Using a Layered Model to place EW in Context within the Information Sphere

F.D.V. Maasdorp, W.P. Du Plessis

Council for Scientific and Industrial Research (CSIR),
Defence Pease Safety and Security (DPSS),
Pretoria, South Africa,
E-mail: fmaasdorp @csir.co.za;wduplessis@csir.co.za

Abstract:

In recent years, a discussion on the relationship between Electronic Warfare (EW), Information Warfare (IW), Cyber Operations, Net-Centric Warfare, Command and Control, Information Operations (IO) and otherconstructs haveemerged. This paper proposes a three-layer model in an attemptto provide a new perspective on this discussion. Each layeris defined and the rolesand relationships between EW, IW, and IOareexplained accordingly. Using this approach is extremely powerful as it emphasises the complementary natures these fields should have, rather than the rivalrywhichis often the present. An attack on an 802.11g (WiFi) wireless link is used as an example to display the value this layered approach can offer.

Keywords:*Electronic Warfare (EW), Information Operations (IO), Information Warfare (IW), Cyberspace, Electro Magnetic Spectrum (EMS), Information Sphere*.

Introduction

In recent years, a common trend within the Electronic Warfare (EW) community involves debates on the rightful place of EW among other constructs such as Cyberspace(Hahn, 2010; Kunkel, 2008; Borque, 2008a, 2008b), IW(Smith and Knight, 2005), Net-Centric Warfare(Smith and Knight, 2005) and Information Operations (IO)(Wolf, 2011a, 2011b). The latest trend in this regard includes the involvement of physics into arguments that defend the rationale for involving EW in categories such as Cyberspace, Information Operations (IO) (Clifford, 2011; Hahn, 2010) etc. Therefore, the authors as observers to this debate and with a background in the telecommunications industry would like to propose an alternative perspective which it is believed will help simplify the discussion.

Some definitions of concepts that are key to this discussion are initially presented. Cyberspaceis defined by Hahn (2010, p.45)as

> "*A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers*."

From this definition, it can be seen that Cyberspace cannot exist without physical networks to connect systems to form networks. These physical connections rely on the Electromagnetic Spectrum (EMS) to convey data. The EMSis thus a key component of physical networks, and by extension,Cyberspace.

Elder (2010, p.11) defines the EMS as

> "*EMS refers to the range of frequencies of the electromagnetic radiation from zero to infinity. The spectrum is divided into bands ranging from radio frequencies at the low end to x-ray and gamma frequencies at the high end*."

Although not directly stated in the quote, the electro-optical region is also part of the EMS and is situated between the radio frequency region and the x-ray region. EW traditionally refers to a military action involving the use of electromagnetic (EM) and directed energy to control the EMS by means of sensing, attack, and protection. These abilities are known as Electronic Support (ES), Electronic Attack (EA) and Electronic Protection (EP) and are the cornerstones of EW.Lately, EMS control (EMC) has also been added to EW nomenclature to allow for a better effects-based emphasis.

A practical example of EMS utilisation is shown in Figure 1. A radar is deployed at a geographical position to alert Head Quarters (HQ) of air activity in the vicinity. Upon the radar detecting a target, the positional information is sent to HQ via a wireless linkto allow a decision to be made by the commanding officer. Note that a land line or fibre optic cable could also have been used to communicate the information without affecting the principles.

In this scenario, the role of EW would traditionally be limited to the accurate detection of the target by the radar; or prevention of such detection by an adversary as these processes are inherently based on the EMS. However, as the wireless link also utilises the EMS, EW applies to this network as well. For example, an adversary could use EW jamming at the EMS level to alter the target position information sent over the wireless link. If caution is not exercised, the HQ would never know about this deception/denial because the radar would report no jamming. Therefore, EW's capability to manipulate and exploit the EMS is a valuable capability in the communications aspects of this scenario.

