symmetry

MDPI

Article

Method for Effectiveness Assessment of Electronic Warfare Systems in Cyberspace

Seungcheol Choi [1], Oh-Jin Kwon [1,*], Haengrok Oh [2] and Dongkyoo Shin [3]

[1] Department of Electrical Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea; choisc@sju.ac.kr
[2] Agency for Defense Development (ADD), Seoul 05771, Korea; haengrok@add.re.kr
[3] Department of Computer Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea; shindk@sejong.ac.kr
* Correspondence: ojkwon@sejong.ac.kr

Received: 27 November 2020; Accepted: 16 December 2020; Published: 18 December 2020

Abstract: Current electronic warfare (EW) systems, along with the rapid development of information and communication technology, are essential elements in the modern battlefield associated with cyberspace. In this study, an efficient evaluation framework is proposed to assess the effectiveness of various types of EW systems that operate in cyberspace, which is recognized as an indispensable factor affecting modern military operations. The proposed method classifies EW systems into primary and sub-categories according to EWs' types and identifies items for the measurement of the effectiveness of each EW system by considering the characteristics of cyberspace for evaluating the damage caused by cyberattacks. A scenario with an integrated EW system incorporating two or more different types of EW equipment is appropriately provided to confirm the effectiveness of the proposed framework in cyber electromagnetic warfare. The scenario explicates an example of assessing the effectiveness of EW systems under cyberattacks. Finally, the proposed method is demonstrated sufficiently by assessing the effectiveness of the EW systems using the scenario.

Keywords: battle damage assessment; cyberspace; effectiveness assessment; electronic warfare

1. Introduction

Cyberspace is a global information environment composed of independent networks that include information technology infrastructure such as the internet, communication networks, computer systems, and embedded processors [1]. Rapid advances in cyberspace and information and communication technologies (ICT) have made them the significant enablers of the Fourth Industrial Revolution, which refers to the accelerated shift in industrial technologies characterized by hyper-connectivity and super-intelligence. The cyber physics system that blurs the boundary between cyberspace and physical space has been realized by deploying a network capable of exchanging information between objects and people. Therefore, cyberspace in our environment is no longer a conventional network infrastructure because all other systems that can communicate with systems in the network are considered to belong to cyberspace.

In today's information-oriented age, countries, economies, and societies are highly susceptible to cyber threats. An increasing number of attempts to exploit cyberspace are being conducted. Cyberspace offers attackers the desired anonymity and cyberattacks are usually low-cost. Furthermore, advances in technology have dramatically increased the level of cyber threats: from simple threats through viruses to advanced persistent cyberattacks targeting major social facilities, including governments; such attacks are already taking place [2].

Meanwhile, a paradigm shift in modern warfare has been caused by the convergence of existing defense technologies and the following ICT technologies [3]:

- Data, human–machine integrated systems;
- Artificial intelligence (AI), Internet of Things (IoT), big data technology;
- Mechanized intelligence across the battlefield and weapon systems;
- New technologies such as 3D printing and robots.

These technological breakthroughs are expected to find their way into future battlefields. Robots armed with smart sensors and AI will be the main subjects of combat. Human forces will become super-dominant by using the robotic exoskeleton, advanced weapons, and muscle- and sensory-enhancement genetic engineering technology. Hacking technology, fueled by AI, advances, and cyber warfare, which can be defined as information warfare performed by collecting, analyzing, and processing information distributed in cyberspace, will become a significant part of the war [4]. Cyber warfare has far-reaching implications and can prove detrimental in war situations. For example, it can be used to disrupt the weapon systems and critical infrastructure of the enemy even before a physical attack has commenced.

ICT technology has led to the development and expansion of cyberspace and many advances in electronic warfare (EW) systems. EW refers to military actions performed by controlling the electromagnetic spectrum through Command and Control (C2)'s five military actions: operation security, EW, psychological operation, military deception, and physical strike [5]. EW, as shown in Figure 1, consists of an electronic attack (EA), which controls the enemy's electromagnetic spectrum; electronic protection (EP), which is used for defense; and electronic warfare support (ES), which supports tasks such as surveillance and reconnaissance [5–7].

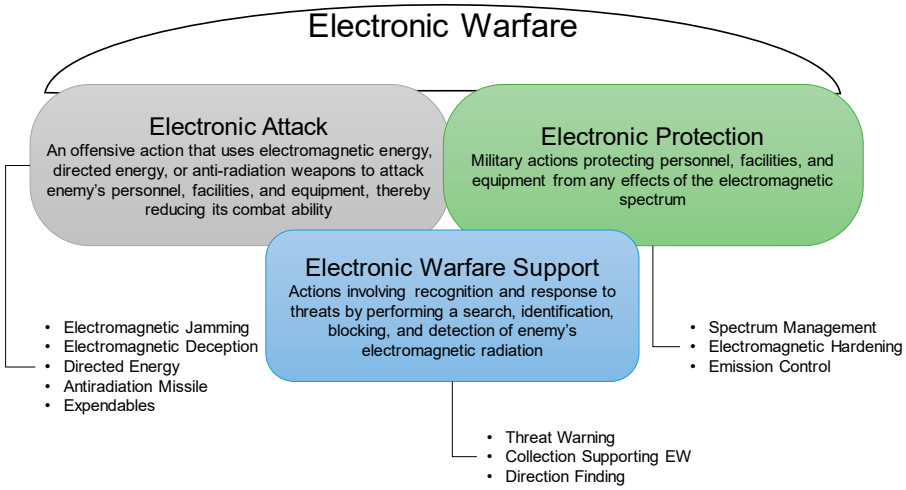

Figure 1. Electronic warfare sub-divisions and applications [6].

Owing to the convergence of ICT technology and defense science and technology, EW is widely conducted in modern military activities with military activity convergence, and in particular, it is used in cyberspace. The US Army emphasizes that cyber warfare and EW should be carried out in a converged form, as both are mostly conducted for similar purposes [8].

This paper proposes an efficient assessment framework for different EW systems that operate in the cyber environment as a new form of modern warfare. The proposed framework defines how to assess the effectiveness of EW systems operating in response to threats and attacks on cyberspace.

This study aims to obtain an index that measures the impact of cyberattacks on electronic warfare systems operating in cyberspace. Applying this study will allow us to:

- Help commanders make decisions effectively to protect the EW systems by observing the state of the cyber-electronic warfare system in a real environment.
- Estimate the resistance or resilience of EW systems by simulating cyberattacks of various types and strengths.
- Be able to understand the regularity of system architectures that resist attacks by monitoring the systems.

