*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1447

# 사이버공격에 의한 사이버공간 전투피해평가 방안 연구*

장 원 구,† 이 경 호‡
고려대학교 정보보호대학원

# A Study on the Assessment Method of Battle Damage in Cyberspace by Cyberattacks*

Won-gu Jang,† Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

전쟁수행 간 선정된 표적에 대한 공격 실행 후 전투피해를 평가하는 것은 현대전에서는 필수적인 요소이다. 하지만 아직까지 사이버공격에 따른 전투피해평가 방안은 제한적인 상황 하에서 가능한 방법들만이 제안되었다. 이에 본 논문에서는 사이버공간에 대한 이해를 바탕으로 전투평가 이론상의 전투피해평가 방법에 근거하여 군사적으로 적용 가능한 포괄적이고 구체적인 전투피해평가 방안을 제시하였다. 사이버공간 구성 요소를 이용하여 사이버 표적을 분류하고 이를 대상으로 기존의 전투피해평가 방법인 물리적 피해평가, 기능적 피해평가, 표적체계 평가 외 데이터 피해 평가, 사회인식적 피해 평가, 파생적 피해평가 방안을 제시하였으며 과거의 실제 사이버 공격 사례에 적용이 가능함을 예시하였다.

ABSTRACT

Evaluating battle damage after conducting an attack on selected targets during warfare is essential. However, regarding the assessment of battle damage caused by cyber-attacks, some methods available under limited circumstances have been suggested so far. Accordingly, this paper suggests a militarily applicable, comprehensive, and specific method of battle damage assessment from battle damage assessment methods in combat assessment theories from the understanding of cyberspace. By using cyberspace components, this paper classifies cyber targets, suggests the assessment methods of data damage, social cognitive damage, derived damage, and the existing battle damage assessment methods such as physical damage, functional damage, and target systems, and provides an example to demonstrate that this method is applicable to the actual past cyberattack cases.

**Keywords:** Combat Assessment, Cyber Battle Damage Assessment, Cyberspace, Cyber Attack

## I. 서 론

현대전에서는 군사과학기술의 발달에 따른 첨단 정밀무기의 등장과 군사목표 달성을 위한 다양한 전략, 전술의 효과적인 운영에 따라 피·아를 가리지 않는 과거의 무차별적이고 물량위주의 공격과 달리 불필요한 피해를 줄이면서 적에게는 아측이 원하는 피해를 최소의 노력으로 최대한 줄 수 있는 효과적인 전쟁방식을 추구하고 있다. 이에 따라서 지휘관은 최종적인 군사목표를 달성하기 위하여 매순간 전장상황을 종합적으로 파악하여 작전방향을 제시하는데 이를 위해서는 군사작전 수행간 적에 대한 공격시행 후 적의 피해와 무기사용 효과를 확인함으로써 작전의 성

Received(09. 16. 2019), Modified(1st: 11. 01. 2019, 2nd: 11. 29. 2019), Accepted(12. 03. 2019)
* 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다. (UD190016ED)
† 주저자, goo1019@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

과를 측정하고 다음 작전 수행 여부를 판단하는 절차 즉 전투평가를 수행한다. 전투평가는 이미 현대전쟁에서 필수요소로 자리 잡았는데 전투평가 중에서도 전투피해평가는 적이 입은 피해를 평가하는 것으로 전문인원들이 다양한 출처로부터 수집되는 정보를 바탕으로 표적정보를 수집하고 공격 후에 그 피해평가를 실시하여 왔다. 하지만 사이버 공간의 급속한 발달은 사이버전쟁을 가능하게 하고 다양한 공격방법에 의해 막대한 피해를 발생시키는 수준까지 도달했지만 아직까지 물리전과 같은 포괄적이고 정확한 피해평가를 할 수 있는 방법은 충분히 발전되지 않았다. 이는 사이버공간이 물리공간과는 다른 차원의 공간이어서 기존의 방식을 적용하기에는 부적합함에 기인하고 있는데 사이버공간은 물리공간과 달리 시간과 공간의 제약이 없고 컴퓨터 네트워킹을 근간으로 하는 공간으로서 지속적으로 변화하고 있는 공간이다. 또한 사이버공격 방식도 최초에 프로그램이나 네트워크 구조상의 단순한 오류를 찾는 것에서 벗어나 최종목적 달성을 위해 오랜 기간 동안 정보를 수집하고 이를 통해 알려지지 않은 취약점을 파악하여 은밀히 행동하는 등 끊임없이 진화하고 있다. 따라서 사이버공격에 의한 전투피해평가도 물리전과 동일하게 시행됨으로써 불필요한 피해와 노력을 최소화해야 하지만 아직까지 군사적인 관점에서 사이버공격에 대한 포괄적이고 정확한 전투피해를 평가할 수 있는 방안은 마련되지 않은 실정이다. 이에 본 논문에서는 사이버공간을 중심으로 적의 사이버 공격에 따른 전투피해평가 방안을 마련하고자 한다.

본 논문 구성으로 제2장에서는 사이버 피해평가 방안과 관련된 선행연구와 관련이론들, 그리고 연구방법을 알아본다. 제3장에서는 사이버공간과 전투피해평가와의 관계를 살펴보고 사이버공격의 대상인 사이버 표적을 분류하여 전문가 설문조사를 통해 검증하고 이에 따른 실질적인 피해평가 방안을 군사 분야와 민간 분야로 구분하여 알아본다. 이후 과거에 발생하였던 주요 사이버 공격사례를 선정하여 전투피해평가 방안을 실질적으로 적용한다. 제4장에서는 연구 결과를 요약하고 향후 연구 과제를 도출한다.

