multistate, intercultural, and international communications. Information Operations are planned and executed in order to cause an adversary to pursue an action favourable to a friendly course of action or cause a potential adversary to not impede friendly actions.

Cyberspace operations are the employment of cyber capabilities, where the primary purpose is to achieve military objectives or effects in, or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. Cyber networks cannot exist without the physical networks, and the EMS is a key part of this physical networks. Therefore Cyber effects can be created by EW effects and effectors.

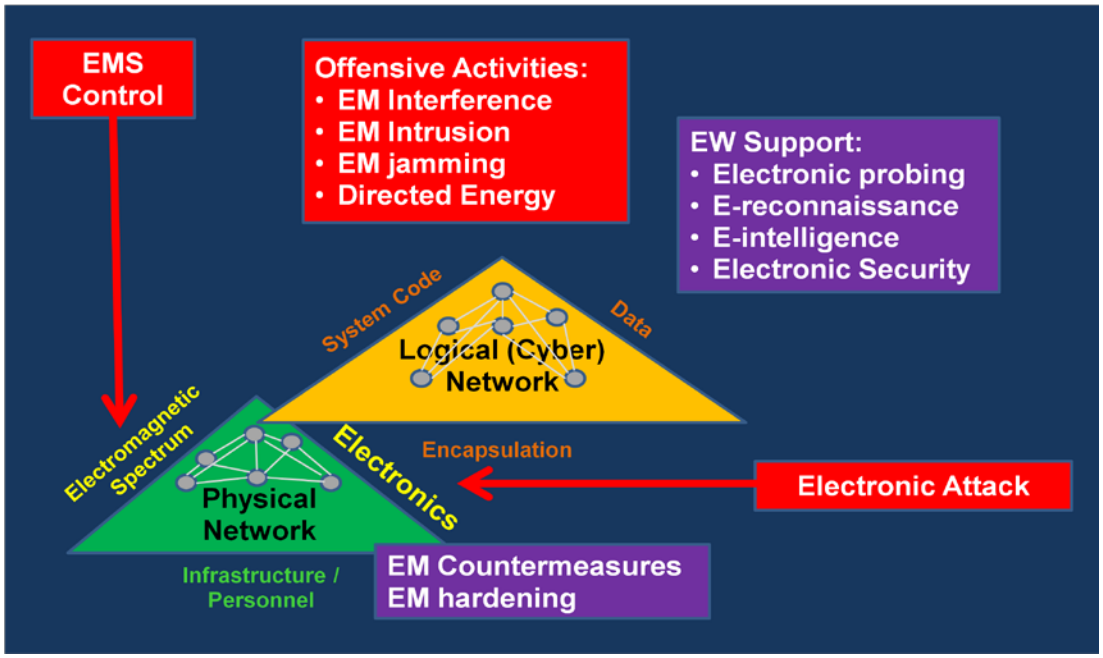

Figure 11: EW Cyber Effects (with some use cases).

EW also contributes to the success of information operations and cyberspace operations by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EMS while protecting friendly freedom of action in that spectrum. Expanding reliance on the EMS increases both the potential and the challenges, in not only EW, but also in IO and cyberspace. The increasing prevalence of wireless telephone and computer usage extends both the utility and threat of EW, offering opportunities to exploit an adversary's electronic vulnerabilities and a requirement to identify and protect our own from similar exploitation.