This paper's subject is significantly important because it can provide enhanced information on critical security required in cyber-electronic warfare by successfully applying evolved frameworks and algorithms to analyze various types of electronic warfare systems and complex cyberattacks.

The remainder of this paper is organized as follows. Section 2 presents background and literature review that were conducted for damage assessment on cyberspace and provides an overview of EW. In Section 3, we present a scenario and target EW systems for implementing the proposed method. Section 4 details the analysis of the cyberspace and EW systems. Section 5 introduces an evaluation method based on the results of the analysis and evaluates the actual effectiveness of EW systems based on the scenario presented in Section 3. Finally, Section 6 concludes this paper.

2. Background and Literature Review

This section analyzes the requirements for designing a methodology that assesses the effects of threats and attacks on the cyber environment linked with EW systems. To achieve this, we consider related research conducted on damage assessment of cyberspace, concurrently with analyzing features for measuring the performance of EW and target systems.

2.1. Damage Assessment in Cyberspace

This paper focuses on cyberattacks, defined by the National Institute of Standards and Technology (NIST) as attacks that target cyberspace to disrupt, deactivate, destroy, or maliciously control the computing environment and infrastructure, damage the integrity of data, or steal controlled information [9]. Battle damage assessment (BDA) is a significant factor that affects the time and space in which military activities take place. Several studies that evaluate the impacts of cyberattacks have been published in the literature.

Denning [10] introduced a framework for assessing cyber warfare. The framework is used as its foundation risk assessment that assesses the risks to cyber systems, operations, and organizations, from cyberattacks in terms of threats, vulnerabilities, impacts, and possibilities. The framework assesses risks based on NIST's guide for conducting risk assessments [11] and provides an assessment of cyber battle damage and cyber strength to assess cyber warfare.

Kotenko and Chechulin [12] suggested a framework modeling cyberattacks and evaluating impacts, considering a common approach based on providing risk analysis procedures. It is a framework that graphically traces all possible sequences of actions to determine an attacker's purpose and evaluate the impact on the action through graphical analysis.

Musman and Temin [13] implemented the Cyber Mission Impact Assessment (CMIA) method to simulate the application of potential security and resilience methods to a system within a mission context and perform assessments of the system. They implemented a functional subset of the business process modeling notation (BPMN) to present the mission and its cyber dependencies. After defining measures of effectiveness (MOE) and measures of performance (MOP) for the cyber mission, the method identifies how the performance of mission activities contributes to achieving them. The CMIA model considers only the effects of successful cyberattacks: degradation, interruption, modification, fabrication, unauthorized use, and interception (DIMFUI). The model is executed both with and without cyberattack effects to compute MOE, MOP, and KPP; changes in these performance parameters reflect mission impacts.

Kim et al. [14] proposed a framework that assesses cyber battle damage by measuring MOP and MOE before and after cyberattacks. They designed a framework to communicate and integrate with other systems, such as physical warfare and EW.

To the best of our knowledge, the primary method of evaluating the impact or damage to cyberspace is to use MOP and MOE. The effectiveness of objects constituting cyberspace is quantified, and then the damage is evaluated by comparing the cyberspace before and after cyberattacks. The result of the assessment helps C2 when it plans and executes the mission successfully. Generally, cyberspace evaluation methods are divided into the evaluation of damage and the relative ability to respond to cyberattacks. This paper focuses on how to assess the damage caused by a cyberattack.

2.2. Electronic Warfare

Nowadays, EW has become an increasingly important factor in military operations; it is highly dependent on electronic equipment, and has been used in military operations in complex information environments integrated with the electromagnetic spectrum.

EA refers to an offensive action that uses electromagnetic energy, directed energy, anti-radiation weapons, etc., to destroy, damage, or degrade the enemy's personnel, facilities, and equipment, thereby reducing its combat ability. As shown in Table 1, EA is classified according to the type of attack.

Table 1. Types of electronic attack [6,7].

Category	Type	Description
Destructive	Directed energy	Weapon that destroys or neutralizes high-power energy by directly irradiating it on a target. These include laser, high-power microwave, particle beam, and X-ray weapons.
	Anti-radiation missile	Missile that detects and destroys an enemy's defense system by backtracking radio emission source from an opponent's radar base.
Non-destructive	Jamming	Most representative EA method. Electronic or mechanical interference that interferes with aircraft markings on the radar, radio communications, radio navigation, etc.
	Expendable countermeasures	Attacks using Chaff [a], Flare [b], Towed Decoy [c], etc., to disturb enemy EA.

[a] Metal foil, such as aluminum, sprayed in the air to interfere with the opponent's radar detection; [b] disturbance grenade fired to disturb infrared tracking (heat tracing) missiles; [c] equipment for deceiving radar-guided missiles.

ES refers to military activities involving immediate recognition and response to threats by performing a search, blocking, identification, and location detection of enemy electromagnetic radiation. It is also called electronic support measure (ESM), and its primary function is the production/collection of tactical information. Table 2 lists the steps to achieve the ultimate goal of ES, that is, the analysis and judgment of enemy intentions and abilities. It is classified into signal intelligence, electronic intelligence, and communications intelligence, according to the target of information collection. Typical types of ES systems include a radar warning receiver, missile warning receiver, laser warning receiver, and surveillance radar.

Table 2. Steps of collecting tactical information [6,7].

Step	Description
Search	Process of searching for specific signals
Intercept	Process of identifying type and characteristics of bandwidth, modulation method, etc., by monitoring/recording the searched signal
Direction finding	Process of locating the physical location of the signal
Analysis	Process of analyzing the enemy's intentions, abilities, etc.

EP refers to the act of protecting a friendly electronic facility from enemy EAs. It is divided into anti-ES, which suppresses the enemy's ES ability against allies, and anti-EA, which responds

to the enemy's EA attacks. The types of EP activities include emission control (EMCON), shielding, and communication security (COMSEC). EMCON attempts to suppress unnecessary electromagnetic radiation as much as possible when the enemy tries to collect intelligence on allies by conducting ES activities against allies.

