현대 사이버전 사례 분석과 AI 기반 동향

Case Analysis of Modern Cyber Warfare and AI-based Trends

이종원*[1] 김환[2]

Jongwon Lee*,[1] Howard Kim[2]

[초 록]

사이버 공간은 현대 전쟁의 새로운 주요 전장으로 부상하고 있다. 물리적 전장과 달리 무형적 형태를 띠고 있으나, 지휘체계 해킹, 핵심 인프라 마비, 온라인 심리전 등 다양한 방식으로 상당한 파괴력을 발휘할 수 있다. 전통적인 사이버전은 네트워크와 컴퓨터 시스템을 공격하여 국가의 주요 기간시설과 정보 시스템을 무력화하는 형태로 나타났다. 사이버전은 공격 원점을 파악하기 어렵고 피해 규모를 예측하기 어렵다는 점에서 기존 전쟁 양상과 구별되는 특징을 가진다. 최근 주요 인물 체포 및 암살 작전, 러시아-우크라이나 전쟁, 이스라엘과 주변 무장세력 간의 갈등 사례에서도 사이버 공격의 영향력이 강화되는 것을 확인할 수 있다. 한편 Anthropic, OpenAI와 같은 대형 인공지능(AI) 기업들이 사이버 보안 분야에 점차 큰 영향을 미치고 있으며, AI 기술의 발전은 사이버 공격과 방어 모두에 새로운 가능성을 제시하고 있다. 본 연구에서는 현대 사이버전의 주요 동향과 그 의미를 살펴보고자 한다.

[ABSTRACT]

Cyberspace has emerged as a major battlefield in modern warfare. Although intangible compared to traditional physical battlefields, its destructive impact can be significant. Cyber operations include command-and-control system hacking, critical infrastructure disruption, and online psychological warfare. Recent conflicts—such as the Russia–Ukraine war and clashes between Israel and surrounding armed groups—demonstrate the increasing role of cyber attacks in modern warfare. Cyber warfare is also characterized by the difficulty of identifying attackers and assessing the scale of damage, distinguishing it from conventional warfare. Meanwhile, major AI companies such as Anthropic and OpenAI are beginning to influence the cybersecurity field, as the rapid development of generative AI creates both new opportunities and risks for cyber operations. Therefore, this study examines recent developments in cyber warfare and its growing impact on national security and modern conflict.

Key Words : Cyber warfare(사이버전), AI Cyber Security(인공지능 사이버 보안), Anti-Tampering(안티 탬퍼링)

1. 서 론

장기간 수행된 사이버전의 결과, 이스라엘은 헤즈볼라 지휘부에 심각한 타격을 가한 것으로 알려졌다. 러시아-우크라이나 전쟁에서는 사이버 공격이 드론과 더불어 전쟁의 주요 전력 요소로 부상하였으며, 미국이 실시한 대 베네수엘라 및 이란 군사 작전에는 인공지능(AI) 기술이 본격적으로 사이버전에 사용되기 시작했다.

현대 사이버전은 다양한 양상으로 발전하고 있다. 전통적인 사이버 공격은 주로 악성코드를 이용하여 국가의 기간시설을 무력화하는 데 목적이 있었다. 그러나 최근 사례에서는 컴퓨터 네트워크 공격을 넘어 상대국 군인과 민간인을 대상으로 한 심리전에서도 큰 영향을 미치고 있다.

과거에는 인간 정보원을 침투시켜 상대의 사기를 저하시키고 정보를 획득하는 방식이 주로 사용되었으나, 이제는 딥페이크로 생성된 가짜 뉴스의 확산이나 지휘체계 해킹 등을 통해 저렴한 비용으로 상대 내부의 혼란을 유도하는 방식이 활용되고 있다. 사이버전은 이제 명실상부하게 현대 전쟁의 주요 전장으로 부상하고 있다[1].

사이버 공간은 기존의 전통적인 전장과 달리 무형적이지만, 그 파괴력과 공격 효과는 물리적 타격에 비견되고 있다. 본 연구에서는 사이버전에 대한 개념과 대표적 무기를 알아보고, 최신 사례를 분석하여 현재 사이버전이 어떻게 진행되고 있는지 살펴본다.

1) 서울사이버대학교 컴퓨터공학과 (The Department of Computer Science and Engineering, Seoul Cyber University, Korea), E-mail: jlee@iscu.ac.kr
2) 서울사이버대학교 AI크리에이터학과 (The Department of AI Creation, Seoul Cyber University, Korea), E-mail: howardkim@iscu.ac.kr

Received : March 17, 2026 Revised : March 30, 2026
Accepted : March 30, 2026

2. 사이버전의 개념

2.1 사이버범죄와 사이버전

UN 제10차 범죄 방지 및 범죄자 처벌을 위한 회의(Commission on Crime Prevention and Criminal Justice)에서 사이버 범죄는 '네트워크 또는 컴퓨터 시스템의 보안 및 데이터를 대상으로 하는 컴퓨터 사용의 위법행위'로 정의되었다[2]. 여기서 정의된 불법 활동은 사이버전 개념의 기반이 된다. 사이버전은 영어로 Cyber War가 아닌 Cyber Warfare로 표기한다. Warfare는 특정 도메인 또는 특별한 유형의 무기체계가 사용되는 전쟁 행위를 의미하고, War는 두 단체 간 무력충돌을 뜻한다[3]. 즉, 사이버전은 사이버 공간이라는 영역에서 수행하는 전투를 의미한다고 할 수 있다.

2.1.1 미국

2010년 미국 정부의 보안 전문가 Richard Clarke는 사이버전을 '특정 국가가 다른 국가의 컴퓨터나 네트워크를 공격하여 피해를 입히거나 파괴할 목적으로 취하는 행동'이라 정의하였다. 미국 국제전략연구소(CSIS)는 사이버전을 '정보시스템과 네트워크를 겨냥하여 데이터, 소프트웨어, 물리적 공격이 대규모로 이루어지는 상태'로, 미국 랜드연구소(RAND)는 '상대국 정보 및 통신 시스템을 파괴 또는 무력화하는 군사작전'이라고 정의하였다.

표 1. 사이버전 정의
Table 1. Definition of cyber warfare

연구자	정의
Clarke	상대국 네트워크를 공격하여 피해를 유발하는 것
CSIS	정보 시스템과 네트워크에 대한 대규모 공격
RAND	정보통신 시스템 파괴 및 무력화 목적의 군사작전

2.1.2 국내

국내에서는 2007년 '합동·연합작전 군사용어사전'에서 사이버전을 '컴퓨터가 합성한 가상현실의 세계와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간(cyber space)에서의 전쟁으로, 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 가할 수 있는 총체적인 가상공간에서의 정보마비전을 추구하는 전쟁수행 방식'이라 정의하였다. 국방기술품질원의 '국방과학기술용어사전'에서는 사이버전을 '디지털화된 정보가 유통되는 가상공간에서 적의 정보 체계를 교란, 통제, 파괴하는 공격과 방어 활동'으로 기술하고 있으며[4], 현재 국내에서는 이 정의가 널리 사용되고 있다.

2.2 제5의 전쟁영역

2010년 7월 영국의 유력지 이코노미스트는 '사이버 공간은 제5의 전쟁영역'이라 기술했다[1]. 전통적인 전장인 육지, 해상, 공중, 우주에 이어 '사이버 공간'을 새로운 공간으로 규정한 것이다. 또한 같은 해 미국 국방부 부장관인 William J. Lynn은 '펜타곤은 공식적으로 사이버 공간을 전쟁의 새로운 영역으로 인식하고 있으며 육, 해, 공, 우주의 군사 작전에 있어 매우 중요한 부분이 되었다.'고 언급하였다.