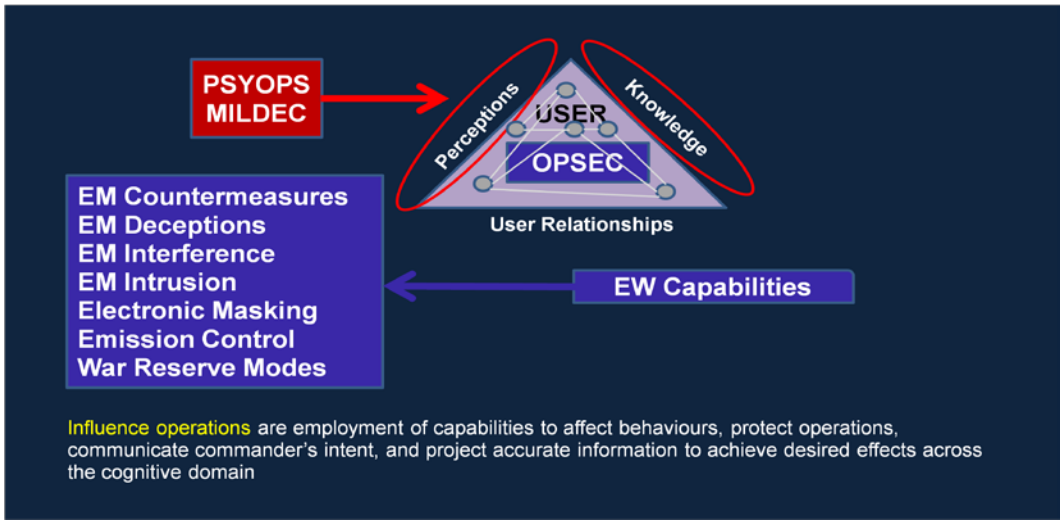

Figure 12: EW Cognitive Effects.

Figure 12 shows a list of some of the EW capabilities that can support influence operations – EW is a means to conduct Information Operations – it is not in itself Information Operations.

EW and Command & Control Warfare

EW is important for Net-enabled Warfare, also referred to as Command & Control Warfare (C^2W), because it is the EMS that tie together the sensor to the shooter, as shown in Figure 13 with John Boyd's OODA Loop, Observe, Orient, Decide and Act. If one loses the EMS, you lose situational awareness, you lose the ability to link operational centres.

EW should be viewed as a non kinetic precision weapon.

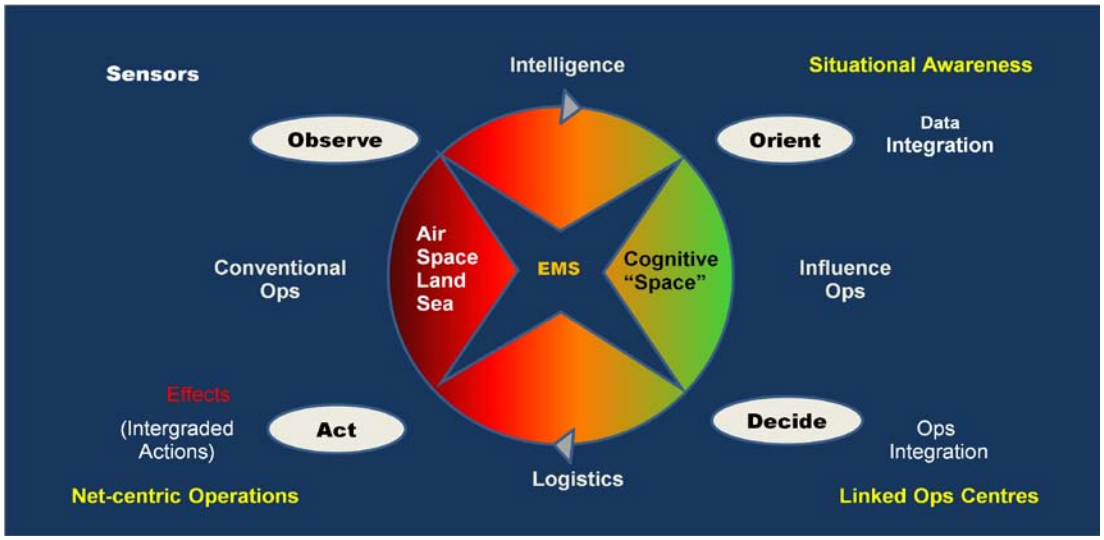

Figure 13: EW and Net-enabled Operations (also referred to as C^2 Warfare).

From a Command & Control standpoint, EW can disrupt sensors, manipulate data or degrade systems completely. Also, the ability to protect against such exploitation, is where EW have a huge contribution.

