Electronic Warfare and Cyber Warfare During the Time of Computers

Gökhan Küçükayan[1], Hüseyin Aslanoğlu[1], Recep Benzer[2*]

1 Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., **2** National Defense University, * Corresponding author, rbenzer@kho.edu.tr

Abstract

By the significant roles of computers and computer systems in both military and governmental issues, related to these, electronic and cyber warfare subject has become a huge subject to learn search and discuss. In this paper, the definitions of both electronic warfare (EW) and cyber warfare (CW) will be explained, historical examples around the world will be given and the both similarities and differences will be discussed.

Keywords: Electronic warfare, Cyber warfare, Espionage.

Citation: Küçükayan, G., Aslanoğlu, H., Benzer, R. (2018, October) *Electronic Warfare and Cyber Warfare During the Time of Computers*. Paper presented at the Fifth International Management Information Systems Conference.
Editor: H. Kemal İlter, Ankara Yıldırım Beyazıt University, Turkey
Received: August 19, 2018, **Accepted:** October 18, 2018, **Published:** November 10, 2018

IMISC 2018 PAPER

Electronic Warfare and Cyber Warfare During the Time of Computers

Abstract

By the significant roles of computers and computer systems in both military and governmental issues, related to these, electronic and cyber warfare subject has become a huge subject to learn search and discuss. In this paper, the definitions of both electronic warfare (EW) and cyber warfare (CW) will be explained, historical examples around the world will be given and the both similarities and differences will be discussed.

Keywords

Electronic Warfare; Cyber Warfare; Espionage

Introduction

The electronic warfare has begun with the first electronic tools, especially telegraph has signed the first point of the electronics in war and this was the start of the electronic warfare. As the technology has been developed and the number of tools has increased, the electronic warfare has become a significant part of the electronics and security. Similarly, effective use of internet in business, military operations, governmental issues and telecommunication has made the cyber security to become the most important value of information systems.

It is not surprising talking on electronic and cyber warfare on military issues while computers have become the main subject of the operations, developments, decisions and attacks. The computers are on the central point in military, as well as in political matters, and this is the source of the both electronic and cyber warfare issues in order to both defense and offense.

In this paper, the definition of both electronic warfare and cyber warfare will have shared with historical examples, processes and discussions.

Electronic Warfare

What is EW?

The article, The Future Roles of Electronic Warfare in the Information Warfare Spectrum, written by B.Van Niekerk and M. Maharaj defines the information warfare (IW) as an organization of six functional areas namely command and control warfare (C2W), intelligence-based warfare (IBW),

information infrastructure warfare (IIW), network warfare (NW), psychological operations (PsyOps) and electronic warfare (EW) (Van Niekerk & Maharaj, 2009).

Electronic warfare is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via spectrum. The goal of electronic warfare is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the electromagnetic spectrum(Staff, 1996). According to NATO doctrines, the term electronic warfare consists of three divisions: electronic attack (EA), electronic protection (EP), and electronic support (ES).

INSERT FIGURE 1 HERE

Electronic Attack (EA)

First division of electronic warfare is electronic attack (EA) involving the use of electromagnetic, energy or anti-radiation weapons to attack any personnel or equipment with destroying enemy combat capability. The division also have subdivisions including actions to prevent or reduce effective use of the electromagnetic spectrum by an enemy and to employ the weapons using either electromagnetic or directed energy as their primary destructive mechanism (lasers, particle beams)(Powers, 2018).

EA includes electronic jamming which is the deliberate radiation or reflection of electromagnetic energy to prevent or to reduce enemy's effective use of the electromagnetic spectrum and the intent of degrading or neutralizing the enemy's combat energy and electromagnetic deception which is the deliberate radiation, re-radiation, alteration, absorption, enhancement or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy, thereby degrading or neutralizing the enemy's combat capability(Sullivan, 2001).

Electronic Protection (EP)

Electronic protection division of electronic warfare stands for the actions taken to protect personnel or the equipment from either the effects of friendly or enemy employment of electronic warfare which degrade, neutralize, or destroy friendly combat capability(Powers, 2018).

Electronic Support (ES)

Electronic warfare support is the division of electronic warfare used to define actions taken tasked by, or under direct control of an operational commander to search for, to identify, and to locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of

immediate decisions involving electronic warfare operations and other tactical actions such as avoidance, targeting, threat or homing (HAIG, 2015).

