Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.905

사이버무기 분류체계에 관한 시론

이 용 석,[1†] 권 헌 영,[1] 최 정 민,[2] 임 종 인[1‡]

[1]고려대학교, [2]서강대학교

A Study on the Cyber Weapons Classification System

Yongseok Lee,[1†] Hunyeong Kwon,[1] Jeongmin Choi,[2] Jongin Lim[1‡]
[1]KOREA University, [2]SOGANG University

요 약

주권국가는 외국으로부터 영토에 대한 침해를 받으면 자위권을 발동하거나 안보리 승인을 받아 전쟁을 할 수 있는 권리를 가진다. 전쟁은 자위권의 필요성과 비례성의 원칙하에 진행된다. 사이버공격 발생 시 공격수단과 효과 분석을 통해서 비례적 대응을 하여야 하며, 이를 위하여 사이버무기에 대한 분류가 필요하다. 따라서 본 연구는 사이버무기에 대한 정의와 분류기준을 제시함으로써 자위권 조치를 위한 필요성과 비례성에 따라 합리적이며 합법적인 대응을 가능케 하고자 한다. 본 연구에서는 사이버무기를 『군이 작전목적에 따라 사이버공간에서 사이버기술을 사용하여 정보수집, 공격, 방호활동 등을 하는 수단』으로 정의하였다. 또한 기존의 무기체계 현황과 공개된 사이버무기 사용 사례를 바탕으로 사이버무기를 ① 정보수집(획득)용 사이버무기, ② 공격(제압)용 사이버무기, ③ 방호용 사이버무기로 분류하였다. 이러한 기능적 분류에 따라 비례적 대응을 적용하기 위한 고려사항을 제시하였다. 향후에는 사이버공격에 대한 비례성 원칙을 보장하기 위해서 사이버무기 효과에 기반 한 등급화 연구가 이루어져야 하며, 본 연구는 비례성 원칙의 한 축을 이루는 사이버무기의 분류에 관한 탐색적 연구를 하였다는데 그 의의가 있을 것이다.

ABSTRACT

The sovereign state has the right to engage in self-defense or war with the approval of the Security Council when it receives an invasion of territory from a foreign country. War is conducted under the principle of the necessity and proportionality of self-defense. In case of cyber attack, proportional countermeasure must be made through attack means and effect analysis, and cyber weapons need to be classified for this purpose. Therefore, this study aims to provide a rational and legitimate response according to the necessity and proportionality of the self - defense right by suggesting definition and classification criteria of cyber weapons. In this study, cyber weapons were defined as "means of collecting, attacking, and protecting information using cyber technology in the cyber space according to military objectives. Based on existing weapon systems and public cyber weapons cases, cyber weapons were classified as ① cyber weapons for information gathering, ② cyber weapons for attack, and ③ cyber weapons for protection. We suggest the considerations for applying the proportional response according to this functional classification. In order to guarantee the principle of proportionality to cyber attacks in the future, the classification study based on the cyber weapon effect should be conducted. This study has conducted an exploratory study on the classification of cyber clusters which constitutes one axis of the proportionality principle.

Keyword: Cyber weapons, Cyber weapons classification, Kind of Cyber weapons

Received(03. 06. 2018), Modified(1st: 05. 30. 2018 2nd: 07. 09. 2018), Accepted(07. 09. 2018)

† 주저자, hong@paper.hankook.ac.kr
‡ 교신저자 jinlim@korea.ac.kr(Corresponding author)

I. 서 론

사이버공간이 활성화되고 이로 인한 사건과 피해가 빈발함에도 불구하고 사이버무기에 대한 연구는 부족하다. 이는 사이버무기가 컴퓨터 프로그램이 가능한 사람들에 의해 손쉽게 개발이 가능하기도 하고 사이버무기를 개발하였다고 해도, 그것을 물리적인 무기처럼 화력시범을 보이거나 퍼레이드를 통해 과시할 수 없기 때문이다. 또한 사이버무기는 가용성 측면에서 1회성에 가깝다. 한 번 사용된 사이버무기는 그 취약성이 노출되어 쉽게 패치가 가능하고 대응방안 및 방호태세를 갖출 수 있기 때문이다.

사이버무기는 다음과 같은 특성〔1〕을 가진다. 첫째, 비정형성이다. 사이버무기는 사이버공간에서 주고받는 명령어인 컴퓨터 언어로 제작되어 물리적 정형성을 갖지 않는다. 둘째, 광범위성이다. 사이버무기는 네트워크상에서 활동하기 때문에 백신에 의한 제거활동이 개시되기 전에는 지속적인 감염과 전파가 필연적이다. 따라서 즉각적인 방호활동을 통해 네트워크를 보호하는 조치를 필요로 한다. 셋째, 개발의 은밀성과 신속성이다. 통상 물리적 무기의 경우 개발을 위해서는 무기의 필요성 제기-개념/선행연구-작전운용성능(ROC : Required Operational Capability) 구체화-개발착수-개발/시험평가-전력화의 단계를 거친다. 그러나 사이버무기는 사이버공간에서 제작되기 때문에 외부에 드러날 가능성이 없고 따라서 무기개발도 은밀하게 이루어진다. 또한 개발 후에도 은밀하게 보유하고 사용되어 전쟁의 책임에서도 회피하고자 한다. 넷째, 다양한 파괴성이다. 사이버무기는 물리적 환경에 대한 은밀한 공격으로 나타나기 때문에 심리적인 공포감을 극대화하고 심리적인 극심한 마비를 달성할 수 있기 때문에 의지전의 무기라고도 할 수 있다.

사이버무기의 이러한 특성으로 인해 피해 즉시 무엇에 의해 공격을 받았는지도 모르고, 피해규모 또한 시간이 지나가면서 증가하기 때문에 공격받은 당시에는 공격수단과 규모를 알 수 없다. 이는 비례성의 원칙에 의한 대응을 어렵게 한다. 따라서 사이버적인 침해가 테러와 범죄수준을 넘어서서 국가 간의 공격의 수준에까지 이른 현 시점에서 사이버무기에 대한 정의와 분류기준은 정당한 대응을 위하여 반드시 필요하다고 할 것이다. 본 연구는 사이버무기에 대한 정의와 사이버무기의 분류기준을 제시하고 이를 통해 비례적 대응을 위한 고려사항을 제시하고자 한다.

II. 사이버무기의 분류 및 분류의 필요성

2.1 일반적인 무기의 분류

일반적으로 무기의 분류는 운용목적, 용도 및 필요성 등을 고려하여 분류한다〔2〕. 첫째, 군사작전에 직접 운용되거나 전투력발휘에 직접 영향을 미치는 장비·물자, 둘째, 무기체계의 전투력 발휘에 영향을 미치는 장비·물자, 셋째, 전투력 발휘에 영향을 미치는 주요 전술훈련장비 및 소프트웨어(이하 SW), 관련시설 등이다.

방위사업법〔3〕 제3조 3항에서는 '무기체계'를 유도무기·항공기·함정 등 전장에서 전투력을 발휘하기 위한 무기와 이를 운영하는데 필요한 장비·부품·시설·SW 등 제반요소를 통합한 것으로서 대통령령이 정하는 것을 말한다고 정의하고 있다. 동법 시행령〔4〕 제2조에는 무기체계를 8종으로 대분류하고 있다. 1. 통신망 등 지휘통제·통신 무기체계, 2. 레이다 등 감시·정찰무기체계, 3. 전차·장갑차 등 기동무기체계, 4. 전투함 등 함정무기체계, 5. 전투기 등 항공무기체계, 6. 자주포 등 화력무기체계, 7. 대공유도무기 등 방호무기체계, 8. 모의분석·모의훈련 SW, 전투력지원을 위한 필수장비 등이다.

