Abstract

Purpose: The importance of electronic warfare in modern warfare is increasing day by day. In particular, North Korea has a relative weakness of conventional weapons systems, and has focused on developing asymmetric weapons systems and electronic warfare as a way to overcome them. North Korea is currently expected to further expand its application to some aircraft and guided weapons operations under satellite navigation systems such as GPS, GLONASS, COMPASS and Beidou.

Method: This study studied the prior theory of electronic warfare at home and abroad. Prior research examined the military doctrines of the United States and trends in Europe. In particular, I studied the doctrines of the United States Joint Navigation Center (Navigation Warfare Center, JNWC) and the Education Command. Based on these prior research materials and literature reviews, I wanted to specifically review North Korea’s electronic warfare cases and present our response in terms of legal and institutional aspects.

Results: The South Korean military should recognize the importance of navigation warfare (part of electronic warfare) that protects our troops' location, navigation and square information so that they can be used without interruption, prevent the enemy’s use of related information, and ensure the peaceful use of such information outside the light bulb. In addition, we need to build an electronic warfare simulator and continue to promote training based on various scenarios.

Conclusion: Efforts to train and support professionals are urgently needed. In parallel with these efforts, joint efforts to develop electronic technologies between the civilian and military should be preceded. To win a high-tech war in the 21st century, it is essential, among other things, to have precision weapons and original electronic warfare support capabilities. In addition, it is necessary to foster R&D and defense companies to secure domestic technology.

Keywords: Electronic Warfare, Navigation, Jammers, Satellite Navigation Systems, PNT

1. Introduction

Most of human life today depends on information received from satellites[1].

It uses satellite information not only in the private sector but also militarily, such as taking off and landing aircraft and operating ships. Therefore, it is hard to imagine the possible damage caused by GPS disturbances[2].

For example, even though the aircraft is landing normally, is there a situation in which the aircraft computer system is not aware of this and the emergency warning lamp flashes?

In particular, if such incidents occur in fishing boats and ferries operating near the NLL in the West Sea, they are likely to be abused as means of kidnapping. In such cases, the military’s
damage is likely to be serious. In other words, when intercepting enemy missiles or attacking with allies' missiles on the contrary, it would be necessary to calculate the landing point, but it would be impossible to calculate the exact point of attack in case of GPS jamming[3].

Today's war patterns are changing from the past to network warfare and high-tech information warfare using advanced science and technology and information technology. In this situation, the importance of electronic warfare is increasing day by day[4].

In particular, North Korea has a relative weakness of conventional weapons systems, and has focused on developing asymmetric weapons systems and electronic warfare as a way to overcome them[5]. North Korea launches a full-fledged radio disturbance, it is expected that there will be great confusion not only in military operations of air and naval forces but also in the private sector such as telecommunications and transportation. It is known that the North Korean military has been preparing for electronic warfare more than a decade ahead of South Korea.

North Korea is expected to further expand its application to GPS, GLONASS, COMPASS and Beidou satellite navigation systems when operating some aircraft and guided weapons[6]. In particular, the importance of electronic warfare and navigation warfare by satellite navigation system is increasing day by day[7].

Electronic warfare will play an important role in keeping the enemy under control and winning victory in the first place by blocking the eyes and ears of the enemy and maximizing our allies' full power with this non-lethal operation without damage to life and property caused by physical strikes.

2. Theoretical Discussion on Electronic Warfare

2.1. Concept of electronic warfare

Electronic warfare is a non-destructive electronic attack, and electronic jamming and electronic devices, which are mainly aimed at undermining and incapacitating the enemy's weapons functions, are essential in carrying out efficient electronic warfare. Electronic warfare in the military sense means military action that paralyzes or disables the functions of the enemy's C4I (command control system) and the electronic weapons system. Electronic warfare is also defined as a military operation that controls the low magnetic spectrum[8].

In other words, it means using electromagnetic waves in military operations to support smooth operation. It is also regarded as an activity that utilizes electromagnetic waves to ensure the efficient operation of the friendly electronic weapons system and to prevent the efficient operation of the enemy's electronic weapons system.

Recently, there have been incidents in the government and private sector that have been highly dependent on GPS or GNSS use[9].

Many accidents have occurred due to so-called electronic warfare attacks such as Jamming, Spoofing and Mi-coning. Electronic attacks, which form part of an integrated navigation battle, are expensive attacks that require high-tech skills and high power[10].