The primary activities of ES are threat recognition, targeting, planning and conducting future operations. Also, ES data can be used to produce signal intelligence (SIGINT), both communication intelligence (COMINT) and electronics intelligence (ELINT).

Historical Perspective of Electronic Warfare

The roots of EW history can be found in U.S. Civil War in 1861. The primary communication between the Navy Department in Washington, DC and the U.S. Navy Pacific Squadron was a dispatch vessel (Van Niekerk & Maharaj, 2009). During the U.S. Civil War, telegraph wires were one of the most important targets for cavalry, thus cavalry men switched military telegraph traffic to the wrong destination and transmitted false orders to Union commanders. That attempt was the first use of electronic warfare in history with cutting the wires to mislead information to the Union forces (Van Niekerk & Maharaj, 2009).

There might be opponent thoughts about the nature and definition of telegraph as “electronic” because it does not radiate electromagnetic energy. So, let us turn to first electromagnetic energy used as warfare, in which radio jamming was used purposefully. The aim of this first attempt is to gain tactical advantage during the Russo-Japanese War between 1904 and 1905.

Russo-Japanese War (1904-1905)

During Russo-Japanese War, a Russian warship captain recognized that a Japanese ship was transmitting the position of the Russian fleet to the Imperial Navy. He requested to jam its signals however his superiors denied this request which definitely played an effective role in Japan's overwhelming victory at the Battle of Tsushima Strait, where 80% of the Russian Baltic Fleet was destroyed. As a result, Czar Nicholas II abandoned efforts to curtail Japanese expansion in East Asia, enabling to emerge as a major world power.

The First Gulf War

The computers and chips played a significant role in warfare during the First Gulf War, delivering the information, intelligence and fire power than even seen before. During the war, the strategy was to build enough coalition forces that they can contain an Iraqi attack and reduce their ground forces' effectiveness (Knights, 2005). Tomahawk cruise missiles were used to match the video to preloaded

maps onboard, enabling the missile to cruise over the terrain using reference points. Also, Iraqi command and control systems are disrupted and communication and transportation systems are controlled as an achievement to air superiority (Knights, 2005).

Cyber Warfare (CW)

What is CW?

The U.S. National Research Council defines cyber-attack as “deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.” (Lin, 2009). In order to illustrate the cyber warfare, it is significant to compare cyber-attack to cyber warfare. Both of the terms include the objective to undermining the function of a computer network and having a political or national security purpose. The term cyber warfare differs from cyber-attack with the point of that the effects of cyber ware should be equal to an armed attack or an activity should occur in the context of an armed conflict. There are a few types of cyber-attacks including SQL injection, DDOS method and Trapdoors or Trojans.

In fact, cyber warfare is distinctive among three cyber-categories mentioned here in that cyber warfare should also establish a cyber-attack and there are two types of attacks between cyber-attack and cyber warfare which have overlapping area (Hathaway et al., 2012). The first type includes attacks carried out by an actor in the context of an armed conflict and the second type includes the attacks carried by a state actor which produce effects equivalent to those of a conventional armed attack (Hathaway et al., 2012). So, a cyber warfare meets the conditions of a cyber-attack but it should be noted that not all the cyber-attacks are cyber warfare. There a few forms of cyber warfare where there are proportional but significant differences among the definitions;

Espionage

Espionage can involve a government, a company or individuals obtaining information considered secret or confidential without the permission of the information holder (Joint Chiefs of Staff, 2015). In terms of cyber warfare, it is the case that anonymous hackers log into networks illegally and copy, delete or alter the computer data or communication network information. This means reaching the governments' secrets without any permission and having political or military implications on the country attacked.

Propaganda

Propaganda is the information that is not objective and which is mostly used to influence an audience and further an agenda. It is presenting the facts selectively in other words, possibly lying by omission for encouraging a particular synthesis, or using preplanned and loaded messages to produce an emotional reaction rather than rational response about the information presented (Briant, 2015). In some cases this information is spread rapidly over the internet and the fastest way to harm the reputation of the enemy.

Data Modification

It is a part of Espionage as it occurs when the anonymous hackers log into computers without any permission and the data reached by the hackers are changed. This may be more dangerous than the espionage phase as the changed information would cause the wrong decisions on the data or future model of the government for some cases would have wrong points in terms of decision making.