국방부훈령에서 무기체계에 대한 정의는『전력발전업무훈령』제3절에 기록되어 있다. 여기에서는 무기체계를 '유도무기, 항공기, 함정 등 전장에서 전투력을 발휘하기 위한 무기와 이를 운영하는데 필요한 장비, 부품, 시설, SW 등 제반요소를 통합한 것을 말한다.'고 정의하였다. 무기체계 분류는 대분류, 중분류, 소분류로 구분한다. 대분류는 지휘통제·통신무기체계(중분류 3, 소분류 11), 감시·정찰무기체계(중분류 6, 소분류 19), 기동무기체계(중분류 6, 소분류 16), 함정무기체계(중분류 4, 소분류 21), 항공무기체계(중분류 4, 소분류 17), 화력무기체계(중분류 7, 소분류 22), 방호무기체계(중분류 3, 소분류 7), 그 밖의 무기체계(중분류 3, 소분류 7) 등 8종으로 분류하였다.

2015년 8월에 개정된 동 훈령에 '사이버작전체계'가 추가되면서 사이버체계의 대부분이 서버, 네트워크, 단말기 등으로 구성되어 지휘통제체계와 유사하고 사이버작전이 합참 수준의 작전임을 고려하여 「합동지휘통제체계」로 분류하기 시작하였다. 그러나 대분류(지휘통제통신체계 무기체계), 중분류(지휘통제체계), 소분류(합동지휘통제체계)하고 대상 장비를

KJCCS, MIMS, 사이버작전체계로 한정함으로써 사이버 전 영역에 걸쳐 운용되는 현실과는 다소 괴리가 있는 분류라고 할 수 있다.

세계적으로 권위를 인정받는 영국의 제인연감은 먼저 군을 분류하고 각 군에서 사용하는 병종별 무기체계로 구분한다. 한국판 제인연감이라는 한국군 무기연감(2016~2017)[5] 역시 무기체계를 육군, 해군, 공군, 해병대로 구분하여 각 군에서 사용하는 병종별 무기체계로 구분하였다. 예를 들어 육군 무기체계의 경우 소총, 전차, 장갑차, 화포·대공화기, 헬기, 대공·대전차 미사일, 현무 미사일 등으로 분류하고 있다. 그러나 사이버무기의 위력에도 불구하고 육·해·공군 무기체계에 대한 분류 외에 사이버무기에 대한 분류는 미흡한 실정이다.

2.2 사이버무기의 분류 필요성 : 비례대응

사이버공간에서의 주권은 어떻게 지켜낼 수 있을 것인가? 기존의 주권은 주로 물리적 공간에서 논의되었으나 최근 IT기술의 발전으로 인하여 사이버공간에서의 주권 문제가 대두되었다. 일반적으로 주권국가는 외국으로부터 영토에 대한 침해를 받으면 자위권을 발동하거나 안보리 승인을 받아 전쟁을 할 수 있는 권리를 가진다. 전쟁은 자위권[6]의 필요성과 비례성의 원칙하에 진행된다. 자위권은 공격을 받은 후에 발동하는 반격(Reactive)이 우선 고려되지만 합리적 추정에 의한 선제공격(Proactive)과 예방공격(Preemptive)으로 구체화 될 수 있다. 이것은 헌법에 명시된 국가의 의무인 국민의 생명과 재산을 보호하는 구체적인 행위라고 할 수 있다.

2007년 러시아가 에스토니아에 대한 사이버공격을 감행함에 따라 2009년 탈린(에스토니아 수도)에 국제 전문가 그룹이 모여 사이버국제법으로서의 '탈린매뉴얼'을 작성하였다. 탈린매뉴얼은 사이버공간에서 발생한 악의적인 국가 간 행위를 사이버전쟁으로 규정하였다. 이에 따라 국가는 사이버공격에 대한 공격수단과 효과분석을 통해 비례적 대응을 하여야 하며, 이를 위해 사이버무기의 분류 필요성이 대두되었다. 이하에서는 사이버무기 분류 이전에 사이버공격에 대한 자위권, 자위적 조치에 대한 필요성과 비례성을 살펴보고자 한다.

사이버공간에 대한 국제적 규범이라고 할 수 있는 『탈린매뉴얼』의 제1부는 국제 사이버 안보법이다. 이 법 규칙 13은 사이버공격에 대한 자위권에 대하여 14는 자위권 행사의 필요성과 비례성[7]에 대하여 설명하고 있다.

규칙 13- 무력 공격에 대한 자위

무력 공격의 수준에 이르는 사이버공격의 목표가 된 국가는 자위의 고유한 권리를 행사할 수 있다.

사이버 작전이 무력 공격을 형성하는지 여부는 그 규모와 효과에 따라 결정된다.

규칙 14-필요성과 비례성

자위권의 행사에 있어 일국이 취한 사이버 작전을 포함하는 무력 사용은 반드시 필요하고 비례적이어야 한다.

첫째, 자위권과 관련하여 국제연합헌장이 인정하는 관습법상의 자위권은 일국이 무력공격으로 인정되는 사이버작전을 수행하거나, 그 장소와 무관하게 비국가적 행위자가 사이버작전을 지시하는 경우 기준을 충족한다고 본다[8]. 자위권의 범위는 물리적인 무력공격을 넘어서 사이버작전 전반을 포괄하는 무력공격에까지 미친다.

둘째, 탈린매뉴얼에서 말하는 필요성은 무력의 사용이 긴박한 무력공격을 성과적으로 방어하거나 진행중인 무력공격을 파쇄 시키기 위한 불가피한 수단이어야 함을 말한다. 사이버공간에서의 필요성은 무력사용을 하지 않아도 되는 대안을 가지고 있느냐 없느냐에 달려있다[9]. 따라서 필요성은 당연히 피해국의 관점에서 판단되어야 하며 합리적이어야 한다[10].

셋째, 비례성은 사이버무력으로 대응할 때 어느 정도의 무력을 허용할 것인가를 정하는 것이다. 비례성을 다룰 때는 자위권의 행사를 정당화하는 방어적인 대응규모, 기간, 강도, 범위를 제한한다. 비례성은 과소해서도 안 되지만 과도한 것은 더욱 거부된다. 사이버작전은 목적에 부합되어야 하지만 사이버공격자의 추가적인 사이버공격[11] 의도를 분쇄시키기 위한 물리적인 작전이 완전히 거부되는 것은 아니다.

비례대응을 하려면 적성국가의 공격수단과 효과에 대하여 정확히 파악하고 있어야 한다. 사이버공간에서 비례대응의 원칙을 지킨다는 것은 공격당한 국가의 자존심을 지키면서 확전을 방지하기 위한 것[12]이다.

