ELECTRONIC WARFARE IN INFORMATION AGE

Laurian GHERMAN

"Henri Coandă" Air Force Academy, Brasov

Abstract: *In this paper the importance of electronic warfare is presented taking into consideration the information age environment. In order to understand the electronic warfare this in information age, first we should understand what information age is and how the electromagnetic spectrum is used today. The Information age has changed every aspect of our life. For the first time in history we can create, access and store a high amount of information and all this happen during our life span. How has the military field been affected by all these changes? The military answer to the information age was the network centric warfare (NCW). As we can see, this concept NCW is affecting every aspect of the military field creating the evolution path from platform-centric to network-centric forces. When all military tools are physically limited in order to achieve military superiority we should exploit the new domain the information domain. Without this transformation it is not possible to achieve victory.*

Key worlds: *Electronic warfare, information age, network centric warfare*

1. INTRODUCTION

Electronic warfare is defined as the military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1).

In order to understand the electronic warfare in the information age, first we should understand what information age is and how the electromagnetic spectrum is used today.

First let us go back in history when all these things started. The information age follows the industrial age and the question is what happened.

The information age is deeply rooted in the industrial age, when James Clerk Maxwell (1831-1879) proved theoretically the existence of the electromagnetic field.

In 1865, he published his work "A dynamical theory of the electromagnetic field" where he demonstrated that the electric field creates magnetic field and the magnetic field creates electric field and both travel in space in form of waves, at the speed of light. He told us that we are surrounded by an electromagnetic spectrum.

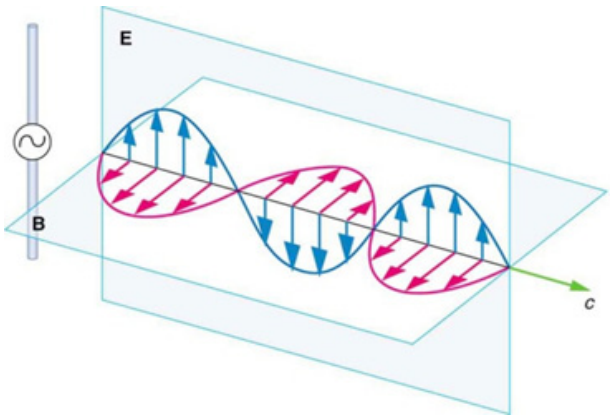

Fig. 1 Electromagnetic waves

The next big step was taken by Heinrich Rudolf Hertz (1857-1894) who practically demonstrated the existence of the electromagnetic waves. This research gave us the possibility to communicate over very long distances. For the very first time in history, we were able to communicate over long distances at the speed of light. But this big step was not enough to change the industrial age into another age.

Let us find out what happened in the military field in this period. We started to increase the use of the electromagnetic spectrum and to share it, with civilian application.

Now this process is still ongoing and in the future we will depend more and more on the electromagnetic spectrum.

During this time weapons had reached their physical limits and the speed of evolution decreased. In order to prove this I will give you a few examples. Let us talk about aviation. In order to achieve aerial superiority we have started to push the physical limits of airplanes. First, aircraft were developed to fly at higher altitudes. One example is the U2 Dragon Lady aircraft.

Fig. 2 U2 Dragon Lady Aircraft

This approach was not enough for the military demands. The design was fragile and could be shot down by surface to air missiles.

Secondly, it was developed an aircraft designed for high speed like Lockheed SR 71 Blackbird. Even this approach was not enough for the military demands. The aircraft achieved high speeds at high costs.

Fig. 3 Lockheed SR 71 Blackbird

The third step was the airplane Lockheed F117 Nighthawk which was designed to be less detectable by radars. This direction is under development but it is not enough to achieve aerial superiority.

As we can see, all the directions of development involved higher energy consumption and one design could solve only one problem, but leaving many others unsolved.

