J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr
Copyright ⓒ 2020 KSII

사이버전 연계 전자전 전투피해평가 지표 산출을 위한 연구☆

A Study on Battle Damage Assessment of Electronic Warfare associated with Cyber Warfare

최 승 철[1] 조 준 형[1] 권 오 진[1*]
Seungcheol Choi Joonhyung Cho Oh-Jin Kwon

요 약

본 논문은 사이버전과 연계된 전자전에 대한 전투피해를 평가하기 위한 프레임워크를 제안한다. 정보통신기술의 급격한 발전으로 사이버 공간에서 이루어지는 사이버전과 전자전의 중요도가 날로 증가하고 있다. 따라서 사이버 공간에서 이루어지는 사이버전, 그리고 이와 연계된 전자전에 대한 BDA (Battle Damage Assessment)는 군사 작전의 성공 또는 실패에 영향을 주는 중요한 요소이다. 본 논문에서는 전자전의 종류에 따라 전자전 시스템을 대/중/소분류로 구분하여 성능지표, 영향지표를 산출하는 방법을 정의하고 전자전 전투피해평가 지표 산출을 위한 프레임워크를 제안한다. 가상 시나리오를 설정하여 제안하는 프레임워크의 효용성을 보였다.

☞ 주제어 : 사이버전, 전자전, 전투피해평가, 전자전 피해평가

ABSTRACT

This paper proposes a framework for the battle damage assessment (BDA) of electronic warfare linked to cyber warfare. Thanks to the rapid development of information and communication technology, the importance of cyber warfare and electronic warfare in cyberspace is increasing. Therefore, the BDA for cyber warfare and its associated electronic warfare in cyberspace is an important factor that affects the success or failure of military operations. In this paper, we propose a method to calculate measure of performance and measure of effectiveness by classifying the electronic warfare system into large / medium / small classes according to the type of electronic warfare. By setting up a hypothetical scenario, we show the effectiveness of the proposed framework.

☞ keyword : Cyber warfare, Electronic warfare, Battle damage assessment, Electronic warfare battle damage assessment

1. 서 론

정보통신 기술 (Information and Communication Techonology, ICT)의 발전은 3차 산업분야의 획기적 발전을 이루기 위한 환경을 제공하였으며, ICT는 발전을 거듭하여 다양한 산업들 간의 연계와 융합을 통하여 4차 산업혁명을 맞이하였다. 사이버 공간은 더 이상 사람과 사람간의 정보 교환을 위한 공간으로 머무르지 않고, 사물과 사물간의 정보교환이 가능한 사회가 되었다. 이와 함께, 스마트 디바이스의 발전은 시간과 장소에 얽매이지 않고 언제 어디서나 일할 수 있는 체제인, 스마트 워크가 우리의 업무환경을 사이버 공간으로 이동하게 하였다.

국방 분야에서도 ICT 기술과 국방과학기술이 융합함으로써, 현대의 군사 활동에서 광범위하게 전자전 (EW : Electronic Warfare)이 수행되고 사이버 공간에서는 군사 활동과 EW가 융합되는 군사 활동의 형태로 발전하였다. 미 육군에서는 사이버전과 EW작전은 대부분 유사한 목적으로 수행되기 때문에 융합된 형태로 수행되어야만 한다고 강조하고 있고, 국방부에서는 사이버 공간에서의 작전 능력을 향상시키기 위한 활동을 수행하는 사이버 사령부를 설립하였다[1].

한편, 군사 작전으로 인한 전장의 피해를 평가하는 것은 군사 작전의 성공 또는 실패에 영향을 줄 수 있는 중요한 요소 중의 하나이다. 최근 사이버 공격 이후 피해를 평가하기 위한 다수의 연구가 이루어졌지만, 사이버전자전 또는 사이버전 연계된 전자전의 피해 평가에 대한 연구는 찾기 어렵다.

본 논문에서는 사이버전과 연계된 EW장비의 피해를

1 Department of Electrical Engineering, Sejong University, Seoul, 05006, Korea.
* Corresponding author (ojkwon@sejong.ac.kr)
[Received 14 November 2019, Reviewed 21 November 2019, Accepted 10 December 2019]
☆ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다. (UD190016ED)

EW 장비의 성능 측정과 효과 측정에 기초하여 수치 형태로 제공하는 전투 피해평가 (BDA : Battle Damage Assessment) 모델을 제안한다. 그런 다음 EW 장비에 대한 사이버 공격을 가정하여 모델의 적용 예를 제공하는 시나리오를 설정하였다.

본 논문은 다음과 같이 구성된다. 2장에서는 사이버전과 전자전에 대한 관련 연구 내용을 소개한다. 3장에서 전자전 BDA 지표를 위한 프레임워크를 제안하고 가상 시나리오를 통해 프레임워크의 수행 절차와 방법을 설명한 후, 5장에서 결론을 맺는다.