사이버 공간은 가상공간의 하위개념으로, 컴퓨터 기술로 인해 만들어졌으며 상호 커뮤니케이션이 일어나는 공간을 말한다. 정보의 접근성과 이동성이 높고, 단순한 현실 모사가 아닌 또 다른 실재이면서, 비선형적이고 입체적인 성격을 지닌다. 감시와 통제가 용이하며 그 방식도 고도화된 특징을 지니고 있다[5][6]. 2010년 미국에서 사이버 사령부가 창설된 것은, 군사적 전장 측면에서 사이버 공간을 고려하기 시작한 것이라 할 수 있다.

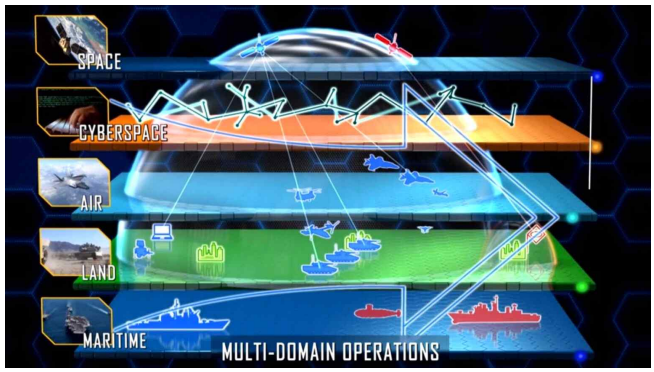

그림 1. 다전장 운영[7]
Fig. 1. Multi domain operations

이상과 같이 지금까지 이루어진 국내외 연구를 종합하면, 사이버전이란 '사이버 공간에서 벌어지는, 컴퓨터 또는 네트워크를 이용하여 상대국의 시스템을 무력화하는 일련의 활동'이라 규정할 수 있다. 다만, 컴퓨터 네트워크를 이용한 모든 공격을 사이버전이라 지칭할 수는 없다. 사이버전은 일반적인 사이버 공격과 구분되며, 국가 또는 배후 조직이 상대 국가의 안보 시스템 및 기간시설 등에 중대한 위협을 가하는 공격 수준이어야 사이버전이라 할 수 있다[8].

2.3 사이버전 특징

2.3.1 전통적 공격과 차이

사이버 공격은 전통적인 군사 공격과 구별되는 몇 가지 특징을 가진다. 첫째, 물리적 무기가 필요하지 않아 비용이 적게 든다. 사이버 공격은 코드와 소프트웨어를 이용하여 컴퓨터 시스템과 네트워크의 취약점을 악용하며, 비교적 낮은 비용으로도 수행될 수 있다. 둘째, 높은 파급력과 막대한 피해 가능성이다. 사이버 공격은 즉각적인 물리적 파괴를 동반하지 않더라도 국가 기반시설, 정보 시스템, 경제 활동 등에 심각한 영향을 미칠 수 있으며, 데이터 유출이나 서비스 중단과 같은 피해를 초래할 수 있다. 셋째, 익명성과 추적의 어려움이다. 공격자는 다양한 기술을 이용해 신원을 숨길 수 있어 공격 주체를 규명하기 어렵다. 넷째, 빠른 확산 가능성이다. 인터넷의 특성상 사이버 공격은 빠르게 확산되어 여러 국가와 조직에 동시에 영향을 미칠 수 있다[9]. 다섯째, 비대칭성으로 인한 비국가 행위자의 참여이다. 해커 그룹이나 민간 조직 등 다양한 비국

가 주체들이 사이버 공격에 관여할 수 있어 사이버 위협은 더욱 복잡한 양상을 보인다[10].

표 2. 사이버전 특징
표 2. Features of cyber warfare

특징	설명
저비용	전통적 무기보다 비용 낮음
높은 파급력	국가 기능 마비 가능
익명성	공격자 추적 어려움
빠른 확산	인터넷의 특성상 전지구적으로 빠르게 확산
비대칭성	국가뿐 아니라 해커 등 비국가 행위자가 관여

이러한 사이버전 공격은 시설 무력화, 선전 선동, 간첩 활동 등 다양한 군사 작전에 적용되고 있다. 시설 무력화는 군사, 전력, 운송, 통신, 금융 시스템 등 주요 기간시설의 정상작동을 방해하는 것으로, 물리적 공격과 유사한 효과를 초래할 수 있다. 특히 DDoS(Distributed Denial-of-Service, 분산서비스거부) 공격을 통해 보안이 취약한 시스템을 손쉽게 일정 시간 작동 불능 상태로 만들 수 있다. 이는 포, 미사일 등 물리력을 동원하여 무력화하는 것보다 훨씬 저렴하고 안전한 방식이다. 또한 공공서비스, 운송 조직, 금융기관 등에 거짓 정보를 삽입하여 혼란을 야기할 수 있다. 이를 빠른 시간에 수습하지 못한다면, 실제 우크라이나 사례와 같이 국가 경제 시스템도 일정 부분 붕괴될 수 있다. 최근 대중화된 SNS를 이용한 선전선동 형태의 공격도 널리 감행되고 있다. 가짜 뉴스 등으로 국내외 여론에 영향을 미치는 심리전을 유발하는 것으로, 선전선동은 현대전에서 급속도로 그 활용성이 증가하고 있다[8]. 이 외에도 해킹, 도용 등을 이용한 대규모 간첩 활동이 사이버전을 통하여 이루어지고 있다.

2.3.2 공격 사례

대표적 악성코드 중 하나인 Regin은 상대 네트워크에 장기간 잠입하면서, 필요시 지령을 받아 상대측 정보를 빼내는 활동에 주로 사용된다. 윈도우 운영체제가 설치된 컴퓨터를 대상으로 동작하며 표적에 따라 다른 기능을 호출하여 맞춤식 첩보 활동을 가능하게 한다. 암호화된 여러 계층의 전개를 거쳐 작동되므로 코드의 존재 여부 파악이 쉽지 않기 때문에, 대상 표적에 대한 장기간 감시에 활용된다. 서버로부터 받은 지령에 따라, 입력 조작, 정보 수집, 네트워크 감시 등 필요한 기능 모듈을 작동한다. 2014년 발견되었고, 러시아와 사우디아라비아가 감염 사례의 50% 이상을 차지하고 있으며, 배후는 영국으로 추정되고 있다[11].

사이버전의 위력을 세상에 알린 악성코드는 Stuxnet이라 할 수 있다. 대상을 가리지 않고 무차별적으로 확산하는 반면, 특정 산업 시스템만을 표적으로 삼아 악성 기능이 발현한다[12]. 이란 원자력 발전소의 SCADA(Supervisory Control and Data Acquisition) 시스템을 파괴한 것이 그 대표적 사례이다. 해당 기관 연구원의 자택에 잠입하여 USB 플래시 메모리를 통해 원자력 발전 시스템으로 침투된 것으로 여겨지며[13], The New York Times에 따르면, 이 공격으로 인하여 이란의 핵무기 개발이 3년 이상 지체된 것으로 보고 있다.

WannaCry는 2017년 시작된 랜섬웨어 공격으로, 전 세계 99개국 약 23만 대의 컴퓨터를 감염시킨 대규모 사이버 공격 코드이다. 감염된 시스템에는 비트코인을 지급하면 데이터를 복구해 주겠다는 메시지가 약 20개 언어로 표시되었으며, 스페인의 텔레포니카, 영국의 NHS, 페덱스, 도이체반 등 주요 기관과 기업이 피해를 입었다[14]. 공격 규모가 매우 커 마이크로소프트는 지원이 종료된 Windows XP 등 구형 운영체제에 대해 예외적으로 보안 업데이트를 제공했으며, 공격의 배후로 북한이 지목되고 있다.