EW systems can be classified into standalone, federated, and integrated systems according to the type of operation [6,7]. Standalone systems are mainly used in scenarios that require a rapid response. An example is a decoy system for promptly responding to an unexpected anti-ship missile attack during a regular voyage or at the berth when the ship is not ready for combat. The federated system can be configured by adding a data-sharing function through a network/bus to an independently operating system. A standalone radar warning receiver (RWR) system that performs simple self-defense and threat alert can be extended to detect and identify remote threats by additionally configuring data link equipment for electronic information transmission.

Unlike conventional tactical systems with "federated" EW systems, modern fighter planes and Aegis ships use an integrated system that shares resources across all EW components and electronic systems. F-35, for example, is highly integrated. Radio-frequency and electro-optical receivers are built around the edge of the airframe allowing continuous detection of unfriendly emitters from all directions. All sensors are fused through a central computer and displayed on the visor of the pilot's helmet. The system also merges information from off-board sensors to provide a comprehensive view of the local electronic environment [15].

EW systems in complex electromagnetic environments play a crucial part in modern warfare. Therefore, evaluation of the effectiveness of EW in such environments has become a crucial factor responsible for establishing and maintaining a favorable position in the combat environment. To achieve this critical mission, NATO tests and evaluates the equipment used in modern EW systems with a wide range of testing techniques to ensure the readiness of the EW system for users to complete their mission in the combat environment [7].

NATO introduces a disciplined approach to the test and evaluation (T&E) for EW systems, including the technical considerations for planning execution and operations. Although the specification concentrates on radio/radar frequency and infrared systems operating in EW frequency ranges, all system types are covered for EW T&E capabilities.

The T&E objectives are derived from the operational requirements of the users and the requirements of the specification to ensure survivability and operational effectiveness in the military action. It defines the T&E process of EW systems, as depicted in Figure 2. The process continuously improves the estimated performance, allowing the tester to provide decision-makers with quantifiable technical risks [7].

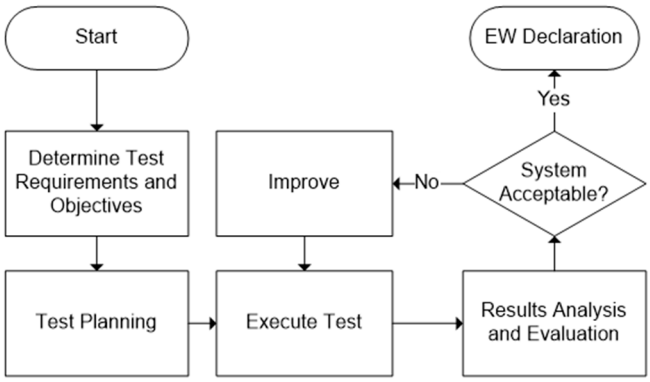

Figure 2. Overview of the electronic warfare support (ES) test and evaluation (T&E) process [6].

The capabilities of an EW system are assessed using a wide range of test resources, such as measurement facilities, system integration laboratories, hardware-in-the-loop facilities, installed system

test facilities, open air ranges, and modeling and simulation [7]. When the tester designs the T&E, it must be ensured that two questions are answered as follows:

- The test must determine if the manufacturer has met each of the specification requirements.
- The EW system must be evaluated to determine if the military utility is feasible to perform a dedicated operational T&E, i.e., field test.

The T&E objectives must verify both the specification compliance and military utility. Once they are established, the test team must determine to evaluate the performance or effectiveness. These are known as the MOP and the MOE. NATO defines the MOP as generally suitable for development T&E and relevant to technical performance requirements, and the MOE applies to operational T&E.

A large T&E charged with acquiring several potentially integrated sub-systems might have a hierarchy of test objectives. For example, it has an overall test objective: "evaluate the performance of the F-XX aircraft." The objective could consist of lower-level objectives: "evaluate the tactical avionics suite" or "evaluate the fire control radar system." An objective to evaluate EW systems of the aircraft could have sub-objectives: "evaluate the performance of the RWR system" or "evaluate the expendable countermeasures system." A small T&E might have a single stand-alone objective, such as "evaluate the infrared countermeasure."

In the abovementioned context, the MOP must be measurable attributes related to operational functions. Most performances of the EWs are measured based on whether the value of the attribute, such as response time, meets the expectations.

2.3. Cyberspace and Electronic Warfare

Today's armed forces also operate in cyberspace, a network-based environment, and leverage the more congested electromagnetic spectrum (EMS). According to the U.S. Army, wireless cyberspace capabilities use the EMS as a transport medium to form links in the Department of Defense Information Network (DODIN) [16]. Moreover, it is emphasized that cyber warfare and EW operations must be performed in a converged form because they are mostly used for similar purposes; such military activities are called cyberspace electromagnetic activities (CEMA), as shown in Figure 3 [8].

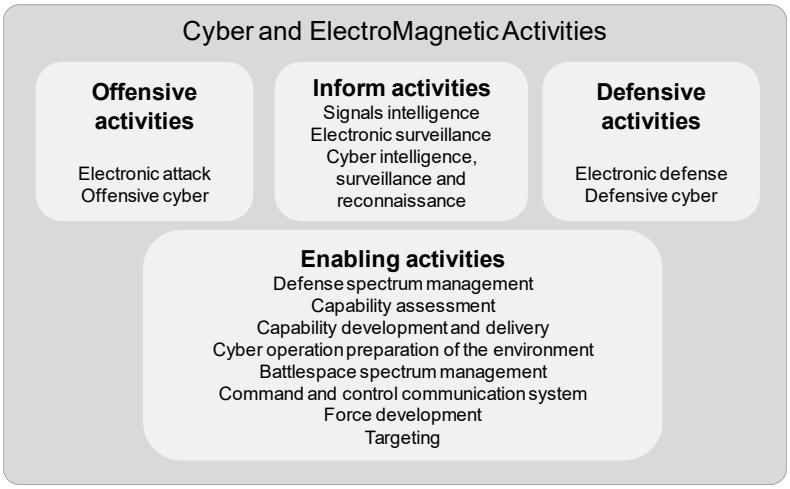

Figure 3. Definition of cyber and electromagnetic activities (CEMA) [8].

CEMA is defined as the synchronization and coordination of offensive, defensive, informing, and enabling activities across the electromagnetic environment and cyberspace, as depicted in Figure 3. CEMA operations are divided into cyberspace operations, EW, and spectrum management operations, as presented in Figure 4 [17], and include internet communication networks, computer systems, and embedded processes/controllers.

