사이버안보연구, 2집 1호 2025 여름, 091-112

국가 상황에 따른 사이버 침해 분류 및 주관기관 정립 연구

0201-091112

강정민 | 고려대학교(세종), 1저자
손기욱 | 서울과학기술대학교, 교신저자

논문접수일 2025년 6월 1일 | 논문심사일 2025년 6월 26일 | 게재확정일 2025년 6월 28일

논문 요약

국가 안보 위협 요인으로 급부상된 사이버 위협과 함께 '사이버 전쟁' 용어가 자주 등장하고 있다. 특히, 사이버 전쟁 용어를 오·남용함으로써 전쟁 발발이라는 여론을 조성하여 대국민 혼란을 일으킬 수 있으며, 사이버 전쟁에 대한 명확한 개념 구분 없이 혼재된 상태로 사용되어 국가 안보 정책 수립에 혼란이 초래될 가능성이 존재한다. 본 논문은 세계적으로 대표적인 미-러 양자 협의 용어 정의 및 우리나라 국가 위기관리를 고려하고, 국가 상황과 공격 주체를 반영한 사이버 침해를 '사이버 범죄', '사이버 테러', '사이버 분쟁', '사이버 전쟁'으로 분류·재정의 하였다. 또한, 사이버 침해 중 특히 국가 간 사이버 충돌로써 가장 중요시되는 사이버 분쟁과 사이버 전쟁 대응 주관기관 정립을 위하여 국가 안보·국방, 법·제도 및 사이버 역량 측면에서, 평·위기 사이버 분쟁 발생 시 국가 위기 상황을 타개하기 위한 국가정보원 주관의 위기 대응 체계가 필요하며, 전시 사이버 전쟁 주관기관으로써 국가정보원은 국가 사이버 역량을 총집결하고 전시 사이버 안보 업무를 총괄해야 하며, 국방부는 공격 위주의 사이버 군사작전 수행 역할이 요구된다.

주제어 사이버 안보, 사이버 분쟁, 사이버 전쟁, 사이버 테러, 사이버 범죄

Ⅰ. 서론

사이버 위협은 대량파괴 무기(WMD: Weapons of Mass Destruction) 확산, 테러, 기후변화와 함께 심각한 국가 안보 위협 요인으로 인식되고 있다. 2022년 러시아-우크라이나 하이브리드전쟁 및 북한 등 국가 배후의 지속적인 사이버 공격은 국가 안보 위협이라 할 수 있다. 이런 사이버 공격으로 인한 피해 발생을 두고 자주 등장하는 용어들은 사이버 범죄, 사이버 테러, 사이버 분쟁, 사이버 전쟁 등이 있다. 각 용어의 무분별한 사용을 지양하고 세계적인 공통의 정의가 필요하다는 주장이 제기되고 있으며, 미-러는 양자 간 사이버 용어들을 정의하는 활동을 시작하였다.

특히, 국가 상황을 평시·위기·전시로 구분하고 전쟁이 국가 간 무력 충돌 전시 상황이라는 점을 고려하였을 때 언론·매체 등에서 사용하는 사이버 전쟁 용어는 국가가 전시 상황이 아님에도 불구하고 확대 오용되고 있다. 또한 국가 개입 확증이 없고 심지어 비정부 단체나 민간에 의한 사이버 부정행위를 사이버 전쟁으로 간주하는 등 용어가 남용되고 있다. 이에 따라 평시·위기 사이버 침해에 대해 사이버 전쟁이라는 용어의 오·남용은 전쟁 발발에 대한 불필요한 여론을 조성하여 대국민 혼란을 초래할 수 있으며, 개념의 명확한 구분 없이 혼재되어 사용될 경우 국가 안보 정책 수립에 큰 혼선을 줄 수 있다.

본 논문은 기존 사이버 침해에 대한 용어 사용의 혼선을 없애고 국가 안보 정책 수립 시 활용할 수 있는 사이버 침해에 대한 용어 정의를 제시하고, 각 사이버 침해 대응 역할을 위한 주관기관 정립을 제안

한다. 본 논문의 구성은 다음과 같다. II 장에서는 가장 빈번하게 사용되는 사이버 전쟁에 대한 기존 정의들과 미-러 간 양자 협의를 통해 발표한 사이버 용어 정의들을 살펴본다. III 장에서는 국가 상황에 따른 사이버 침해를 분류하고 각 침해에 대한 정의 및 주요 사이버 사고 사례 분석을 통해 사이버 침해 용어들을 적용해본다. Ⅳ장에서 각 사이버 침해 별 대응 주관기관을 정립하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 기존 동향