Historical Perspective of Cyber Warfare

Chechnya Propaganda in 1994

The incident may has the most significant value to force the Russian government to increase the cyber security level, as the videos and pictures of the Russian military activities appeared on the web while the passenger on a us were killed by the bus was attacked. This was not the only cyber war between Russia and Chechen, as Chechen forces website hacked by Russian services.

The Estonia Hacking in 2007

Estonia hacking was a series of hacking on media websites, government, military and banking. As the most of the services of Estonian banks goes online, the significant damage was on the banks during these attacks (Pye & Warren, 2009). The hackers also attacked to the political party of the prime minister of Estonia and they have changed the content of the website with an apologize message from Estonian government to Russian's memorial statue. The official website of NATO states that the attacks were more like cyber riots than crippling attacks, and the Estonians responded successfully by relaunching some services within hours or at most days (Anuta, 2011).

The GhostNet Cyber Espionage in 2009

"March 2009, The Philippine Daily Inquirer publishes a report citing GhostNet that the computer network of the Philippines' Department of Foreign Affairs (DFA) has been hacked by cyber spies based in China." (Krekel, 2009). The GhostNet was discovered after IWM researchers approached the Dalai Lama's representative suspecting that their computer network had been infiltrated. Also,

compromised systems were discovered in India, South Korea, Indonesia, Romania, Cyprus, Malta Portugal, Germany and Pakistan. Since than GhostNet has attacked most of the governments' computer systems, lastly Canadian official financial departments in 2011 making them offline (Information Warfare Monitor, 2009).

Similarities Shared by EW and CW

Firstly, electronic warfare capabilities include electromagnetic, directed energy to damage or deceive an enemy's electromagnetic capability and EW operations are dependent on electronic support information. Cyber warfare operations are not so different from EW with same information requirements.

Secondly, CW is used in information systems, business and official or governmental resources with the help of software tools and algorithms. It is true that CW uses software more than EW, however, one cannot argue that EW systems such radars or monitoring systems are developed and used with the help software tools and algorithms. EW is an operational element of information operations which has an influence on operations and computer network operations that contribute to the integrated air, space and land operational plans. Those plans use information tactics to disrupt, corrupt or change targeted human and automated decision makings (Information Warfare Monitor, 2009).

Finally, acquisition of information is a requirement to success the work either EW or CW. In order to obtain the effective data or in order to work on significant case, the right information should be reached at the right time. Acquiring the information will provide significant levels to work on and collect the data ensuring defenses. "The soldier operator behind a computer monitor (cyber) or screen (electronic) is usually the front line of defense in the battle to detect and understand electronic intent." (Information Warfare Monitor, 2009). Hence, the true information at true time is the key for both electronic warfare and cyber warfare.

After defining both electronic warfare and cyber warfare with their targets, systems, victims and types of attacks, Table 2 can be considered in order to compare the EW and CW.

INSERT TABLE 1 HERE

Conclusion

Electronic warfare (EW) is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via spectrum. Its significant examples include Russo-Japanese War and the First Gulf War in which radar techniques,

missiles and monitoring are used. Cyber warfare (CW) is to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. The significant examples are signed in Chechnya Propaganda, Estonia Hacking and The GhostNet Cyber Espionage with the purpose of attacking the official website, governmental information and espionage.

After the definition of both electronic warfare and cyber warfare, one may argue that the two subjects are clearly different from each other. However, it is now clear that there is an acquisition between electronic warfare and cyber warfare as they both process the true information on true time and it is the key point of the two subjects. Also, the methods used in the process would share the same process as they would use the same software tools and algorithms as they both use technical points. Additionally, electronic warfare capabilities include electromagnetic, directed energy to damage or deceive an enemy's electromagnetic capability and EW operations are dependent on electronic support information. So, cyber warfare operations are not so different from EW with same information requirements.

Regardless of who owns the electronic war or cyber war, these two subjects will continue to support the war-fighters in the feature. Increasing the intelligence of the machines, information on the networks and the data shared within the network will force the “owners” to attack the networks and get the information whether in order to damage or change. The combinative effect of electronic and cyber warfare will shift the balance of enabling the data and the control over them by the power of the technology.

References

Anuta, C. (2011). International Relations 2.0: the Balance of Power in Cyberspace. *Routledge Handbook of American Foreign Policy*, (3).