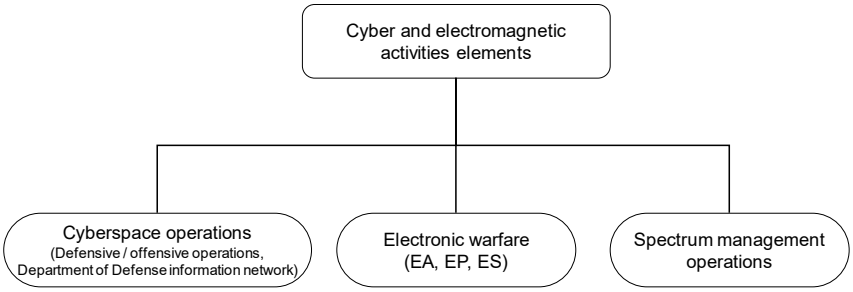

Figure 4. Cyber and electromagnetic activities elements [17].

Military operations of the U.S. Army, such as information management, operation, command transmission, and situational awareness, can be conducted anywhere through the DODIN, in places, i.e., homes, temporary residences, camps, and base stations. However, when conducting operations in cyberspace, a plan for risk management must be prepared. Risk management is a critical decision-making process to identify hazards, control risks, and increase operational effectiveness and mission-achievability. The U.S. Army faces multiple, simultaneous, and continuous threats in cyberspace. Table 3 lists the sample threat capabilities in cyberspace and EW [18].

Table 3. Sample cyberspace and electronic warfare threat capabilities [18].

Capability	Methods	Indicators	First-Order Effects
Denial of service attack	Malicious attacks to the server or other network nodes to waste resources and prevent intended traffic	Network degradation, inability to access resources, malicious spam, and uncontrolled system reboots	Degraded network capabilities varing from limited services to complete denial of use
Network penetration	Man-in-the-middle attacks, phishing, poisoning, stolen certificates, and exploiting unencrypted messages and homepages with poor security features	Unfamiliar e-mails, official-looking addresses requiring urgent reply, internet protocol packets replaced, non-legitimate pages with the look of legitimate sites, directed moves from site to site, requests to upgrade and validate information, and unknown links	Uncontrolled access to networks, manipulation of networks leading to degraded or compromised capabilities that deny situational awareness or theft of data
Emplaced malware (virus, worms spyware, and rootkits)	Phishing, spear phishing, pharming, insider threat introduction, open source automation services, victim activated through drive-by downloads, and victim-emplaced data storage devices	Pop-ups, erroneous error reports, planted removable storage media, unknown e-mail attachments, changed passwords without user knowledge, automatic downloads, unknown apps, and degraded network	Spyware and malware-affected systems allow electronic reconnaissance, manipulation, and degrading system performance
Disrupt or deny information systems in the EMS	Prevent friendly antennas from receiving data transmitted in the EMS by using military or commercially available high-powered lasers, high-powered microwaves, and repurposed or reengineered communications systems	Symptoms may not be evident if passive; may manifest as transmission interference, software or hardware malfunctions, or the inability to transmit data	Degraded or complete denial of service inability to control the EMS-denying situational awareness

Moreover, EW systems have achieved many advances owing to the development of ICT technology. They have been developed to operate by interlocking/integrating with multiple EW systems rather than an individual system that operates in a single form; therefore, they provide advanced functionalities, including the characteristics of cyberspace where necessary information is exchanged by sharing network assets.

Most of the studies have considered cyberspace as an actual physical battlefield and evaluated its impact on military operations. This paper presents a method for assessing the effect on cyberspace in terms of ES systems that conduct electromagnetic activities in cyberspace, rather than assessing the impact of physical operations on military activities in cyberspace.

3. Scenario and Target Systems

This section introduces a scenario and the target systems of EW, concurrently with the necessary preliminary assumptions. The EW systems operate in an integrated form as part of the destroyer.

3.1. Scenario

The tactical C2 system is a critical element in all military activities and provides the ability to collect, process, create, display, and distribute information for joint and combined operations for the military commander's decision-making. The tactical C2 system mainly uses database, web, and e-mail linkage, and has used the Link-11 tactical data link developed by the United States Navy for anti-air warfare purposes. Although Link-16 has been adopted to supplement Link-11's shortcomings and enhance security, Link-11 is still used as an auxiliary tool [19].

In this paper, a scenario is explained to evaluate the damage to the integrated EW system, considering malicious network penetration to the tactical data link as a threat to cyberspace. The destroyer, which operates anti-ship, anti-submarine, and anti-aircraft capabilities using various EW systems at sea, can process essential information necessary for battlefield situations in real-time by easily interlocking various data through a tactical C2 system and a tactical data link.

In this paper, the tactical C2 system is assumed to be cyberspace, and the EW system mounted on the Gwanggaeto the Great-class destroyer of the Korean Navy [20], is set as an integrated EW system that performs operations in cyberspace. A cyberattack on a friendly destroyer equipped with integrated EW systems is assumed. Based on these assumptions, a scenario is developed for this study, as listed in Table 4.

Table 4. Scenario of Cyberspace and Electronic Warfare.

Scenario	Description		
Mission	The destroyer undertakes coastal surveillance and defense missions in the operation area with its radar equipment to monitor enemy missile and torpedo attacks.		
EW Configuration	ES	MW–08	Target indication 3D radar
		AN/SPS–49(V)5	2D long range air search radar
		STIR–180	Signal tracking and illumination radar
	EA	DAGAIE Mk.2	Chaff
		SLQ–25	Towed torpedo decoys
Cyber attack	Enemy forces operate cyberattack on the destroyer's tactical data links using backdoors and malware before conducting the attack operation, causing network delays between the destroyer's EW systems that perform detection and defense missions.		
Damages	Due to backdoors and malicious code, network traffic has increased, and the detection and defense capabilities of destroyers have been reduced owing to delays in the operation of ES systems capable of defending against anti-ship missiles.		

In this scenario, when the Korean Navy builds destroyers, some functions are developed by individual companies that are not actively managed by the government and the Navy, owing to economic factors. The first cyberattack is conducted by hacking companies' networks participating in the development of the destroyer and hiding the backdoor or malware worm on the system under development [21].

The scenario focuses on evaluating the damage centered on the EW system mounted on the destroyer interlocked with the control system when subjected to a cyberattack. This paper does not directly evaluate the tactical C2 system designated as cyberspace. However, organizations with access to all military information may expand this research and use it in evaluating cyberspace linked to other EW systems.