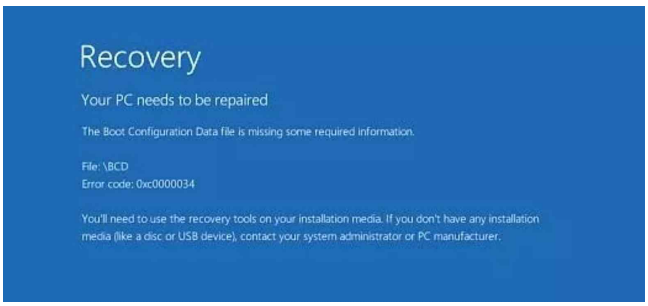

그림 2. 마스터 부트 레코드가 감염된 시스템
Fig. 2. System MBR damaged

Petya는 마스터 부트 레코드를 감염시켜 운영체제의 부팅을 방해하는 악성코드이다. 특히 2017년에 등장한 변종은 우크라이나를 공격하여, 약 4억 달러 이상의 손실을 발생시킨 것으로 알려졌다[15]. 하드디스크나 메모리의 데이터를 삭제하는 악성코드인 Wiper는 러시아-우크라이나 전에서 대대적으로 사용되었다[16]. 컴퓨터 시스템을 복구하지 못하도록 파괴한다. 2012년부터 2016년 사이에 소니 픽쳐스, 사우디아라비아의 국영에너지 기업 아람코 등에도 공격 흔적을 남겼다.

표 3. 주요 악성코드
Table 3. Malwares

악성코드	시기	목표	특징
Stuxnet	2010	이란핵시설	산업제어시스템 파괴, 최초의 사이버 무기
Regin	2014	통신·정부기관	모듈형 스파이웨어
BlackEnergy	2015	우크라이나 전력망	정전 유발
Industroyer	2016	전력망	전력 프로토콜 공격
Petya	2017	우크라이나 글로벌기업	파괴형 악성코드
WannaCry	2017	전 세계	랜섬웨어 및 웜 확산
WhisperGate	2022	우크라이나 정부	랜섬웨어 형태 wiper
AcidRain	2022	위성통신망	위성 모뎀 공격

2.4 사이버전 전문 조직

앞서 살펴본 것과 같이 치명적인 피해를 입힐 수 있는 사이버전에 대비하기 위해, 각국에서는 군에 사이버 작전을 전문적으로 담당하는 기관을 두고 있다.

2.4.1 미국

그림 3. 사이버 공간에서의 네 가지 행동[17]
Fig. 3. Cyber actions

사이버 공간의 공격 및 방어가 군사작전의 중요 영역으로 부상하면서, 군 관련 네트워크를 보호하고 다른 국가 시스템을 공격하기 위한 목적으로 미군은 2010년 사이버 사령부(USCYBERCOM)를 창설하였다.

Brett T. Williams 장군이 기술한 바에 의하면, 사이버 사령부는 사이버 공간 내 자유로운 활동을 보장하고, 사이버 공간에 전력을 투사하는 것을 목표로 한다. 사령부의 임무는 정보네트워크(DODIN, Department of Defense Information Network)를 운영하고, 사이버 공간 방어작전(DCO, Defensive Cyber Operations)과 사이버 공간 공격작전(OCO, Offensive Cyber Operations)을 수행한다. 이에 대한 실행 조치로 사이버 환경작전준비(OPE, Operational Preparation of the Environment), 사이버 감시정찰(Intelligence, surveillance, and reconnaissance), 사이버 공간 방어, 사이버 공간 공격 등을 열거하고 있다[17].

2.4.2 국내

2010년 국방정보본부 예하로 국군사이버사령부가 창설되었다. 2019년 사이버작전사령부로 명칭이 변경되었고 현재 합동참모의장의 통제를 받는 합동부대이다. 2019년 2월 시행된 사이버작전사령부의 시행령에 의하면 사이버작전의 계획 및 시행, 사이버작전과 관련된 사이버 보안 활동, 사이버작전에 필요한 체계 개발 및 구축, 사이버작전에 필요한 전문 인력의 육성 및 교육훈련, 사이버작전 유관기관 사이의 정보 공유 및 협조체계 구축, 사이버작전과 관련된 위협 정보의 수집·분석 및 활용 등을 사이버작전사령부의 임무로 규정하고 있다.

3. 사이버전 양상의 역사적 전개

3.1 이스라엘과 무장세력 갈등

2023년 10월 발발한 이스라엘과 하마스, 헤즈볼라 등 무장세력과의 갈등 과정에서도 사이버전은 중요한 역할을 담당하였다. 특히, 평상시에는 정보 수집과 감시를 중심으로 이루어지다가, 실제 충돌이 발발하였을 때 쌓아온 정보를 이용하여 무력의 효과를 극대화하는 특징을 보여주었다.

3.1.1 하마스의 사이버전

하마스는 이스라엘 병사들이 많이 사용하는 스마트폰 앱에 악성코드를 심어, 군사 정보 및 시설 영상 등 다양한 정보를 사전에 해킹하였다. 대대적인 물리적 공격과 동시에 수집한 정보를 바탕으로 공공 기관 대상 사이버 공격을 시행하였다. 특히 미사일 경보 시스템을 공격하여 거짓 경보 등을 발생시키고, 소셜 미디어 플랫폼에 가짜 뉴스를 확산시켜 전쟁 초기 시민의 혼란을 조성하였다[18].

그림 4. 베이루트 폭발 호출기[19]
Fig. 4. Pager in Beirut

3.1.2 이스라엘의 사이버전

이스라엘은 헤즈볼라의 작전을 감청하여 무선호출기를 구비할 계획이 있다는 사실을 알아내었다. 이후 무선호출기 유통망에 잠입하여 수십 그램 이내의 군용 폭약을 각 호출기마다 설치하고, 특정 번호를 수신할 때 폭약이 폭발하도록 프로그래밍하였다. 2024년 9월 17일 해킹당한 무선호출기가 폭발하면서 헤즈볼라 지휘부와 그 가족 등 약 4,000명이 사망하거나 부상당하며 헤즈볼라 지휘부에 심대한 타격을 입혔다[20]. 2024년 9월 27일에는 사이버 스파이 활동을 통해 파악한 헤즈볼라 지휘부의 잠입 장소를 조준하였다. 해당 지점에 벙커버스터 수백 발을 2초 간격으로 정밀하게 집중적으로 타격하여 헤즈볼라 지휘부를 사실상 궤멸하였다. 이스라엘은 2006년 헤즈볼라와의 무력 충돌 이후 거의 20년간 이를 준비해 왔던 것으로 알려졌다[21].

3.1.3 특징

사이버전은 전쟁 발발 이후뿐 아니라 전쟁 발발 이전의 평상시에도 그 위력을 발휘한다는 특징이 있다. 특히, 이스라엘은 레바논 헤즈볼라와 2006년 교전한 이후 정보전의 중요성을

깨닫고 다양한 채널을 통하여 꾸준히 사이버전을 진행해 왔다. 이스라엘 군이 전통적으로 중시하고 있는 압도적인 공군력 우세전략보다, 이러한 사이버 정보전이 비용 대비 효과 면에서 더 뛰어난 것으로 밝혀지고 있다.