## II. 선행연구와 연구방법

### 2.1 선행연구

사이버공간이 공격을 받았을 때 가장 먼저 생각할 수 있는 것은 네트워크 자체와 서버, 클라이언트에 대한 피해이다. 공격자가 네트워크 장비나 컴퓨터를 망가트리는 물리적 피해가 가장 손쉬운 방법이며 다음으로 악성프로그램을 통하여 컴퓨터 작동을 방해하거나 기능을 저하시키는 것이다. 그 외에 사회적으로 문제가 되고 있는 신용카드 번호와 같은 개인정보 탈취가 있으며 지능적이고 지속적인 APT공격으로 국가 기간시설에 침투하는 경우도 있다. 이와 같이 사이버공격에 따른 피해는 다양하게 나타나고 있는데 피해평가관련 선행연구를 살펴보면 조완수[1]는 국방과학연구소에서 개발하고 있는 모의분석 도구인 CMT(Cyber Warfare Modeling Technology using LVC)를 이용하여 시스템에 대한 APT, DDOS공격 피해평가 모델을 제안하였다. 김두회 등[2]은 MOE(Measure of Effectiveness)와 MOP(Measure of Performance)를 이용하여 사이버공격 전후의 로그데이터를 비교하는 방식으로 Interception, Interruption, Modification 3종류의 사이버 공격에 의한 사이버자산, 시스템 피해평가 프레임워크를 제안하였다. 유승근[3]은 국방임무수행체계를 계층 구조화하고 이를 대상으로 다양한 사이버공격 전후의 임무수행능력의 변화를 측정하는 피해평가방안을 제시하였다. 김기환 등[4]은 시뮬레이션을 이용하여 육군전술지휘 정보체계(ATCIS : Army Tactical Command Information System) 기반 하에서 적의 웜 공격에 대한 네트워크 피해측정 방안을 제안하였다. 전영배 등[5]은 조직의 자산과 임무에 대한 모델링을 통하여 사이버공격에 따른 피해 영향도를 신속히 계산함으로써 조직 목표달성에 미치는 정도를 판단하는 피해평가방안을 제시하였다. 강정호[6]는 사이버공격에 의한 피해현상 분석을 통해 표적의 비밀성, 무결성, 가용성에 대한 침해정도를 분석하는 피해평가 모델인 M-DCIA(Military-Data, Confidentiality, Integrity, Availity)를 제안하였다. 임선영[7]은 CVE(Common Vulnerability and Exposures), CVSS(Common Vulnerability Scoring System) 등을 이용하여 사이버 자산의 취약점 및 중요도, 시스템 상태를 반영하는 사이버자산 피해평가 방법을 제안하였다. 위 연구들은 사이버공격에 대한 전투피해를 평가하는 다양한 방법이지만 피해평가 대상인 표적과 공격유형, 피해평가 방법, 피해범위가 모두 제각각이며 제한적이어서 실제 적용시 적합한 방법을 매번 찾아야하고 종합적인 피해를 평가하기에

부족하다. 따라서 본 논문에서는 사이버공격에 대한 포괄적이고 구체적인 전투피해평가 방법을 제시함으로써 활용성과 효과성을 제고하고 일목요연하게 피해 상황을 파악하고자 한다.

## 2.2 관련연구

### 2.2.1 사이버 공격과 표적처리

사이버전은 물리전과 달리 그 역사가 길지 않아서 관련된 군사교리나 작전절차 등이 완전히 정립되어 있지 않은 것이 현실이다. 따라서 물리전에서의 공격 시행 절차를 통하여 사이버 표적선정과 공격방안을 알아본다. 미 합동교범에서는 군사작전 간 표적을 처리하는 절차를 Fig. 1.과 같이 6단계로 구분하였다. 먼저 지휘관의 지휘의도와 전장상황의 최종상태에 도달하기 위해 표적을 개발하여 우선 순위화한다. 이어서 아측의 능력을 분석하고 지휘관의 결심에 의거 표적을 처리할 수 있는 전력을 할당한다. 즉, 표적의 위치, 크기, 강도, 적 방어능력, 요구되는 피해 정도 등을 고려하여 무기 종류와, 무기를 사용할 수 있는 전력을 선정하는 것이다. 다음으로 임무계획을 수립한 후 작전을 실행하고 전투평가를 시행하게 된다.

사이버 표적에 대한 공격작전도 이에 준하여 판단해 보면 지휘관의 의도에 따라 사이버 표적을 개발하고 우선 순위화하는데 이때 적의 사이버공간에 대한 취약점을 분석하여야 한다. 이후 아측의 사이버전사를 비롯한 사이버능력을 분석하여 지휘관의 결심에 따라 적절한 사이버무기와 사이버전력을 할당하여 임무계획을 수립하고 작전을 수행한 후 전투평가를 시행하게 된다.

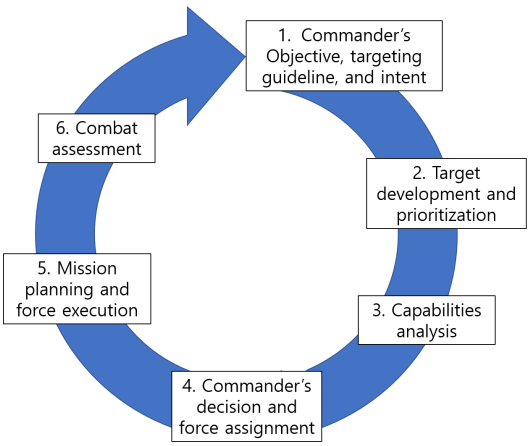


Fig. 1. Joint Targeting Cycle[8]

### 2.2.2 전투평가

지휘관의 의도에 따라 선정된 표적에 대한 공격이 실시된 이후에는 반드시 전투평가(CA: Combat Assessment)를 통하여 수행된 군사작전의 결과를 평가하게 된다. 전투평가는 Fig. 2.와 같이 전투피해평가(BDA: Battle Damage Assessment), 부수적 피해평가(CDA: Collateral Damage Assessment), 무기효과평가(MEA: Munition Effectiveness Assessment), 재공격 건의(RR: Re-attack Recommendation)로 구성되는데 여기서 전투피해평가는 설정된 목표에 대해 무기를 적용하여 공격하였을 경우 발생하는 모든 피해에 대한 정확한 평가와 판단을 내리는 것이다.

전투피해평가는 3단계로 구성되는데 1단계는 물리적 피해 평가(Physical Damage Assessment)로 표적의 물리적인 피해정도를 평가하는 것이다. 2단계는 기능적 평가(Functional Damage Assessment)로 해당 표적이 피해를 입었더라도 본래 기능 중에서 어느 정도로 기능을 수행할 수 있는지를 평가하는 것이다. 이때 표적의 복구시간 및 작전가능 여부를 포함하여야 한다. 3단계는 표적체계 평가(Target System Assessment)로서 전체 표적체계상에서 해당 표적의 손실, 손상이 어느 정도의 영향을 미치는 가를 평가하는 것이다. 전투피해평가의 예를 들면 적의 정유시설 ○개소를 파괴(물리적 피해)하여 1일 정유능력을 ○% 저하(기능적 피해)시키며 이는 결국 적 연료보급 능력을 ○% 제한(표적체계 평가)하게 되는 것이다. 부수적 피해평가는 공격수행간 표적 범위내에서 발생한 민간 피해와 같이 의도하지 않았던 피해를 말한다. 무기효과평가는

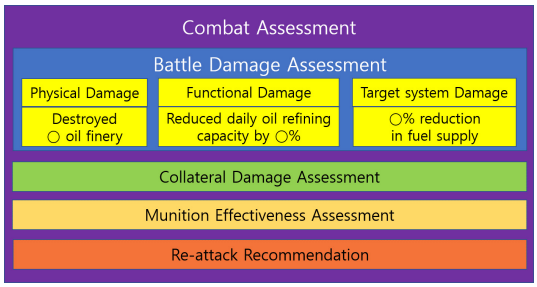


Fig. 2. Battle Damage Assessment[8]

무기를 표적에 적용함에 있어 사전 예측한 효과와 실제 효과를 비교함으로써 충분한 효과를 달성하였는지를 평가하는 것이다. 마지막으로 재공격 건의는 전투평가의 목적으로서 전투피해평가, 부수적 피해평가, 무기 효과평가 등을 통하여 적의 남은 전력과 능력, 잠재적 회복력을 판단하고 작전수행 목적을 고려하여 추가적인 공격시행여부를 결정하는 것이다. 물리전에서 이러한 평가는 주로 정찰기, 인공위성과 같은 정찰자산이나 임무수행 조종사에 의해 수집된 정보들이 전문분석관들에 의해 분석됨으로써 그 결과를 정밀하게 판단하게 된다. 사이버 공격에 대한 전투평가도 마찬가지로 이와 유사하게 선정된 표적에 대하여 물리적, 기능적 피해를 평가해야 하지만 외형적으로 피해가 쉽게 드러나는 물리전보다 피해측정이 더욱 어렵다. 따라서 정확한 사이버 전투피해평가를 위해서는 전문가들에 의해 표적에 대한 정확한 정보수집 및 분석이 지속적으로 이루어져야 한다.