3.2. Target Electronic Warfare Systems

As discussed in Section 2, in modern warfare, the EW systems have developed into an integrated form, an essential factor that allows friendly forces to be in a dominant position during war and during regular times. The scenario presented in this paper also assumes a destroyer that integrates several ES and EA systems. The necessary functional specifications of the EW systems targeted in the scenario are as follows:

- ES Systems: Radar
  - AN/SPS-49(V): Air surveillance radar provides long-range, two-dimensional air search capabilities. Anti-aircraft radar with a detection distance of 400 km (missile detection 100 km, aircraft 400 km) operating in the 850–942 MHz L band.
  - MW-08: 3D radar tracks 160 air targets or 40 sea targets simultaneously, and can detect and track aircraft up to 55 km (missile 20 km). The target is searched and tracked using 3D information on the direction, distance, and altitude of the target to transmit data to the command and control system.
  - STIR-180: Medium-to-long-range fire-control radar system that tracks targets through high-power tracking energy and complements AN/SPS-49.
- EA Systems: Expendable countermeasures
  - DAGAIE Mk.2: An anti-missile deceptive system receives information from a ship's EW equipment or detection system and automatically deploys the chaff and flares.
  - SLQ-25: Towed torpedo decoys consist of a towed decoy device (TB-14A), and a shipboard signal generator. The decoy emits signals to draw a torpedo away from its intended target.

Modern warfare is being developed into a network-centered war that overpowers the enemy based on the information superiority and increased command delivery speed of battlefield situations. A tactical data link is a core system of network-centered warfare that enables rapid recognition of the situation through real-time tactical information exchange.

4. Effectiveness Analysis

This section details the proposed assessment and analysis methodology designed to enable communications with a damage assessment framework. Section 4.1 introduces the cyberspace analysis, whereas Section 4.2 describes the methods based on the performance of the EW systems.

4.1. Cyberspace Analysis

Recently, as cyberattacks have become more common, they are a severe threat to national security, including the nation's social and economic aspects. As discussed in Section 2, evaluation of the effectiveness of military activities on all battlefields is essential. However, unlike physical warfare on the real battlefield, it is difficult to directly identify the damage caused by an attack in cyberspace.

Several methods have been introduced to assess the damage of cyberspace in Section 2. In this study, the cyberspace BDA framework (CBDAF) proposed by Kim et al. [14] is combined with the scenario introduced in Section 3 to evaluate the impact of cyberattacks on EW systems in cyberspace. This section details the analysis of the CBDAF and examinations of how it works with a framework to assess the effectiveness of the EW systems.

U.S. Army defines the mission and means framework (MMF) in a technical report for explicitly specifying the military mission and quantitatively evaluating the mission [22]. The MMF divides the U.S. military activities into seven groups as follows:

- Level-7: Purpose, Mission.
- Level-6: Context, Environment.

- Level-5: Index, Location/Time.
- Level-4: Tasks, Operations.
- Level-3: Functions, Capabilities.
- Level-2: Components, Forces.
- Level-1: Interactions, Effects.

Level-4 specifies operations that provide ways to accomplish the mission. The essential purpose of this level is to organize task outcomes by planning the warfighter uses to determine the functions and capabilities required to accomplish tasks and operations, followed by mission effectiveness evaluation.

Considering the military decision-making process (MDMP) [23], the warfighter iterates recursively between mission analysis and course of action (COA) development and analysis. Mission analysis organizes tasks into operations to measure mission outcomes. COA uses MOP to assign capability in Level-3 to operations. COA analysis uses MOEs to determine whether the assigned capabilities execute tasks to meet mission requirements [22].

To evaluate missions performed in cyberspace, CBDAF applies a model that classifies the effectiveness of cyberattacks by analyzing the attacker intention. In this model, functions are defined according to the availability and capabilities of cyber assets that execute cyber activities. The impact of six cyberattacks, as listed in Table 5 [24], on these functions is evaluated to calculate the final effectiveness of the mission. This model follows the procedure for calculating the MOP and MOE defined in MMF.

Table 5. Cyber effects by attack category [24].

Attack Category	Effect on Process	Effect on Information
Degradation	Speed of process is slowed by some multiple	Rate of information delivery is decreased; quality or precision of information produced by an activity is decreased
Interruption	Process is unavailable for some time period and will not commence until the incident is recovered	Information is unavailable for some time period
Modification	Process characteristics have been altered in a way that can affect the output/result of the process	Information has been altered, meaning that the processes that use it may fail, or produce incorrect results
Fabrication	A false mission instance has been inserted into the system, which may interfere with real mission instances	False information has been entered into the system
Interception	Process (perhaps software or embodied in hardware) has been captured by the attacker	Information has been captured by the attacker
Unauthorized use	Raises the potential for future effects, or unexpected outcomes on processes	Raises the potential for future effects on information

CBDAF considers the characteristics of cyber warfare; it is difficult to identify the direct damage caused by a cyberattack. Therefore, CBDAF conducts damage evaluation by dividing it into a normal stage in which the cyberattack has not been executed and a stage after the cyberattack occurs. In the normal stage before the attack, to calculate the MOP and MOE, asset information and status are collected, and the attack categories are classified based on Table 5. For measures of cyber effectiveness (MOCE), CBDAF selects interception, modification, and interruption attacks because unauthorized use, fabrication, and degradation can be included in interception, modification, and interruption, respectively. *MOCE* is the damage rate to cyber assets caused by three types of attacks and is calculated as follows [14]:

$$MOCE = \frac{\sum_{i=1}^{I} ((w_i \times mop_i + \alpha_i) \times R_i)}{\sum_{i=1}^{I} (w_i \times (mop_i + \alpha_i))} \quad (1)$$

where I is the number of objects in the CBDAF, w is a weight value indicating the importance of the object, mop is a measured value of the object, and R is a binary variable that indicates whether

cyberattacks have damaged the object. α is a variable that is used when auxiliary measures are required. The number of MOP can be flexibly set considering the object's features, whose details are described in [25].

4.2. Electronic Warfare Analysis

The impact on the EW systems is evaluated through the MOP and MOE. The MOP of the integrated EW systems considered in our scenario can be calculated by measuring the performance of the individual EW system's functional features. MOE is a measure that can provide an answer to whether the objectives of military operations by the EW systems have been achieved. The proposed EW damage assessment process measures the MOP and MOE in the EW systems that deteriorate compared to the normal state in the same way as the damage assessment method for cyberspace.