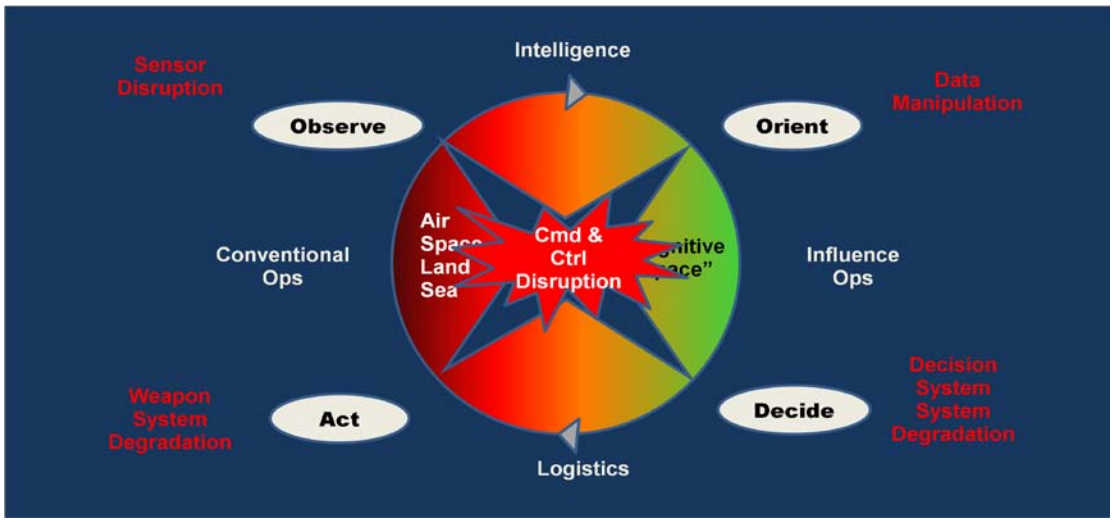

Figure 14: Net-Centric C^2 Attack.

EW in the Operational environment

Operationally EW gives a defence force both an Offensive as well as a Defensive capability. Figure 15 shows how these capabilities fits together with own forces and adversaries as well as how the different EW activities link it together.

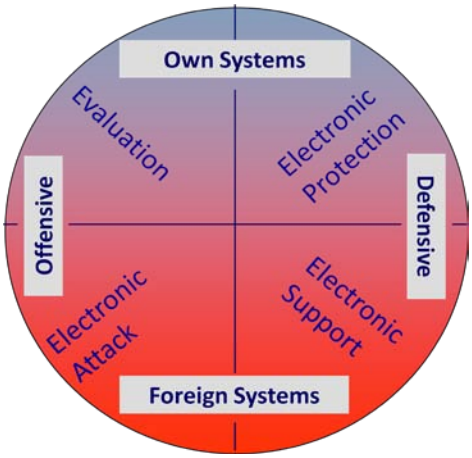

Figure 15: Circle Description of EW, showing how the Offensive and Defensive capabilities tie together.

EW involves many different activities that require decision-making at various levels. Many of this happens concurrently, especially in wartime. Some of the activities and decisions are long-term issues while others need extreme rapid responses.

Figure 16 illustrates the responses of EW to the operational environment at the strategic, operational/tactical and survival levels. At the strategic level, the time-line is measured in years, months, weeks and days. At the tactical level, the time-line in measured in hours, minutes and seconds. At the survival level, the time-line is measured in seconds and milliseconds.