III. 사이버무기 정의와 사이버무기 사용 사례

3.1 사이버무기 정의

현재 사이버무기의 정의에 대한 국제적인 공감대는 없으며[13], 2011년 11월 미 국방성의 내부문서에도 합의가 없다는 것을 지적한 바 있다.[14] 우리나라에서 사이버작전을 위한 군의 가장 권위 있는 문서는 합동교범 3-24『합동 사이버작전』이다. 이 책의 부록 '용어의 정의'에 '사이버무기(Cyber Weapons)는 사이버작전에서 사용하는 무기로서, 공세적 또는 방어적 사이버작전에 사용되는 HW 및 SW'로 정의하고 있다[15]. 해당 정의는 사이버전을 구체화한 '사이버공간에서 맞닥트리는 사이버기술에 의한 전쟁에 사용되는 사이버 기술적인 무기체계'라는 개념이 누락되어 있다. 즉 운용공간에 대한 규명이 없어서 어떤 군이 사용하는 장비인지(사이버 군에 대한 필요성이 이 개념에서 나온다고 본다.)에 대한 설명의 구체성이 결여되어 있다.

사이버무기에 대하여 언급한 또 다른 공식 문서는 2015년 12월 30일에 발령된 국방부훈령 제1862호인『국방사이버안보훈령』이다. 이 훈령 별표 1 '용어의 정의'에서 '사이버무기체계'를 '사이버작전에 직접 운용되거나 능력배양에 직접 관련된 SW・장비・부품・모델 등 조직화된 체계를 말한다.'라고 정의하였다.[16] 이는 사이버무기를 정보통신시스템적인 차원에서 정의한 것으로 정작 사이버무기가 무엇이라는 정의와는 다소 초점이 안 맞는 정의라고 보인다.

사이버무기의 정의에는 아래와 같은 내용이 포함되어야 할 것이다. 'Who'에 관한 것으로 무기체계를 운용하는 군을 사용주체로 명시하여야 한다. 'What'은 해킹, 컴퓨터 바이러스, 서비스방해, 논리폭탄 등 사이버기술을 수단으로 사용한다는 개념을 포함하여야 한다. 'Where'는 사이버공간에서 사용되어야 한다는 공간적 개념을 명시하여 무기체계의 운용지역을 특정함으로써 영토적인 개념을 유추할 수 있어야 한다. 'When'은 작전목적에 따라 사용하는 것을 밝힘으로써 작전형태에 따른 운용개념이 필요하다. 'Why'는 정보수집(획득), 공격(제압), 방호활동으로 규정함으로써 사이버작전의 형태를 포함해야 한다. 종합하면, 본 연구에서는 사이버무기를 **『군이 작전목적에 따라 사이버공간에서 사이버기술을 사용하여 정보수집(획득), 공격(제압), 방호활동 등을 하는 수단』**으로 정의하고자 한다.

3.2 사이버무기 유형

사이버공간은 금융, 병원, 교육, 군과 같은 인간의 모든 물리적인 생활공간과 동일하다고 할 수 있다, 사이버공간의 급속한 성장은 기술을 사용하여 타인을 착취하려는 개인의 비윤리성도 크게 증가시켰다. 보안정보에 접근하여 정보를 감시하고 네트워크를 사용하지 못하도록 하며 데이터와 돈을 훔치는 것을 목적으로 하는 사이버공격 사례도 점차 증가하고 있다.

사이버공격은 데이터 또는 정보의 무결성, 신뢰성의 붕괴와 프로그램의 논리를 변경하고 출력해 오류를 일으키는 악성코드, 네트워크 Scanning을 통해 보안 취약점을 찾아내는 것 등을 포함한다. 통상 공격자(해커)들은 다음과 같은 절차를 통해 공격작전(해킹)을 수행한다. 첫째, 공격자는 시스템을 감염시키기 위해 프로세스의 조화를 기대하며, 정보탈취를 위한 요구단계가 동기화되기를 기다린다. 둘째, 논리적으로 체계화된 방법을 통해 보다 효율적인 결과를 얻을 수 있도록 시스템을 조직화한다. 셋째, 조직화된 공격자는 일시에 대규모의 컴퓨터를 감염시켜 데이터 및 재정적 손실을 유발한다. 넷째, 정치적인 목적을 가진 공격자들일수록 완벽하게 연계되어 있다. 다섯째, 공격자는 공격일시가 도래하기 전까지는 최대한 신중한 계획을 수립하고 은밀히 행동함으로써 결정적인 피해를 유발한다. 여섯째, 공격자는 충분한 준비시간을 갖고 대상 체계의 피해를 극대화시키기 위해 노력한다.

3.3 사이버무기 사용 사례

사이버무기가 사용된 새로운 개념의 전쟁은 1991년 미국과 이라크와의 '1차 이라크전(사막의 폭풍작전)'에서 미국이 공습이전에 이라크 방공망을 교란하기 위하여 취한 일련의 사이버 활동을 사이버전[17]의 효시로 보고 있다. 이 전쟁은 여러 가지 면에서 그 때까지의 전쟁양상과는 다른 면을 보여주었다. 전쟁 및 교전상황을 CNN을 통해 안방에서 볼 수 있었다거나, 400시간 만에 지상군의 진격이 완료되어 최종목표를 탈환한 것 등이다. 그러나 그것들보다도 획기적인 전쟁양상의 변화는 사전에 사이버기술을 사용하여 적을 무력화 시킨 후, 대항하지 못하는 적에 대하여 원활한 공격활동을 할 수 있었다는 것이다[18]. 세계는 이 작전을 통해 사이버전의 효과를 직접 확인하게 되었고 사이버전에 대한 준비를 시작하게 되었

Table 1. Major cyber weapon use cases since 2000

Date	Attacker - victim	Contents	Cyber weapon type
1991.	U.S. - Iraq	First Iraqi front-end disturbance disturbance	Malware
2001. 7.13	China - U.S.	Code Red worm (buffer overflow exploit) infected 359,000 PCs in 9 hours. 8.4 A variant (Code Red-II) occurred in the last 1 million PC infections, $ 2.6 billion in monetary damages.	Worm, DDoS
2003. 7.19.	China - U.S.	Michigan, Ohio, New York, and Canada (55 million people / 1st blackout).	Slammer worm
2007.	Russia - Estonia	Government, media, broadcasting, financial network infringement, two-month paralysis	DDoS
2008.	Russia - Georgia	Georgia President's Homepage, Congress, Ministry of Defense, DDoS attack on Ministry of Foreign Affairs	DDoS
2008. 10.24.	Afghanistan - U.S.	US Central Command Server Infection, Buckshot Yankee Operation	
2009.	U.S. - Iran	1,000 centrifuges destroyed	Stuxnet
2009.	China - U.S.	Penetration of F-35 design data, electronic system information leak	
2011.	U.S. - Al Qaeda	Al Qaeda's cell phone, location confirmation, Osama bin Laden murder	Spyware
2011. 4.12.	(China)-Korea	Nonghyup Outsourced Employee Using a Notebook Taking Information on IP, Super Administrator Password, etc. for 7 Months. Destroyed 273 servers. It is presumed that the NACF who used RSA Secure ID had rehearsed before attacking Lockheed Martin using the same system.	
2011. 5.21.	China-U.S., Lockheed Martin	F-35 design leak Lockheed Martin's "cyber kill chain" [19] Attacking RSA's Secure ID	
2017. 5.12.	NK - World	It exploited a vulnerability in server SMB, which is used for Microsoft's file sharing of eTorner Blue, infected with more than 120,000 PCs in 150 countries. Requires 300 to 600 $ Bitcoin (can be prevented through Microsoft's MS17-010 vulnerability patch)	Ransomware
2017. 6.10	?-Korea	Internet web hosting company 'Nayana' Web attacked 153 backup servers, negotiated key decryption to 1.3 billion won in 5 days (Ransomware the highest amount of damage)	Ransomware

다고 할 수 있다.