### 2.3 연구방법

본 논문에서는 사이버공간 구성에 대한 이해를 바탕으로 분류된 사이버 표적에 대해 적합한 피해평가 방안을 제시한다. 연구방법으로 먼저 전투피해평가의 의미와 범위를 다양한 각도에서 알아보고 이러한 것들이 사이버공간 구성과 관련하여 어떻게 적용될 수 있는지를 살펴본다. 다음으로 사이버 표적이 사이버공간 상에서 어떻게 구성되고 분류되는지 알아보고 이러한 사이버 표적 분류의 적정성에 대해 다수의 전문가를 대상으로 설문조사를 실시하여 검증한다. 다음으로 분류된 사이버 표적에 대하여 군사부문과 민간부문의 피해평가방안을 각각 세부적으로 도출하고 이를 종합하여 최종 전투피해평가 방안을 제안한다. 이어서 과거 실제 발생한 사이버공격 사례에 적용하여 전투피해평가를 시행함으로써 제안한 방안이 실질적으로 적용됨을 증명한다.

## III. 사이버공간에서의 전투피해평가

### 3.1 사이버공간과 전투피해평가

#### 3.1.1 보안 3요소와 전투피해평가

보안은 일반적으로 정보시스템을 사용함에 있어 3가지 요소, 즉 기밀성, 무결성, 가용성을 유지하는 것을 목표로 한다. 해커와 같은 공격자는 원하는 목적을 달성하기 위해 이 3요소를 깨트리는 행위를 하는 것이고  이것이 Table 1.과 같이 사이버전에서는 전투피해평가의 기본요소가 된다고 할 수 있다. 좀 더 세부적으로 살펴보면 기밀성의 대상은 비밀 시스템과 중요 데이터이며, 무결성의 대상은 파일, 데이터가 되며 가용성의 대상은 시스템, 파일, 데이터로서 각각 물리적 피해와 기능적 피해를 유발할 수 있으므로 전투피해평가의 측정대상이 된다고 할 수 있다. 이때 기밀성은 침해되었을 경우 그 자체로 사이버공간에서의 물리적 피해나 기능적 피해를 유발한다고 보기보다는 데이터나 시스템이 노출, 유출됨으로써 다른 피해를 유발하게 된다.

Table 1. Three elements of security and BDA[9]

| Classification | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Definition | Protection from random exposure, access of only authorized personnel | Protection from unauthorized changes | Available whenever rightful users want |
| Object | Data, system | File, data | System, file, data |
| Damage | Open to the public, exposure, leakage | Falsification, destruction | delay, unusable |
| BDA | Derived damage | Physical and functional damage | Physical and functional damage |

#### 3.1.2 사이버공간 구성과 피해평가

사이버공격에 대한 피해를 평가하기 위해서는 먼저 사이버공간이 어떻게 구성되어 있는가를 알아야 한다. 사이버공간 구성은 장원구[10]가 제안한 사이버공간 구성모델에 따라 물리, 논리, 데이터, 사회영역의 4개 Layer와 물리 네트워크와 지리적 요소, 논리 네트워크와 소프트웨어 논리, 일반 데이터와 중요/비밀 데이터, 인물정보와 사회활동의 8개 Component로 구성한다. 이제 각각의 구성요소를 피해

의 관점에서 정리하면 Table 2.와 같다. 스마트 폰과 그 지리적 위치와 같은 물리영역에서는 파괴나 소멸과 같은 피해를 입을 수 있기 때문에 물리적 피해와 기능적 피해가 발생하고 네트워크, 소프트웨어의 논리적 구성에 해당하는 논리영역에서는 기능중단, 기능저하, 오작동과 같은 피해가 나타날 수 있으므로 마찬가지로 물리적 피해와 기능적 피해가 발생한다. 인터넷 뉴스나 군사비밀과 같은  데이터 영역에서는 데이터 유출, 위조, 변조 등의 피해가 나타날 수 있으므로 사회인식적 피해나 파생된 피해가 나타날 수 있다. 인터넷 상에서 활동하는 가상인물과 이들의 활동을 나타내는 사회영역은 위장, 노출, 변조 등의 피해가 나타날 수 있으므로 사회인식적 피해가 나타날 수 있다. 마지막으로 이러한 피해가 확대될수록 개인과 사회를 넘어 국가에까지 영향을 미칠 수 있다.

사이버공격은 공격 형태에 따라 특정한 한 가지 영역에만 영향을 미치는 경우보다는 오히려 여러 영역에 걸쳐 있는 경우가 많다. 예를 들어 데이터를 훔치기 위해서는 관리자 권한 상승이나 버퍼 오버플로우 공격과 같이 네트워크, 서버, 메모리 등을 이동하여 결국 외부로 유출되므로 그 영향은 한가지에만 머무르지 않는다. 또 다른 예로 2016년 국방망 침투사건의 경우를 보면 적이 백신 중계서버와 국방망간의 접점을 통해 국방망에 침투하여 장기간에 걸쳐 은밀히 정보를 획득하고 군사비밀을 탈취한 사실이 드러났으며 이 사건은 국가적으로나 사회적으로나 큰 충격을 준 사건이었다. 또한 2017년 웹호스팅 업체 나야나 랜섬웨어 공격의 경우 해당 웹호스팅 업체에 기반을 두고 있는 업체들은 공격자의 렌섬웨어에 의해 웹 서버 내 파일들이 강제로 암호화됨으로써 영업 불능, 매출손실 및 이에 따른 기업이미지 하락을 겪었으며 유사한 다른 업체들은 대응방안을 마련하기에 이르렀다. 따라서 사이버공격에 대한 피해를 평가하려면 피해범위를 물리영역부터 사회영역까지 확대해야 한다.