Electronic warfare attacks are heavily influenced by the use of GNSS's measurements, navigation, and visual information before and during use of any kinetic energy weapon[11].
Figure 1. Ground-based augmentation system (GBAS) [12].

Such cases also occurred in Ukraine and South Korea. Many fighter jets and ships were confused in August 2010 and May 2013 when GPS signals caused confusion due to jamming from North Korea [13].

In Ukraine, the European Organization for Security and Cooperation reported that there was GPS Jamming during drone operations.

On November 8, 2018, during NATO military exercises in Finland and Norway, a navigation system failure caused the aircraft carrier to crash into a tank [14].

Incidental damage also resulted in civil aviation, car and cargo ships, smartphone operation and similar mix-ups. However, for civil airlines, navigation devices are used optionally. The U.S. Department of Defense told CNN that Jamming had little or no impact on U.S. military equipment. This effect is due to the use of military P/Y codes - rarely affected by jamming.

On the other hand, electronic warfare attacks can be extensive, with cheap, low-powered electronic warfare attacks called the so-called Personal Defense Agency (PPD). Personal protection is a small, low-cost, lightweight jammers that can be easily purchased on the Internet.

The use of such jammers is prohibited in most countries, but their ownership is not strictly limited to the same level as that of use.

2.2. Classification of electronic warfare

Electronic warfare is divided into electronic attack, electronic reporting, and electronic warfare support depending on utilization patterns and performance [15].

2.2.1. Electronic Attack (EA)

It refers to the act of attacking radar, communications and electronic weapons systems using radio waves to destroy and reduce enemy combat capabilities. These include physical electronic attacks that physically destroy the enemy’s electronic warfare systems with anti-radiation missiles (ARMs) and non-physical electronic attacks such as jamming and deception.

2.2.2. Electronic Protection (EP)

As an act of defending our electronic system, there is a great electronic warfare support such as electronic radiation control, avoidance, and electronic camouflage to donate the enemy’s electronic information collection, and a great electronic attack, an activity that minimizes our military’s influence from the enemy’s electronic attack.
2.2.3. Electronic Warfare Support (ES)

It means comprehensive activities such as collecting information and supporting operations for planning and implementing electronic warfare.

2.3. Electronic Warfare Cases in Modern War

2.3.1. Gulf War Case

Electronic warfare operations were carried out in the Gulf War, divided into operational readiness and execution stages. Prior to the start of the operation, the top priority for the multinational force is to identify the capabilities of the Iraqi forces and the Electronic Order of Battle, and to focus on the weapons systems in the field of electronic warfare.

EF-111A, EA-6B aircraft carried out electronic jamming on early warning radar and ground-based control stations, and EC-130H Compass Call aircraft conducted disturbances on the air defense network’s command, control and communication systems. In order to carry out effective anti-aircraft suppression missions in the early stages of the operation, non-destructive radio disturbances were essential to prevent the enemy’s main system from operating normally[16].

2.3.2. Case of Iraq War

In the Iraq war, radio disturbances were carried out in the "Protection of Sovereignty" phase. It began jamming and paralyzing operations through electronic attacks on Iraq's air defense network, war leadership and command, control and communications systems. As part of the non-destructive electronic attack, radio disturbance operations were carried out. EC-130H Compass[17].

Case of disturbance foreign include Moss Landing Port in the United States in 2001, SanDiego in 2007, and German Airport in Germany In the form of radio disturbance around the Newark airport in 2010, a Personal Privacy Devices (PPD) was used inside the vehicle to prevent some private users from exposing their location.

2.4. Current status of domestic and foreign satellite navigation system disturbance technology and equipment

2.4.1. Domestic and foreign global navigation system disturbance techniques and levels

Satellites in the global positioning system transmit signals at a distance of about 20,000 kilometers from Earth, so they are weak in reception and very vulnerable to interference(interference). Accordingly, the enemy will use the following three disturbing techniques to prevent satellite navigation signal reception in military situations using the vulnerabilities of these GPS signals[18].

(1) Jamming (jamming, noise)

It interferes with satellite navigation by approving the same frequency signal of strong power in the frequency band to which the global navigation signal is used.