표 1은 사이버전이 최초로 수행된 1991년 사례와 2000년 이후 지금까지 식별되고 보고된 주요 사이버 무기가 사용된 사례를 정리한 것이다. 사이버무기는 초기에는 전쟁에만 사용되었으나 이후에는 군, 공공기관 뿐만 아니라 금융, 민간기관 등을 대상으로 광범위하게 사용되고 있다.

3.4 사이버전 대응 관련 사이버무기 R&D

기술의 발달이 사회적인 변화양상을 결정할 것이라는 기술결정론[20]은 첨단기술의 군사 분야 진입이 향후 전쟁양상을 변화시킬 것이라는 믿음을 가져왔다. 그러나 군은 보수적인 집단이어서 신기술이 고유의 군사전통이나 문화와 충돌할 경우에는 전통을 고수해 왔다. 기술 환경이 물리적인 공간에서 사이버공간으로 급속히 전환되어 가고 있음에도 불구하고 사이버공간을 새로운 전장으로 인식하는 나라와 사이버군대를 창설하는 나라가 많지 않은 것도 사실이다.[21] 사이버공간에서 사이버기술을 통해 컴퓨터 시스템 및 통신망을 공격하여 사이버체계를 파괴하고 아측의 사이버체계는 보호하는 것을 의미하는 사이버전의 개념[22]은 정립하였으나 아직도 사이버전에 대한 대비태세 확립은 미미한 수준이다.[23]

미 DARPA(방위고등연구계획국 : Defence Advanced Research Project Agency)는 1958년 위성개발에서 러시아에 선두자리를 빼앗긴 이후(일명 '스푸트니크 쇼크')에 창설되면서 '경쟁국가에게 기술로 기습당하지 말자'를 모토로 정하고, 인터넷의 기원이 되는 ARPA Net을 최초로 만들어냈으며 최근에는 사이버무기에 대한 연구도 꾸준히 진행하고 있는 것으로 알려져 있다. 미국이 사이버전을 준비하기 위한 사이버무기 관련 R&D는 표2과 같으며, 공격 관련 내용은 비밀로 공개되지 않았다.

또한 DARPA는 2012년 9월부터 '플랜 X'를 가동하여 미 국방부의 사이버임무를 실시간으로 파악하고 대규모 네트워크 환경을 이해, 운용할 수 있는 혁신적 기술개발을 목표로 추진하고 있다. '플랜 X'의 핵심전략은 첫째, 공격국가의 통신 및 레이더를 무력화하여 공격국가의 정보시스템을 교란하고 재래식 혹은 디지털 전투력을 지원하는 것이다. 둘째, 전 세계 컴퓨터의 위치를 담은 사이버지도를 작성하여 사이버공격으로부터 미국을 보호하고 즉각적인 대응으로 공격국가를 반격하거나 제압하는 것을 목표로 하고 있다.

Table 2. R & D cases related to inter-version technology types and inter-US version [24]

Main Category	Mid. class	Small Category	US DARPA Research Program
Said version defense weapon system technology	prevention	User Authentication	Active authentication
		Military Data and Comsec	Execute Encrypted Data
			Secure field communication
		Defense Systems / Network Minimization of Vulnerability, Information Assurance, Supply Chain Security	Automatic Analysis of Cyber Security Program
			Secure host design
			High Trust Cyber Convergence Weapon System
			Verification of crowd source formatting technique
			Military Network Protocol
			Reliable integrated circuit
	prepare	Insider threat detection	Large anomaly detection
			Cyber insider threat
		Defense system threat monitoring	Integrated Cyber Analysis System
			Resilient mission-based cloud
			Scalable network monitoring
	Response	Defense system attack countermeasures and forensics	Dynamic quarantine for computer-based worm attacks
			Cyber Genome ProjectCyber Genome Project
	restore	Defense system, data, communication restoration	Resilient mission-based cloud
			Secure field communication
Interim Support Infrastructure Technology		Developed cross-reference data set	Cyber Genome Project
		Develop cyber battlefield framework and visualization technology	Plan
			Integrated Cyber Analysis System
		Development and operation of cyber training center	National Cyber Training Center

사이버전에서도 앞서가고 있는 미국은 표3에서 보는 바와 같이 사이버공간을 어떻게 방호할 것인가에 대한 끝없는 연구와 기술개발에 박차를 가하고 있다. 특히 이것을 정부가 주도함으로써 국가가 안전한 사이버공간을 국민들에게 제공해 주고 있는 것이다. 우리나라는 사이버전을 대비하기 위한 높은 기반기술을 확보하고 있음에도 불구하고 사이버무기를 무기체계로 뒤늦게 편입하였으며, 운영개념 확립 또한 미미하다. 이에 따라 국가 및 군사적으로 정보통신망에 대한 공격(침해)이 급증함에도 불구하고 공격에 대한 능동적인 대응이나 공격자에 대한 신속한 식별이 불가하여 적절한 대응을 못하고 있는 실정이다.

IV. 사이버무기의 분류

4.1 사이버무기 개발 절차

사이버무기를 개발하기 위한 절차는 개념설계단계-기획단계-개발단계-실전적용단계-목적달성단계-검증단계의 6단계로 이루어진다.

첫째, 개념설계단계는 사이버무기를 사용하는 측이 어떤 활동을 사이버공간에서 하려고 하는가라는 목적을 정하고 그에 따라 사이버무기에 대한 운용개념을 설계하는 것이다. 운용개념설계단계에서 공격자라면 지금까지 획득한 정보를 이용하여 취약점을 파고들기에 적합한 방법을 상정하고 그에 맞춘 사이버기술을 사용한 무기(체계)를 설계하는 것이다. 이 단계에서 사용자는 목적에 특화된 무기체계 즉 운용개념을 구현하기 위한 구상을 하게 되는 것이다.

둘째, 기획단계에서 사용자는 사이버무기를 사용할 절차와 경로를 판단하여 이를 위한 물리적인 조건들까지 구체화 하게 된다. 다양한 방법의 물리적, 비 물리적인 정보수집을 통해 대상체계를 사용하는 사람들의 활동특성까지를 고려하여 이용할 수 있는 물리적 또는 비 물리적 취약성을 고려한 사이버무기체계의 사용 환경을 기획하는 것이다.

셋째, 개발단계이다. 기획의 단계를 거쳐 구체화된 사용 환경과 사이버기술은 개발자에 의해 통합되어 최적의 사이버무기(체계)로 실체화된다. 개발자는 개념적으로 구상되고 기획과정을 통해 그려진 밑그림에 채색을 하고 음영을 주어 작품을 완성하는 것이다. 개발자에 의해 제작된 사이버무기(체계)는 개념설계와 기획의도에 따라 정보수집용 사이버무기(체계)라면 사회공학적인 기법을 이용할 것인지, Zeroday Attack용 자료를 수집할 것인지, Warning 체계를 만들 것인지 등을 구체화하는 것이다.

이렇게 만들어진 사이버무기체계는 넷째, 실전에 적용하게 된다. 실전에 적용한 사이버무기는 역시 개념설계와 기획의도에 따라 목적을 달성하면 파괴 되(하)거나 지속적인 변종을 만들어 생존을 유지하는 활동을 하게 된다. 이 과정에서 만일 상대방에 의해 발각되어도 쉽게 흔적을 남기거나 사용자를 특정할 수 있는 Smoking Gun을 남겨서는 안 된다. 증거

는 반격의 필요성을 충족하는 요인으로써 공격을 받을 수 있는 빌미를 제공하기 때문이다. 따라서 적용단계에서 가장 중요한 것은 은밀성과 추적 불가성이다.