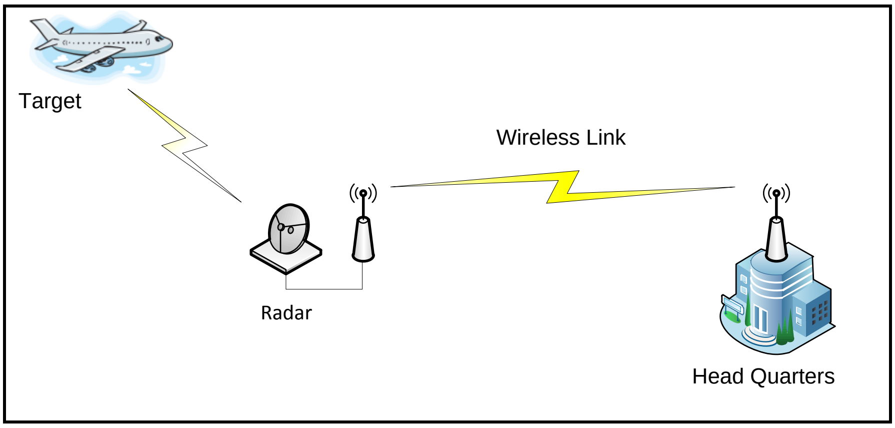

Figure 1: Utilisation of the EMS.

OSI Model

As stated in the introduction, the main underlying principle of EW is its interface to the EMS. However, EW systems are increasingly required to provide input to and take instructions from other networksand systems in order to achieve the desired operational effect. Keeping this in mind, the focus is now shifted to the computers/telecommunication domain.

In the early 1980s (the early days of the Internet), the computer and telecommunications industries experienced a similar dilemma, that is defining protocols to connect multiple computers for the mass distribution of information, while exploiting different fields of expertise stretching from antennas to operating systems.

The solution to this problem came in the form of the development of anarchitecture for computer communications. This development was undertaken under the auspices of the International Organisation for Standardisation (ISO) and the result was the Open Systems Interconnection (OSI) model. The model, displayed in Figure 2(Stallings, 2000), consists of seven layers, namely the application, presentation, session, transport, network, data-link and the physical layers. The key to this model is the principle of abstraction whereby the intricacies of each layer are hidden (abstracted) in every other layer while still allowing relevant information about other layers to be communicated. This approach is extremely powerful because it allows engineers to focus on the issues related to each layer without requiring a detailed knowledge of every aspect of all layers. In this way, engineers working on the application layer (for example software running on a system) do not need detailed knowledge of the physical layer (the physical wires or EM waves connecting systems), but still have access to information they require (for example bandwidth, latency, etc.). Note that higher levels in the model do not imply additional or reduced complexity, or any kind of superiority or inferiority, merely a different view of the system.

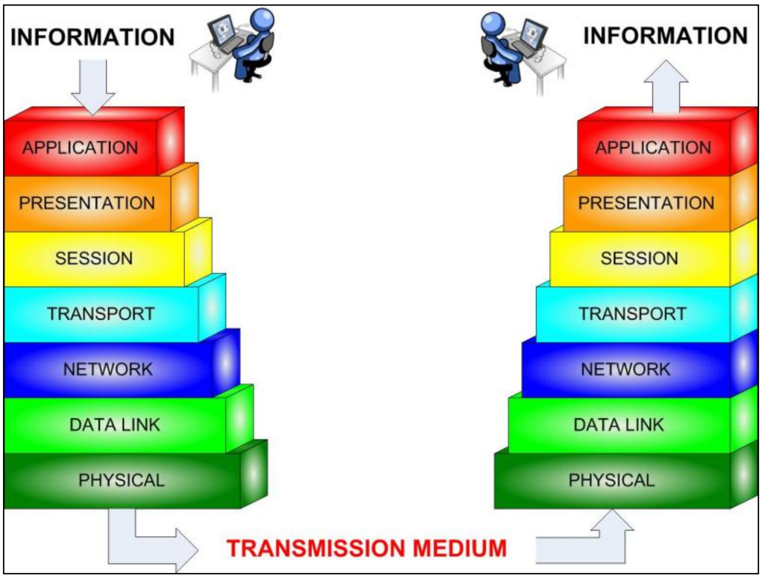

Figure 2: OSI model(Stalling, 2000).

Proposed Model

In the case of the relationships between EW, Cyberspace, IW, and IO within the defence domain, a similar architecture or model can be used, hopefully addressing many of the debates surrounding this topic. Therefore, it is proposed that the adoption of a similar approach to the OSI model for this purpose but define new layers. This is crucial as a lack ofclear definitions is one of the underlying causes of confusion about the roles and responsibilities of each field.