2. 관련 연구

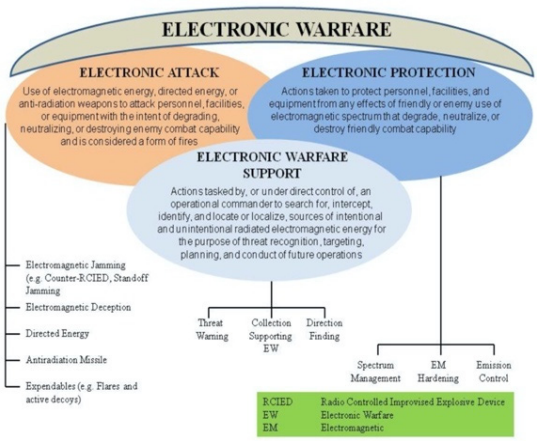
2.1 사이버전과 전자전

사이버 공간에서의 위협과 공격은 잠재적 피해가 매우 크고, 눈에 보이지 않은 곳에서 이루어지기 때문에 더욱 중요하게 다루어져야 한다. 특히, 사이버 공격 능력이 미국에 버금가는 것으로 여겨지는 북한으로부터의 사이버 위협이 가장 심각한 것으로 간주되고 있다.

사이버 공격의 목적은 직접적인 공격 효과뿐만 아니라 이차적 효과나 간접적인 효과에 초점을 맞출 것으로 보인다. 예를 들어, 원자력 발전소의 제어 시스템을 공격하여 방사능이 유출되거나 적군의 대공방어 시스템 공격으로 인하여 아군의 항공작전을 지연시킬 수 있는 효과를 얻게 된다. 이는 사이버 공격으로 인해 국가안전에 위협을 가하고, 국민들에게는 불안과 공포를 일으킴으로써 간접적인 효과를 얻을 수 있게 된다[2].

한편, 전자전은 Command & Control (C2)의 5가지 군사 행동인 Operation Security, EW, Psychological Operation, Military Deception, 물리적 타격 중 하나로 전자기파 스펙트럼을 제어함으로써 수행하는 군사 행동을 지칭한다[3]. 전자전은 그림 1에서 도시한 바와 같이, 적의 전자기파 스펙트럼을 제어하는 전자 공격 (EA : Electronic Attack), 방어적 수단으로 사용하는 전자 보호 (EP : Electronic Protection), 그리고 공격과 방어에 대한 지원 및 감시 정찰 등을 주요 임무로 하는 전자 지원 (ES : Electronic Support) 3가지 로 구분한다[3][4].

하지만, ICT 기술과 군사 기술 발달로 인하여 현대전에서는 사이버전과 전자전을 통합적으로 대응해야 하는 필요성이 대두 되고 있다. 예를 들어, 미국은 발사 후 대응(Right of Launch)에 대비되는 개념인, 발사 직전 교란(Left of Lauch) 개념을 2017년 3월에 합참의장이 최초로 발표한 바 있는데, 이는 적의 미사일 발사 전에 아군의 전자기파와 사이버 공격으로 적 C2 체계와 미사일에 내장된 전자 장비를 교란하여 무력화 시킨다는 구상이다[5]. 한국군의 경우 표 1과 같이 전자전, 사이버전, 사이버전자전에 대한 기본 개념을 정립하고 있으나, 사이버전자전의 경우는 한국군 차원의 체계적인 운용 개념이 정립되지 않은 것으로 보고되고 있다[5].

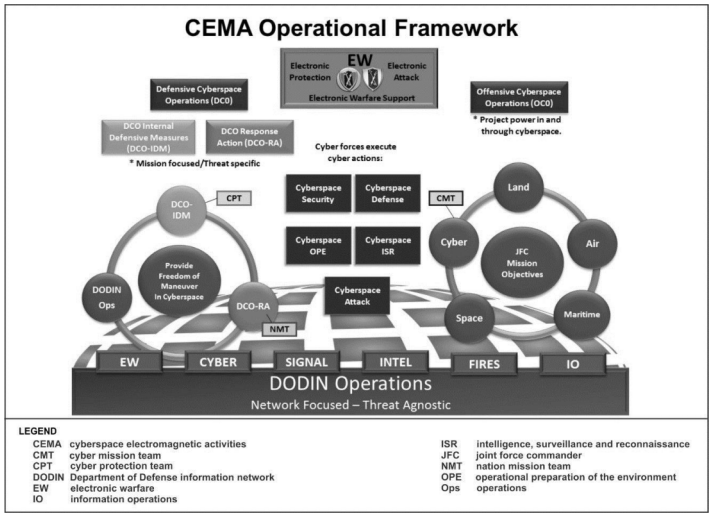


(그림 1) 전자전 분류[4]
(Figure 1) EW Sub-Divisions[4]

미 육군은 현대전의 한 형태로 사이버전자전 (CEMA : Cyberspace Electro-Magnetic Activities) 개념을 정립하였다. 사이버전과 전자전은 과거와 같이 서로 독립적인 군사 활동으로 수행하는 것이 아닌 상호 융합된 형태의 군사 활동으로 발전하였다는 것이며, 대부분 비슷한 목적을