As the MOP items of the EW systems used in this study have difficulty obtaining accurate capability information, the MOP items were defined by referring to general functions of radar equipment, and expendable countermeasure equipment published in the literature [7,26–30], as shown in Table 6. Since the EW system is classified into EA, EP, and ES as described in Section 2.2, the functional items for MOP calculation are classified and defined according to the type of EW.

Table 6. Definition of measures of performance (MOP) for electronic warfare (EW) systems [7,26–30].

EW Systems	MOP Items	Descriptions
Radar	Response time	Time taken to generate an alarm following an intrusion
	System sensitivity	Minimum detectable target size
	Scan range	Detectable range in degree
	Track consistency/correctness	Target tracking accuracy, number of simultaneous tracking targets, detection time of targets' disappearance
	Identification/classification	Accuracy of the target physical size, aspect, radar cross-section, etc.
	Maximum detection distance	Maximum detectable distance
	Angle of arrival measurement	Incidence angle of the received signal
	Geolocation	Accuracy of the tracking target geolocation
	System dynamic range	Range of system's out signal
Expendable countermeasures	Radar cross section	Measure of how detectable an object is
	Miss distance	Maximum distance at which the explosion of a missile heads
	Survival probability	Probability of avoiding attacks such as missiles and torpedoes

The items defined in Table 6 are reorganized into main and sub-categories to calculate the MOP, and the weighted sum of the measured values for each item yields the MOP for the EW system, as shown in Table 7. The MOP of sub-categories is calculated as a weighted sum of the MOP items defined for each category. The MOP value of the integrated ES systems is calculated as follows:

$$\begin{aligned} MOP &= \sum_{i=1}^{I} \left({w_i}^M \times {M_i}^{sys} \right) \\ M^{sys} &= \sum_{j=1}^{J} \left({w_j}^S \times {M_j}^{sub} \right) \\ M^{sub} &= \sum_{k=1}^{K} \left(w_k \times Measured_k \right) \end{aligned} \tag{2}$$

where M^{sub} and M^{sys} are the weighted sum values of the sub-category and items of the primary category, respectively. I, J, K are the number of primary categories, sub-categories, and MOP items, respectively. The weight w of each MOP item and category is set differently by the commander according to the result of planning/reviewing the mission. Then, the MOP of the primary categories is calculated in the same manner.

Table 7. *MOP* values of EW systems for the scenario.

Primary Category	w^M(%)	M^{sys}	Sub-Category	w^S(%)	M^{sub}	MOP Items	w (%)	Measured
ES_Radar	70	34.3	Scan range	50	62	Searchable degree	50	24
						Max. distance (100 km)	50	100
			Accuracy	50	6.6	System sensitivity	30	10 *
						Number of tracking	40	3
						Identification	30	8 *
EA_Expendablecountermeasures	30	10	Chaff	50	10	Cross-section	50	10 *
						Miss distance	50	10 *
			Towed decoy	50	10	Survival probability	100	10 *

* Score from 0 to 10 evaluated by staff based on the identified performance items of the EW system.

The MOE of the EW systems measures the achievement level of EA, EP, and ES missions, and sets MOE items for the following elements in consideration of the relationship, such as the EW operation and its impact on assets:

- E_EA: A mission to inflict personnel/physical/functional damage using electromagnetic attacks for the purpose of attenuating/invalidating/destroying combat capabilities.
- E_EP: A mission to defend against personnel/physical/functional damage from electromagnetic attacks.
- E_ES: A mission to search/intercept/identify/localize intentionally and unintentionally generated electromagnetic attack for immediate threat recognition/targeting/military operation, etc.
- *MOCE*: A measure of cyberspace delivered by CBDAF to identify the effect of cyber elements on EW systems.

Unlike the *MOP*, the MOE items of the EW system have the characteristic of being flexible according to the operational environment and EW assets. These four items are separated in detail, and their weighted sum is used to measure the *MOE* of the EW systems as follows:

$$\begin{aligned} MOE &= \sum_{l=1}^{L} \left({w_l}^M \times M_l \right) \\ M &= \sum_{m=1}^{M} \left(w_m \times Measured_m \right) \end{aligned} \tag{3}$$

where L and M are the number of primary categories and MOE items, respectively.

5. Effectiveness Assessment

This section provides the use of the proposed assessment method to evaluate the effectiveness of the integrated EW systems associated with the CBDAF. Figure 5 shows the interlocking between the CBDAF and EW damage assessment processes. In CBDAF, the process of evaluating the damage to cyberspace is divided into attack detection, initial evaluation, damage evaluation, and final reporting. The framework provides rough cyber damage assessment information by performing an initial evaluation with asset information registered in cyberspace.

As described in Section 4.1 and Figure 5a, the CBDAF provides *MOCE* and attack information, including assets information, according to the cyberattack. A sub-system, depicted in Figure 5b, receives the information from the CBDAF in the same cyberspace and evaluates the damage to the EW assets. Then, the system returns the results of the evaluation for EW systems. Asset classification, *MOP* calculation, *MOE* calculation, and EW BDA results generation constitute the system's process.

It provides more specific damage information in conjunction with a subsystem that performs damage assessment for EW systems, helping the commander to make more accurate situation-based decisions.