다섯째 요망하는 목적달성을 측정하는 것이다. 만일 요망하는 목적을 달성하지 못했다면 즉시 다른 사이버무기를 사용할 것인지 아니면 흔적누설을 방지하기 위하여 철수하거나 파괴시킬 것인지를 판단해야 한다. 이 단계는 기획의도를 충족했느냐와 흔적 누설이 가능한가가 가장 중요한 기준이 될 것이다.

여섯째 검증단계이다. 검증을 통해 개념설계자와 기획자는 목적달성 여부를 평가하여 사용한 사이버무기의 지속사용 가능성을 평가한다. 이 단계는 사이버무기 사용과정에서 발생한 사이버무기의 취약성을 보완하여 새로운 무기를 개발하기 위한 개념설계에 반영하게 되는 것이다. 이 사이버무기 개발 6단계는 계속하여 상호 영향을 주며 발전하게 된다.

4.2 사이버무기의 분류

국방 무기체계를 분류할 때 기준이 되는 문서는 국방전력발전업무훈령이다. 동 훈령 제14조(무기체계 분류)에 운용목적, 용도, 필요성 등을 고려하여 분류한다고 명시하고 있다. 전술한 바와 같이 무기체계의 분류는 물리적인 환경에서 활동하는 군종을 육·해·공·우주군 으로 나누었을 때 그 군종이 전투에서 사용할 무기체계를 대상으로 한다. 무기체계를 분류할 때 대분류는 사용군, 중분류는 부대운용 목적, 소분류는 작전형태에 따라 분류하고 소분류 밑에 구체적인 필요성에 의해 대상 장비로 구분한다.[25] 사이버무기도 이 분류기준에 따라 표3과 같이 대분류(사이버무기체계), 중분류(정보수집, 공격, 방호)된 무기체계를 소분류(정보수집(6), 공격(7), 방호(9))하였다.

우리나라에서 사이버전에 사용될 무기분류를 처음 소개한 것은 2013년도에 국방기술품질원에서 발간한 국방과학기술조사서를 통해서이다. 이 문서에서 사이버전체계를 신규로 작성하였는데 기존 무기분류 범주인 지휘통제통신(대분류)영역에 사이버전체계(중분류)를 포함하여 분류하고, 사이버체계에 대한 기술분류는 대분류(3), 중분류(20)으로 구분하였다. 이를 소개한 이호균의 논문[26]에서는 사이버전에 적용될 수 있는 국방정보기술과 민간기술을 망라하여 표로 제시하고 있는데, 이 논문이 제시하는 분류는 국방전력발전업무훈령이 2017년 개정하면서 반영하지 않은 것으로 보아 국방 무기체계 분류기준과는 다른 사이버기술을 분류한 것으로 판단된다. 따라서 본 논문은 국방전력발전업무훈령 제14조에서 제시하는 기준을 따라 사이버무기에 대하여 분류하였다.

Table 3. Classification table of cyber weapons (technology)

Main Category	Mid. class	Small Category	Case
Cyber weapon system	Information gathering (acquisition	Weapon system for Zeroday Attack	Vault 7 Star virus Careto FinFisher Pegasus X-Agent Infojack Phishing SCAN attack Snufing Spoofing Sniffing Social engineering hacking
		Weapon System for Social Engineering Data Collection	
		Signs of infringement For Warning Weapon system	
		Weapon for Vulnerability Identification	
		Situation recognition weapon system	
		Weapon system for abnormal state reasoning	
	Attack	Weapon systems linked to physical weapon systems	CryptoLocker Zeus Mirai Petya Shamoon Metulji botnet Mahdi StarDust Dexter Cardtrap.A. Infojack WinCE/TerDial RedBrowser Gabir Gavno Locknut Skulls DDoS EMP Trojan Session Hijacking Electronic Jamming Nano Machine
		Latent / standby weapon systems	
		Closed network weapon system	
		Controlled weapon system after invasion	
		Robotic weapon system	
		Continuous variant-generated weapon systems	
		Nano weapon system for HW attack	
	protection	Surveillance technology system	Monitoring technology Authentication (expression) technology Cryptography DDoS technology ID technology (Dong) Image technology Biometrics technology Subchannel attack prevention technology Forensic Technology Attack Location Tracking Technology Cyber mines Cyber booby trap
		Authentication and Recognition System	
		Cryptographic system	
		Specific attack response system	
		Attack prevention system	
		Forensic system	
		Traceback system	
		BDA system	
		Cyber mines and booby traps	

4.2.1 정보수집(획득)용 사이버무기

사이버무기체계도 사용목적, 용도 및 필요성에 따라 정보수집(획득)용 사이버무기, 공격(제압)용 사이버무기, 방호용〔27〕 사이버무기로 중분류 할 수 있다. 이하에서는 각각의 중분류 내 소분류 항목을 구체적으로 살펴보고자 한다.

사실 정보수집활동은 국제법적으로 불법이 아니다. 그것은 사이버공간에서도 통용된다. 그러나 정보수집이 법에서 금지하는 수단을 통해 수행될 경우에는 불법이라고 해야 할 것이다. 불법적으로 수집한 정보는 반드시 제2의 범죄로 이어지게 된다. 따라서 사이버 정보수집 활동도 공개정보에 대한 수집활동(OSINT : Open sauce Intelligence)은 보장되나 불법적인 정보수집 활동은 거부된다. 2017년 8월 미 육군은 중국산 DJI社의 드론제품을 군에서 사용하지 못하도록 지시를 하였다. 이는 동 제품이 GPS정보, 실시간 (동)영상을 자국 및 전 세계에 퍼져있는 데이터센터에 자동전송 하는 것을 알았기 때문이며, 언제라도 미군의 주요 군사정보를 중국에 보낼 수 있다는 가능성 때문이다.〔28〕

정보수집(획득)용 사이버무기체계는 Zeroday Attack용 무기체계, 사회공학적 자료수집용 무기체계, 침해징후 Warning용 무기체계, 취약점 식별용 무기체계, 상황인식용 무기체계, 이상상태 추론용 무기체계로 분류하였다. ①'Zeroday Attack'은 최근 각광받는 공격방법이다. 기존의 패치는 반응이 늦을 수밖에 없으며 알려진 취약성을 즉각적으로 패치하는 개인이나 조직도 많지 않기 때문이다. 미 NSA는 이러한 공격방법에 적극적으로 대응하기 위하여 Zeroday Attack을 위한 자료를 공식적으로도 수집하고 있다. ②'사회공학적 자료수집'은 공격자를 특정하거나 공격할 대상의 취약성을 찾아내기 위해 반드시 필요한 과정이기 때문에 이를 위한 무기체계는 앞으로도 계속 발전할 것이다. 개인정보를 보호하기 위한 노력과 찾아내고 이용하기 위한 싸움에서 유용한 무기체계이다. ③'침해징후 Warning용 무기체계'는 피아 공히 정보수집 활동이 적극적으로 전개될 때 그것을 회피하고 찾아내어 경고하고 역이용하기 위한 무기체계이며, 전략 및 전술적으로도 반드시 필요한 무기체계이다. ④'취약점 식별용 무기체계'는 아 체계의 취약점을 적의 입장에서 식별하는 무기체계이다. 특히 Zeroday Attack의 관점에서 끊임없이 취약점을 식별하는 것은 군사의 일상이다. ⑤'상황인식용 무기체계'는 동시다발적인 사이버상황의 인식에서 혼란을 방지하기 위한 무기체계이다. 상황이 동시다발적으로 발생했을 때 시간대별로 지역별로 대상별로 공격의 유형별로 분석하고 정리하여 인식하는 것은 대응의 절차와 수준을 정하는 것을 용이하게 할 것이다. ⑥'이상상태 추론용 무기체계'는 정밀한 사이버공격 시에 사이버상의 이상 징후도 매우 미약할 것-또는 전혀 없거나-이므로 작은 이상 징후도 놓치지 않기 위한 무기체계이다. 특히 이 무기체계는 침해징후를 경고해 주는 것과는 다르게 작은 이상 징후에 대한 경고와 빈도, 사례를 분석하는데도 용이하게 적용될 것이다. 정보수집용 사이버무기는 사이버무기 개발의 개념설계와 기획단계에서 사이버무기의 개발방향, 사이버활동의 기법과 기술, 물리적 환경을 이용할 방법을 구상하는데 사용될 것이다.