1. 사이버 전쟁 기존 정의들

사이버 전쟁을 정의하는 핵심은 “국가 간에 이루어지는 적대적 행위”와 “사이버 공간에서 정보기술을 이용하여 이루어지는 공격과 방어 행위”라는 점을 제시한다. 한국 합동참모본부는 사이버전(Cyber War)을 컴퓨터 네트워크를 통해 디지털화된 정보가 유통되는 가상 공간에서 다양한 사이버 공격 수단을 써 적의 정보체계를 교란, 거부, 통제, 파괴하는 등의 공격과 이를 방어하는 활동이라고 한다(합동참모본부 2004, 214). 미국 랜드연구소는 사이버전을 정보 관련 원칙에 따라 군사작전을 수행하는 것으로 정보 및 통신 시스템을 방해하거나 파괴하는 것으로 정의한다(Arquilla, John J 2000, 4). 미국 다트머스 대학 연구진은 사이버 전쟁을 국가 경계에 따라 조직된 부대가 컴퓨터를 사용하여 전자적 수단을 통해 다른 컴퓨터나 네트워크를 공격하는 공격 및 방어 작전을 포함한다고 정의하였다(Charles G. Billo 2004,

17). 미국 국제전략문제연구소는 정보시스템과 네트워크에 대한 데이터 공격, 소프트웨어 공격, 물리적 공격이 대규모로 발생하는 상태라고 하였다(James A. Lewis. 2002, 1).

기존 사이버 전쟁 정의 대부분은 국가 상황(평시·위기·전시)의 구분 없이 군사작전 일환의 국가 간 사이버 공격·방어에 초점이 맞추어져 있어서, 평시·위기 시 전쟁이 발발할 것처럼 긴장감을 조성하여 국가 혼란을 초래할 수 있다. 사이버 전쟁의 "전(戰)"은 국가 간 무력 분쟁인 전쟁을 의미하므로 사이버 전쟁의 의미는 국가 상황 중 전시 상황을 반영하여야 타당하다. 한편, 평시·위기 시 빈번하게 발생하는 국가 간 적대적 사이버 행위 또는 상태에 대한 용어 및 정의를 도출하여 용어 사용의 혼선을 방지해야 할 것이다.

2. 미-러 양자 협의 사이버 안보 용어 정의

2012년 유엔 정부 전문가 그룹(GGE: Group of Governmental Experts) 회의 이후 사이버 분야에서 지속적인 정의 작업의 중요성에 대한 국제적인 관심이 증가하였다. 2013년 미국 오바마 대통령과 러시아 푸틴 대통령은 사이버 보안에 대한 협력을 시작하는 역사적인 협약에 서명하였다. 이에 2014년 미국 동서연구소와 러시아 모스크바 대학 정보보안연구소는 양자 간 협의를 통해 세 개 분야 총 20개의 사이버 안보 용어 정의를 발표하였다(James B. Godwin III 2014, 28-32). 이 중에서 본 연구와 밀접한 관련이 있는 두 번째 악화 형태(Modes of Aggravation)에서 사이버 범죄, 사이버 테러, 사이버 분쟁, 사이버 전쟁에 대해 정의를 하였다.

사이버 범죄(Cyber Crime)는 자국법 또는 국제법에 따라 정의된 대로 사이버 공간을 범죄 목적으로 사용하는 것이다. 사이버 테러(Cyber Terrorism)는 자국법 또는 국제법에 따라 정의된 대로 사이버 공간을 테러 목적으로 사용하는 것이다. 사이버 분쟁(Cyber Conflict)은 국가들 또는 조직된 단체들 사이의 긴장된 상황으로, 사이버 공격이 보복을 초래하는 상황을 의미한다. 사이버 전쟁(Cyber War)은 국가 간 또는 국가들 사이의 사이버 분쟁 상태가 고조되어, 군사 캠페인의 일부로 국가 행위자들에 의해 사이버 인프라에 대한 사이버 공격이 수행되는 상황을 의미한다. 사이버 분쟁의 확대된 상태를 사이버 전쟁으로 정의함으로써 국가 상황을 반영하고 있음을 알 수 있다. 한편 사이버전(Cyber Warfare)은 정부 캠페인과 연계하여 국가 행위자들이 승인한 사이버 인프라에 대한 사이버 공격을 의미한다(James B. Godwin III 2014, 43). 다시 말해 군사작전의 목적으로 사이버전은 사이버 전쟁 시 행해지는 공격의 의미로써 사이버 전쟁의 일부라고 볼 수 있겠다.