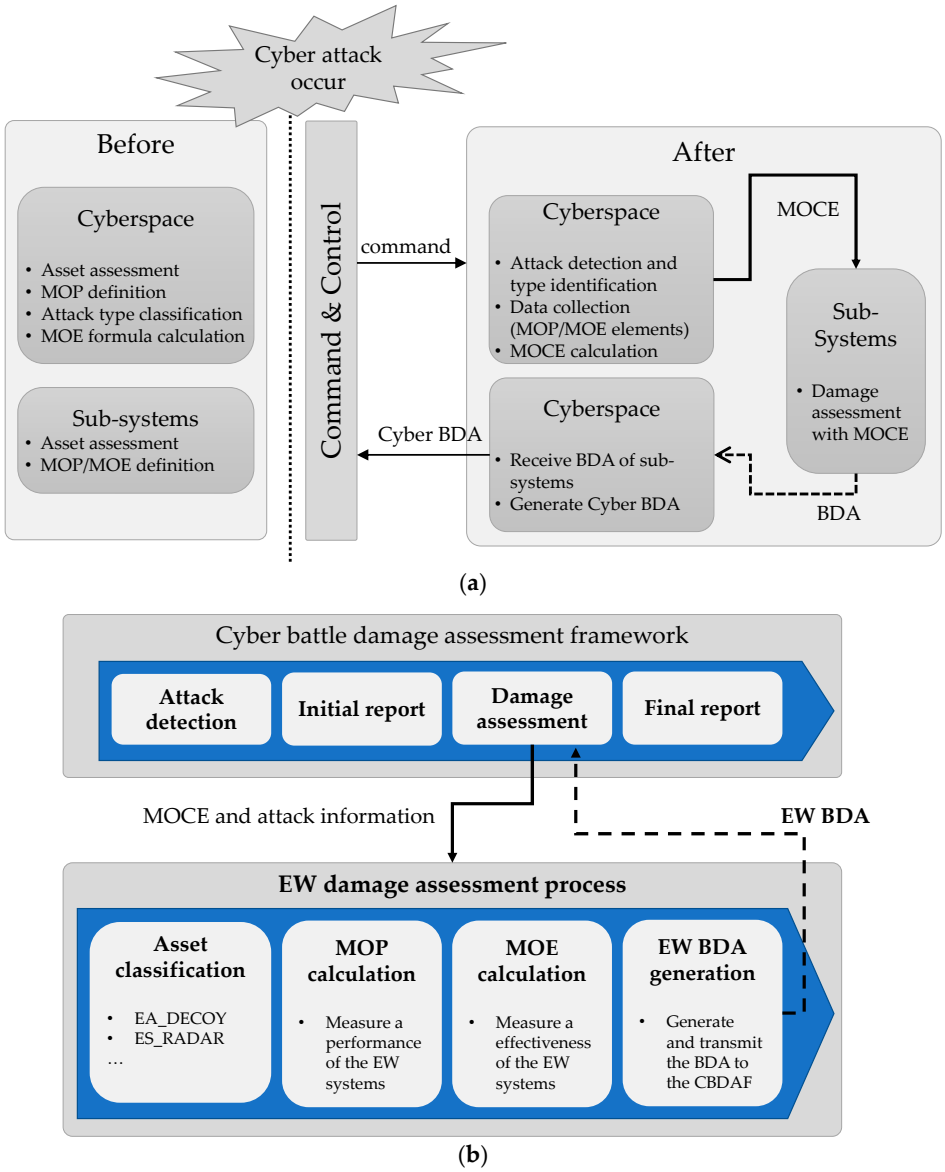

Figure 5. Overview of the effectiveness assessment. (**a**) Cyber battle damage assessment framework, and (**b**) workflow of EW damage assessment, which is a sub-system of cyberspace battle damage assessment framework (CBDAF).

Based on the scenario proposed in this paper, the damage assessment process of the EW systems associated with cyber warfare can be described as follows.

(1) CBDAF detects an attack on cyberspace and analyzes it to classify its category.
(2) CBDAF reports to C2 that the attack category is a degradation/interruption on the network associated with the ES systems.
(3) The classified attack and EW asset information are transmitted to the EW damage assessment process.
(4) The EW damage assessment process classifies the EW systems associated with cyber warfare.
(5) The MOP and MOE items for the radar and expandable countermeasures EW systems are derived based on the proposed scenario and *MOCE* transmitted from the CBDAF.
(6) The proposed process measures the actual values of MOP and MOE items defined in the MOP and MOE metrics, as shown in Tables 7 and 8, using (2) and (3). The measured *MOP* and *MOE* are 27.01 and 8.32, respectively.

(7) Finally, an EW damage assessment index reflecting the *MOP* and *MOE* values is output to the CBDAF.

Table 8. Measures of effectiveness (MOE) values of EW systems for the scenario.

Primary Category	w^M(%)	*M*	MOE Items	w (%)	Measured *	Remark
E_EA	40	10	Effects of the EA systems Deception ratio	60 40	10 10	Commander's decision
E_EP	0	0	N/A	0	0	
E_ES	40	7	Effects of the ES systems Identification/classification accuracy	60 40	7 7	Commander's decision
MOCE	20	7.6	Effects of the EW systems Secured system ratio	60 40	8 7	Commander's decision

* Score from 0 to 10 evaluated by staff or commander.

In this scenario, a cyberattack using a backdoor or worm was performed, causing a load on the tactical data link, which prevented the transmission of radar information in real-time. CBDAF derives the assessment result by comparing the value of the normal state of the EW with those after the cyberattack, and finally evaluates the damage caused by cyberattacks through combination with *MOCE*.

6. Conclusions

As our daily life is transforming into a hyper-connected era connected by a network, defense science and technology is also developing into a form where traditional physical warfare systems operate in cyberspace. Therefore, damage assessment of EW systems connected to cyberspace using a tactical data link must be done since a BDA for all military operations is essentially required.

This paper presented an easy-to-use assessment framework for assessing the effectiveness of EW systems related to cyber warfare in conjunction with the cyber battle damage evaluation framework. We set up an appropriate scenario, including an integrated EW system incorporating two or more different types of EW equipment, and experimentally confirmed that the proposed framework could be effectively applied to cyber electromagnetic warfare by evaluating the effectiveness of the EW systems using this scenario.

To the best knowledge of the authors, the proposed method is a novel method to evaluate EW systems in cyberspace, and its advantage is that the method can be easily linked with an existing framework for evaluating cyberspace. The result of this study can be considered necessary for designing BDA systems based on existing EW systems and cyberspace, owing to the paucity of relevant literature survey on assessing the effectiveness of EW systems.

Author Contributions: Conceptualization, S.C., O.-J.K. and H.O.; Funding acquisition, D.S.; Methodology, S.C and H.O.; Project administration, H.O.; Supervision, O.-J.K.; Writing—original draft, S.C.; Writing—review and editing, O.-J.K. and D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Agency for Defense Development (ADD) grant number UD190016ED.

Acknowledgments: This work was supported by the Defense Acquisition Program Administration and Agency for Defense Development under the contract UD190016ED.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript.