Table 2. Components of cyber space and BDA[10]

| Domain | Component | Example | Damage type | Security-related element | BDA | Derived damage |
|---|---|---|---|---|---|---|
| Physical | Physical network | Server, network equipment | Destruction | Confidentiality, availability | Physical and functional damage | Derived damage (Individual, corporate, national security) |
| | Geographical element | Location | Destruction, extinction | Confidentiality, availability, integrity | Physical damage | |
| Logical | Logical network | Protocol | Function halt, degradation, | Availability, integrity | Physical and functional damage | |
| | Software logic | Operating system, Application program | Function halt, degradation malfunction | Confidentiality, availability, integrity | Physical and functional damage | |
| Data | General data | Advertisement, broadcasting, announcement | Falsification | Integrity | Social-cognitive damage | |
| | Critical/secret Data | Corporate and Military secrets | Deletion, exposure, falsification | Confidentiality, availability, integrity | Derived damage | |
| Social | Character | Virtual and real characters | Exposure, disguise | Confidentiality, availability | Social-cognitive damage | |
| | Social activity | SNS | Exposure, Falsification, disguise | Confidentiality, availability, integrity | Social-cognitive damage | |

### 3.1.3 사이버공간 구성과 표적

사이버공간에 대한 공격을 위해서는 표적선정이 매우 중요하다. 사이버 표적은 스마트 폰과 같은 작은 장비에서부터 선박, 항공기, 인공위성 등 크기도 다양하며 SCADA 시스템이나 다국적 기업처럼 광범위한 지역에 걸쳐 있기도 한다. 하지만 사이버 공간에서는 네트워크와 노드로 구분할 수 있다. 네트워크는 기간 통신망을 비롯하여 메쉬 형태로 얽혀져 있으며 노드는 장비나 시스템이 될 수 있다. 따라서 사이버 공격을 위해서는 군사목적에 적합한 표적을 선정하고 그 범위와 구성요소를 파악하여야 한다. 네트워크와 노드는 사이버공간 구성요소에서 물리영역과 논리영역에 해당하는 것으로서 사이버공간을 이루는 기본적인 요소이므로 일체적인 관점에서 판단해야 한다. 즉, 사이버공간은 근본적으로 운영체제와 응용소프트웨어로 동작하는 물리장비인 컴퓨터들을 네트워크를 동작시키는 프로토콜로 운영되도록 만들어져 있으므로 물리영역과 논리 영역은 별개가 아닌 하나의 구성으로 보는 것이다. 이 구성은 표적의 관점에서 보면 크게 기간 통신망인 네트워크와 이에 연결된 각종 시스템으로 구분할 수 있다. 이를 기반으로 네트워크상에서 사용자들이 데이터들을 주고 받으며 다양한 활동을 하는 것이고 이 과정이 발전해서 개인의 생각과 행동에 영향을 미침으로서 사회적인 활동이 파생되는 것이다. 따라서 사이버 표적은 네트워크, 시스템, 데이터, 사회인식으로 나누어진다.

### 3.1.4 피해복구

사이버 공격은 앞서 언급한 바와 같이 기밀성, 무결성, 가용성을 대상으로 공격을 실행하는 것이며 공격 시에는 기본적으로 시스템과 네트워크를 이용하는 것에서 부터 시작한다. 공격방법은 공격대상과 취약점에 따라 다양하게 변할 수 있으며 그 피해 또한 공격의 효과에 따라 다양하게 나타난다. 이때 피해복구 방안으로 네트워크나 시스템 전체를 교체할지, 부분적으로 교체할지, 소프트웨어에 대한 패치만 할지, 전면 교체할지 등을 결정해야 하는 데 전쟁 상황이나 시간적 여유가 충분치 않은 상황이라면 최대한 빠른 시간에 결정을 내려서 시스템 운영에 영향이 없도록 해야 한다. 다음으로 특정 시간과 장소에 사람들이 모여 논의하고 토론하던 과거와 달리 사이버 상에서는 시간적, 공간적 제약없이 실시간 여론형성과 같은 사회인식적인 측면이 발달해서 이제는 이로 인한 공포심과 스트레스를 유발하고 사망까지 유도할 수 있게 되었으며 이에 따라 사회에 대한 대규모 유언비어나 가짜뉴스 등으로 사회인식적 피해를 유발할 수 있게 되었다. 이와 같은 피해를 극복하기 위해서는 올바른 판단과 건전한 상식에 근거한 게시물을 게시하고 가짜뉴스, 유언비어 등은 신속히 삭제, 차단해야 하는데 사이버공간에서 이러한 조치에는 한계가 있으며 잘못된 정보로 인한 피해복구에는 사안에 따라 수개월이상이 걸리거나 복구가 불가능할 수도 있다.

## 3.2 사이버 표적

### 3.2.1 사이버 표적 선정

현대전에서는 최소의 노력으로 불필요한 희생을 줄이면서 최대의 효과를 얻기 위한 효과중심의 작전을 수행하는데 이를 위해서는 적을 하나의 거대한 복합체계로 인식하여 복합체계분석(SoSA: System of Systems Analysis)을 해야 한다. 복합체계는 여러 체계로 구성되어 있거나 체계 간에 연계성이 있는 것을 말하는데 Fig. 3.과 같이 적의 정치, 군사, 경제, 사회, 기반 구조, 정보체계들을 분석하여 의존성이나 강점, 약점을 찾아내어 적의 전체 체계에 영향을 미치도록 지식 기반을 구축하고 분석하는 활동이다.

또한 군사목적 달성을 위한 효과 중심의 작전을 펼치기 위해 군사력 외에도 외교, 정보, 경제의 요소

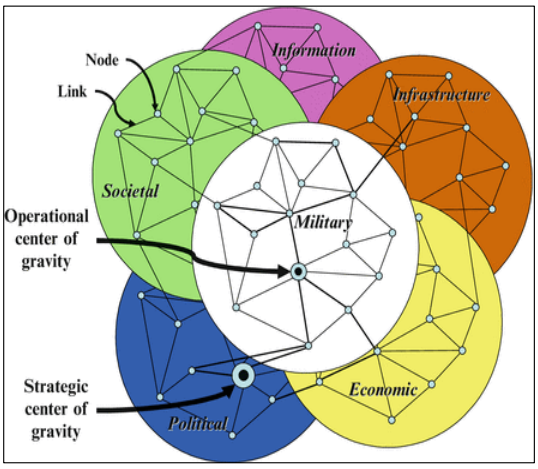


Fig. 3. The Interconnected Operational Environment[11]

가 종합적으로 작용하여야 한다. 이러한 요소들은 사이버공간에서 표현될 수 있으며 동시에 표적이 될 수 있다. 사이버표적은 앞서 언급한 바와 같이 네트워크와 시스템, 데이터, 사회인식으로 구성되는데 이러한 사이버 표적 분류가 실제로 적합한가에 대한 검증을 위해 설문조사를 실시하였다. 조사대상자는 Table 3.과 같이 사이버 국방/안보 또는 중요 공공기관, 연구기관, 대기업 등에서 관련 업무를 담당하는 전문가 21명(석사 학위 또는 근무경력 10년 이상)을 대상으로 2019. 8.29 ~ 10.29까지 개별 설문조사하였으며 설문내용은 부록과 같다. 설문방법은 네트워크와 시스템의 일체화된 관점과 사이버공간 구성을 고려하여 가급적 다양한 사이버 표적들을 선정하기 위해 과거 실제 피해사례 및 보안전문가들의 사이버 공격위협 경고대상을 중심으로 항목들을 구성하여 표적 가능성 유무와 위협순위를 조사하였으며 다음으로 부족한 표적들을 보완하기 위해 표적을 추가하도록 하여 최종적으로 다양한 표적들에 대해 적합성을 확인하였다.