(표 1) 전자전, 사이버전, 사이버전자전 비교
(Table 1) Comparision between EW, CW and CEW

구분	전자전 (EW)	사이버전 (CW)	사이버전자전 (CEW)
태동시기	1940년대	2000년대	2010년대
범위	전자기 스펙트럼	사이버공간	전자기스펙트럼+사이버공간
통신방법	무선 위주	유선, 무선	유선, 무선
총괄	합참 전자전과	합참 사이버작전과	합참 사이버작전과, 전자전과/정보본부
주요교리	전자전 전자전 종합발전계획 등	합동사이버작전교범 등	-
주요과제	자율형 전자공격장비 등	사이버전 능동대응 작전체계 등	-



(그림 2) CEMA 작전 프레임워크[6]
(Figure 2) CEMA Operational Frameowork[6]

위해 수행되기 때문에 반드시 융합된 형태로 수행해야 함을 강조하고 있다[6]. 미 육군에서 정의하는 CEMA 작전의 전체 프레임워크는 그림 2와 같다.

CEMA 작전의 수행은 미 육군 군정보망운용국 (DODIN : Department Of Defense Information Network)의 통제하에 사이버 공격과 방어, 전자전 공격/지원/보호, 전자기파 스펙트럼 관리의 3가지 군사 활동의 융합을 통하여 수행된다. 미 육군의 모든 정보 군사 활동 (정보의 관리, 운용, 명령 전송, 상황 인식 등)은 DODIN을 통해 이루어지고, 집, 임시 거처, 초소, 야영지, 기지국 등 네트워크가 연결된 모든 곳에서 접속이 가능하다.

2.2 사이버전자전 전투피해 평가

CEMA 교범에서는 공격 임무 (Mission)를 정의하고 있으며, 이는 적군에 미치는 피해 효과의 유형 및 등급에 따라 표 2와 같이 분류하고 있다.

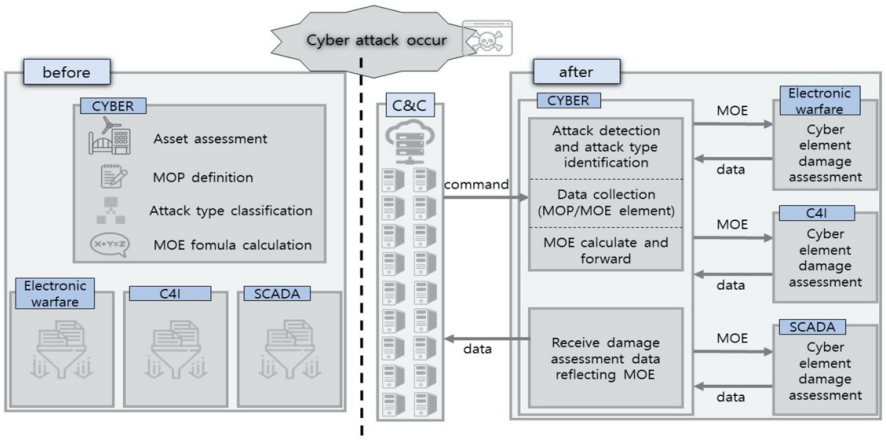
CEMA의 임무는 군사활동에 따라 사이버전 요소와 전자전 요소를 포함하고 있다. 사이버전이 수행되는 공간을 Cyber Persona, Physical, Logical의 3단계 계층으로 나누어 계층별 임무의 대상을 구분하고 있다. 개인 정보를 통해 물리적인 컴퓨터나 장비에 접근하고 물리 계층을 통해 비인가 네트워크 등에 접근하여 공격하고자 하는 구상이다. 이를 위하여 사이버공간에서 이루어지는 군사행동을 ISR (Intelligence, Surveillance and Reconnaissance),

(표 2) CEMA 임무 유형
(Table 2) CEMA Mission types

임무	피해 효과	CEMA 공격 예
Denial	적의 전투 기능을 아군이 지정한 기간 동안 마비시킴	• EW Jamming • Router blocking
Degrade	적의 전투 기능을 약화시킴	• 통신 속도 저하 공격
Disrupt	적의 전투 기능을 교란시킴	• 통신 방해
Destroy	적의 전투 기능을 파괴함. HW/SW적으로 재구축을 하여야만 하는 피해를 끼침	• 모든 DB 파일 삭제 • 시스템 overheating 파괴
Manipulate	아군의 의도대로 적의 자산을 제어 또는 변경함	• 적 DB 데이터를 아군에 유리하게 변경
Deceive	거짓 정보로 적의 잘못된 결정에 이르게 함	• 타부대로 변경 메시지 발송

작전 준비, 보안, 공격, 방어로 구분하여 사이버 공간 계층에서 수행된다. 이 때, 네트워크에 직/간접적으로 연결된 전자전 장비 및 외부 네트워크까지도 공격 대상에 포함되고, 전자전 요소는 2.1절에서 언급된 EW의 3요소가 활용된다.