4.2.2 공격(제압)용 사이버무기

공격(제압)용 사이버무기는 물리적 무기체계와 연동되는 무기체계, 잠복/대기형 무기체계, 폐쇄망용 무기체계, 침입 후 조종 가능형 무기체계, 로봇형 무기체계, 지속적인 변종 생성형 무기체계, HW 공격용 나노형 무기체계로 분류할 수 있다. ①'물리적 무기체계와 연동되는 무기체계'는 향후 전쟁은 사이버전과 물리전이 동시에 이루어질 것을 고려한 무기체계이다. 또한 물리적 무기체계도 첨단화 되면서 모든 통제가 사이버공간에서 이루어질 것이다. 따라서 사이버와 물리적 차원의 공격은 연동되고 통합되어 동시 통합작전에 운용될 것이기 때문에 필요한 무기체계이다. ②'잠복/대기형 무기체계'는 물리적인 무기의 SW나 일반 전산장비에 미리 침투하여 공격자의 명령을 대기하거나, 대상자의 특정한 상황이 발생할 때까지 잠복하다가 동시에 특정임무를 수행하는 무기이다. ③'폐쇄망용 무기체계'는 통상 폐쇄망은 안전하다는 믿음을 갖고 있기 때문에 그 공간의 사용자는 오히려 많은 자체 취약점을 가지고 있다는 상황을 고려하여 구상되었다. 따라서 폐쇄망에 대한 공격자의 도전은 계속되고 있으며 최근 북한에서는 그러한 공격능력을 확보했다고 한다〔29〕. ④'침입 후 조종 가능형 무기체계'는 잠복/대기형이 사전 약정된 상황이나 조건에 따라 움직이는 피동형 무기라고 한다면 이 무기는 능동형이라고 할 수 있다. 공격자에게 사전 약정된 조건의 도래를 신호하여 공격자가 능동적으로 조종을 하도록 하는 무기이다. 이는 상황변화에 대한 인간의

판단과 평가를 동시에 적용하면서 상황을 조절하기 위한 목적으로도 사용될 것이다. ⑤'로봇형 무기체계'는 AI형 무기라고 할 수도 있는 것으로 방어자의 퇴치활동에 능동적으로 반응하면서 자기 방호력을 가지고 목적을 달성하기 위한 무기이다. ⑥'지속적인 변종 생성형 무기체계'에 대한 방어자의 패치는 공격자에게는 치명적이다. 방어자의 패치가 적용되면 스스로 변종을 만들어 임기응변함으로써 최초의 목적을 달성하거나 바뀐 상황에 대한 목표를 수정하고 대상에게 최고의 피해를 강요할 수 있는 무기이다. ⑦'HW 공격용 나노형 무기체계'는 물리적 무기와 사이버무기의 경계에 존재한다. HW를 파괴하기 위해서는 프로그램에 의한 것도 가능하지만 극초소형의 무기가 적의 정밀한 무기체계에 침투하여 SW와 HW에 동시에 공격을 하게 된다면 적에게는 보다 심대한 피해가 될 것이기 때문이다.

4.2.3 방호용 사이버무기

방호용 사이버무기는 공격발생 즉시 공격자를 특정하기 위해 Smoking Gun을 찾는 DB구축으로부터 시작되며 감시기술체계, 인증 및 인식체계, 암호체계, 특정 공격 대응체계, 공격방지체계, 포렌식 체계, 역추적체계, 피해평가체계, 사이버 지뢰 및 부비트랩 등이 있다. ①'감시기술체계'는 적의 공격형 사이버무기를 즉시 식별하거나 아군 체계의 피해를 즉시 식별해 냄으로써 전투지속능력을 확보하기 위한 무기체계이다. ②'인증 및 인식체계'는 적을 식별해 내는 것 못지 않게 아군임을 인증해 내는 것 또한 매우 중요하기 때문에 고안된 무기체계이다. 이것을 무기로 분류한 것은 적의 사회공학적인 공격에 효과적으로 대응하기 위한 것이다. 적이 사회공학적으로 찾아낼 수 없는 미세하지만 매우 특징적인 부분을 독자적 영역으로 구축하는 것은 방호에 매우 효과적이기 때문이다. ③'암호체계'는 정보보호의 가장 첨단이자 핵심적인 수단이다. 강한 내성을 가진 암호를 통해 피아를 구별하는 것은 방호능력을 강화해 줄 것이다. ④'특정 공격 대응체계'는 적은 사이버공간에서 기상천외한 방법으로 아군의 취약점을 찾아낼 것이기 때문에 이에 대응하기 위한 아군의 방법도 기상천외한 상상력을 동원해야 한다. 따라서 다양한 공격방식을 상정하고 시뮬레이션 할 수 있는 대응체계는 반드시 필요하다. ⑤'공격방지체계' 관련하여 적의 대규모 공격은 아무리 징후를 감추려 해도 반드시 노출될 것이다. 따라서 대규모 공격을 방지하기 위한 방호수단의 필요에 의해 고려되었다. ⑥'포렌식 체계'는 적의 공격 후 신속하게 공격자를 특정해 내야 하는 중요한 방호용 무기가 된다. 전술한 필요성과 비례성을 위한 무기이다. ⑦'역추적체계' 관련하여 대부분의 잠복/대기형 무기의 공격은 매우 은밀히 이루어지기 때문에 식별하기가 어렵다. 그러나 식별된 후에는 그것을 즉시 공개하기 보다는 공격자를 특정하고 그 의도를 평가하는 것이 더욱 중요하다. 더 나아가서 그 의도에 따라 역으로 이용할 가능성도 있기 때문이다. 따라서 은밀하게 공격자를 역추적 하는 기술은 방호 및 역이용을 위한 핵심기술이다. ⑧'피해평가체계' 관련하여 얼마만큼 신속하게 그 피해규모를 특정 하느냐 하는 것은 방호자의 사이버능력을 가늠하는 바로미터가 될 것이다. 사건발생 시 피해를 평가하고 그 규모를 산정할 때 시간은 방호자의 편이 아니기 때문이다. ⑨'사이버 지뢰 및 부비트랩'은 적 공격 시 흔적을 통해 경고해 주는 매우 전술적인 무기이다. 공격자의 수준이 항상 최상일 수는 없기 때문에 작은 사이버기술을 이용해서도 방호를 효과적으로 해 낼 수 있을 것이다. 따라서 공격자가 쉽게 접근할 수 있는 곳에 임기응변식으로 설치하여 사용할 수 있다.