(2) Mi Conning(meaconing, rerun)

This is a technique in which a disturbing transmitter intentionally receives and stores a global navigation signal and then reruns it at a time lag to cause confusion in the receiver.

(3) Spoofing(spoofing, propagation deception)

It is a technique that mimics the commercial GPS signal structure (signal frame) open to the general public to generate high-power satellite navigation signals containing false signal information so that the global navigation receiver can recognize the wrong location. Among them, jamming can easily produce jammers (radio jamming devices) with low cost and simple technology to deploy attacks. Because the range of jamming in electronic warfare is very wide, and like
windows and shields, the possibilities of jamming and anti-jamming exist simultaneously, and the technological development of jamming and anti-jamming can be carried out at the same time, attention is focused on the development of various anti-jamming satellite navigation system technologies to cope with jamming attacks worldwide. For a large-scale electronic attack, it is necessary to ensure continuous use by minimizing the impact of electronic equipment of our allies due to enemy electronic jamming or deception. Various anti-jamming techniques have been studied to efficiently remove or suppress interference and jamming signals entering the global navigation receiver. Jamming and anti-jamming are like spears and shields, so Pia will have to attack the opponent by surpassing the opponent’s skills, and the technique of avoiding the jamming attack will have to proceed at the same time.

Figure 2. The jamming situation of fighter jet[19].

Types of anti-jamming techniques are as follows. Antenna technology This is a technology that uses an adaptive array antenna (adaptive array antenna), and there is a beam arrangement (beam-steered array) technology that increases profit by forming a very narrow beam-width beam in the direction of the satellite signal and null steered array technology that forms a null in the direction of the jamming signal to suppress the jamming signal. Front-end (front-end) filtering technology It is a technology that blocks jamming power that flows strongly into the receiver and uses a band filter with sharp cut-off characteristics that suppresses the jamming signal other than the global navigation signal band and passes only the global navigation signal. AGC (Automatic Gain Control) technology Under the roaming environment, the global navigation signal is distorted, and if the satellite signal is tracked using the wrong signal, the signal is lost (synchronization). Therefore, not transmitting signals to the receiver when jamming is present is one way to respond to jamming. Advanced satellite navigation receivers with anti-jamming functions have a mode transition function, so they control the capture (acquisition) and tracking of receivers according to the power level of the jamming signal. Digital anti-jamming signal processing technology It is a representative preprocessing anti-jamming satellite navigation system technology that removes jamming and interference signals using digitized signal samples before the satellite navigation reception signal is copied.

3. North Korea’s Electronic Warfare Capability

3.1. North Korea’s electronic warfare capability
North Korea has relative weaknesses in its conventional weapons system, and has focused on developing asymmetric weapons systems as a way to overcome them [20][21].

In particular, the military aims to strengthen its military power by acquiring asymmetric weapons and technologies, such as cyber warfare and radio disturbances, in order to cope with the advanced weapons system in the West. North Korea has been on the Military Demarcation Line since 2010.

Some advanced weapons systems (guide weapons, drones, missiles, and aircraft) currently operated by North Korea are believed to be equipped with GPS, GLONASS, COMPASS, and Beidou receivers, and North Korea is expected to further increase its dependence on satellite navigation systems in the near future, focusing on advanced weapons systems. North Korean troops are equipped with 100W portable radio disturbance equipment and above 1,000W.

North Korea started preparing and developing electronic warfare in the 1970s. Currently, North Korea is known to be operating dozens of bases charge of conducting electronic warfare south of the plain, and Haeju and Kaesong are also believed to have electronic warfare bases. North Korea has introduced Russian-made jamming equipment to mount vehicles capable of jamming GPS signals in a range of 50 to 100 kilometers, thus providing a military demarcation line.

![Pattern of disturbance of North Korea](https://m.blog.naver.com/(2011)).

Recently, it is believed to have introduced a new 24-W jamming device to Russia that could hinder the use of GPS receivers within 400 kilometers of the Korean Peninsula. It is expected that electronic warfare capabilities will continue to be improved by installing and operating electronic information collection bases and radio interference bases near the mid- and western regions where South Korea's radio waves can be detected. North Korea was under the General Staff's Office of Information Control in 2001.

Commanded by the Center for Information Control, 121 reconnaissance stations and 204 red air stations are organized specializing in cyber warfare. North Korea is expected to develop EMP missiles that will neutralize the enemy's electronic device system by creating high-energy Electro-magnetic pulses in the future.
Table 1. Cases of radio disturbance in North Korea.