최근 UN 사이버안보 논의는 GGE(Group of Governmental Experts)와 OEWG(Open-ended Working Group)를 통해 국가 간 신뢰구축과 책임성 있는 사이버 행위 기준에 대한 공감대를 확산하고 있으며, 특히 사이버 위협을 분류하고 책임 주체를 특정하는 방향에서 본 연구의 문제의식과 연결된다(GGE, 2021, OEWG Final Report, 2023). 사이버 침해 중 사이버 전쟁은 국가 공격 주체 간 군사작전이 요구되는 국가 전쟁 상황이라고 할 수 있듯이, 공격 주체와 국가 상황을 사이버 침해를 분류·정의하기 위한 기준으로 제시한다.

Ⅲ. 사이버 침해 분류

기존 동향에서 살펴본 바와 같이 사이버 침해를 분류하는 기준은 국가 상황과 공격 주체라고 할 수 있다. 다시 말해 특정 공격 주체(예: 범죄자, 테러리스트, 국가)의 사이버 공격으로 인한 국가 위기 상황(예: 긴장 상태, 분쟁 확대 상태)이 발생하고 이를 해결하기 위한 정부 주관기관의 개입이 요구되는 것이다. 특히 사이버 전쟁은 국가 공격 주체에 의해 상대국에 사이버 공격을 수행함으로써 심각한 상황(예: 전쟁)을 유발하는 가장 자극적인 표현이다. 이런 이유로 일반 여론에서 사이버 공격 발생 상황에 대해 강한 전달을 목적으로 사이버 전쟁 용어를 사용하는 것으로 풀이된다. 현실 세계에서 공격 주체와 위기 상황에 따라 범죄, 테러, 분쟁, 전쟁으로 구분하듯 사이버 공간에서 발생하는 사이버 침해 분류도 같은 맥락으로 분류될 수 있다. 본 장에서는 국가 상황, 공격 주체 두 기준을 중심으로 사이버 침해를 분류·정의하고, 주요 사이버 사고 사례 분석을 통해 사이버 침해 용어들을 적용해 본다.

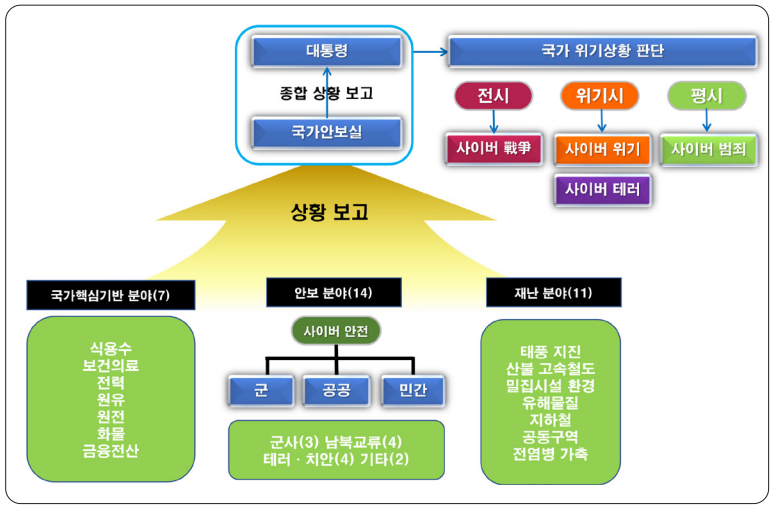
1. 국가 상황에 따른 사이버 침해 분류

1) 국가 상황

국가 상황은 국가 위기관리 기본지침(대통령 훈령 124호) 등에 따라 국가 핵심 기반 분야(7개 위기 유형), 안보 분야(14개 위기 유형), 재난 분야(11개 위기 유형)에서 발생한 상황들에 대해 피해 규모를 기준으로 심각성, 시급성, 확대 가능성, 전개 속도, 지속 시간, 파급 효과, 국내외

여론, 정부의 대응 능력 등을 종합적으로 고려하여 **평시·위기·전시**[1] 상황이 결정된다〈그림 1〉.

〈그림 1〉 국가 상황 판단 체계



2) 공격 주체

위기 및 전시에 정치·외교·무력 등 국가 역량을 동원한 총 대응을 위해서는 공격 주체 식별이 필수적이며, 사이버 공격을 수행하는 주체로는 국가, 비정부조직 또는 개인 및 단체로 구분하였다. 국가는 정규군뿐만 아니라 고용 형태로 국가에 개입된 단체와 개인을 포함(국가 정보기관, 사이버전 전사 등)한다. 비정부조직은 정치·사회적 특수 목적의 산업스파이집단, 테러 집단, 범죄집단 등을 일컫는다. 개인 및

1) 전쟁법상 군사력 사용이 정당화되는 전쟁 상황

단체는 국적에 의하여 국가에 속하는 사람 및 단체(해커, 컴퓨터 범죄자)를 의미한다. 사이버 특성상 공격 주체를 식별하는 것이 쉬운 일은 아니지만, 공격 주체를 추정할 수 있는 증거로 아래와 같은 여러 예를 들 수 있다.