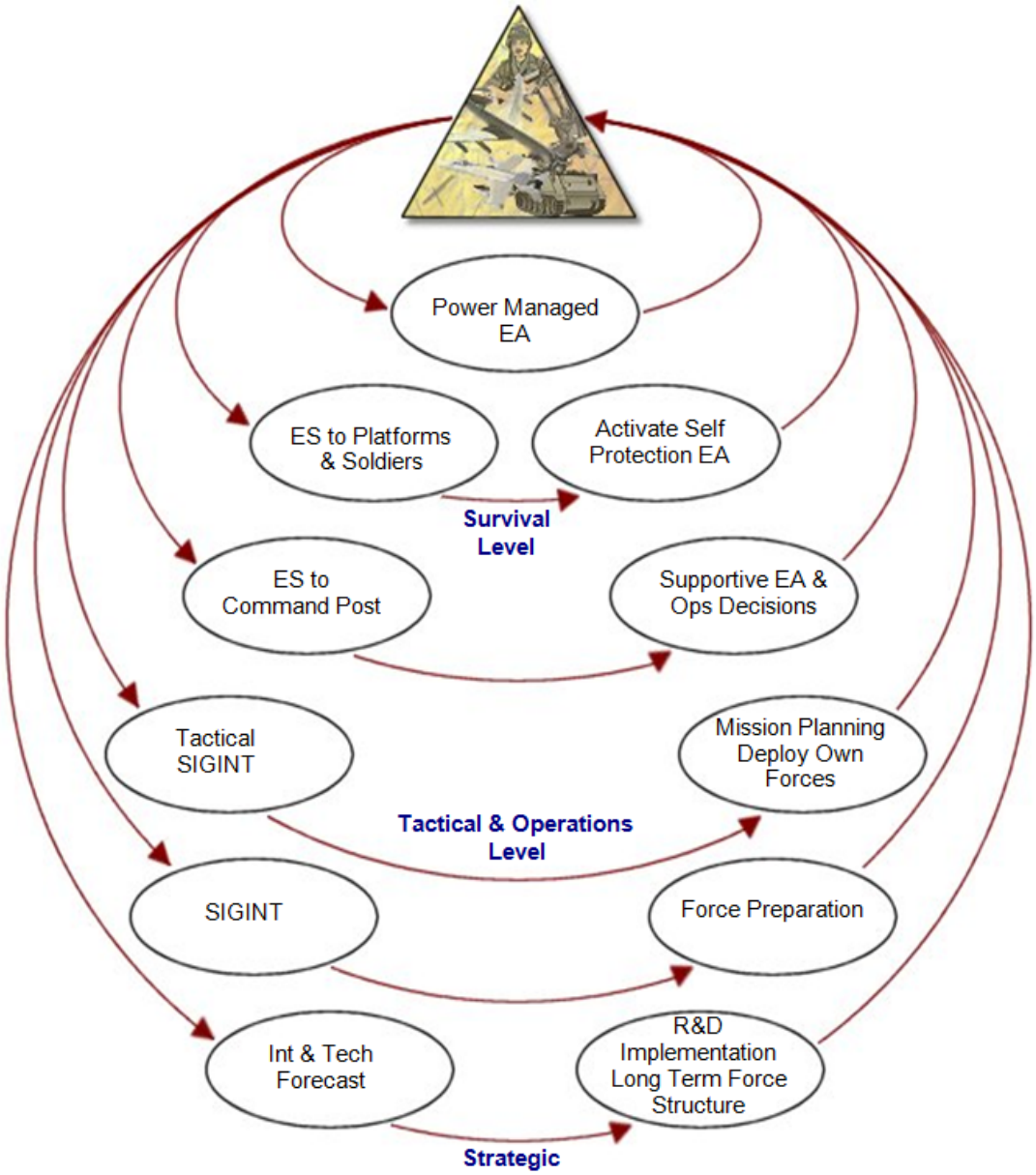

Figure 16: A typical EW operational concept example.

1.4 Conclusion

The use of the EMS affords commanders the opportunity to make decisions rapidly, conduct operations, and deliver effects at speeds that were previously incomprehensible. Loss of this capability is critical to 21st Century warfare. The employment of electronic fires, both lethal and non-lethal, requires considerable coordination between the roles of Command and Control, intelligence gathering, spectrum management, and active fire support, so that one effort is not hindered by the other's mission. This coordination requires trained EW personnel equipped with essential EW planning tools. Furthermore, there is a critical need to develop strategic and operational leaders with expertise and experience in EW. EW operators require education and the opportunities to develop themselves as practitioners of the strategic and operational art.

EW relationships with IO and cyberspace operations must be understood to fully exploit and leverage warfighting capabilities. EW is conducted in the EMOD, the global domain of electronic systems operating in the EME which create, control, exchange, and employ electromagnetic energy across the EMS to achieve physical, informational, and cognitive effects. Cyberspace is a global domain in the information environment; however, cyberspace and EMOD share one common feature - the dependence on electronic systems and the EMS to establish and maintain the domain. For practitioners of EW, it is useful to distinguish effects of IO from the ways and means employed to achieve these effects. EW can provide these effects, but is not an element of IO since it produces physical and cyber effects as well.

The global nature of the EMS and the potential for interference from systems operating in EMOD have created a demand for international, multi-service, and industry EW standards which establish mechanisms to foster EW system's interoperability across warfighting domains and organizations, and provide industry a foundation for rapidly integrating cutting edge technologies into existing EW capabilities.

The overarching goal of 21st Century Electronic Warfare is to ensure that warfighters in all domains are properly prepared for operations in a contested EMS environment. Meeting this goal requires advancements in doctrine and concepts, development of the spectrum enterprise workforce, fielding systems reflecting advancements in science and technology, and adopting system standards that are applicable across domains and mission sets.