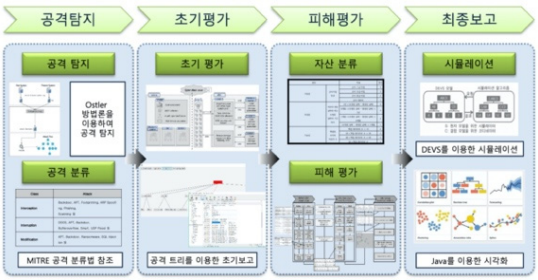
마지막으로, 모든 군사 작전에서는 반드시 전투피해 평가를 수행하여 C2의 작전 운용을 위한 정보를 제공하여야 하기 때문에, CEMA 교범에서는 BDA를 위한 주요 원칙들을 다음과 같이 정의하고 있다.



(그림 3) 사이버 전투피해평가 프레임워크
(Figure 3) Cyber Battle Damage Assessment Framework

- CEMA 작전 양상의 특성상 즉각적이고 실시간적인 BDA를 요구한다.
- 작전 계획 단계에서는 전장 상황을 지휘관이 이해하는데 도움을 줄 수 있는 사이버 공간에서의 정보수집에 초점을 두는 반면, 작전 준비 및 실행 단계에서는 실시간 변화 상황과 진행 과정을 모니터링 하는데 초점을 둔다.
- MOE (Measure Of Effectiveness)와 MOP (Measure Of Performance)는 CEMA BDA의 핵심적 지표이다.

CEMA 교범에서는 MOP를 주어진 임무의 완성도를 측정하는 군사 활동의 성능을 평가하는 지표로 정의하고, MOE는 시스템의 동작, 능력, 운용 환경의 변화를 측정하여 군사 작전의 목적이 달성되었는가에 대한 답을 줄수 있는 지표로 정의하고 있다. 따라서 얼마나 정확한 MOP, MOE지표를 도출할 수 있는지가 사이버전 연계된 전자전 또는 사이버전자전 BDA의 핵심이라고 말할 수 있다.



(그림 4) 사이버 전투피해평가 절차
(Figure 4) Procedure of the CBDAF

3. 제안 BDA 프레임워크

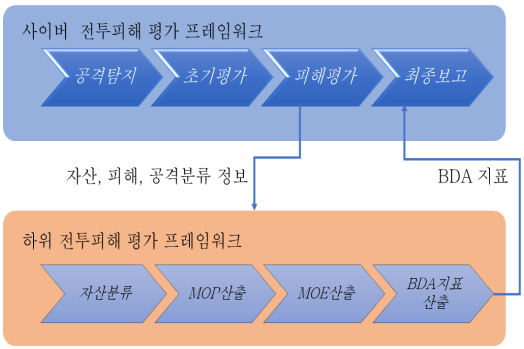
3.1 사이버 피해평가 프레임워크

최근에 물리전, 전자전과 연계한 사이버 공격의 피해를 평가하기 위한 Cyber BDA Framework (CBDAF) 가 제안되었다[1]. CBDAF는 장비의 손상과 임무 또는 작전의 영향을 평가하여 그림 3과 같이 사이버 공격으로 인한 피해를 C2에 알려준다. 이 프레임워크는 공격이 발생하기 전에 동일한 사이버 공간에 있는 모든 자산에 대한 정보를 실시간으로 모니터링한다. 사이버 공격이 발생하면 자산 상태의 변화를 감지하고 어떤 유형의 공격이 발생했는지, 어떤 유형의 손상이 자산에 발생했는지 분석하여, 각 요소의 평가를 위한 각 하위 시스템에 유효성 정보 측정 값을 전송한다. 각 하위 시스템은 전달된 자산의 유효성 정보를 이용하여 평가 결과를 프레임워크에 제공하여 마지막으로 사이버 전투 피해를 평가한다.

3.1.1 사이버 피해평가 절차

CBDAF는 그림 4에서 보이는 바와 같이 사이버 피해평가의 절차는 크게 공격탐지, 초기 평가, 피해 평가, 최종보고의 4단계로 구분된다. 이때, 사이버 공간에 등록되어 있는 자산 정보로 초기평가를 수행하여 개략적인 사이버

피해평가 정보를 제공 가능하지만, 사이버 공간에 등록되어 있는 자산에 대한 전자전, 물리전 등의 피해 평가를 수행하는 하위 시스템과 연동하여 구체적인 BDA를 제공함으로써 상황에 기반한 지휘결심을 더 정확하게 만들 수 있다.



(그림 5) 사이버 전투피해평가 프레임워크 연동 개념도
(Figure 5) Overview of communication between CDBAF and Sub-systems

3.1.2 프레임워크 하위 시스템 연동

CBDAF는 전자전, 물리전, SCADA의 피해를 평가하는 하위 시스템을 포함하여 BDA를 산정하도록 설계되었다. 본 논문에서는 CBDAF의 기본 피해평가 절차에 기반을 두어, 전자전 BDA 하위 시스템과의 연동 절차를 제안하며, 전자전의 피해를 평가하는 프레임 워크의 기본 모델을 제안한다. 하위 시스템과의 연동은 그림 5의 절차로 이루어진다. 제안 절차는 전자전뿐만 아니라 여타 물리전과의 연동을 위한 절차로 활용이 가능하다.