〈표 1〉 공격 주체 추정 증거

항목	증거	설명
공격 IP, URL	• 공격 진원지 IP, 경유지 IP • 공격무기 유포 도메인 또는 URL	• 공격 명령 서버 IP • 공격 코드 유포 웹사이트 URL 등
공격 분석	• 공격무기 유포 경로 및 방식	• 웹하드를 통한 유포(7.7, 3.4 DDoS, 4.12 농협사태) • 이메일, 메신저, USB 등을 이용한 유포
	• 알려진 공격 코드와의 유사도	• 공격 명령 전송방식 등의 코드 유사도 • 공격 코드 확장자
	• 공격 코드 내 특정 (문자열) 패턴	• 이메일 주소 또는 제작자 이름 등 • 예: 7.7 DDoS '독립기념일'
	• 공격 대상 및 공격 목적	• 공격 대상 목록 • 정보 절취 또는 무력화
정치·사회 상황	• 정치·사회적 사이버 공격 예고 또는 암시	• 언론을 통한 공격 예고 등 • 예: 북한 조평통의 사이버스톰 비난 성명서 발표 등

3) 사이버 침해 분류

세계적으로 대표적인 미-러 양자 협의 용어 정의 및 우리나라 국가위기관리를 고려하여, 국가 상황과 공격 주체를 반영한 사이버 침해를 다음과 같이 네 가지로 분류·재정의 하였다. 특히, 국가 간 사이버 전쟁은 국가 차원의 전쟁 수단으로써 국제 사회에서 규율을 준수하

고 실익을 보장받기 위해서 전쟁법(국방부 2003)을 기반으로 정의를 도출하였다. 그리고 현재도 진행 중인 국가 간 사이버 공격과 방어로 인한 위기 상황을 사이버 분쟁으로 정의함으로써 평·위기 "사이버 전쟁" 용어의 부적절한 사용으로 인한 혼란과 혼선을 제거하고자 하였다.

- **사이버 전쟁**: 둘 이상의 서로 대립하는 **국가** 또는 이에 준하는 집단 간에 자위권을 행사하거나, 선제적 자위권 행사의 목적으로 행해지는 **전시** 군사목표[2]에 대한 사이버 공격[3]과 방어 행위 또는 상태
- **사이버 분쟁**: 사이버 공간에서 정보기술을 이용한 **타국**의 적대적 사이버 공격으로 인해 국가 **위기** 상황을 유발, 이를 방어하는 행위 또는 상태
- **사이버 테러**: **비정부** 공격 주체(미확인 포함)가 정치·사회 등의 국가 혼란을 목적으로 사이버 공격을 수행하여 국가 **위기** 상황을 초래하는 행위 또는 상태
- **사이버 범죄**: **개인** 및 **단체** 공격 주체(미확인 포함)가 경제적 이익·반문화적 행위 등의 목적으로 정보기술을 악용, 국가 상황이 **평시** 상황을 유지할 수 있는 정도의 행위 또는 상태

2) 군사행동에 효과적으로 기여하는 목표로서 파괴·포획 또는 무력화를 통해 명백한 군사적 이익을 얻을 수 있는 대상(物)

3) 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입, 교란, 마비, 파괴하거나 정보를 절취, 훼손하는 일체의 공격행위(국가사이버안전관리규정)

2)에서 언급한 바와 같이 익명성이 강한 사이버 공간에서 공격 주체를 바로 식별하는 것은 어려울 수 있다. 공격 주체 미확인 경우 국가 상황을 기준으로 사이버 침해 분류는 위기 일 경우 사이버 테러, 평시 일 경우 사이버 범죄로 분류한다. 예를 들어 3.4 DDoS, 4.12 농협 사태와 같이 사건 초기 공격 주체가 미확인인 경우, 국가위기상황(주의)을 기준으로 사이버 테러로 분류할 수 있으며, 사고 조사를 통해 공격 주체(북한)가 밝혀지면 사이버 분쟁으로 정의할 수 있다.