Fundamental Principles for 21st Century Electronic Warfare:

1. The Electromagnetic Spectrum (EMS) provides the manoeuvre space that allows unified action across all warfighting domains.
2. Electronic Warfare creates physical, informational, and cognitive effects through the use of electronic systems operating in the Electromagnetic Environment (EME) which create, control, exchange, and employ electromagnetic energy across the frequency spectrum.
3. Electronic Warfare consists of four elements: Electronic Attack (EA), Electronic Protect (EP), Electronic Warfare Support (ES) and EMS Control (EMC).
4. Electronic Warfare controls and exploits use of the EMS to enable friendly freedom of action in all domains (to include cyberspace) and to deny freedom of action to adversaries.
5. EW and Cyber operations both require use of electronic systems and electromagnetic spectrum but are very different: EW is conducted in the electromagnetic environment while Cyber ops are conducted in the information environment.
6. Electronic Warfare can be employed in support of Information Operations (IO) to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

2 Electromagnetic Spectrum Protection

2.1 EW “Threats”

The defensive part of Electronic Warfare deals with threat detection, recognition and identification of any electromagnetic radiation, being intentional or unintentional, as well as protecting personnel and own equipment against exploitation and harm caused by the use of the EMS. Offensively EW aims at harming and exploiting adversaries through the use of the EMS.

In the realm of electronic warfare, the target is generally the signal that is emanating from, or being used by a targeted system, and not the system itself - the exception being some applications of Directed Energy Weapons.

Unintentional emissions do not mean somebody not adhering to the Emission Control (EMCON) order, but rather emissions “leaking” from equipment (e.g. radios’ local oscillators, jammer systems not switching off properly etc.). Examples of intentional emissions are normal radio, radar, radio altimeter and cell-phone transmissions.

If a signal/emission can be detected, it can be:

- Classified (e.g. friend, foe, cell-phone, satellite phone, search radar, tracking radar, airborne radar etc.).
- Identified as a specific type of transmitter (in certain instances belonging to a certain type of weapon platform). An example is a Slot Back fire control radar of a MiG-29 aircraft.
- Uniquely identified, also called Specific Emitter Identification (SEI), for example radio C21, serial number 302. This functionality is not necessary always possible in the communications domain, but more readily achievable in the radar domain.
- Geolocated. The first step is to determine the bearing of the emission relative to the receiver, but if more than one Direction Finding (DF) receiver is available, or either the DF receiver or emitter is moving, the emitter’s actual position can be plotted on a map.
- Demodulated. For communication emissions, the signal will also be demodulated and the data/message content extracted. The function of decryption falls outside the EW domain.

Having performed the SIGINT functions (described above), it is possible to obtain the Electronic Order of Battle (EOB), for example the communication nets, troop movement etc.

Once a signal has been detected and identified, the emission can be further exploited:

- This can be done by denying the intended receiver of the emission the use of the information, for example, through noise jamming break the data-link so that no information is received.
- The intended receiver of the emission can be deceived through false information, for example, showing the tracked aircraft at a different position than it actually is, or injecting false data into the datalink.
- The decision making process can be saturated by presenting the receiver with multiple false targets, which could, for example tie up the Threat Evaluation and Weapons Assignment (TEWA) processor.
- The communications net can be brought down by altering the GPS time, used to synchronize the frequency hopping tables.

It is not always necessary to detect an emission before action can be taken, because the potential emissions will follow a certain standard (frequency and waveform). GPS jamming is such an example (not only position, but also timing).

All this leads into the EMS protection, because what we can do to our adversaries, they can do to us. All our own emissions can be intercepted, altered and jammed. We therefore have to develop the appropriate doctrine and harden our own equipment and procedures against exploitation or denial.

The following section lists some equipment/systems/approaches that can either be used by own forces to intercept and deceive the adversary’s EM sensors and communications or can be deployed by own forces to protect themselves against the adversary’s exploitation of the spectrum. Control of the EMS works both ways.

2.2 Communications

Communications, by definition, carry information. In the world of EW, communications means electromagnetic signals carrying information from adversary systems, which they are seeking to defend, and we are seeking to degrade or deny its use by our adversaries. Communications signals are generally from

Extremely Low Frequency (ELF) for submerged submarine communication, all the way through to the Super High Frequency (SHF) for data-links and satellite communications.