3.2 러시아 우크라이나 전쟁

2022년 2월 발발한 러시아-우크라이나전은 드론과 사이버전의 전쟁으로 볼 수 있다. 양측은 지속적으로 사이버 공격을 시도하고 있으며, 특히 우크라이나는 해외 기관과 협력하면서 사이버 방어 능력을 강화하였다. 미국, EU 및 거대 IT기업들과 협력하여 러시아의 공격에 대처하고 있다.

3.2.1 전쟁 발발 전

러시아는 우크라이나에 악성코드 등을 이용한 공격으로 전력망을 해킹하고, 국가 재정 마비를 시도하는 등 여러 가지 사이버 공격을 감행하였다. 이에 우크라이나는 미국 사이버사령부와 공동작전을 실시하여 실전과 유사한 경험을 축적하면서, 정책적으로도 사이버 보안 프로그램을 통해 다수의 IT 전문가를 배출하는 등 사이버전 대응 능력을 강화하였다.

3.2.2 전쟁 발발 후

전쟁 초기 러시아는 우크라이나 군이 사용하는 위성 통신망을 공격하여 군 통신 체계를 마비시켰다. 이로 인해 우크라이나의 군사 지휘통제 체계가 상당 부분 무력화되었으며, 전쟁 초기 우크라이나의 작전 수행 능력에 심대한 영향을 미친 것으로 평가된다[22].

또한 러시아는 전쟁 발발과 동시에 DDoS 공격과 악성코드를 활용하여 우크라이나의 공공기관과 민간기업 수백 개 조직의 시스템을 공격해 정상적인 운영을 어렵게 만들었다. 국영 원자력 기업 웹사이트에는 약 700만 개의 악성 봇을 동원해 3시간 동안 공격을 가하는 등 여러 기관의 기능을 일시적으로 마비시켰다. 또한 주요 방송사가 해킹되어 가짜 뉴스가 전파되는 사례도 발생하였다. 글로벌 인터넷 감시 단체인 넷블록스(NetBlocks)에 따르면, 이러한 기간시설 공격의 영향으로 우크라이나의 네트워크 연결성은 전쟁 이전 대비 약 13% 수준까지 감소한 것으로 보고되었다[23].

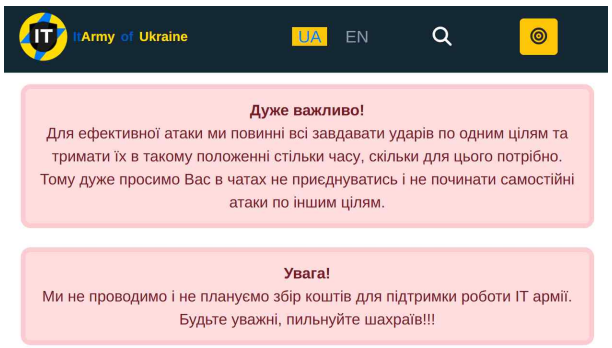

그림 5. 우크라이나 IT Army 사이트[24]
Fig. 5. Website of IT army of Ukraine

이에 우크라이나는 미국과 유럽 연합의 지원을 받아 사이버 공격에 대응했다. IT Army를 모집하여 민간 해커 조직 등으로 구성된 온라인 병사를 동원하였다. 이들은 800개 이상의 목표를 동시에 공격할 수 있다고 알려져 있으며, 러시아 웹사이트를 공격하고 여론전을 펼쳤다.

미국의 IT 대기업들도 사이버전에 참여하여 우크라이나를 지원하였다. Apple, Netflix, Meta, X 등은 러시아에 대한 서비스 제한과 더불어 가짜뉴스 차단방안을 강구하였다. Amazon은 AWS 클라우드를 이용해 우크라이나 정부 데이터를 보호하였고, Google은 우크라이나에서 러시아 국영매체의 애플리케이션 내려받기를 금지시켰다[25][26]. 특히, SpaceX는 스타링크를 공급하여 우크라이나가 통신망 피해로 인해 지휘통제 기능이 마비되는 것을 방지하였다[27].

표 4. IT 대기업의 사이버전 지원
Table 4. Big Tech contributions to cyber warfare

기업	지원 내용
Meta	허위정보 차단 및 정보전 대응
Amazon	정부 데이터 AWS 클라우드 이전 및 보호
Google	DDoS 방어, 해킹 분석, 웹 인프라 보호
SpaceX	Starlink 위성 인터넷 및 통신 인프라 제공
Microsoft	악성코드 탐지 및 Azure 클라우드 이전

3.3 국내 사이버 공격 사례

국내 인터넷 환경이 구축된 이후, 기관을 대상으로 배후 세력이 북한으로 추정되는 사이버 공격이 다수 발생하고 있다. 아래는 주요 공격을 기술한 것이다.

표 5. 국내 주요 사이버 공격 사례
Table 5. Domestic cyber attack cases

연도	대상	공격 유형	주요 특징
2009	정부/금융기관	DDoS	한미 동시 공격
2013	방송사/금융기관	전산망 마비	대규모 시스템 중단
2016	국방부 인트라넷	내부망 침투	백신 공급망 공격
2023	법원 전산망	데이터 유출	장기간 침투
2024	국방부	DDoS	국제 정세 연계 공격
2025	글로벌 거래소	자산 탈취	역대 최대 규모

3.3.1 대한민국 및 미국 공공기관 DDoS 공격

2009년 7월 7일부터 10일까지 약 4일간 청와대, 국회, 국방부 등 대한민국 국가기관 및 금융기관 17곳이 DDoS 공격의 피해를 입었다. 이는 7월 4일부터 미국 백악관과 국방부, 아마존 등 미국의 공공 및 민간기관 14곳이 공격을 받은 후 연속적으로 발생한 사이버 공격이었다. 국정원은 북한 사이버 세력 라자루스가 공격의 배후로 추정된다고 발표하였다[28].

3.3.2 방송국 및 금융기관 전산망 공격

2013년 3월 주요 방송국, 금융기관 등 6곳의 전산망이 네트워크를 통한 공격을 받아 마비되었고, 시스템 운영에 차질이 생기며 업무가 중단되었다. 민관군 합동대응팀은 북한 정찰총국 소행으로 추정하였다[29].

3.3.3 군 내부 인트라넷 해킹

2016년 9월에는 군 내부용 인트라넷이 해킹당하고 악성코드가 전파되었다. 군 내부용 인트라넷은 외부선과 물리적으로 단절되어 있다. 조사 결과 국방부 백신 납품업체의 컴퓨터를 해킹하여 국방부 인증서와 백신 코드 정보를 탈취하고, 이를 이용하여 국방부 내부망에 침입한 것으로 확인되었다. 이 공격으로 군 인터넷 PC 약 2,500대와 내부용 PC 700대 등 총 3,200여 대의 컴퓨터가 감염 피해를 입었다. 공격에 사용된 IP 중 일부가 북한 해커용 IP로 식별되었고, 북한 해커가 사용하는 악성코드와 유사한 것으로 확인되었다[30].

3.3.4 가상자산 거래소 해킹

2019년 11월 27일 가상자산 거래소인 업비트가 해킹당하였다. 업비트의 이더리움 342,000개가 탈취되었는데, 이는 해킹 당시 약 580억원 정도의 수량으로 2026년 현재 1조원 이상의 가치를 지니고 있다. 코드에서 북한 어휘가 사용된 흔적이 발견되었으며, 북한 정찰총국과 해커조직 라자루스, 안다리엘이 공격에 동원된 것으로 추정된다. 해킹된 가상자산은 13개 국가의 거래소 51곳으로 전송되어 자금 세탁이 이루어졌다[31].