2. 주요 사례별 사이버 침해 분류 예시

〈표 2〉는 주요 사이버 사고에 대해 공격 주체와 국가 상황을 기준(해외 사례 경우 국가 상황은 국내 기준으로 추정함)으로 사이버 침해를 적용한 결과이다. 2022년 2월 우크라이나 대상 러시아의 전방위적 사이버 공격과, 2008년 8월 조지아 대상 러시아의 사이버 침해는 전시에 수행된 사이버 전쟁으로 분류될 수 있으며, 그 밖에 국가 공격 주체에 의한 사이버 공격으로 국가 위기 상황을 유발한 사이버 분쟁이 대부분을 차지함을 알 수 있다. 사이버 분쟁은 이처럼 국가 간 사이버 공격·방어 행위로 위기 상황을 유발하는 현시대 대표적인 국가 간 충돌 현상이며, 사이버 전쟁으로 확대될 수 있는 여지를 제공한다고 할 수 있겠다.

〈표 2〉 사례별 사이버 침해 분류

사례	공격 주체	내용	국가 상황	사이버 침해
2022년 2월 ~ 러-우 전쟁	러시아	우크라이나 정부, 기반시설 등 전 방위 공격	전시	사이버 전쟁
2021년 5월 미 콜로니얼 파이프라인 공격	러시아 해킹조직 다크사이드	랜섬웨어 공격으로 5500 마일에 달하는 파이프라인이 마비	위기	사이버 테러
2016년 2월 스위프트 전산망 해킹	북한	방글라데시 중앙은행이 뉴욕 연방준비은행에 예치하고 있던 1억 100만 달러해킹으로 탈취됨	위기	사이버 분쟁
2014년 12월 한수원 자료 유출	북한	한국수력원자력(한수원)의 직원 이메일을 통해 악성코드를 유포 및 자료유출	위기	사이버 분쟁
2013년 3월 3·20 전산대란	북한	KBS, MBC, YTN을 비롯한 방송사와 신한은행, 농협을 비롯한 금융기관 3만2천 여대 컴퓨터 하드디스크 파괴	위기	사이버 분쟁
2011년 7월 네이트, 싸이월드 고객개인정보유출	미확인	국내 포털 사이트 네이트와 싸이월드 3,500만 회원 정보 유출	평시	사이버 범죄
2011년 4월 4.12 농협 사태	북한	국내 농협 서버 파괴 및 뱅킹 업무 장애	위기	사이버 분쟁
2011년 3월 3.4 DDoS 공격	북한	국내 40개 공격 대상 사이트 중 일부 사이트 접속 장애	위기	사이버 분쟁
2010년 9월 이란 Stuxnet 공격	미국, 이스라엘	전 세계 45,000여 대 호스트 감염 및 이란 1,000여 대의 원심분리기 고장	위기	사이버 분쟁
2009년 1월 키르기스스탄 DDoS 공격	러시아 비정부집단	키르기스스탄 내·외부 네트워크 트래픽 7일 이상 차단	위기	사이버 테러

사례	공격 주체	내용	국가 상황	사이버 침해
2009년 7월 한국 7·7 DDoS 공격	북한	한국 정부 기관과 주요 은행, 언론사, 포털 사이트, 인터넷 쇼핑몰 사이트 3일간 마비	위기	사이버 분쟁
2008년 8월 조지아 DDoS 공격	러시아	조지아 정부, 언론, 은행, 교통 등 사이트 마비	전시	사이버 전쟁
2008년 2월 옥션 개인정보유출	개인 (중국 해커)	옥션 가입자 1,863만 명 개인정보유출	평시	사이버 범죄
2007년 4월 에스토니아 DDoS 공격	러시아 비정부 집단	에스토니아 정부, 은행, 언론, 포털 사이트 3주간 마비	위기	사이버 테러
2004년 6월 미국 기밀정보절취	중국 사이버 부대 (타이탄 레인)	미군 항공기 및 미사일 기지, 항공우주국(NASA), 세계은행 네트워크 침투 및 정보 절취	위기	사이버 분쟁
2004년 6월 Peep, Revacc 악성코드	북한	국가공공기관 PC 211대 (해양경찰청 77대, 국회 69대, 원자력연구소 50대 등), 민간 기업과 대학, 언론사 등의 67대 해킹	위기	사이버 분쟁
2003년 1월 슬래머웜 미국 DavisBesse 원전 정지	미확인	미 원자력 발전소 안전변수표시반과 발전소감시계통 5시간 정지	위기	사이버 테러
2000년 4월 호주 오폐수처리 제어시스템 해킹	개인 (전직 직원)	호주 퀸즈랜드주 오폐수처리 제어시스템 3달 동안 46차례 오·폐수 방출	평시	사이버 범죄