3.2 제안 전자전 BDA 프레임워크

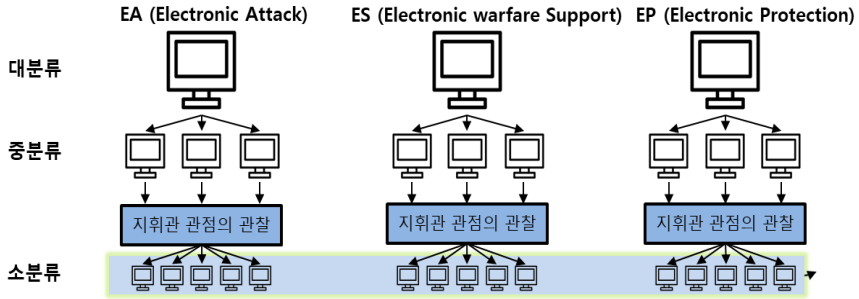
BDA 지표를 설계/산출하기 위하여 문헌을 통해 전자전의 정의, 전자전 장비의 종류, 전자전 시스템의 구성 형태를 파악하였으며, 전자전 BDA를 위한 MOP와 MOE를 설정하고 이들 지표들이 정상 상태에 비해 악화되는 측정치를 이용하도록 설계되었다. 본 논문에서 제안하는 BDA 지표의 효용성을 제시하기 위하여 가상 시나리오를 통한 사례 연구를 수행하였다.

3.2.1 전자전 BDA 지표 설계

제안하는 전자전 BDA를 설계하기 위하여 다음의 용도를 고려하였다

- 사이버 공격 후 전자전 능력에 미친 영향을 평가하여 사이버 지휘통제 체계에 도움이 되는 정보를 제공할 수 있어야 한다.
- 전자전 능력에 미친 영향은 사이버 감시정찰 체계의 활동을 통하여 파악되므로, 사이버 감시정찰 체계에 획득할 정보를 지정하는데 사용되는 구체적인 항목을 제공할 수 있어야 한다.
- 사이버 공격전, 다양한 공격 방법의 효과에 대한 시뮬레이션 결과를 제공할 수 있어야 한다.
- 아군 전자전 능력에 대한 BDA 지표의 수시 변동 상황을 파악하여 공격 여부 및 시도를 포착하여야 함으로, 사이버 지휘통제 체계와 감시정찰 체계에 유사시 필요한 정보를 제공할 수 있어야 한다.

이를 위하여 사이버 공격에 의한 전자전 BDA는 다음의 3가지 요소로 구분하여 평가가 가능하다.



(그림 6) 전자전 장비 분류
(Figure 6) Classes of the EW systems

(표 3) 전자전 시스템 MOP 지표 산출 예
(Table 3) A sample of MOP for EW systems

MOP_EW		4.61										
대분류	중분류	A 가중합	가중치 (%)	MOP	소분류	a 가중합	가중치 (%)	A	개별 MOP 항목	측정값	가중치 (%)	a
EA	MOP_EA_Jammer	10.25	40	4.1	對레이더	10.5	50	5.25	타겟추적 정확도	15	50	7.5
									유효 면적 영역	0	20	0
									신호 cross-correlation	10**	30	3
					對통신	10	50	5	JSR* 감소율	10	100	10
ES	MOP_ES_Radar	0.85	60	0.51	탐지영역	1.7	50	0.85	탐지 가능영역 각도	24	50	12
									최대 탐지 거리(150km)	10**	50	0.5

* JSR : Jamming to Signal Ratio
** 0~10 범위

- MOP 요소 : 전투자산의 성능에 대한 물리적/기능적 피해
- MOE 요소 : 전투 임무 수행 효과의 저하 피해
- 피해 복구 요소

전투 자산은 인적 요소와 물적(장비/시스템) 요소로 구분할 수 있으나, 본 논문에서는 물적 요소에 대한 물리적/기능적 피해 평가 지표 설계만을 고려하였으며, 기본적으로는 새로운 전투 자산이 없은 경우 고정적인 지표로 설정하였다. MOP 지표는 전자전 시스템 구성 형태 (Stand alone, Federated, Integrated)별로 확장성을 고려하여 설계하였다. 또한, MOE 요소에 대한 지표는 전자전 임무 수행 효과에 대한 평가지표이다. 임무전술에서의 과업, 작전개념, 예하부대 과제부여 및 협조지시의 식별을 포함하는 계획검토의 표준을 제시하는 미군의 Universal joint task list (UJTL)과 같은 형태로 전자전 임무의 분류가 가능하며, 이에 따른 임무 수행 효과 항목을 설정할 수 있도록 설계하였다[7]. 추가적으로, 물적 자산에 대한 피해 복구 요소(예: 네트워크 복구)를 고려하여 MOP 지표에 포함하여 산출하도록 설계하였다.