3.3.5 법원 전산망 해킹

2023년 2월 법원 전산망이 해커에게 침투되었다. 국내 4곳과 해외 4곳에 위치한 총 8대의 서버가 해킹되어 2년간 약 1천GB 이상의 자료가 유출된 것으로 밝혀졌다. 7대 서버는 저장기간이 만료되어 해킹된 흔적이 삭제되었으나, 남은 1대 서버에서 개인정보 파일 등을 포함하여 5천여 개의 파일이 유출된 것으로 확인되었다. 국정원, 검찰, 경찰 합동 수사 결과 북한 해킹조직 라자루스를 배후로 추정하였다[32].

3.3.6 가상자산 자금 세탁

2023년 8월 라자루스와 북한 정찰총국 소속 단체가 비트코인 약 1,580개를 해킹한 것이 미국 FBI에 의해 관찰되었다. 해킹한 가상자산은 6개 주소로 분배되었으며, 9개월 후 자금이 저장된 6개의 주소 중 한 주소에서 비트코인 287개가 이동하는 것이 실시간으로 포착되었다[33]. 가상자산은 자금 흐름의 기록이 남기 때문에 해킹 당시의 배후를 추적할 수 있다면 이후의 자금 흐름을 상대적으로 수월하게 알아낼 수 있다.

3.3.7 국방부 홈페이지 공격

2024년 11월 5일 국방부와 합동참모본부의 홈페이지에 대한 DDoS 공격이 발생하였다. 러시아-우크라이나 전쟁과 관련하여 우리나라가 우크라이나에 무기 지원을 암시하고, 전쟁 참관단을 파견하는 것 등에 자극을 받은 러시아가 공격의 배후로 추정되고 있다[34].

3.3.8 가상자산 탈취

2025년 2월 21일 전세계 주요 가상자산 거래소 중 하나인 Bybit에서 역대 최대인 14.6억 달러 상당의 가상자산이 탈취된 사고가 발생하였다. 배후는 북한의 라자루스로 추정된다. 국가 간 사이버전이 이제 사이버 범죄와 병행되는 양상을 보이고 있다.

3.3.9 그 외

상대국의 무기나 군 시스템에 가짜 반도체 칩을 설치한 것이 속속 밝혀지고 있다. 가짜 칩은 원본과 똑같은 모양을 하고 무기체계 내에서 기능상 차이가 없다. 기존의 칩 위에 있는 정보를 지우고 제작한 가짜 칩을 아군 시스템의 서버에 넣은 것으로, 이를 이용한 정보 탈취가 의심되고 있다[35].

4. AI 기반 사이버 보안 기술

4.1 AI 기반 사이버 보안 기술의 발전

최근 AI 기술의 발전은 사이버 보안 분야에도 큰 변화를 가져오고 있다. 전통적인 사이버 보안 시스템은 주로 규칙 기반(rule-based) 탐지 방식이나 서명 기반(signature-based) 탐지 방식에 의존해 왔다. 이러한 방식은 이미 알려진 공격 패턴을 탐지하는 데에는 효과적이지만, 새로운 공격 방식이나 제로데이 취약점을 이용한 공격을 탐지하는 데에는 한계가 존재한다.

이러한 문제를 해결하기 위해 최근 사이버 보안 분야에서는 AI를 활용한 보안 기술이 적극적으로 도입되고 있다. AI는 대규모 보안 로그, 네트워크 트래픽, 소프트웨어 코드 데이터를 분석하여 정상적인 패턴과 이상 행위를 구분할 수 있으며, 이를 통해 새로운 유형의 사이버 공격을 탐지할 수 있다. 특히 생성형(Generative) AI의 발전은 보안 분석 과정의 자동화를 크게 향상시키고 있다. 생성형 AI의 자연어 처리 능력과 코드 해석 능력을 활용하여 보안 취약점을 탐지하고 공격 패턴을 찾아낸다.

4.1.1 OpenAI의 Aardvark

주요 AI 개발 기업인 OpenAI가 2025년 11월 공개한 바에 의하면, Aardvark라는 자동화된 사이버 보안 분석 도구를 보안 문제 해결에 활용할 수 있다. 이 도구는 생성형 AI를 활용하여 복잡한 보안 문제를 분석하고 해결 방안을 제시하는 시스템이다.

Aardvark 시스템을 작동하면 첫째, 보안 문제에 대한 질문을 분석하고 모호한 부분을 식별한다. 둘째, 문제를 여러 관점에서 분석하는 분리된 관점(Disentangled Perspective) 접근 방식을 적용한다. 셋째, 각 분석 관점에서 도출된 결과를 통합하여 최종 보안 대응 방안을 제시한다.

이와 같은 방식은 보안 분석 과정에서 인간 전문가의 의사결정을 지원하는 역할을 수행한다. 특히 복잡한 보안 문제를 여러 관점에서 분석함으로써 기존 보안 도구가 놓칠 수 있는 취약점을 발견하는 데 도움을 줄 수 있다.

또한 CrowdStrike, Palo Alto Networks와 같은 기존 보안

기업들도 소프트웨어 개발 과정에 AI 기반 보안 도구를 도입하고 있다. 이는 AI 기술이 기존 사이버 보안 산업 구조에도 영향을 미치고 있음을 보여준다.

4.1.2 Anthropic의 Claude Code Security

Anthropic은 생성형 AI 모델인 Claude를 기반으로 Claude Code Security라는 AI 기반 보안 분석 기술을 개발 중이다. 기존의 규칙 기반 보안 스캐너는 알려진 취약점 패턴을 코드와 대조하여 취약점을 탐지하는 방식으로, 새로운 유형의 취약점을 발견하는 데 한계가 있다. 반면 Claude Code Security는 AI의 추론(reasoning) 능력을 활용하여 전체 코드베이스를 분석한다. AI는 소프트웨어 구성 요소 간의 상호작용을 분석하여 기존 보안 도구나 인간 분석가가 놓칠 수 있는 복잡한 취약점을 탐지할 수 있다. 또한 AI 시스템은 발견된 취약점의 심각도를 평가하고, 문제에 대한 설명과 함께 권장되는 보안 패치까지 자동으로 생성한다.

Anthropic의 연구 결과에 따르면 이 기술은 이미 운영 중인 오픈소스 프로젝트에서 500개 이상의 심각한 보안 취약점을 새롭게 발견한 것으로 보고되었다. 이러한 취약점은 과거 수년간의 보안 검토 과정에서도 발견되지 않았던 것이다[36].

4.2 AI 기반 사이버 보안 기술의 양면성

AI 기술은 사이버 방어 기술이 되는 동시에 새로운 사이버 공격 도구로도 활용될 수 있는 양면성을 가진다. AI 보안 도구는 코드 취약점 탐지, 보안 로그 분석, 악성 코드 분석, 자동 보안 패치 제안 등 기능을 수행할 수 있다. 그러나 이러한 기능은 공격자에게도 활용될 수 있다. 공격자는 AI를 활용하여 소프트웨어 취약점을 빠르게 탐색하거나 자동화된 공격 도구를 개발할 수 있다.

이를 방지하기 위해 Anthropic의 보안 시스템에서는 다단계 검증 과정(multi-stage verification)을 적용하고 있다. AI가 자동으로 코드 수정 사항을 적용하지 않도록 하고, 모든 변경 사항은 개발자의 승인 과정을 거치도록 설계되어 있다.