설문조사 결과 제시된 항목들은 모두 사이버 표적이 될 수 있는 것으로 나타났으며 ⑭ 개인 PC, 스마트폰 등 장비, ⑯ 기업 개별컴퓨터, ⑲ 각 종 콘텐츠 등은 낮은 위협순위로 나타났다. 그 외 사이버 표적이 될 수 있는 기타의견으로 자율 주행차, 드론, 스마트시티, 스마트 팩토리, 스마트 그리드, 차량/선박, 수력/원자력 시스템, 교통망(철도/항공 등), 보안 관제센터, 병원 응급시스템, 우주/위성시스템, 클라우드 시스템, 대형 온라인 쇼핑몰이 제시되었는데 이를 분류해보면 네트워크와 시스템, 데이터, 사회인식이 사이버 표적 분류로 적합함을 알 수 있다. 여기서 네트워크와 시스템은 앞서 언급한 바와 같이 기간통신망과 여기에 연결된 시스템으로 구분하되 시스템의 구성요소와 연결 범위를 고려하여 군사작전 상 적정한 것으로 판단하는 것이 중요하다. 이에 따라 전투피해평가의 마지막 단계인 표적체계 평가는 적이라는 거대복합체계 속에서 선정된 표적의 피해에 따른 영향을 판단하는 것인데 이는 네트워크, 시스템, 데이터, 사회인식, 파생적 피해 평가를 종합하여 전체적인 관점에서 평가하는 것이다.

Table 3. Survey respondents

| Category | Bachelor | Master | Ph. D candidate | Ph. D |
|---|---|---|---|---|
| Private | 1 | 2 | | 2 |
| Public | 1 | 4 | 2 | |
| Military | 1 | 7 | 1 | |

#### 3.2.2 피해평가 판단기준

사이버공격에 따른 피해를 평가하기 위한 기준을 살펴보면 예를 들어 기간 통신망을 연결하는 케이블, 라우터 등은 사이버 공격시 경로로 이용되었다고 해서 무조건 바꾸거나 철거하는 것은 아니다. 공격 형태에 따라 대역폭을 늘리거나 프로토콜을 최신화해야 하며 공격자가 반드시 거쳐야 하는 방화벽, IDS, IPS를 교체하거나 그 안의 방어논리를 바꾸는 것을 고려하여야 한다. 각 종 시스템의 소프트웨어나 네트워크의 논리구성에 대한 공격으로 발생한 피해비용은 해당 취약점을 식별해서 패치 업무를 담당하는 인력의 인건비와 이들의 작업시간을 계산하여 평가하여야 한다. 또한 사이버공격에 따른 전투피해평가는 실제로 피해가 유발되는 것만 전투피해평가에 포함시킨다. 예를 들어 인증 및 세션 관리의 취약점을 이용하여 시스템에 침투하였더라도 네트워크, 시스템을 마비시키거나 중요 데이터를 유출, 변조와 같은 실질적 행위를 하지 못했다면 시스템에 대한 무단 침입으로 판단할 수는 있지만 실질적인 피해가 발생하지 않았으므로 패치를 통하여 취약점을 제거하되 전투피해평가에는 포함시키지 않는 것이다.

### 3.3 세부 전투피해평가 방안

#### 3.3.1 군사부문 전투피해평가

지금까지의 내용을 요약하면 Table 4.와 같으며 사이버공격에 의한 군사부문 전투피해평가는 다음과 같다.

$$\text{군사부문 사이버전투피해평가} = \sum \text{네트워크피해} + \sum \text{시스템피해} + \sum \text{데이터피해} + \sum \text{사회인식적피해}$$

네트워크 피해에는 완전 기능중단, 일시 기능중단, 기능 지연이 있으며 복구방안으로는 네트워크 대체, 복구, 우회가 있고 복구소요시간은 몇 시간에서 몇 일이 소요된다. 시스템 피해에는 기능저하, 기능

Table 4. Cyber targets and BDA[12]

| Attack object | Damage type | Content | Relevant domain | Military /civil | BDA method | Recuperation method | Recuperation time |
|---|---|---|---|---|---|---|---|
| Network | Complete halt | The network function is completely down and unusable until its recovery. | Physical and logical | Both | Physical and functional damage, cost | Replacement, repair, diversion | Hours ~ days |
| | Interruption | The network function is down during a certain time and unusable until its recovery. | | | | | |
| | Delay | Processing time is delayed due to excessive process input against the network bandwidth. | | | | | |
| System | Degradation | The working speed of the system considerably decreases and its overall performance (e.g., accuracy of information production) declines. | Physical and logical | Both | Physical and functional damage, cost | Replacement, repair | Hours ~ months |
| | Interruption | Certain or all functions of the system are down, during a certain time or a period of time, and unusable until their recovery. | | | | | |
| | Unauthorized use | Unexpected unknown results occur due to what is inserted (e.g. a program) by an intruder in the system. | | | | | |
| Data | Deletion | General/critical/secret data are deleted by attack. | Data | Both | Influence, cost | Recovery, replacement | Hours ~ unrecoverable |
| | Alteration | General/critical/secret data are randomly changed by attack. | | | | | |
| | Leakage | Critical/secret data are randomly leaked by attack. | | | | | |
| Social cognition | Turmoil | Situations of excessive disorder occur due to cyber-attack, fake news, and groundless rumors. | Social | Both | Indirect indicator | Stabilization | Days ~ unrecoverable |
| | Terror | Increased social turmoil leads to a situation of terror. | | | | | |
| Derivation | Individual damage | Getting out of residence, treatment, death, other pecuniary losses | Real world | Civil | Cost | Compensation, Stabilization | Days ~ unrecoverable |
| | Corporate damage | Stock price fluctuation, increase and decrease in sales, brand value fluctuation, bankruptcy | | | | | |

정지, 허가되지 않은 사용이 있으며 복구방안으로는 시스템 대체, 보수가 있으며 복구소요시간은 몇 시간에서 몇 개월이 소요된다. 이때 네트워크와 시스템에 대한 피해평가는 기존의 피해평가방법인 물리적 피해평가과 기능적 피해평가를 이용하여 평가한다. 다음으로 데이터 피해에는 데이터 삭제, 변조, 유출이 있으며 복구방안으로는 데이터 복구 또는 대체가 있고 최악의 경우 복구불가한 상황을 맞을 수 있다. 사회인식적 피해에는 사회적 혼란과 공포상황이 있으며 복구방안으로는 올바른 정보를 통한 안정화 방안이 있으나 최악의 상황에는 복구불가할 수 있다. 마지막으로 파생피해에는 사이버공간의 피해로부터 야기되는 현실세계에서의 개인피해와 기업피해가 있으며 복구방안으로는 금전적 보상과 치료와 같은 안정화 방안이 있으나 이 역시 최악의 경우 복구 불가할 수 있다. 지금부터는 각 피해를 좀 더 세부적으로 파악해 본다.