3.2.2 제안 전자전 MOP 지표

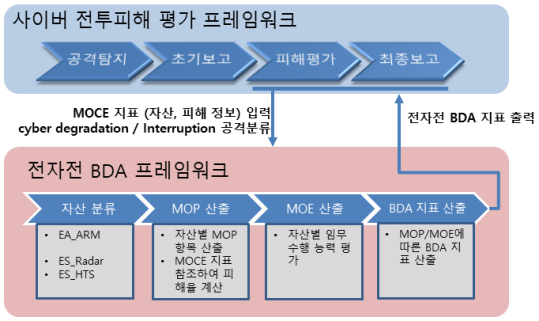
전자전 시스템은 EA, ES, EP로 크게 분류하고, 개별 Stand alone 시스템에 대한 성능 항목을 중/소분류로 세분화하여, 중/소분류의 항목별 지표에 대한 가중 합으로 MOP 지표를 산출한다.

Stand alone 시스템은 주로 네트워크에 연결되지 않은 독립시스템으로 운용되지만 네트워크를 통해 데이터를 공유하는 Federated 시스템과 모든 리소스와 DB를 공유하는 Integrated 시스템을 구성하는 개별 시스템이 된다. 따라서 Federated와 Integrated 시스템의 MOP 지표는 시스템을 구성하는 Stand alone 시스템의 MOP 항목 지표를 기반으로 식 1과 같이 산출한다.

$$MOP_{EW} = \sum_{k=1}^{K} (MOP_k \times w_k)$$
$$MOP = \sum_{n=1}^{N} (A_n \times w_n) \qquad \text{(식 1)}$$
$$A = \sum_{m=1}^{M} (a_m \times w_m)$$

이 때, MOP는 중분류의 가중합, A는 소분류 가중합, a는 소분류의 개별 MOP 항목의 가중합이다. K는 대분류 전자전 시스템의 개수, N은 개별 전자전 시스템의 개수, M은 각 시스템의 MOP 항목 지표의 개수이다. 각 분류의 가중치 w는 임무전술에 대한 계획검토의 결과에 따라 지휘관에 의해 다르게 설정된다.

표 3은 전자전 시스템의 MOP 지표 예이다. 이 예에서는 EA Jammer와 ES Radar 시스템이 Federated형태이다. 각 시스템의 기능에 따라 소분류로 나뉘고 개별 MOP 항목이 설정되었다. EA의 Jammer 시스템은 기능에 따라 對레이더와 對통신으로 분류되어, 각 기능별로 MOP 항목[8]을 설정하여 MOP 성능을 측정하고, Radar는 탐지영역을 중심으로 MOP 항목[9]을 설정한 예이다. 논문에서 제시한 MOP 항목들은 문헌을 통하여 조사된 시스템의 성능 항목을 기반으로 작성하였으며, 실제 시스템에 따



(그림 7) 전자전 BDA 지표 산출 절차
(Figure 7) Procedure of EW BDA framework

라 다른 항목을 가질 수 있다.

3.2.3 제안 전자전 MOE 지표

전자전 시스템의 MOE는 전자전 작전의 임무별, 즉, EA, EP, ES별로 목적 성취 정도를 측정하기 위한 지표이며, 군사 작전 및 자산에 미치는 영향 등의 인과 관계를 고려하여 설정한다.

- MOE_EA : 전투능력을 감쇄/무효화/파괴할 목적으로 전자기파를 이용하여 인적/물리적/기능적 피해를 가하는 임무
- MOE_EP : 전자기파 공격으로부터 인적/물리적/기능적 피해를 방어하는 임무
- MOE_ES : 즉각적인 위협인지/표적설정/군사활동계획 등을 위해 의도적/비의도적으로 발생한 전자기파 발생원을 탐색/intercept/identifying/localizing하는 임무

전자전 시스템의 MOE 지표 항목은 MOP 지표와는 다르게 작전 환경과 자산의 형태에 따라 유동적으로 변경이 가능하도록 설계되어 있다. 전자전의 군사 행동에 따라 위의 세 가지 MOE 항목을 세부적으로 분리하고 이 항목들의 가중 합으로 MOE 지표를 산출한다.

3.2.4 제안 전자전 BDA 지표

전자전 BDA 지표는 평상시의 MOP와 MOE 요소들의 수치에 비하여 사이버 공격 시 저하된 수치를 제시함으로써 산출이 가능하다. 모든 지표는 계층적 구조로 설계하며 상위 계층의 지표는 하위 계층의 함수 형태에 추가적인 요소를 가미함으로써 설정이 가능하며, 기본적으로는 하위 계층 지표의 가중 합 개념을 도입하여 설계되었다.