4.3 기존 사이버 보안 산업에 미치는 영향

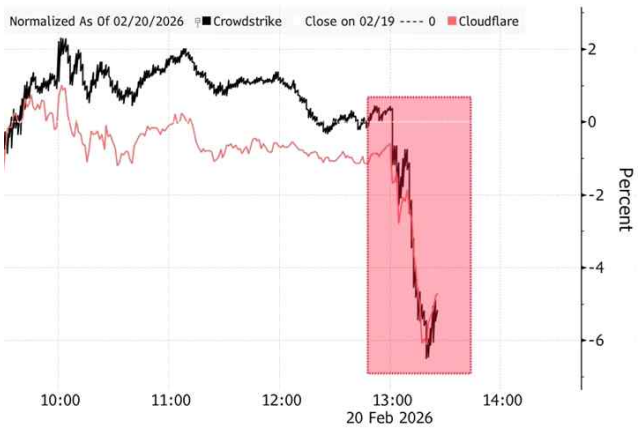

그림 6. AI 등장으로 인한 기존 사이버 보안 기업 주가하락[37]
Fig. 6. Impact of AI on cyber security firms' stock prices

AI 기반 보안 기술의 발전은 기존 사이버 보안 산업에도 영향을 미치고 있다. 과거 규칙 및 서명 기반 탐지에 의존하던 보안 시스템은 이제 대규모 데이터 분석과 자동화된 대응을 지원하는 AI 중심으로 패러다임이 전환되고 있다. 생성형 AI 기업들의 보안 시장 진출로 기존 제품군의 수요 감소 우려가 커지는 것은 금융시장의 반응을 통해 확인할 수 있다. Claude Code Security 발표 이후 CrowdStrike, Cloudflare, GitLab, Okta, Palo Alto Networks, Zscaler와 같은 주요 사이버 보안 기업들의 주가가 크게 하락하였다. 글로벌 사이버 보안 상장지수 펀드 역시 약 5% 하락한 것으로 나타났다[38]. 기존 보안 기업의 솔루션 또한 AI 기반 보안 플랫폼으로의 전환이 요구되는 추세이다.

4.4 정부와의 갈등

AI 기술의 군사적 활용을 둘러싸고 기술 기업과 정부 사이의 갈등도 나타나고 있다. Anthropic은 미국의 군사 기밀에 자사의 AI를 적용한 최초 기업 중 하나이지만, 자사의 AI 기술이 기업의 이념과 다르게 사용되는 것에 대해 우려를 표명하고 있다. Anthropic의 창립자이자 최고경영자인 Dario Amodei는 자사의 AI 모델인 Claude가 자율 무기 시스템이나 대규모 민간인 감시 체계에 사용되는 것을 금지하는 정책을 발표하였다[39].

반면 미국 국방부는 군사 작전에 AI 기술을 활용하는 것이 국가 안보 차원에서 필요하다는 입장을 보이고 있다. 국방부는 군의 AI 도구 활용은 법률에 의해서만 제한될 뿐, 기업이 설정한 가이드라인에 의해 제한되어서는 안 된다고 주장하였다[40]. 또한 미국 정부는 기업이 군사적 활용을 거부할 경우 해당 기업을 공급망 위험 요소로 간주할 수 있으며, 기존의 법률을 활용하여 기업의 기술을 군사적으로 활용할 수 있다는 입장을 밝히기도 하였다.

4.5 AI 기술의 군사적 활용

AI 기술은 실제 군사 작전에서도 활용되고 있다. 미국이 실행한 2026년 1월 베네수엘라 마두로 대통령 체포 작전과 2026년 2월의 이란 공습에서, Anthropic의 Claude AI는 정보 분석, 목표물 식별, 전투 시나리오 시뮬레이션 등 군사 작전에 활용된 것으로 알려져 있다[39]. 미국의 대표적인 국방·정보 분석 기업 Palantir는 사이버 보안, 군사 정보전 및 디지털 전장 운영 지원과 더불어, 사이버전과 기존의 전통적인 군사작전을 통합하는 AI 기반 디지털 전장 플랫폼을 개발 중인 것으로 알려져 있다. 이와 같은 사례는 AI 기술이 단순한 보안 도구를 넘어 군사 전략에서 중요한 역할을 수행하기 시작하였음을 보여준다.

5. 사이버전 대비 현황

5.1 기술 현황

적국의 정보 탈취 및 시스템 무력화 시도를 원천적으로 차단하기 위한 하드웨어 방어 기술 등 사이버 보안 기술 동향을 살펴본다.

5.1.1 안티 탬퍼링 과제

외부에서 기술 자산을 탈취할 수 없도록 방어하는 기술을 안티 탬퍼링이라 한다. 안티 탬퍼링에는 물리적 방책부터 전문적 지식을 이용한 소프트웨어적 방책까지 다양한 분야가 있다. 하드웨어적 안티 탬퍼링은 기술 자산을 하드웨어를 이용하여 방어하는 기술이다. 핸드폰 덮개를 떼어낼 때 모양이 맞지 않는 렌치로 무리하게 힘을 주면 기기가 고장 나는 것이 한 예이다. 특히 반도체 공급망이 글로벌화됨에 따라 이러한 위협에 대비하기 위한 하드웨어적 안티 탬퍼링 기법 연구가 활발히 진행되고 있다. 대표적인 기법인 논리 잠금(Logic Locking) 기술은 칩 설계 단계에서 추가적인 논리 게이트를 삽입하여, 인가된 키값이 입력되지 않으면 하드웨어가 정상 동작하지 않도록 기능을 잠그는 방어 기술이다[41].

소프트웨어적 안티 탬퍼링은 주로 프로그래밍을 이용한 방법으로 기술 유출을 방지하는 것을 말한다. 코드에서 클래스명, 변수명 등의 정보를 제거하는 안티 리버싱, 리버스 엔지니어링을 막기 위해 디버깅이 불가능하도록 코드를 작성하는 안티 디버깅, 코드에 대한 바이너리 분석을 시도할 때 실제와 다른 명령어들을 보이게 하는 안티 디스어셈블리, 리버스 엔지니어링 시도 시 코드 이해를 어렵게 하도록 하는 난독화 등 다양한 기법이 있다. 현재 민군 여러 조직에서 다양한 세부 분야에 대한 안티 탬퍼링 과제들이 진행되고 있다[42][43].

5.1.2 사이버 보안 기술 수출

북한의 공격 등으로 인하여 쌓아온 노하우를 바탕으로 국내 사이버 보안 기술을 외국에도 전수하고 있다. 국내 사이버 보안 기관인 KISA는 이탈리아 기업 Ferrovie dello Stato를 공격한 해킹그룹인 Hive Ransomware에 대한 암호 해독기를 공개하여 사이버 보안 기술을 지원한 바 있다[44].

5.2 정책 현황

5.2.1 RMF

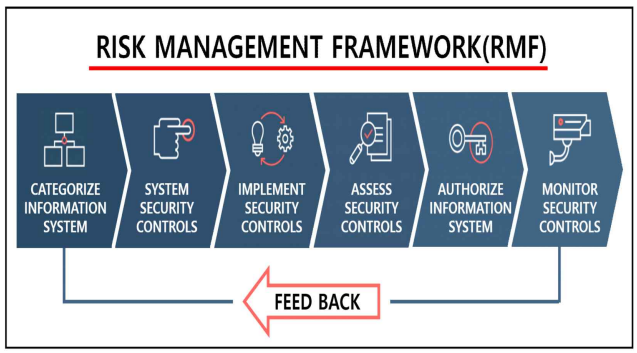

그림 7. 위험관리체계 절차[45]

Fig. 7. Process of risk management framework

RMF(Risk Management Framework, 위험관리체계)는 미국의 국립표준기술연구소에서 최초로 개발한 표준 및 절차 규정 지침이다. RMF는 국방 분야에 도입되는 무기체계, 전력지원체계 등 각종 체계에 대하여, 기획부터 도입 및 폐기까지 전 단계에 걸쳐 보안 개념을 적용한다는 것이다. 기존의 체크리스트 방식에서 벗어나, 위험을 평가하고 해당 항목에 대한 접근 권한을 부여하는 인가방식으로 보안대책을 전환한다. 우리나라는 2026년까지 K-RMF(한국형 위험관리체계) 적용을 확대하는 방향으로 목표를 세우고, 표준 연구와 인력 양성 등 세부사항을 계획하고 진행 중이다[46]. 또한, 분산되어 있는 사이버 보안 지휘체계를 하나로 통합하려는 시도도 정책적으로 시행하고 있다. 대통령 직속 '국가사이버안보위'를 설치하여 컨트롤타워 운영체계 및 기관별 역할 등을 규정한 법령 제정을 추진하고 있다[47].