Ⅳ. 사이버 침해 대응 주관기관 정립

1. 해외 주요국 주관기관 사례

미국은 2018년 CISA(Cybersecurity and Infrastructure Security Agency)를 국토안보부 산하에 설립하여 민간 및 중요 기반시설에 대한 사이버 위협 대응을 총괄하게 하였고, 사이버 군사작전은 미 사이버사령부(USCYBERCOM)가 전시 및 국가안보 상황에서 수행한다. 이에 따라 사이버 침해 유형(범죄/테러/분쟁/전쟁)에 따라 FBI, CISA, NSA, CYBERCOM 등이 분담된 역할을 수행하고 있다.

일본은 총무성 산하의 사이버 보안 전략본부(NISC)가 민간·정부기관 사이버 대응을 총괄하고 있으며, 위기 또는 전시 수준의 사이버 공격이 발생할 경우 방위성 사이버 방위대가 직접 개입한다. 또한 사이버 범죄 및 테러 대응은 경찰청(NPA)이 담당하며, 이러한 분화는 사이버 위협의 유형에 따른 합리적 기관 배분 모델로 평가된다.

2. 사이버 침해 대응 주관기관 정립

Ⅲ 장에서 분류한 사이버 침해 중 특히 국가 간 사이버 충돌로써 가장 중요시되는 사이버 분쟁과 사이버 전쟁 대응 주관기관 정립을 위하여 국가 안보·국방, 법·제도 및 사이버 역량 측면에서 살펴보면 다음과 같다.

첫째, 우리 정부는 사이버 공격이 국민의 재산과 국가 안보[4]를 위협하는 상황에 이르렀다고 판단, 사이버 위협에 총체적으로 대응하기 위한 다양한 국가사이버안보 관련 정책들을 수립해오고 있다. 한편, 종래 국방의 정의가 전적으로 군사력에 의하여 전쟁을 방지하고 불가피할 때는 실력행사를 하는 일이었다면, 최근 국방의 정의는 군사력을 포함한 모든 수단과 방법을 동원하여 전쟁을 방지하고 다른 나라의 도전을 억제하되, 만약 전쟁이 일어났을 때는 국가의 총력을 기울여 전쟁에 이길 수 있도록 도모하는 일로써 정의되고 있다(네이버 지식백과 2023). 이처럼 국방은 국가와 민족의 안전을 보장하기 위한 모든 수단과 체제의 총칭을 의미한다. 따라서 사이버 전쟁은 국가 안보를 위하여 사이버 군사력 이용뿐만 아니라 정치·외교 등 국가 역량을 총집결하는 개념으로 접근해야 타당하다. 이런 관점에서 국가정보원은 사이버 전쟁 수행의 총괄 주관기관으로 기능하고, 국방부는 군사적 측면의 사이버전[5](Warfare) 수행을 담당해야 한다. 한편 평·위기 시 사이버 분쟁은 국가 사이버안보업무를 수행하는 국가정보원 주관이 되어야 한다.

둘째, "국가사이버안전관리규정(국가법령정보센터 2023)" 제18조에 의하면 국방 분야의 사이버 안전 관련 업무는 국방부가 수행하게 되어 있으나 국가 안보에 필요하다고 판단될 때는 관련 내용을 국가정보원에 통보하도록 하여, 사실상 평·위기 시 발생하는 사이버 분쟁

4) 국가가 외부로부터의 공격·침략에 대비하여 자국의 안전을 유지·확보하는 일

5) 사이버 군사력을 이용한 군사 전략적 목표 수행을 위한 군사작전

및 사이버 테러에 대한 주관기관은 국가정보원이 담당하고 있다. 한편 평·위기 시 국가사이버안전업무의 단절 및 혼란 없이 전시 국가사이버안전업무로의 전환을 고려했을 때, 군은 공격 위주의 사이버 군사작전을 수행하고 국가정보원은 국가 안보 차원의 사이버 위기 대응에 온 힘을 다함으로써 전쟁 승리와 국가 안전을 담보할 수 있을 것이다.