그림 7의 제안하는 전자전 BDA 프레임워크는 사이버 전투피해 프레임워크에서 자산, 피해정보, 공격의 형태에 대한 정보를 입력받아 앞 절에서 제안한 MOP와 MOE를 산출하여 전자전에 대한 BDA 지표를 출력한다.

(표 4) 전자전 가상 시나리오
(Table 4) A sample scenario of EW

시스템 구성 형태	네트워크에 연결된 AN/APG-65 Radar 시스템[1] (ES) + HTS[2](ES) + HARM[3](EA)
시스템 임무	AN/APG-65 Radar와 HTS의 지원하에 AGM-88 HARM을 사용하여 아군의 데이터를 수집하는 적군의 레이더를 파괴
사이버 공격 유형	• 적군이 지역 A에 Transportable Radar를 설치하여 아군의 정보를 수집 • 아군 지휘관은 F/A-18 Hornet을 이용한 적 레이더 파괴 작전 수행 • 임무 수행중 아군 Federated 시스템이 사이버 공격을 받음 • 확인 결과, 적군의 사이버 부대는 아군의 구형 시스템 기반의 Federated 시스템이 보안에 취약하다는 것을 알고 해킹 공격 • 아군은 적군의 사이버 공격을 Degradation/Interruption 공격으로 분류
피해 상황	• 해킹으로 인한 아군 시스템 일부의 통제권 상실 • F/A-18 Hornet의 HTS의 무력화로 Targeting 시스템 지원을 받지 못하여 타격 임무 수행하지 못함 • 임무 실패로 적군 레이더의 정보 수집 지속 • 피해가 3600초간 지속

[1]F/A-18에 탑재되어 조종사의 임무를 지원하는 Radar
[2]적 레이더의 위치를 특정, HARM 미사일과 조종사에게 정보를 전달
[3]Radar를 주 타겟으로 하는 공대지 미사일

3.3 전자전 BDA 가상 시나리오

전자전 BDA의 효용성을 제시하기 위하여 표 4의 가상 시나리오를 설정하였다. 2개의 ES 시스템과 1개의 EA 시스템으로 구성된 Federated 시스템에 대하여 그림 7에서 보이는 것과 같이 CBDAF에서 전자전 BDA 프레임워크로 전자전 BDA를 요청하는 예이다. 이 시나리오는 2018년 미국 의회의 회계감사원의 사이버 취약성 실험*결과를 토대로 작성하였는데[10], 일반적으로 무기체계 개발은 긴 시간이 소요되며, 이로 인해 오래된 콤포넌트/소프

* 2012년부터 2017년까지 미국의 모든 무기체계에 대하여 실험을 수행함.

(표 5) 시나리오에 대한 전자전 MOP 산출
(Table 5) A result MOP for EW systems

MOP_EW	1.672											
대분류 (가중치)	중분류	A 가중합	가중치 (%)	MOP	소분류	a 가중합	가중치 (%)	A	개별 MOP 항목	측정값	가중치 (%)	a
EA (40)	MOP_EA_ ARM〔11〕	0	100	0	-	0	100	0	LOS: Line Of Sight	N/A	-	-
									사격 오차 거리	N/A	-	-
									사격 거리 (150Km)	0	100	0
ES (40)	MOP_ES_ Radar	4.7	40	1.88	탐지영역	1.5	50	0.75	탐지 가능영역 각도	24	50	1
									최대 탐지 거리(150km)	10*	50	0.5
					정확도	7.9	50	3.95	System Sensitivity	10*	40	4
									동시추적 타겟수	3	30	0.9
									피아 판별 정확도	10*	30	3
	MOP_ES_ HTS	0	60	0	정확도	0	100	0	타겟 탐지 정확도	0	100	0
NW (20)	-	4.6	100	4.6	네 트 워 크 복구	4.6	100	4.6	정상 시스템 비율	4*	60	2.4
									복구 가능 시스템 비율	2*	20	0.4
									복구 예정 남은 시간비율	9*	20	1.8

* 0~10 범위

(표 6) 시나리오에 대한 전자전 MOE 산출
(Table 6) A result MOE for EW systems

MOE_EW	3.12							
분류	a 가중합	가중치(%)	A	임무 수행 효과 지표	측정값*	가중치 (%)	a	비고
MOE_EA_ARM	0	30	0	목적한 EA의 효과가 있는가?	0	60	0	지휘관 판단
				타겟이 영향을 받았는가?	0	40	0	
MOE_ES_ Radar	8	30	2.4	ES 작전의 정상 수행 여부	7	50	3.5	지휘관 판단
				피아 식별 여부	8	25	2	
				타겟의 위협 등급을 판별 여부	10	25	2.5	
MOE_ES_HTS	1.8	40	0.72	ES 작전의 정상 수행 여부	1	60	0.6	지휘관 판단
				시스템간 통신 여부	3	40	1.2	

* 0~10 범위

트웨어가 사용되는 취약점을 가지고 있다고 보고되었다.