With reference to Figure 3, the bottom or first layer is defined as the layer responsible for access to the EMS and label it the Access Layer. EMS systems, such as EW systems, communication systems and radars operate at this layer as they all provide an interface to the EMS. In the light of a recent article published in the Journal of Electronic Defence (JED)(Clifford, 2011), this seems reasonableas the article argued that every EW practitioner should have some knowledge of physics, including electromagnetic wave propagation, and modulation types. Thus, the Access Layer, in which EW resides, is seen as having the ability to manipulate and exploit the EMS, and pass information to and from higher layers in the model.

Thesecond layer is labelled the Connection Layer and is defined as the layer responsible for themanipulation and transport of data within a network. At this point, data would be manipulated as bits or packets, rather than modulated signals as is the case in the Access Layer. This layer is also commonly referred to as Cyberspaceand is the region in which IW practitioners typically operate. Thus, IW practitioners are not required to have expert knowledge of interactions with the EMS – or even whether data are transferred via coaxial cable, fibre optic link or radio link – but rather to focus on the manipulation of data at bit or packet level to accomplish the appropriate objectives.

The third and final layer, labelled the Utility Layer is placed at the top of the model and is defined as the layer which exploits the lower layers to achieve a desired effect, again without requiring detailed knowledge of those lower levels. The Utility Layer is thus the level in which operations are conducted, for example PsyOps, and IO.

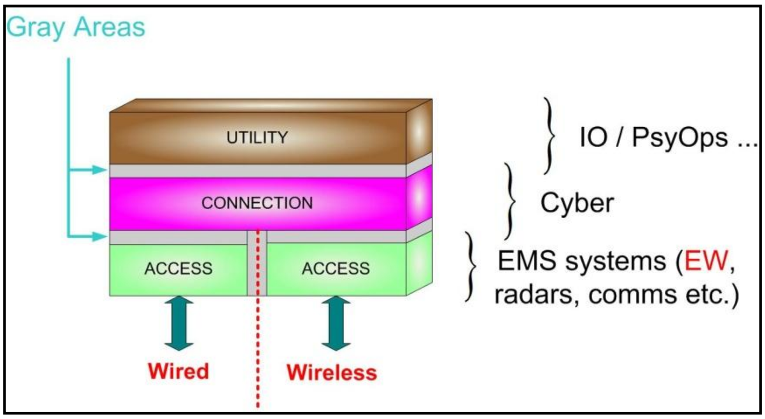

Figure 3: Proposed model to place EW in context.

This approach demonstrates the differences between EW, Cyberspace and IO in a very natural way, emphasising both the importance and complementary nature of each of these fields. The grey areas displayed in Figure 3, illustrate that the interfaces between the layers are not intended as clear dividing lines and that subject matter expertise can overlap. For example, the interface between EW operating at the Access Layer, and Cyberspace operating at the Connection Layer could vary depending on the task at hand, but the for example the transition from modulation in the Access Layer to binary ones and zeros in the Connection Layer is seen as a common transition. However, this should be determined by the subject-matter experts residing in the respective layers. Lastly, note the Access Layer has been split into two sections to emphasise the fact that EW focuses predominantly on the wireless scenario (though EW expertise can be relevant to the wired case). Furthermore, all layers in the model do not necessarily need to be present in every situation. For example, an EW protection system such as a Directed Infrared Countermeasures (DIRCM) system on board an aircraft would respond immediately to a missile fired on it without waiting for a command to be issued from the Utility Layer.

Quoting from Lonsdale (2004):

> "*Strategic power can be projected over the current known dimensions such as sea, land, air and space. A fifth dimension in which strategic power can be projected is also described as the infosphere. The infosphere is the environment where shapeless information exists and flows both in structured and or random ways. The infosphere is where facts or knowledge reside and is represented or conveyed by a particular sequence of symbols, impulses or characterisations. It is also the domain where command and control takes place. The Electromagnetic Spectrum, Network Spectrum and the Human Domain (cognitive domain) are the spine of the infosphere*."

With reference to this quotation, the information sphere is made up of the EMS, network spectrum and the human domain. The proposed model mirrors this approach with the Access Layer,which accesses the EMS, the Connection Layer,which is equivalent to the network spectrum, and the Utility Layer, which is the human domain in which operations are conducted. Therefore, this model is clearly supported by the infosphere approach presented by Lonsdale (2011).