Fig. 4 Lockheed F117 Nighthawk

At this point through the history, in the middle of the 20th century something very important happened. The digital revolution started.

What's more the speed of evolution was grew exponentially. According to Gordon Moore's observation, the number of transistors doubles every two years. And the Moore law is applied in every digital domain.

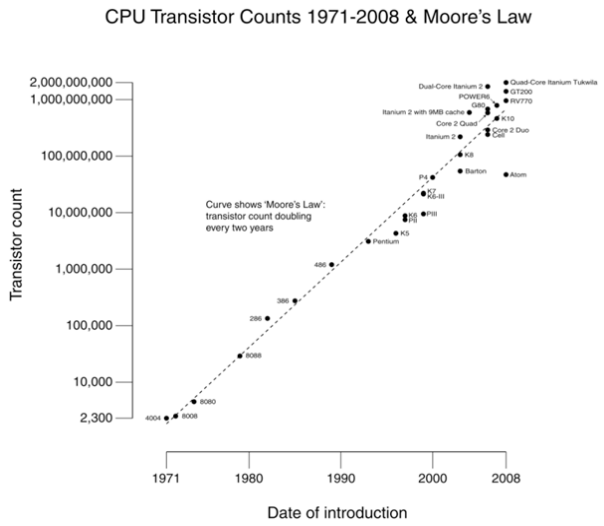

Fig. 5 Moore law

Now we move from industrial age to information age.

Practically now we can transmit a great amount of information over long distances virtually at the speed of light.

2. INFORMATION AGE

The Information age has changed every aspect of our life. For the first time in history, we can create, access and store a high amount of information and all this happens during our life span. How has the military field been affected by all these changes? The military answer to the information age was the network centric warfare.

According to Alberts et al. the definition of NCW is:

Network centric warfare is the best term developed to date to describe the way we will organize and fight in the information age. ... We define NCW as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

As we can see, this concept - NCW - is affecting every aspect of the military field creating the evolution path from platform-centric to network-centric forces.

Also, we have changed our way of thinking from keeping the information to sharing the information. This approach requires a new type of commanders and a new type of military organization structure.

When all military tools become physically limited in achieving military superiority, we should exploit the new domain: the information domain.

Without this transformation, it is not possible to achieve victory.

A good definition of information superiority is: *"the operational advantage gained by the ability to generate and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same"*. (FM 1-02)

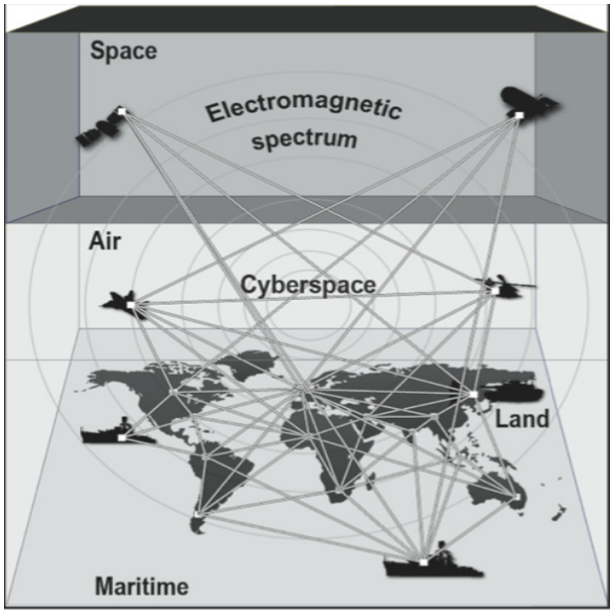

Fig. 6 Network centric warfare

From the electronic warfare point of view, the network should be created by using the electromagnetic waves connections because of the mobility of systems.

From my point of view, it is very hard if not impossible to cut all connections in a large network. The network will survive an electronic attack. It is important to protect the information in this network but this task does not relate to electronic warfare job.