CBDAF에서는 분류된 공격의 형태와 자산의 정보를 제안 전자전 BDA 프레임워크로 입력하면 절차에 의해 자산을 분류하고, 해당 자산에 대한 MOP 항목에 대한 성능을 측정하게 된다. 그런 다음 해당 자산에 대하여 미리 설정하여 둔 MOE 항목에 대하여 지표를 산출하여 최종 전자전 BDA 지표를 CBDAF로 출력하는 과정을 거친다. 특히, 이 시나리오에서는 추가로 네트워크에 대한 피해복구 요소(NW)을 고려하여 산출하였다. 시나리오에 따른 MOP와 MOE 지표는 표 5과 6과 같이 산출된다.

최종적으로 CBDAF에서는 전자전 BDA의 정상 상태 값과 사이버 공격 이후에 값을 비교하여 피해평가 결과를 도출한다.

4. 결 론

현대의 전장에서 사이버전과 전자전의 중요도는 점점 증가하고 있다. 본 논문은 사이버 전투피해 평가 프레임워크와 연동하여 사이버전 연계한 전자전의 BDA 지표를 산출하는 프레임워크를 제안하였다. 가상 시나리오를 설정하여 제안한 프레임워크의 BDA 산출 절차와 방법을 실험하여 보았으며, 이를 통해 제안한 전자전 BDA 프레임워크의 효용성을 보였다.

전자전 BDA 지표 개발의 예는 미국을 포함한 군사 선진국에서도 그 결과가 문헌에 보고된 바가 없기 때문에 본 논문이 실 전자전 무기체계를 기반으로 하는 BDA 평가 지표를 설계하는데 중요하게 다루어질 수 있는 연구라고

할 수 있다.

참고문헌(Reference)

[1] D. Kim, Y. Kim, D. Kim, D. Shin, and D. Shin, “Cyber Battle Damage Assessment Framework,” The 9th international conference on Internet (ICONI 2017), KSII, Dec. 2017. https://doi.org/10.3745/PKIPS.y2017m11a.178

[2] H. Shin, J. Eom, “Establishment of Cyber Security Strategy according to the change of cyberspace environment,” Journal of Security Engineering, Vol. 14, No. 4, pp. 251-262, 2017. http://www.riss.kr/link?id=A105121312

[3] M. R. Frate, M. Ryan, “Electronic Warfare for the Digitized Battle Field,” 2001. https://dl.acm.org/citation.cfm?id=559487

[4] AGARDograph, R. T. O. and Series-Volume, F. T. T. “Electronic Warfare Test and Evaluation,” 2000. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1000.1658&rep=rep1&type=pdf

[5] T. Son, “사이버전자전, 개념과 운용방향을 정립해야,” KIDA Defense Issues & Analyses, Vol. 1759, No. 19-20, 2019. http://www.kida.re.kr/cmm/viewBoardImageFile.do?idx=27078

[6] FM3-38, “Cyber Electromagnetic Activities,” Dept. of the Army, 2014. https://fas.org/irp/doddir/army/fm3-38.pdf

[7] https://www.jcs.mil/Doctrine/Joint-Training/UJTL/

[8] L. Zhang, “Spectrally Efficient Anti-jamming System Design in Wireless Networks,” Michigan State University, 2011. https://d.lib.msu.edu/islandora/object/etd:868/datastream/OBJ/download/Spectrally_efficient_anti-jamming_system_design_in_wireless_networks.pdf

[9] D. Adamy, “A First Course in Electronic Warfare,” 2001. http://cds.cern.ch/record/1967970

[10] https://www.bbc.com/news/technology-45823180

[11] A. Awad, H. Wang, “Evaluation and Enhancing Missile Performance via Real Time Flight Simulation Model,” IEEE 33rd Chinese Control Conference (CCC), pp. 6324-6329, 2014. https://doi.org/10.1109/ChiCC.2014.6896029

◐ 저 자 소 개 ◑

최 승 철(Seungcheol Choi)
1998년 세종대학교 전산과학과(이학사)
2001년 세종대학교 일반대학원 전산학과(이학석사)
2017년 세종대학교 일반대학원 전자공학과(공학박사)
2017년~현재 세종대학교 전자정보통신학과 책임연구원
관심분야 : 신호처리, 이미지 프로세싱, 이미지 코딩, JPEG
E-mail : choisc@sju.ac.kr

조 준 형(Joonhyung Cho)
2019년 세종대학교 정보통신공학과(공학사)
2019년~현재 세종대학교 대학원 전자공학과 석사과정
관심분야 : 이미지 프로세싱, 압축, JPEG
E-mail : whwnsgud510@sju.ac.kr

권 오 진(Oh-Jin Kwon)
1984년 한양대학교 전자공학과(공학사)
1991년 남가주대학교 대학원 전기전자공학과(공학석사)
1994년 메릴랜드대학교 대학원 전기전자학과(공학박사)
1999년~현재 세종대학교 전자정보통신공학과 교수
관심분야 : 이미지/비디오 퓨전, 압축, 워터마킹, 이미지 분석 및 프로세싱
E-mail : ojkwon@sejong.ac.kr