Briant, E. L. (2015). Allies and Audiences: Evolving Strategies in Defense and Intelligence Propaganda. *International Journal of Press/Politics*.

HAIG, Z. (2015). Electronic Warfare in Cyberspace. *Security and Defence*, *2*(7), 22–35.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*.

Information Warfare Monitor. (2009). Tracking GhostNet. *Network*.

Joint Chiefs of Staff. (2015). Department of Defense Dictionary of Military and Associated Terms.

US Department of Defense Joint Publication, *2001*(June), 513.

Knights, M. (2005). *Cradle of conflict: Iraq and the birth of the modern US military*. Naval Institute.

Krekel, B. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. *Computer*.

Lin, H. (2009). Lifting the veil on cyber offense. *IEEE Security and Privacy*.

Powers, R. (2018). Army Electronic Warfare Specialist. Retrieved July 10, 2018, from https://www.thebalancecareers.com/military-careers-in-depth-electronic-warfare-specialist-3345995

Pye, G., & Warren, M. J. (2009). An emergent security risk : critical infrastructures and information warfare. *Journal of Information Warfare*.

Staff, J. (1996). Joint Doctrine for Command and Control Warfare (C2W). *Joint Publication 3-13.1*.

Staff, J. (2000). Joint Doctrine for Electronic Warfare. *Joint Publication 3-51*.

Sullivan, D. S. (2001). *Javelin; the Potential Beginning of a New Era in Land Warfare*.

Van Niekerk, B., & Maharaj, M. S. (2009). The future roles of electronic warfare in the information warfare spectrum. *Journal of Informafion Warfare*, *8*(3), 1–13.

Figures and Tables

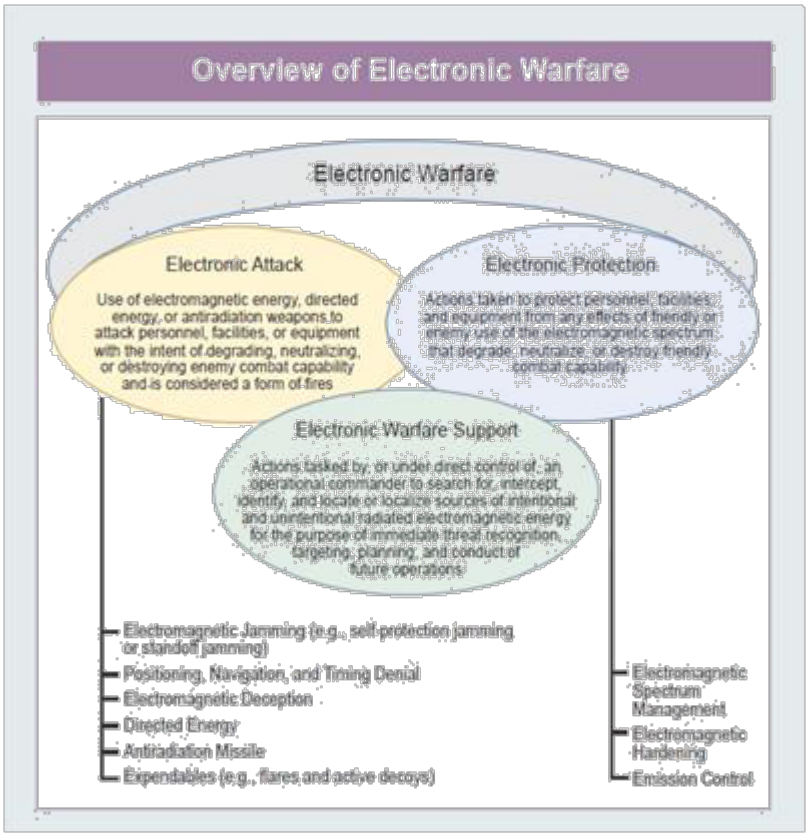

Figure 1. Concept of Electronic Warfare(Staff, 2000)

Table 2

Comparison of EW and CW

	EW	**CW**
Mission	• Air-position monitoring • Missiles • Navigation	• Information Technologies • Business • Government Systems
Intelligence	• COMINT • ELINT	• Hacking
Victim	• Radars • Communication Links	• Network Services • Resources
Attack Type	• Jamming (Spoofing) • Deception (Missile Stealing)	• Jamming (DDOS) • Deception (Trojans)