4.3 비례적 대응을 위한 고려사항

물리적 상황에서 비례대응은 공격한 적의 규모, 공격수단, 아군이 받은 피해 정도에 따라 대응하며, 사이버상황에서의 비례적 대응도 동일한 고려사항을 가지고 시행해야 한다. 비례적 대응을 위한 첫 번째 고려사항은 규모의 비례성이다. 이는 공격규모에 대한 비례성으로 물리적인 상황에서라면 포 1개 대대로 공격했을 경우 우리도 그에 상응하는 규모로 공격하는 것이다. 이는 반드시 같은 종류의 공격무기가 아니어도 된다. 공격받은 규모와 유사한 수준으로 공격하는 것이다. 둘째, 수단의 비례성이다. 이는 반드시 동종의 무기로 대응하는 것을 말한다. ICBM급 미사일로 공격하면 우리도 ICBM급 미사일로 맞 공격한다는 것이다. 이는 동종의 수단을 보유하고 있다는 전제하에 가능한 대응방법이다. 셋째, 피해의 비례성을 들 수 있다. 이는 아군 관점에서 평가되며 적의 규모, 수단과 상관없이 우리가 받은 피해에 상응한 대응을 한다는 것이다. 일례로 수류탄을 인구밀집 지역에서 터뜨린다면 야지에서 터뜨리는 것보다 인명피해가 클 것이다. 그 때의 대응은 우리가 받은 피해의 규모와

상응한 효과를 달성할 수 있는 무기를 사용한다는 것이다.

이를 사이버무기 분류에 따른 정보수집, 공격, 방호에 각각 적용하면, 정보수집용 사이버무기는 평시 경보와 피해발생 시 공격자를 특정하고 규모, 수단, 피해정도를 확인하기 위하여 사용한다. 따라서 비례적 대응을 위해서는 상시 운용이 필수적이다. 공격용 사이버무기는 수집된 정보로 판단된 규모, 수단, 피해정도에 따라 상응하는 대응을 위해 공격직전 선택된다. 방호용 사이버무기는 상시 사용되어 아 체계를 보호해야 한다. 이를 표로 구성하면 다음과 같다.

Table 4. Consider proportional response to cyber weapon classification

Division	Information gathering	Attack	Protection
Scale proportionality	always	Optional use in the event	always
Proportionality of means	always		always
Proportionality of damage	always		always

V. 결 론

전쟁은 물리공간을 넘어 사이버공간으로 확대되고 있다. 2013년 12월에 Wassenaar Arrangement (바세나르체제) 가입국들은 '스파이 행위나 해킹을 통한 사이버전쟁 억제를 위하여 사이버 보안기술 수출의 통제'에 합의하였다. 바세나르체제는 '이중용도 품목 및 기술'에 사이버기술의 일부를 포함하여 규제대상 품목으로 정하였다[30]. 세계는 이미 모든 시스템이 네트워킹 되어 있고 따라서 사이버정보수집과 사이버공격에 취약하다. 또한 사이버공격은 흔적을 남기지 않으면서 인명피해 없이 목적을 달성할 수 있는 저렴한 공격수단이 되었다. 공격의 가능성이 많아질수록 그에 대한 대비책도 강구되어야 한다. 그 대비책은 공격 즉시 국제법상의 필요성과 비례성의 원칙에 따라 대응할 수 있는 능력을 갖추는 것이다.

이를 위해서는 공격에 대한 정확한 피해가 신속히 산정되어야 하고 그 피해에 걸 맞는 대응능력을 갖추어야 한다. 따라서 모두가 공감하는 사이버무기에 대한 정의는 시급히 확립되어야 한다. 본 연구는 사이버무기란 **『군이 작전목적에 따라 사이버공간에서 사이버기술을 사용하여 정보수집, 공격, 방호활동 등을 하는 수단』**이라고 정의하였다.

또한 사이버무기에 대한 분류기준을 명확히 하는 것은 적대세력이 사이버무기로 공격해 왔을 때 즉시 사이버무기를 특정하여 대응할 체제를 가능케 한다. 본 연구에서 사이버무기는 앞서 표4와 같이 정보수집용, 공격용, 방호용으로 분류하였다. 그러나 식별되지 않은 보다 정교한 무기체계들이 더 많을 것으로 판단된다. 사이버공격이 전시 또는 그와 유사한 상황을 고려하여 준비된다면 사전에 공격할 체계에 대하여 Backdoor를 통해 악성코드를 설치하는 것이 유리하기 때문이다. 또한 공격자만 아는 Zeroday Attack을 통해 미리 악성코드를 설치하였다 하더라도 언제든지 방호자에 의해 노출되거나 제거될 우려가 있으므로 가능한 한 은밀성을 확보한 가운데 설치된 사이버무기에 대한 지속적인 관리가 이루어져야 한다. 따라서 한 번 공격받은 사이버체계에는 이미 다종의 사이버무기 즉 악성코드가 설치되어 있다고 판단하는 것이 타당하다. 따라서 공격받은 사이버체계는 반드시 다수 인원과 오랜 시간을 투자하여 취약점을 식별 추적하여 위협을 제거하는 과정을 거쳐야만 한다. 이를 위해서 사이버무기체계 중에서도 정보수집과 방호용 무기체계 개발에 우선권을 두고 개발해야 한다.

사이버무기를 3가지로 분류하였지만 정보수집과 공격용, 정보수집과 방호용은 사용절차나 개발절차에서 동시 또는 긴밀한 협력의 과정을 통해 제작되고 운용된다. 물리적인 무기보다도 사이버무기는 은밀성을 확보하는 것이 중요하다. 4차 산업혁명 시기에는 사이버무기도 AI와 Big data의 활용성이 높아질 것이고, 4차 산업혁명과 결합한 사이버무기는 사용 목적의 다양성과 요구되는 정밀성의 증가로 인하여 용량은 지속적으로 증가할 것이다. 따라서 사이버무기의 원활한 사용을 지원하기 위한 패킷분할기술과 라우팅기술, 정상코드로 위장하는 기술 등이 필수적으로 뒷받침되어야 할 것이다. 또한 적 공격용 사이버무기의 규모, 수단, 아측의 피해정도를 고려하여 상응하는 사이버무기를 통해 비례적인 대응을 함으로써 주권국가의 존엄을 확립하고 과도과소 대응의 우를 범하는 일이 없어야 한다. 그러나 아직 사이버무기는 등급이 없어서 과연 어떤 효과를 노리고 활동하였는지를 특정하지 못하는 상황이다. 이는 공격받은 국가의 대응이 자칫 소총으로 공격받고 핵무기로 대응하게 되거나 그 반대의 결과가 될 수도 있다. 따라서 향후 사이버무기의 효과에 기반 한 등급화 연구가 이루어져야 할 것이며, 본 연구는 비례성 원칙의 한 축을 이루는 사이버무기체계 분류에 관한 논의를 시작했다는 데 의의가 있을 것이다.