<table>
<thead>
<tr>
<th></th>
<th>First case (2010.8.23.~26)</th>
<th>Second case (2011.3.4.~14)</th>
<th>Third case (2012.4.28.~5.13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Gaesung</td>
<td>Gaesung, Haezu</td>
<td>Gaesung</td>
</tr>
<tr>
<td>Signal strength</td>
<td>-70~-60dBm</td>
<td>-60dBm</td>
<td>-80~-60dBm</td>
</tr>
<tr>
<td>Signal inflow area</td>
<td>Northwest of the Seoul</td>
<td>Northwestern part of the</td>
<td>Northwest of the Seoul</td>
</tr>
<tr>
<td></td>
<td>metropolitan area such as</td>
<td>Seoul metropolitan area,</td>
<td>metropolitan area such as</td>
</tr>
<tr>
<td></td>
<td>Gimpo and Paju</td>
<td>such as Gimpo and Paju,</td>
<td>Gimpo and Paju</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and Gangwon Province</td>
<td></td>
</tr>
<tr>
<td>Facility, etc.</td>
<td>2G and WiBro base stations</td>
<td>15 air craft twenty-one</td>
<td>Naval ship</td>
</tr>
<tr>
<td></td>
<td>181 stations</td>
<td>aircraft</td>
<td>One ship</td>
</tr>
<tr>
<td></td>
<td></td>
<td>106 aircraft</td>
<td>Naval ship, seven ships</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21 aircraft</td>
<td>Two ships</td>
</tr>
</tbody>
</table>

4. Conclusion and Policy Suggestions

Future warfare is changing into network warfare and advanced information warfare, and the importance of electronic warfare and navigation warfare by satellite navigation system is increasing day by day. In particular, the importance of electronic warfare plays an important role in defeating the enemy in the first place and winning the victory by covering the enemy's eyes and ears with non-lethal operations and maximizing our allies' power, without the damage to life and property caused by physical strikes. The recent war between Ukraine and Russia is well illustrated[23].

North's weapons systems and technologies are imported from Russia and China, the satellite navigation system available to the North is estimated to be GPS in the U.S., GLONASS in Russia and COMPASS in China, and the advanced weapons system is expected to be equipped with the satellite navigation system in general to enhance its precision.

North Korea has a relative weakness in its conventional weapons system, and has focused on developing an asymmetric weapons system as a way to overcome it, and will try to counter the enemy by acquiring asymmetric weapons and technologies, such as cyber warfare and radio disturbances, in particular to counter the advanced Western weapons system.

In future warfare, the enemy's command and control system (C4I) and precision guided weapons system should be broken, operated in a way that could neutralize the enemy's war will be in the early stages of the war, and electronic and navigation warfare will be necessary as part of our efforts to deal a blow to the enemy who is focusing on nuclear tests and missile development. To prevent nuclear and missile launches in advance, which are part of the asymmetric forces the enemy is preparing for.

5. References

5.1. Journal articles


5.2. Additional references

6. Appendix

6.1. Author’s contribution

<table>
<thead>
<tr>
<th>Initial name</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>HJ</td>
<td>- Set of concepts ☑</td>
</tr>
<tr>
<td></td>
<td>- Design ☑</td>
</tr>
<tr>
<td></td>
<td>- Getting results ☑</td>
</tr>
<tr>
<td></td>
<td>- Analysis ☑</td>
</tr>
<tr>
<td></td>
<td>- Make a significant contribution to collection ☑</td>
</tr>
<tr>
<td></td>
<td>- Final approval of the paper ☑</td>
</tr>
<tr>
<td></td>
<td>- Corresponding ☑</td>
</tr>
<tr>
<td></td>
<td>- Play a decisive role in modification ☑</td>
</tr>
<tr>
<td></td>
<td>- Significant contributions to concepts, designs, practices, analysis and interpretation of data ☑</td>
</tr>
<tr>
<td></td>
<td>- Participants in Drafting and Revising Papers ☑</td>
</tr>
<tr>
<td></td>
<td>- Someone who can explain all aspects of the paper ☑</td>
</tr>
</tbody>
</table>

*Copyright: ©2023 by the authors. Licensee J-INSTITUTE. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).