Abbreviation	Full name
AI	Artificial intelligence
BDA	Battle damage assessment
BPMN	Business process modeling notation
C2	Command and control
CBDAF	Cyberspace battle damage assessment framework

CEMA	Cyberspace electromagnetic activities
CMIA	Cyber mission impact assessment
COA	Course of action
COMSEC	Communication security
DIMFUI	Degradation, interruption, modification, fabrication, unauthorized use, and interception
DODIN	Department of defense information network
EA	Electronic attack
EMCON	Emission control
EMS	Electromagnetic spectrum
EP	Electronic protection
ES	Electronic warfare support
ESM	Electronic support measure
EW	Electronic warfare
ICT	Information and communication technologies
IoT	Internet of things
KPP	Key performance parameters
MDMP	Military decision-making process
MMF	Mission and means framework
MOCE	Measures of cyber effectiveness
MOE	Measures of effectiveness
MOP	Measures of performance
NIST	National institute of standards and technology
RWR	Radar warning receiver
T&E	Test and evaluation

References

1. Bryant, W.D. *International Conflict and Cyberspace Superiority: Theory and Practice*; Routledge: New York, NY, USA, 2015.
2. Lee, Y.-S. Application of Cyber Army to Rep. of Korea Armed Forces based on German Federal Cyber Forces establishment and implementation. *Q. J. Def. Policy Stud.* **2017**, *33*, 203–244.
3. Ministry of National Defense. *2016 Defense White Paper*; Ministry of National Defense (Republic of Korea): Seoul, Korea, 2016.
4. Song, J.-I. A Study on Enhancing Joint Cyber Operations of the Republic of Korea(ROK) Forces—Focused on Linkage. *Korean J. Mil. Aff.* **2017**, 147–186. [CrossRef]
5. Frater, M.; Ryan, M. *Electronic Warfare for the Digitized Battlefield*; Artech House, Inc.: Norwood, MA, USA, 2001.
6. FM 3-36, Electronic Warfare. Available online: https://www.globalsecurity.org/military/library/policy/army/fm/3-36/fm3-36_2012.pdf (accessed on 25 November 2020).
7. Electronic Warfare Test and Evaluation. Available online: https://apps.dtic.mil/dtic/tr/fulltext/u2/a130624.pdf (accessed on 25 November 2020).
8. Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf (accessed on 25 November 2020).
9. Cyber Attack—Glossary. Available online: https://csrc.nist.gov/glossary/term/Cyber_Attack (accessed on 25 November 2020).
10. Denning, D.E.; Blanken, L.; Rothstein, H.; Lepore, J. *Assessing Cyber War*; Georgetown University Press: Washington, DC, USA, 2015; pp. 266–284.
11. NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. Available online: https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1 (accessed on 25 November 2020).
12. Kotenko, I.; Chechulin, A. A cyber attack modeling and impact assessment framework. In Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 4–7 June 2013; pp. 1–24.
13. Musman, S.; Temin, A. A cyber mission impact assessment tool. In Proceedings of the 2015 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 14–16 April 2015; pp. 1–7.

14. Kim, D.; Kim, D.; Shin, D.; Shin, D.; Kim, Y.-H. Cyber Battle Damage Assessment Framework and Detection of Unauthorized Wireless Access Point Using Machine Learning. In *International Conference on Frontier Computing*; Springer: Singapore, 2018; pp. 510–519.
15. Electronic Warfare: The Part of the F-35 Fighter Story You Haven't Heard. 2018. Available online: https://www.forbes.com/sites/lorenthompson/2018/01/09/electronic-warfare-the-part-of-the-f-35-fighter-story-you-havent-heard/#61f4706d68cc (accessed on 25 November 2020).
16. Wade, N.M. *The Cyberspace Operations & Electronic Warfare SMARTbook*; The Lightning Press: Lakeland, FL, USA, 2019.
17. FM 3-38, Cyber Electromagnetic Activities. Available online: https://www.hsdl.org/?abstract&did=750460 (accessed on 25 November 2020).
18. Army, U. *Cyberspace and Electronic Warfare Operations FM 3-12*; Department of the Army: Washington, DC, USA, 2017.
19. Baek, H.-G.; Jeong, S.-M.; Im, J.-S. Trends of tactical data link technologies for network centric operations. *Commun. Korean Inst. Inf. Sci. Eng.* **2010**, *28*, 59–69.
20. Gwanggaeto the Great-Class Destroyer. Available online: https://en.wikipedia.org/wiki/Gwanggaeto_the_Great-class_destroyer (accessed on 25 November 2020).
21. US Weapons Systems Can Be 'Easily Hacked'. Available online: https://www.bbc.com/news/technology-45823180 (accessed on 25 November 2020).
22. Sheehan, J.H.; Deitz, P.H.; Bray, B.E.; Harris, B.A.; Wong, A.B. *The Military Missions and Means Framework*; Army Materiel Systems Analysis Activity: Aberdeen Proving Ground, MD, USA, 2004.
23. Headquarters, Department of the Army. *101-5, Staff Organization and Operations*; Department of the Army: Washington, DC, USA, 1995.
24. Musman, S.; Tanner, M.; Temin, A.; Elsaesser, E.; Loren, L. Computing the impact of cyber attacks on complex missions. In Proceedings of the 2011 IEEE International Systems Conference, Montreal, QC, Canada, 3–6 April 2011; pp. 46–51.
25. Park, J.; Kim, D.; Shin, D.; Shin, D. Design and implementation of simulation tool for cyber battle damage assessment using MOCE (measure of cyber effectiveness). *J. Korea Inst. Inf. Secur. Cryptol.* **2019**, *29*, 465–472.
26. Adamy, D. *EW 101: A First Course in Electronic Warfare*; Artech House: Norwood, MA, USA, 2001; Volume 101.
27. Hu, Y.; Song, B. Evaluation the Effectiveness of the Infrared Flare with a Tactic of Dispensing in Burst. In Proceedings of the 2010 3rd International Symposium on Systems and Control in Aeronautics and Astronautics, Harbin, China, 8–10 June 2010; pp. 131–136.
28. Pelletier, M.; Sivagnanam, S.; Blasch, E.P. A track scoring MOP for perimeter surveillance radar evaluation. In Proceedings of the 2012 15th International Conference on Information Fusion, Singapore, 9–12 July 2012; pp. 2028–2034.
29. Pouliguen, P.; Bechu, O.; Pinchot, J. Simulation of chaff cloud radar cross section. In Proceedings of the 2005 IEEE Antennas and Propagation Society International Symposium, Washington, DC, USA, 3–8 July 2005; pp. 80–83.
30. Zhou, W.; Luo, J.; Jia, Y.; Wang, H. Performance evaluation of radar and decoy system counteracting antiradiation missile. *IEEE Trans. Aerosp. Electron. Syst.* **2011**, *47*, 2026–2036. [CrossRef]