### 3.3.2 네트워크 피해

사이버 표적으로서 네트워크는 기간 통신망과 같은 순수 네트워크 구조를 의미한다. 네트워크를 기반으로 하는 공격 형태를 살펴보면 스니핑과 같은 네트워크 상의 패킷을 가로채는 공격, 정보 수집을 위한 네트워크 스캐닝 공격, 그리고 DOS와 같은 네트워크 서비스 거부 공격이 있다. 여기서 네트워크 패킷을 절취하는 것은 궁극적으로 데이터에 대한 공격이므로 데이터부문에서 다룰 것이고, 스캐닝 공격은 사전 정보 수집을 위한 것으로 실제 피해를 유발시키지 않으므로 실질적인 네트워크에 대한 피해는 서비스 거부이다. 네트워크 상에서 발생할 수 있는 피해는 물리적으로는 완전파괴, 부분 파괴가 있고 기능적으로는 완전한 기능중단, 부분적인 기능중단 그리고 기능저하를 들 수 있다. 물리적, 기능적 피해시 전장상황과 같은 분초를 다투는 상황에서 네트워크를 포기해야 할 것인지, 우회할 것인지, 긴급히 피해지점을 찾아 수리해야 할 것인지 결정해야 하며 최악의 상황으로 네트워크를 포기해야 할 때에는 ad-hoc과 같은 긴급 네트워크 구성을 고려해야 한다. 따라서 네트워크 피해는 Table 5.와 같이 민간분야에서는 네트워크 장비 대체 비용 또는 긴급 보수비용으로 구분할 수 있으며 군사부분에서 전투 피해평가는 가동율로 나타낼 수 있다.

Table 5. Network damage assessment

| Classification | Content | Damage standard | |
|---|---|---|---|
| | | Civil | Military |
| Physical damage | Complete destruction | Replacement cost | Operating rate |
| | Partial destruction | | |
| Functional damage | Complete halt | Cost of repair, replacement | |
| | Partial halt | | |
| | Degradation | | |

### 3.3.3 시스템 피해

대부분의 시스템들은 기간망에 연결되어 산업, 행정, 국방 등의 업무에 사용된다. 각 종 시스템들은 특정한 지역에 모여 있는 게 대부분이지만 SCADA나 다국적 기업 같은 거대 조직이나 시스템들은 매우 광범위한 지역에 산재해 있다. 사이버 표적으로서 이러한 시스템들은 네트워크에 연결된 장비 같은 단순 노드 형태인지 또는 기간 통신망이나 일부의 네트워크를 포함하는 거대 복합체인지 구분되어야 한다. 시스템 또한 Table 6.과 같이 사이버공격에 따라 물리적 피해와 기능적 피해로 구분할 수 있으며 완전파괴시에는 시스템으로서의 기능을 못 하게 되고 복구시간도 몇 개월 이상 소요될 수 있다. 시스템의 기능적 피해는 데이터를 통하여 시스템을 공격하는 Modification, Fabrication, Interception과 시

Table 6. System damage assessment

| Classification | Content | Damage standard | |
|---|---|---|---|
| | | Civil | Military |
| Physical damage | Complete destruction | Replacement cost | Operating rate |
| | Partial destruction | | |
| Functional damage | Complete halt | patch/ reinstallation | |
| | Partial halt | | |
| | Degradation | | |
| | Malfunction | | |

스템 기능 자체를 공격하는 Degradation, Interruption, Unauthorized ues로 구분된다.[12] 데이터를 통한 공격은 데이터 피해부분에서 다룰 것이므로 시스템에 대한 전투피해평가는 네트워크와 마찬가지로 군사분야에서는 가동율로 평가할 수 있으며 민간분야에서는 비용으로 계산될 수 있다.

### 3.3.4 데이터 피해

데이터 피해는 Table 7.과 같이 데이터 저장매체에 대한 파괴와 데이터 자체의 파괴, 변조, 유출로 나뉠 수 있다. 따라서 물리적인 피해기준은 데이터 저장매체에 대한 보상비용이 되고 기능적 피해는 존재하지 않는 대신 데이터 자체의 가치와 영향력에 따른 피해가 존재하며 특히 중요/비밀 데이터로 인해 발생한 피해에 대한 복구는 대체로 어렵거나 불가능한 것이 대부분이다. 중요/비밀데이터의 가치와 영향력은 천차만별일 것이나 군사부문의 데이터인 군사비밀을 고려해보면 미국의 경우 군사비밀은 Top Secret, Secret, Confidential로 구분하고 있으며 우리나라는 이와 유사한 Ⅰ,Ⅱ,Ⅲ 급으로 구분하고 있다. 비밀은 그 등급이 높을수록 국가안위와 직결되는데 우리나라에서 비밀의 금전적 가치는 장월수[13]의 군사비밀 유출에 따른 피해금액 산정을 위한 모델 연구에서 주장한 바에 의거한다. 민간부문의 중요정보인 개인정보, 영업/기업비밀, 콘텐츠 등은 비용으로 계산되어 질 수 있다. 그 외 네트워크나 시스템 상의 정보유출도 이와 같은 중요 데이터이거나 사이버 공격을 위해 수집하는 정보로 구분할 수 있다.

Table 7. Data damage assessment

| Classification | Content | Damage standard | |
|---|---|---|---|
| | | Civil | Military |
| Physical damage | Damage to Storage medium | Cost | Influence |
| Data damage | Deletion | Cost | |
| | Alteration | | |
| | Leakage | | |

### 3.3.5 사회인식적 피해

과거에는 대형사건, 사고와 같이 사회적으로 관심이 될 만한 큰 일 들이 발생하면 TV 뉴스, 전화나 대면접촉을 통해 전파되었으나 현재에는 인터넷과 스마트폰 등을 통하여 전파되는 속도가 예전과 비할 수 없을 정도로 빨라졌다. 동시에 해당 사건에 대한 다각적인 분석 또한 곧이어 올라오고 이에 대한 다양한 평가나 주장들이 많이 게시된다. 이 가운데는 물론 정도에 의한 올바른 판단과 정확한 분석을 통한 깊이 있는 내용도 많지만 흥미위주의 태도와 단편적이고 저급한 의식에 의한 정제되지 않은 잘못된 내용도 많이 확산되고 있다. 따라서 이와 같은 사회인식적 피해가 발생하였을 때에는 잘못된 정보를 빠른 시간 내에 바로잡을 수 있는 안정화 방안이 피해복구 대책이 된다. 사이버공간에서는 이와 같은 단순한 혼란 외에도 특정 목적을 가지고 사회적 혼란이나 더 나아가 공포를 유발하기 위한 목적의 사이버공격이 발생하고 있다. 2014년 12월에 발생한 한수원 해킹 사건이 대표적인 예로써 북한으로 추정되는 해킹세력이 한수원 내부자료를 공개하며 원전가동중단 및 파괴 협박까지 시도한 사례가 있다. 이 사건은 해킹세력의 요구와 대응이 의도적, 지속적으로 공개됨으로써 사회적 혼란을 넘어서 상황이 완전히 해소될 때까지 국민들에게 원자력 발전소가 실제로 가동중단 또는 파괴될지도 모른다는 불안감을 심어주었다. 이러한 모든 것들이 바로 사이버공격으로부터 발생하는 사회인식적 피해인 것이다. 이러한 피해를 측정하는 방법으로는 Table 8.과 같이 소셜 네트워크 서비스에 대한 빅데이터 분석, 대형 포털사이트의 실시간 검색순 위 및 지속 기간 확인, 인터넷 뉴스 분석 등이 있다.