References

[1] Joint FM 3-24, "Joint Cyber Operation," the characteristics of cyber weapons system are classified into non-formation, ease of development, speed and destructiveness, broadness, and non-killing. pp. 4-5 to 4-6

[2] MND, Seoul, 2016, Article 14 (Classification of Weapon System) Refer to MND Ord No. 1975, Nov. 2016.

[3] Law No. 14182 ('16. 5.29.) See Article 3 (Definitions) of the Defense Business Act

[4] Presidential Decree No. 27618 ('16.11.29.) See Article 2 of the Enforcement Decree of the Defense Business Act

[5] Ahn Seung-bum et al., "The Korean Armed Forces Yearbook 2016~2017,", The Diffusion Times, Seoul, 2016

[6] Article 1059 Charter of the UN (entered into force on Sep 18,1991), see Article 51

[7] Michael N. Schmidt, 『Tallinn Manual』, Institute of Electronics and Telecom Research Institute, Translated, Written and Thought, Seoul, pp. 99-101, 2014.

[8] Michael N. Schmidt, "Tallinn Manual", Institute of Electronics and Telecom Research Institute, Translated, Written and Thought, Seoul, pp. 89-98, 2014.

[9] Some argue that cyber space should not be militarized. Dorothy E. Denning, Bradley J. Strawser, & quot; Moral Cyber Weapons & quot ;, Part-II-CH-6, Oct. 24, Reference

[10] For information on autonomous weapon systems (AWS), see Kenneth Anderson, "Why the Hurry to Regulate the Auto Weapon System? But Not Cyber - Weapons?," Temple Int. l & Comp. L.J. 2016.

[11] Cyber attack procedure: Information gathering (Vulnerability identification) - System / network intrusion (ID, PW acquisition) - Obtain administrator authority (Check system internal vulnerability) - Delete attack trail and install backdoor Version Introduction, Hongleung Science Publishing Co. Seoul, pp. 34-35, 2012.

[12] Nick Ebner, "Cyber Space, Cyber Attack and Cyber Weapons,", IFSH, p. 2, Oct. 2015.

[13] Thomas Rid & Peter McBurney, Cyber weapon, The RUSI journal, vol 157, pp. 6-13, Feb. 2012.

[14] DoD, "Cyberspace Policy Report", p. 2, Nov. 2011

[15] Joint FM 3-24, "Joint Cyber Operation", JCS, Seoul, 2016, Appendix 1 (Definitions of Terms)

[16] Refer to the MND Ord No. 1862 (Dec 30,2015), "Defense Cyber Security Directive," MND, Seoul, 2015, Attached Table 1

[17] The characteristics of the interim version are ① low investment cost ② propaganda ③ difficult to identify the subject ④ unilateral attack is possible ⑤ defense is always post-war ⑥ 24-hour exhibition system ⑦ damage assessment is difficult. Son Yeong-dong, "Endless War of 0 and 1", Informer Books, Seoul, pp. 154-156, 2013.

[18] On Jan 16, 1991, after the desert storm command, the EC-130H electronic electricity neutralized the Iraqi network and the war began, and the war ended at a time when Iraq could not carry out the proper defense operations. http://ko.wikipedia.org/wiki/%EA%B1%B8%ED%94%84_%EC%A0%84%EC%9F%81, Wikipedia, Gulf War, Nov. 2017.

[19] Cyber Kill Chain Step 7: ① Reco-

nnaissance (find out the name of the company's employees, identify key business contacts, and send malicious code to email/attached) (Establishing a database of pdf files that are thought to be infected) ③ Forwarding (sending malware via email or an infected USB drive) ④ Taking (finding zeroday vulnerability) ⑤ Installing ⑥ Command and control ⑦ Execution. Sein Harris, Translated by Jin Seon Mi, "Invisible War @ War", Yangmun, Seoul, 2015.

〔20〕 Kim, In-Soo, "Evaluation and Prospect of NK's Interoperability,", Unification Policy Research 24(1), Seoul, pp. 117-119, Jun. 2015.

〔21〕 Lee, Yong-seok, "Application of Cyber Army to Rep. of Korea Armed Forces based on German Federal Cyber Forces establishment and implementation", The Quarterly Journal of Defense Policy studies. 33(1), Apr. 2017

〔22〕 Um Jung Ho et al., "Introduction to Sai Version,", Hongleung Science Publishers, Seoul,

〔23〕 The views of major countries on cyber warfare are as follows, see Park, Sangseo et al., "Perspectives of Major Countries on Cyber Warfare,", Journal of Korea Institute of Information Security 14(6), pp. 70-74, Dec. 2004.

〔24〕 The R & D case presented in the table does not contain attack weapons, which are confidential and private. Lee, Ho-Gyun, "Development Trends and Development Trends between National Defense Version", Defense and Technology(422), Apr. 2014.

〔25〕 Refer to the Ministry of National Defense Ordinance No. 2114 (Dec. 2017), the Defense Power Generation Directive, Article 14 (Weapon System Classification), and Refer to Attachment 2 (Detailed classification of weapon systems)

〔26〕 Lee, Ho-Gyun, Jong-In Lim, and Kyung-Ho Lee (2016), "A Study on the Comparison of Core Technologies and Characteristics of Defense Cyber Weapons System and Conventional Weapon System,", Journal of Korea Institute of Information Security and Cryptology, 26(4), pp. 985-994

〔27〕 Seo, Dong-il et al., "Current status and prospect of security technologies for interim version,", Journal of Korea Institute of Information Security 21(6), pp. 42-45, Oct. 2011.

〔28〕 DAMO-AV, "US Army calls for units to discontinue use of DJI equipment", Aug. 2017.

〔29〕 Chosun Ilbo, "North Korea's hacking technology, the world's highest level ... Get rid of computer data that is not connected to the Internet,", Feb.12.2018. http://biz.chosun.com/site/data/html _dir / 2018/02/22 / 2018022200344.html , Feb.22.2014.

〔30〕 KISA, "Internet & Security weekly," Korea Internet & Security Agency, p. 6, Dec. 2013.

〈저자소개〉

이 용 석 (Lee Yongseok) 종신회원
1989년: 인하대학교 정치학 학사
2003년: 연세대학교 정치학 석사
2018년: 고려대학교 정보보호대학원 박사수료
〈관심분야〉 사이버국방/안보, 사이버무기체계, 사이버보안, 정보보호, 암호체계 개발

권 헌 영 (Kwon Hunyeong) 종신회원
1992년: 연세대학교 법학과 학사
1998년: 연세대학교 법학과 석사
2005년: 연세대학교 법학과 박사
2008년~2015년: 광운대학교 법학과 교수
2015년 9월~현재: 고려대학교 정보보호대학원 부교수
現 공공데이터법제도전문위원회 위원장, 개인정보분쟁조정위원회 위원, 한국교육학술정보원 이사, 한국인터넷윤리학회장 및 사이버커뮤니케이션학회 부회장 등 역임
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부

최 정 민 (Jeong Min Choi) 정회원
2000년: 한국외국어대학교 행정학 학사
2005년: 서울대학교 행정학 석사
2013년: 서울대학교 행정학 박사
현재: 서강대학교 공공정책대학원 대우교수
〈관심분야〉 정보정책, 전자정부

임 종 인 (Jong In Lim) 종신회원
1980년: 고려대학교 수학과 학사
1982년: 고려대학교 수학과 석사
1986년: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 / 사이버국방학과 교수, 대검찰청 디지털수사자문위원장, 한국CISO협회장, 합참 정책자문위원 등
〈관심분야〉 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안