5.2.2 CMMC

CMMC(Cybersecurity Maturity Model Certification, 사이버 보안 인증제도)는 국방부 공급망 업체들이 충분한 사이버 보안 수준을 갖췄는지 인증하는 제도이다. 군 계약업체는 취급 정보 민감도, 계약 등에 따라 적절한 레벨의 CMMC 인증을 받을 필요가 있다. 미국의 경우 2025년 9월 조달규칙(DFARS)을 개정하여, 향후 미 국방부(DoD) 계약 요구사항에 공식적으로 인증을 포함하도록 하였다.

표 6. RMF와 CMMC 비교

Table 6. RMF vs CMMC

구분	RMF	CMMC
개발 기관	미국 국립표준기술연구소 (NIST)	미국 국방부 (DoD)
목적	정보시스템의 보안 위험을 식별·평가·관리하는 체계	국방 공급망 정보 보호 및 사이버 위협 대응
적용 대상	정부기관 및 관련 정보시스템	국방부 계약에 참여하는 방산 및 공급망 기업
핵심 개념	위험 기반 (Risk-based) 보안 관리	보안 성숙도 기반 (Maturity-based) 인증
평가 방식	내부 평가 및 승인기관의 위험 수용	제3자 인증기관을 통한 인증
특징	위험 관리 중심의 지속적 보안 관리 체계	인증 기반 공급망 보안 관리 체계

5.2.3 글로벌 사이버 안보 정책 동향

국제 사회와 주요국은 거시적인 사이버전 대응 정책을 강화하고 있다. UN은 사이버 공간에서의 '국가 간 책임 있는 행동 규범(Norms of Responsible State Behavior)'을 수립하여 주요 기반 시설 공격을 제한하고 사이버 분쟁을 억제하고자 노력 중이다[48]. 미국은 '국가 사이버 보안 전략(National Cybersecurity Strategy)'을 개정하여 핵심 인프라 방어를 디지털 생태계 전반으로 확대하고, 악의적 행위자에 대한 선제적인 교란 작전과 동맹국 간의 긴밀한 사이버 정보 공유 체계를 구축하는 포괄적 정책을 추진하고 있다[49][50].

5.3 개인에 대한 사이버전 위협

그림 8. 유명인 딥페이크 이미지[51]
Fig. 8. Deep fake images of Barak Obama

사이버전 공격자는 평상시부터 상대의 취약 지점을 탐색하며 시스템 내부로 침투할 수 있는 경로를 확보한다. 개인의 네트워크 이용이 증가함에 따라 사이버 공격 기법 또한 더욱 정교해지고 있으며, SNS 등을 통해 수집된 정보를 최신 AI 기술과 결합하여 공격에 활용하는 사례도 늘어나고 있다. 예를 들어 딥페이크 영상을 이용한 공격뿐만 아니라 개인의 블루투스 태그 정보와 같은 일상적 디지털 정보도 정보 유출에 악용될 수 있다[52]. 이러한 공격은 단순한 네트워크 취약점에만 국한되지 않고 사람을 매개로 이루어지기도 한다. 따라서 물리적으로 분리된 네트워크라 하더라도 완전히 안전한 환경이라고 보기는 어렵다. 이처럼 최근 사이버 위협은 국가기관이나 군사 시설뿐만 아니라 일반 개인을 대상으로까지 확대되고 있는 추세이므로 이에 대한 체계적인 대응이 요구된다[53].

5.4 사이버전 대응 전략 및 정책적 시사점

사이버전은 기술적 문제를 넘어 국가 안보와 직결되는 전략적 영역으로 발전하고 있다. 이에 따라 군·공공·민간을 아우르는 통합 사이버 방어 체계 구축과 CTI 기반 정보 공유 강화, AI 기반 보안 기술 도입을 통한 자동화된 대응 역량 확보, 민관 협력 및 국제 공조 확대, 그리고 개인 대상 사이버 위협 대응 역량 강화가 필요하다. 사이버전 대응은 국가 안보의 핵심 요소로, 기술, 정책, 제도, 협력을 포함한 통합적 접근이 요구된다고 할 수 있다.

6. 결 론

현대 사이버전은 평상시부터 지속적으로 수행되다가 물리적 충돌이 발생할 경우 그 위력이 극대화되는 방향으로 발전하고 있다. 사이버전 능력은 특정 국가의 정보 시스템과 핵심 인프라를 마비시킬 수 있는 수준에 이르렀으며, 전쟁의 양상 자체를 변화시킬 수 있는 게임 체인저로서의 위상을 점차 확립하고 있다. 실제로 미국의 베네수엘라 마두로 대통령 생포 작전 시도 사례를 비롯하여 러시아-우크라이나 전쟁, 이스라엘과 주변 무장세력 간의 갈등, 그리고 미국과 이란 간 군사적 긴장 상황 등에서 이러한 양상을 확인할 수 있다. 사이버전은 정보 수집, 심리전, 그리고 무력 충돌을 지원하는 수단으로 현대 전쟁에서 매우 중요한 요소로 부상하고 있다.

한편, 급속한 AI 기술의 발전은 사이버 보안 환경에 새로운 기회를 제공하는 동시에 위험 요인도 제기하고 있다. OpenAI와 Anthropic과 같은 기업들은 생성형 AI를 활용한 보안 분석 기술을 개발하며 사이버 보안 대응의 자동화를 추진하고 있다. 그러나 AI 기술의 군사적 활용 가능성이 확대됨에 따라 기술 기업과 정부 간의 정책적 갈등 또한 나타나고 있다.

따라서 향후 사이버 안보 전략에서는 AI 기반 보안 기술의 발전을 촉진하는 한편, AI의 군사적 활용과 윤리적 문제에 대한 정책적 논의를 병행할 필요가 있다. 궁극적으로 사이버전 대응 역량을 효과적으로 강화하기 위해서는 기술적 발전을 지속적으로 도모함과 동시에 제도적·정책적 대비 체계를 함께 구축해 나가야 할 것이다.

References

[1] The Economist, “War in the fifth domain,” Jul. 1, 2010.

[2] United Nations, “Report of the Secretary-General on the conclusions of the study on effective measures to prevent and control high-technology and computer related crime,” E/CN.15/2001/4, 2001.

[3] P. Shakarian, J. Shakarian, and A. Ruef, “Introduction to Cyber-Warfare: A Multidisciplinary Approach,” Elsevier, p. 2, 2013.

[4] Defense Agency for Technology and Quality, “Dictionary of Defense Scientific and Technical Terms,” May 31, 2021.

[5] D. Bae, “Definition and Characteristics of Cyberspace - Focused on Some Examples,” Journal of Cultural and Historical Geography, Vol. 27, No. 1, pp. 129-143, 2015.