Jamming example on 802.11b

This section provides an example to illustrate the value of using the proposed model. Recent experimental results published by EW staff at the CSIRhave shown that an 802.11b wireless link is vulnerable to smart attacks (Vlok, 2010).

The classic method of performingsuch an attack is to raise the RF noise floor to levels which prevent the wireless system from transferring data over the link. This attack is therefore aimed towards the Access Layer in Figure 3. However, since the 802.11b standard has built-in intelligence to compensate for RF interference, it senses the link interference and adjusts the link power to a level at which the system is able to re-establish the link and proceed with the data transfer. Therefore, the jammer and the 802.11b communication link enter into a power struggle in which each party aims to emit more power that the other. Furthermore, the user of the 802.11b system will be able to determine that such an attack is taking place from the information captured by the system.

Making use of a more intelligent attack, and aiming more towards the data-link layer of the OSI model, it was proven that an attack could be performed very efficiently (and covertly) without entering into a power struggle (Vlok, 2010). This attack worksby injecting signals at the Access Layer which exploit the access-control mechanism of the 802.11b protocol to cause the desired breakdown in the communications. Furthermore, it would not be easy for a user to determine that an attack was taking place, potentially increasing the value of the attack.

Using a simple noise jamming scheme would clearly reside in the Access Layer and be an EW task. A traditional Denial of Service (DoS) attack where the network is overwhelmed with synthetically generated data would equally clearly reside in the Connection Layer and be a Cyberspace task. While still predominantly working in the Access Layer, the approach used by (Vlok, 2010) moves towards the Connection Layer because knowledge of the access-control mechanism is required. The value of the proposed model in this context is that it shows that EW practitioners need to enlist the help of their Cyberspace colleagues to take this work further because future extensions will rely on knowledge of issues like authentication and encryption which clearly lie in the Connection Layer. In fact, the lack of such knowledge is one of the main factors which have meant that this work has not been continued.

Conclusion

In conclusion, an approach similar to the OSI model is proposed to clarify the relationships between EW, IW, Cyberspace, and IO. This approach would allow debates surrounding EMS and who takes responsibility for it to be placed in context. This approach will go a long way towards clarifying the different, yet complementary roles of EW, IW, Cyberspace, IO and any other system or concept which interacts with the EMS. However, the OSI model is very seldom applied to specific systems without modification, so it is reasonable to expect the same will occur with the proposed model.

Acknowledgements

The authors wish to thank Jacobus Vlok for his assitance with the development of the 802.11b attack described above. The authors also wish to thank Christo Cloete and Joey Jansen van Vuuren for theirinsightful suggestions to this paper.

References

Borque, J. L. (2008a) Why EW is not part of Cyberspace. *Journal of Electronic Defense*, 31(**9**): 38-40.

Borque, J. L. (2008b) A (pragmatic) future for joint electronic warfare: does EW + CNO = cyber?.*Journal of Electronic Defense*, 31(**9**): 30-38.

Clifford, J. (2011) What Electronic Warriors should know about Physics, Language and Concepts. *Journal of Electronic Defense*, 34(**3**): 40-47.

Elder, R.J. (2010) 21st Century Electronic Warfare, URL: http://www.palmettoroost.org/documents/AOC_21st_Century_EW_Report.pdf [Accessed: 19th October, 2012].

Hahn, R. (2010) Physics of the Cyber-EMS Problem, Why We Have the Language Wrong. *Journal of Electronic Defense*, 33(**11**): 44-46.

Kunkel, M. (2008) New cyber definition excludes EW. *Journal of Electronic Defense*, 31(11): 26.

Lonsdale, D. J. (2004) *The Nature of War in the Information Age*, London, Kings College.

Smith, R., Knight, S. (2005) Applying electronic warfare solutions to network security. *Canadian Military Journal*, 6(**3**): 49-58.

Stallings, W. (2000) *Data and Computer Communications 6th Edition*, New Jersey, Prentice Hall.

Vlok, J.D. (2010) Control Jamming of WiFi 802.11b, *Council for Scientific and Industrial Research*, No. 5865-ESDE-00001, Pretoria, Council for Scientific and Industrial Research.

Wolf, W. (2011a) 21st century EM domain capabilities. *Journal of Electronic Defense*, 34(**10**): 12.

Wolf, W. (2011b) EW co-opetition for info ops. *Journal of Electronic Defense*, 34(**6**): 12.