Table 8. Social-cognitive damage assessment

| Classification | Content | Damage Standard | |
|---|---|---|---|
| | | Civil | Military |
| Social-cognitive damage | Turmoil | ·SNS big data analysis<br>- Key word, frequency<br>·Search word service of portal sites<br>- Area, search word, ranking, period of time<br>·News and article analysis<br>- Topic, frequency | |
| | Terror | | |

#### 3.3.6 민간부문 전투피해평가

사이버공격에 의한 군사부문 피해평가에 이어 민간부문에서의 피해 평가는 다음과 같다.

$$\text{민간부문 사이버전투피해평가} = \text{군사부문 피해} + \sum \text{파생된 피해}$$

즉, 군사부문 피해평가에 파생적 피해평가를 더한 것인데 이 때 실제 전투피해평가는 군사부문과 달리 비용으로 계산된다. 파생적 피해평가는 Table 9.와 같이 네트워크와 각 종 시스템이 파괴되거나 기능이 저하되고 데이터가 삭제, 유출되며 사회적 혼란이 야기됨으로써 비롯되는 모든 피해를 말한다. 개인적인 피해로서는 우선 기간망, 시스템 고장에 따라 단순한 불편과 답답함에서부터 개인 사업 결재 불능으로 인한 매출하락, 금융기능 마비로 인한 손해, 이로 인한 불안감, 스트레스 발생과 치료 등 금전적 비용이 발생하고, 기업측면에서는 주가변동, 매출하락에 따른 브랜드 가치하락에 이어 폐업이라는 최악의 상황까지 맞을 수 있다. 이는 생필품 판매 증가량 또는 교통량, 승객 변동량, 병원 치료환자 증가량 등으로 나타나며 비용으로 계산되어질 수 있다. 그리고 기업들의 주가하락이나 기업브랜드 가치 하락, 매출 감소액 등 역시 비용으로 계산되어 질 수 있다.

Table 9. Derived damage assessment

| Classif-ication | Content | Damage standard | |
|---|---|---|---|
| | | Civil | Military |
| Derived damage | Individual damage (Getting out of residence, stockpiling daily necessities, financial transaction restriction, bankruptcy, treatment, death, etc) | Cost | - |
| | Corporate damage (Increase and decrease in sales and stock price, brand value fluctuation, bankruptcy, business closure, etc) | | |

### 3.4 사이버 전투피해평가 제안 및 적용

#### 3.4.1 사이버 전투피해평가 제안

지금까지 분석한 내용을 종합하여 사이버 공격에 의한 전투피해평가는 다음과 같이 제안한다. 사이버 전투피해평가는 Fig. 4.와 같이 군사목적에 의해 선정된 사이버 표적에 대하여 먼저 사이버공간을 이루는 가장 기본요소인 네트워크와 네트워크에 연결된 노드인 시스템에 대하여 유형의 요소로서 기존의 물리적 피해와 기능적 피해평가를 이용하여 가동율로 평가한다. 그리고 무형적 요소인 데이터와 사회인식적 피해는 영향력과 간접지표를 이용하여 평가한다. 그 외 사이버 공간은 현실공간과 연결되어 있으므로 사이버공간의 피해로 인해 파생된 현실세계의 피해를 평가하고 이를 모두 통합하여 적이라는 거대한 복합표적체계에서 종합적인 표적체계평가를 하는 것이다. 본 논문에서 제시한 사이버 전투피해평가 방안은 이전에는 제한적으로만 가능했던 것에 비해 미 교범상의 전투피해평가 이론을 이용하여 사이버 공간을 중심으로 포괄적이고 구체적인 방안을 제시하였다는 데 그 의의가 있으며 동시에 민간부문에서의 피해를 쉽게 이해할 수 있는 비용으로 표현함으로써 사이버공격에 의한 피해발생시 기업에서 활용할 수 있게 하였다.

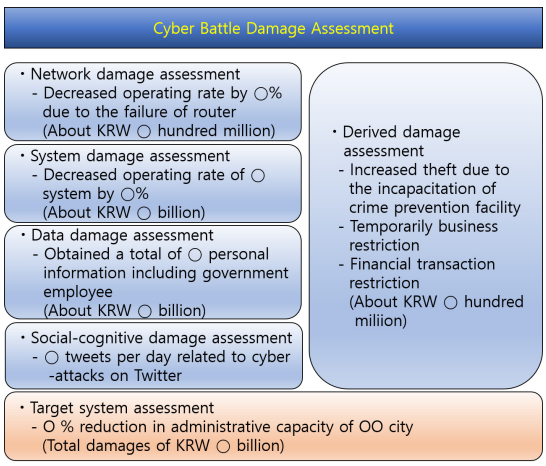


Fig. 4. Cyber Battle Damage Assessment

Table 10. Application of BDA

| Classif-ication | Content of attack | Battle damage assessment |
|---|---|---|
| 6.25 cyber terror | From 25 June to 1 July, 2013, servers of broadcasting and newspaper companies were destroyed, homepages of the Blue House, the Office of Government Policy Coordination, and so on were falsified, and DDOS attack occurred to National Computing and Information Agency | ·Network damage : None<br>·System damage<br>- DDOS attacked websites: 8<br>(○% operating rate as of ○ o'clock, About KRW ○ hundred million)<br>- Destroyed system hard disks : 150 (About KRW ○ billion)<br>- Estimated recuperation time: ○ days<br>·Data damage : About KRW ○○ billion<br>- Websites having homepage data falsified: 47<br>- Personal information leakage : 3.04 million<br>·Social-cognitive damage: turmoil<br>- Relevant Tweets: ○ ten thousand per day<br>- Relevant Internet news: ○ per day<br>- Search words on large portal sites (e.g. Naver): DDOS, etc. were ranked ○ in search words and placed within the top 10 for ○ days.<br>·Derived damage: Inconvenience.<br>*Target system assessment<br>- 84% operating rate as of July 4 in the broadcast, media and government function<br>- Total damages of KRW ○○ billion |

### 3.4.2 사이버전투피해평가 적용

이제부터 과거에 발생한 사이버공격 사례에 대하여 본 논문에서 제안한 전투피해평가 방법을 적용한다. 적용사례는 2013년 발생한 6.25 사이버테러 사건으로서 북한으로 추정되는 해킹세력에 의해 우리의 방송, 언론, 정부 기관이 공격을 당한 사례로서 당시 명확히 드러난 피해는 Table 10.과 같이 홈페이지 변경, 시스템 파괴, 개인정보 유출, 정부기관에 대한 DDOS공격으로 인한 기능마비 등이 있다[14][15][16]