The electronic warfare actions are in physical domain because the electromagnetic spectrum is very physical. The information transported by the electromagnetic waves should be protected by cybersecurity measures.

The real job of electronic warfare is to act on sensors which use the electromagnetic spectrum. The sensors can be any kind of systems, radars, communication systems, optical which work in the physical domain of the electromagnetic spectrum.

So, if the electronic warfare is not able to cut the network connections, because we will always find a path to communicate, the electronic warfare can reduce our capabilities to acquire information about the enemy at a tactical level.

Because the shooters are small and very mobile units, we must collect information about their position via the electromagnetic sensors.

Here, the electronic warfare actions are very important because without good information the whole concept of network centric warfare fails to work.

Because all sensors are networked, I will use the same approach like in a computer network. In order to protect a network it is not enough to install an antivirus software on every computer from a network.

The security measures must be applied to the entire network and the end user computer should be the last line of defense. In our case, the sensors are the end users in our network.

The sensors should be built to resist to electronic attack but this is not enough.

We should also have offensive systems not only defensive measures. This way, the electromagnetic spectrum in an area controlled by our forces can by efficiently used.

The things are simply like that: If you do not control the electromagnetic spectrum, you will be defeated; if you do not have air supremacy, you will be defeated; if you do not have boots on the ground, you do not control that area.

CONCLUSIONS

The real task of the electronic warfare in the information age is to attack and protect sensors. The sensors are our eyes and ears and if we cannot "see" and "hear" the battlefield, we will be defeated.

Today, but also in the future, the sensors will depend more and more on the electromagnetic spectrum. If our ability to acquire and to send information is reduced by the enemy, our concept of information superiority is doomed.

From this point of view, today and in the future, the electronic warfare role will be very important. For this reason, the physical domain of the electromagnetic spectrum should be at the same level as the land, maritime, air and space domains and all should be networked.

BIBLIOGRAPHY

1. FM 1-02, Operational Terms and Graphics, Headquarters, Department of the Army, Washington, D.C., September 2004.
2. D. S. Alberts, Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP publication series, 2000.
3. D. S. Alberts, J. J. Garstka, R. E. Hayes si D. A. Signori, Understanding Information Age Warfare, CCRP publication series, 2001.
4. D. S. Alberts, Power to the Edge: Command... Control...in the Information Age, CCRP publication series, 2005.
5. D. S. Alberts, R. K. Huber si J. Moffat, NATO NEC C2 maturity model, CCRP publication series, 2010.
6. D. Adamy, EW 101: a first course in electronic warfare, Artech House Inc., 2001.
7. D. Adamy, EW 102: a second course in electronic warfare, Horizon House Publications Inc., 2004.
8. D. Adamy, EW 103: tactical battlefield communications electronic warfare, Artech House Inc., 2009.
9. L. Gherman, „Warfare in the Information Age," *Journal of Defense Resources Management,* nr. 1, 2010.
10. L. Gherman, „The Second Revolution in Military Affairs," *Journal of Defence Resources Management,* nr. 1, 2011.
11. L. Gherman, „Information Age view of the OODA loop," *Review of the Air Force Academy,* nr. 1, 2013.
12. D. Maccuish, „Orientation: key to the OODA loop – the culture factor," *Journal of Defense Resources Management,* nr. 2, 2012.
13. E. A. Smith, „Network Centric Warfare: Where's the beef?," *Naval War College Review,* 2000.
14. S. Topor, Război informational, suport de curs, Bucureşti: Editura U.N.Ap., 2004.
15. I. C. Vizitiu, Război electronic. Noțiuni fundamentale, Bucureşti: Editura A.T.M., 2005.
16. I. C. Vizitiu, Război electronic. Aspecte moderne, Bucureşti: Editura A.T.M., 2008.
17. I. C. Vizitiu, Război electronic. Teorie şi aplicații, Bucureşti: Editura A.T.M., 2011.