It is important not to only consider military communication systems - the global commercial communications infrastructure will continue to be used by and against defence forces. There is an ever increasing role for, and reliance on commercial communications to the detriment of traditional military communications – as depicted in Figure 17. This, combined with the fact that the previous EMS segmentation (dedicated commercial, military navigation, communication and radar frequency bands) is no more as clear, have made EW's life a whole order of magnitude more difficult. This is especially true of the irregular (asymmetric) warfare arena where cellular and satellite communications are the biggest threat.

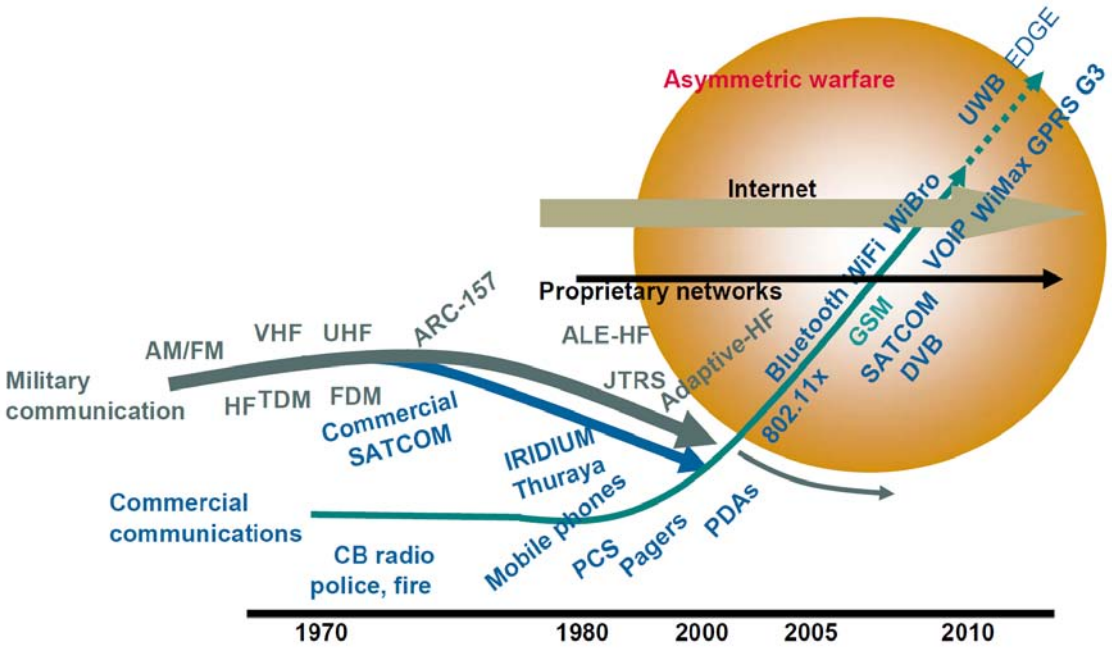

Figure 17: Communication trends.

The main trends in communication, with the associated EW implications are:

- Increasing reliance on commercial communications – which dramatically increase the signal density that the intercept receivers have to cope with, not to mention the huge increase in data volume that must be analysed by the built-in encryption. Currently, specialised EW receivers are required to cope with this environment, and they are not necessarily successful. This environment is EW's current biggest challenge.
- Dynamic Frequency Allocation (DFA). Gone are the days of known users/frequencies; the radio will select the optimum frequency for ensured communication. This makes analyzing and identification against the current generation databases difficult.
- Higher frequencies – allow for higher data bandwidths, and interleave with other spectrum users, for example radars – which traditionally were outside the frequency band of intercept receivers. An additional complication is that some radars transmit very high power, which require the EW receivers to have an even higher dynamic range.
- Stealthier waveforms (more difficult to detect and identify) - frequency and/or time hopping and/or Direct Sequence Spread Spectrum (DSSS) techniques combined with higher spectral efficiency through the use of digital modulation schemes (e.g. orthogonal modulation codes, etc.). This requires modern Digital Signal Processing (DSP) techniques only available in digital receivers.
- Networked communications. An EW system can only detect the transmitter and jam the receiver. Communication systems that have the capability to form ad-hoc networks forces the EA system to be able to jam all the nodes, otherwise the communication link could be re-established via the un-jammed nodes.
- Data security through encryption. This is however not seen as an EW responsibility.

Many of the features listed here are essential to enable the communication system to operate in such a congested EM environment. From an EW point of view, these are Electronic Protection measures, which makes it more difficult to intercept and jam the communications link.