## IV. 결 론

IoT, 4차 산업혁명시대를 맞아 사이버공간은 한 단계 더 고도화되고 있으며 이에 따라 보호해야 할 사이버공간의 범위도 더욱 확장되고 있다. 사이버 공격은 본래 사소하고 간단한 것에서부터 시작되었지만 어느 순간부터 인명피해를 포함한 막대한 금전적 피해를 발생시킬 수 있을 정도로 파괴력이 증가하였다. 이러한 상황 하에서 지능적이고 정교한 사이버공격 위협이 계속 증가할 것이고 공격에 따른 피해발생과 그 영향력 또한 급속히 증가할 것이다. 본 논문에서는 사이버 공격에 따른 전투피해평가방안으로 사이버 표적에 대한 물리적 피해, 기능적 피해, 데이터 피해, 사회인식적 피해, 그리고 파생적 피해로 구분하고 이를 종합함으로써 표적체계평가를 수행하는 방안을 제안하였다. 이를 통하여 그간 제한적이고 제각각이었던 사이버전에서의 전투피해평가 방안이 보다 명확하고 효과적으로 이루어질 것으로 기대한다. 또한 본 논문에서는 포괄적인 전투피해평가 방안을 제시하였지만 향후 각 부문별 보다 정밀한 전투피해평가 방안이 수립되어 보다 정교한 사이버작전 수행이 가능하도록 해야 할 것이다.

## References

[1] Wansoo Cho, Taekyu Kim, "Modeling and Simulation of Cyber Damage Assessment for Cyber Warfare Effectiveness Analysis", JKIIE-S'16, pp. 3119-3125, Apr. 2016.

[2] Duhoe Kim, Yonghyun, Kim, Dongkyoo Shin, "Cyber Battle Damage Assessment Framework", KIPS-F'17, pp. 178-181, Nov. 2017.

[3] SeungKeun Yoo, "Comprehensive Approach to Evaluate the Damage of Cyberattack on the Defense Mission

System", KSS-F'18, pp. 1-11, Dec. 2018.
〔4〕 Kihwan Kim, Wanju Kim, "A Study on Simulation-Based Worm Damage Assessment on ATCIS", Journal of the Korea Institute of Military Science and Technology 11(1), pp. 43-50, 2007.
〔5〕 Youngbae Jeon, Hyunsook Jeong, Insung Han, "An Asset-Mission Dependency Model Adaptation and Optimized Implementation for Efficient Cyber Mission Impact Assessment", KIISE Transactions on Computing Practices 23(10), pp. 579-587, 2017.
〔6〕 Jungho Kang, "Effective Cyber Operation Combat Damage Evaluation Model Design through Tactical Network Integrated Operation", Journal of Security Engineering 14(1), pp. 1-8, 2017.
〔7〕 Sunyoung Im, Hyunsook Jeong, "Damage Assessment for Cyber Assets", KICS-S'18, pp. 310-311, Jun. 2018.
〔8〕 Joint Staff, CJCSI 3162.02: Methodology for Combat Assessment, Joint Staff, Washington D.C., pp. B-1 B-5, 2019.
〔9〕 AhnLab, "AhnLabSabo Security World", https://blogsabo.ahnlab.com/743, 2019. 12.1
〔10〕 Wongu Jang, "Bigdata Governance Model for Effective Operation in Cyberspace", The Korea Journal of Bigdata 4(1), pp. 47, 2019.
〔11〕 Joint Staff, Joint Publication 3-0: Joint Operations, Joint Staff, Washington D.C., pp. IV-4. 2018.
〔12〕 Hyeonsu Youn, Yonghyun Kim, Donghwa Kim, Dongkyu Shin. "Development of Risk Index of Cyber Attack and Damage Assessment Priority Calculation Measures", KIPS-F'17, pp. 224-227, Nov. 2017.
〔13〕 Worlsu Jang, "A Study on a Model for Estimating Damage Costs Emanating from Leakage in Military Secrets", Ph.D. Thesis, Korea University, pp. 37. Aug. 2012.
〔14〕 "67 cyberattacks from 6.25 Cyberterror …14 information destruction", joongan gilbo, 2013. 7. 4, https://news.joins.com/article/ 11981111
〔15〕 "7·7 DDoS, 6.25 Cyberterror, KHNP Hacking Psychological Warfare…Over and over again cyberattacks", etnews, 2017. 2. 21, http://www.etnews.com/20170221000305
〔16〕 Red Alert, "6.25 Cyber terror analysis report", NSHC, 2013.

## 부록 - 사이버 표적관련 설문조사

### 1. 일반적 특성 및 계층구성

1-1) 귀하의 소속 기관은 무엇입니까?
① 민간부문(대학/연구기관, 기업)
② 공공부문(정부/공공기관)
③ 군사부문(군/국방)

1-2) 귀하의 학력은 무엇입니까?
① 학사 ② 석사
③ 박사수료 ④ 박사

1-3) 귀하의 근무기간은 몇 년입니까?
① 5년 이하
② 5년 초과 ~ 10년 이하
③ 10년 초과 ~ 15년 이하
④ 15년 이상

### 2. 사이버 표적 설문조사

2-1) 다음 중 사이버전 상황 하에서 적의 사이버공격을 시행할 때 선정할 수 있는 표적이 될 수 있는 것만을 골라 공격 가능성이 높은 순위로 정렬해 주시기 바랍니다.(표적이 될 수 없다면 표기하지 않음)

① IoT(가전제품 등)
② 머니(은행),사이버 머니(비트코인 등)
③ 기간 통신망
④ 국방 비밀망 (지휘통제망, 방공망 등)
⑤ SCADA (기간통신망 제외한 전력, 상/하수, 석유, 가스 등)
⑥ 군사비밀
⑦ 사회혼란 (가짜뉴스, 유언비어 등)
⑧ 기업 비밀 또는 영업 비밀 (반도체,자동차 등)
⑨ 개인 정보, 사생활 (신용카드 번호 등)
⑩ 각 종 기업서버 (웹 서버, 메일 서버, ftp서버 등)
⑪ 정부망,정부기관, 공공기관
⑫ 금융망,금융기관
⑬ 사이버 주변환경 (출입통제 시스템, 무정전 전원장치, 차폐벽 등)
⑭ 개인 PC, 스마트 폰 등 장비
⑮ 고위공직자, 중요 인사 개인 PC, 스마트폰 등
⑯ 기업 개별컴퓨터 하드디스크 등 시스템 자체
⑰ 비밀망을 제외한 기타 국방망 (복지, 인사, 병무 군수 등)
⑱ 컴퓨터관련 업체 (보안업체, PC 및 S/W생산업체 등)
⑲ 각종 콘텐츠 (미개봉 영화, 노래, 기타 내부 자료 등)
⑳ 방송, 언론사

( , , , , , , , , , , , )

2-2) 위 항목 외에 사이버 표적이 될 수 있거나 별도 항목으로 구성해야 하는 자산이 있다면 무엇입니까? ( )

## 〈저자소개〉

장 원 구 (Won-gu Jang) 정회원
1996년 2월: 공군사관학교 전산학과 학사
2011년 2월: 아주대학교 정보통신대학원 석사
2014년 9월~현재: 고려대 정보보호대학원 박사과정
〈관심분야〉 사이버정보, 사이버안보, 빅데이터

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대 정보경영대학원 박사
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호 정책