셋째, 국가 사이버 안보 위협에 대응하기 위하여 설립된 국가정보원 국가사이버안보센터는 평·위기 시 발생하는 사이버 분쟁 및 사이버 테러 대응에 가장 역량 있는 기관이다. 국내에서 발생했던 사이버 분쟁 발생 시 국가사이버안보센터는 민관군 분야의 사이버 안보 컨트롤 타워 역할을 충실히 수행하였다. 사이버 역량은 최첨단 IT 기술력 확보가 관건인 만큼 국가사이버안보센터의 축적된 노하우는 국가 사이버 안보를 지탱하는 원동력이라 할 수 있다. 2010년 1월 창설된 국방부의 국군 사이버사령부는 북한의 도발에 대한 즉각 대응 등 국방 사이버전 수행 역할을 담당한다. 이를 위해 평시 사이버 전쟁에 대비한 무기 개발 등 사이버전 역량을 강화하여 사이버 전쟁에 대비하는 것뿐만 아니라, 사이버 전쟁에 국제법 적용에 대한 정확한 분석을 통해 적국의 사이버 공격 행위를 규율하고 국제적으로 우리나라 사이버 전쟁의 정당성을 주장할 수 있는 명분 논리를 마련할 필요가 있다.

검찰·경찰은 민간 분야의 사이버 범죄에 대한 예방과 조사 임무를 수행한다. 한편 수많은 사이버 사고 등을 통해 금융 등 민간 분야의 사이버 안전 또한 국가 안보와 직결되었다는 교훈을 얻었으며, 북한

개입의 사이버 분쟁 발생 가능성이 커짐에 따라 국가사이버안보센터의 임무가 더 확대되어야 할 것으로 판단된다.

다시 말해, 사이버 침해 별 대응을 위한 정부 주관기관을 정리하면 다음과 같으며, 〈표 3〉은 사이버 침해 분류 및 대응 주관기관 요약을 보여준다. 사이버 전쟁시에는 국가 안보를 위하여 국가정보원 주관의 국가 사이버 역량을 총집결하여 전시 사이버안보업무를 수행하며, 국방부는 전쟁 승리를 위한 국방 사이버전 수행 체계 편성, 사이버 분쟁 및 사이버 테러시에는 국가 위기 상황을 타개하기 위한 방어 위주의 국가사이버안보업무가 요구되며, "국가사이버안전관리규정"에 의해 국가정보원 주관으로 위기 대응 체계 편성, 사이버 범죄에 대해서는 민간 질서 유지를 위해 검찰·경찰의 수사 체계 편성이 필요하다.

〈표 3〉 사이버 침해 분류 및 대응 주관기관

사이버 침해	국가상황	공격주체	주관(한국)	주관(미국)	주관(일본)
사이버 전쟁	전시	국가	국가정보원·국방부	USCYBERCOM	방위성 사이버방위대
사이버 분쟁	위기	국가	국가정보원	CISA, FBI	NISC, NPA
사이버 테러	위기	비정부, 미확인			
사이버 범죄	평시	개인, 단체, 미확인	검찰·경찰	FBI	NPA

V. 결론

국가 간 전쟁은 흔히 발생하는 것도 아니며, 발생해서도 안 되는 것에 모두가 공감하듯이 언론 매체 등 각 분야에서 사이버 전쟁이라는 용어를 자극적으로 사용하는 것은 바람직하지 않다. 본 논문은 기존 사이버 침해에 대한 용어 사용의 혼선을 없애고 국가 안보 정책 수립 시 활용할 수 있는 사이버 침해에 대한 용어 정의를 제시하고, 각 사이버 침해 대응 역할을 위한 주관기관을 정립하였다. 이를 위해 국가 상황(평시, 위기, 전시)과 공격 주체(국가, 비정부, 개인 및 단체) 기준에 따른 사이버 침해를 네 가지로 분류하였다. 국가가 개입되고 위기 상황을 유발하는 사이버 분쟁, 국가 간 전시 상황에서의 사이버 전쟁, 비정부 또는 미확인 공격 주체에 의한 위기 상황 발생의 사이버 테러, 또한 평시의 개인, 단체, 또는 미확인 공격 주체에 의한 사이버 범죄를 명확히 정의함으로써, 향후 정책 수립과 연구 개발 과정에서 공통 용어의 사용을 통해 혼란을 줄일 수 있을 것으로 기대된다.

사이버 분쟁 수행 주관기관으로서 국가정보원의 역할은 기존 사이버 대응 체계에서의 컨트롤 타워 역할과 잘 부합한다고 할 수 있겠다. 심지어 민간 분야의 사이버 안보가 국가 안보와 직결될 수 있으므로 국가정보원의 역할과 책임이 더 커져야 할 것이다. 전시 사이버 전쟁 수행 주관기관으로서 국가정보원은 국가 사이버 역량을 총집결하고 전시 사이버안보업무를 총괄해야 하며, 국방부는 사이버 무기 개발 등 사이버 전쟁 역량을 강화하여 사이버 전쟁에 대비하는 것뿐만 아니라 사이버 전쟁에 국제법 적용에 대한 정확한 분석을 통해 적국의

사이버 공격 행위를 규율하고 국제적으로 우리나라 사이버 전쟁의 정당성을 주장할 수 있는 명분 논리를 마련할 필요가 있다.