[6] Joint Publication 3-12, “Cyberspace Operations,” Jun. 8, 2018. [Online]. Available: https://irp.fas.org/doddir/dod/jp3_12.pdf

[7] S. J. Freedberg Jr., “Project Convergence: Linking Army Missile Defense, Offense, & Space,” Breaking Defense, May 18, 2020.

[8] T. Song, “The Role of Cyber Warfare in a Full-Fledged Contemporary War: The Case of 2022 Russia-Ukraine War,” Journal of National Defence Studies, Vol. 65, No. 3, pp. 215-236, 2022.

[9] D. Shin, “A Study on the North Korea's cyber threat and its impact on National Security: Focusing on the Nation and Military Countermeasures,” Ph.D. dissertation, Dept. of Political Science and Diplomacy, Chosun Univ.,

Korea, p. 13, 2016.
[10] K. Khoirunnisa, Indrawati, Ambarwati, Y. Rahmadan, and D. Jubaidi, “Modernizing Defense Strategies in the Context of China’s Evolving Cyber Influence,” China Quarterly of International Strategic Studies, Vol. 11, No. 1, pp. 1-20, 2025.
[11] C. Kemp, “Unknown Government Using Advanced Hacking Spyware to Attack Russia and Saudi Arabia,” DataCenter Knowledge, Nov. 25, 2014.
[12] D. Kushner, “The Real Story of Stuxnet,” IEEE Spectrum, Vol. 50, No. 3, pp. 48-53, 2013.
[13] Naked History, “From friend to enemy: Iran vs Israel,” tvN, Jun. 19, 2024.
[14] S. Larson, “Massive ransomware attack hits 99 countries,” CNN, May 12, 2017.
[15] BBC News, “Global ransomware attack causes chaos,” Jun. 27, 2017.
[16] J. Tidy, “Ukraine crisis: 'Wiper' discovered in latest cyber-attacks,” BBC News, Feb. 24, 2022.
[17] B. T. Williams, “The Joint Force Commander's Guide to Cyberspace Operations,” National Defense University Press, Apr. 1, 2014.
[18] G. Kim and G. Jong, “Hamas' Cyber Attacks on Israel and Their Implications,” Issue Brief, Vol. 471, pp. 1-6, 2023.
[19] A. Abbas, “Israel's Mossad planted explosives in Hezbollah's Taiwan-made pagers: Reports,” India Today, Sep. 18, 2024.
[20] Y. Jo, “Israel's 8200 Unit's Secret... Hezbollah's 'Beeper' Explosion, Signal for All-Out War,” News 1, Sep. 20, 2024.
[21] J.-P. Rémy and H. Sallon, “By killing Hassan Nasrallah, Israeli army gets revenge for 2006 affront inflicted by Hezbollah,” Le Monde, Sep. 30, 2024.
[22] S. Koo, “Cyber warfare, psychological warfare ... now in the midst of a 'hybrid war',” YTN, Feb. 28, 2022.
[23] C. Vallance, “Ukraine war: Major internet provider suffers cyber-attack,” BBC News, Mar. 29, 2022.
[24] IT Army of Ukraine. https://itarmy.com.ua/
[25] The New York Times, “Ukraine War Tests the Power of Tech Giants,” Feb. 28, 2022.
[26] K. Collier, “Ukraine foiled Russian cyberattack that tried to shut down energy grid,” NBC News, Apr. 12, 2022.
[27] R. Lerman and C. Zakrzewski, “Elon Musk’s Starlink is keeping Ukrainians online when traditional Internet fails,” The Washington Post, Mar. 19, 2022.
[28] D. Park, “Targeting the most vulnerable days… They attacked the US network on Independence Day,” The JoongAng, Sep. 20, 2024.
[29] J. Park, “Paralyzed broadcasting and financial companies’ computer networks… Defense network breached, confidential information leaked,” Munhwa Ilbo, Aug. 10, 2021.
[30] B. Park, “Military concludes: North Korea was responsible for last year’s hacking of the defense network,” Segye Ilbo, May 2, 2017.
[31] C. Cho, “'58 billion won in Ethereum' stolen from Upbit 5 years ago... It was North Korea's doing,” The Korea Economic Daily, Nov. 21, 2024.
[32] H. Park and K. Park, “North Korea’s Lazarus Court Computer Network Hack: Personal Information of 18,000 People Leaked,” Chosun Ilbo, Oct. 23, 2024.
[33] K. Kim, “North Korean Hacking Group Lazarus Caught Moving Stolen Virtual Assets,” Boan News, May 29, 2024.
[34] T. Kim, “DDoS attack on Ministry of National Defense and Joint Chiefs of Staff… Possibility of Russian attack,” SBS, Nov. 8, 2024.
[35] W. Wan, “Chinese counterfeit parts found in U.S. weapons,” The Washington Post, Nov. 7, 2011.
[36] R. Lakshmanan, “Anthropic Launches Claude Code Security for AI-Powered Vulnerability Scanning,” The Hackers News, Feb. 21, 2026.
[37] R. Bakolia, “Cybersecurity stocks fall after Anthropic unveils Claude Code Security,” Seeking Alpha, Feb. 20, 2026.
[38] C. Hughes, “When the Frontier Labs Sneeze, the Cybersecurity Market Catches a Cold,” Resilient Cyber, Feb. 21, 2026.
[39] K. Hays, “Anthropic boss rejects Pentagon demand to drop AI safeguards,” BBC News, Feb. 27, 2026.
[40] P. Suciu, “Anthropic Set A 'Red Line,' It Won't Be The Only AI Company To Do So,” Forbes, Mar. 2, 2026.
[41] Y. Kim, “Defense technology to prevent theft of technical assets, anti-tampering... What technologies are being applied,” Boan News, Oct. 16, 2023.
[42] J. Lee, H. G. Kim, and H. Kim, “Study on Logic Locking Techniques Against SAT Attacks,” The 17th International Conference on Internet (ICONI), Okinawa, Japan, Dec. 2025.
[43] H. Lee, “ETRI Develops Security Chip Technology to Block Smartphone Hacking,” Aju News, May 22, 2014.

[44] Redazione BitMAT, “Not paying the ransom is the golden rule for 5 reasons,” Jun. 30, 2022.
[45] W. Yang, S. Cha, J. Yoon, H. Kwon, and J. Yoo, “Korean Security Risk Management Framework for the Application of Defense Acquisition System,” Journal of The Korea Institute of Information Security & Cryptology, Vol. 32, No. 6, pp. 1183-1192, 2022.
[46] H. Kim, “Raising the level of domestic cybersecurity by establishing K-RMF,” Engineering Journal, Oct. 13, 2013.
[47] J. Lee, “Establishment of the ‘National Cyber Security Committee’ under the President… Training of 100,000 Cyber Warfare Warriors,” Digital Daily, May 3, 2022.
[48] UNODA, “The UN Norms of Responsible State Behaviour in Cyberspace,” Mar. 2022.
[49] White House, “National Cybersecurity Strategy,” 2023.
[50] M. L. Brown et al., “National Cybersecurity Strategy Outlines A New Era of Cybersecurity Regulation,” Wiley, Mar. 2, 2023.
[51] W. Knight, “A new deepfake detection tool should keep world leaders safe—for now,” MIT Technology Review, Jun. 21, 2019.
[52] K. Balasaygun, “The biggest risks of using Bluetooth trackers like Apple AirTag, Tile,” CNBC, Jan. 14, 2023.
[53] B. Won, “Watering Hole Campaign Targeting Major Korean Portals Discovered! Beware of Login,” Boan News, Apr. 10, 2019.