한편, 국방부는 “국방정보화 기반조성 및 국방정보자원관리에 관한 법률“ 제정을 통해 전시 사이버 군사작전을 위한 법적 근거를 확보했지만, 전시 사이버 안보 업무를 위한 법적 근거는 미흡한 실정이다. 다시 말해, 전시 전환 시 “계엄법” 제8조 제1항에 의해 정보 및 보안업무를 관장하는 기관(국가정보원)이 계엄사령관의 지휘·감독을 받고, 사이버 안보 업무가 군으로 흡수·통합되는 경우, 군 군사작전 수행을 위한 사이버전 업무와 혼선을 빚을 수 있으므로 평·위기 시 국가사이버안보업무의 단절 및 혼란 없이 전시 국가사이버안보업무로 전환을 위한 법적 근거 마련에 대한 논의가 필요하다.

〈참고문헌〉

국가법령정보센터, “국가사이버안전관리규정”, “계엄법”, “통합방위법”, 2023.

국방부, “전쟁법 해설서(Law of Armed Conflict)”, 2003.

네이버 지식백과, “안전보장, 국방의 정의”, 2023.

합동참모본부. 2004. 합동·연합작전 군사용어사전: 합동참고교범.

Alexander Klimburg. 2011. Cyber Confidence Building through Proxy Naming & Shaming: NATO Conference on Emerging Security Challenges.

Arquilla John J. 2000. Cyberwar and Netwar: new modes, old concepts of conflict: RAND corporation.

Boaz Dolev and Assaf Keren. 2010. Cyber Vs. Nuclear: CERI Strategy Papers.

Charles G. Billo, Welton Chang. 2004. Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States: Institute for Security Technology Studies at Dartmouth College.

Dorothy E. Denning. 2000. Information Warfare and Security: Addison Wesley.

Gary Clayton, and Kevin Coleman. 2010. The Right to Bear Cyber Arms: Technolytics.

GGE. 2021. Group of Governmental Experts on Advancing Responsible

James A. Lewis. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Center for Strategic and International Studies.

James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko. 2014. Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity.

Kevin G. Coleman. 2010. Cyber Weapons Threat Matrix: Technolytics.

Martin Libicki. 2009. Cyberdeterrence and Cyberwar: Rand Corporation.

Michael Portnoy and Seymour Goodman. 2009. Global Initiatives to Secure

Cyberspace: Springer.

Michael N. Schmitt. 1999. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework: 37 COLUM. J. TRANSNAT'L L.

Peeter Lorents and Rain Ottis. 2010. Knowledge Based Framework for Cyber Weapons and Conflict: Conference on Cyber Conflict Proceedings 2010.

Richard Ned Lebow and Janice Gross Stein. 1990. DETERRENCE: The Elusive Dependent Variable:World Politics.

Scott W. Beidleman. 2009. Defining and Deterring Cyber War: U.S. Army War College.

Sharp Walter Gary. 1999. Cyberspace and the Use of Force: Ageis Research Corp..

United Nations. 2023. Final Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

A Study on the Classification of Cyber Intrusions Based on National Situations and the Establishment of Governing Bodies

Jungmin Kang | Korea University Sejong Campus
Kiwook Sohn | Seoul National University of Science and Technology

With the rise of cyber threats as a major factor in national security, the term 'cyber war' is frequently appearing. Particularly, the misuse or overuse of the term 'cyber war' can create public confusion, leading to the perception of an outbreak of war, and can cause confusion in the establishment of national security policies due to the lack of a clear distinction in the concept of cyber war. This paper redefines and classifies cyber intrusions reflecting national situations and attacking entities into 'cyber crime', 'cyber terrorism', 'cyber conflict', and 'cyber war', considering the globally representative U.S.-Russia bilateral consultation definitions and our country's national crisis management. Moreover, looking from the perspectives of national security and defense, law and legislation, and cyber capabilities, it is found necessary to establish a crisis response system led by the National Intelligence Service during peace and crisis times for cyber conflicts, which are particularly important as cyber clashes between nations. In the event of cyber war during wartime, the National Intelligence Service should gather and oversee all national cyber capabilities and wartime cyber security operations, while the Ministry of National Defense should play a role in conducting aggressive cyber military operations.

Keyword Cyber Security, Cyber Conflict, Cyber War, Cyber Terrorism, Cyber Crime