한·중 테러대응전략 비교 연구

– 사이버테러 대응을 중심으로

2019년 2월

대통령경호처

유 병 철

목 차

국외훈련개요

1. **훈련국 : 중국**

2. **훈련기관명 : 북경대학교**
(北京大学)

3. **훈련분야 : 국제관계**

4. **훈련기간** : 2016. 2 ~ 2018. 2

훈련기관개요

Ⅰ. 기관개요

○ 훈련국 : 중국

○ 훈련기관명 : 북경대학

- 어학연수(국제합작부)
- 석사과정(국제관계학원)

○ 인터넷 웹주소

- 북경대학 : http://www.pku.edu.cn
- 국제합작부 유학생사무실 : http://www.isd.pku.edu.cn
- 국제관계학원 : http://www.sis.pku.edu.cn

○ 기타(주소 등)

- 학교주소 : 北京市海淀区颐和园路5号
- 유학생사무실(학위 및 어학과정 관련)
  · 전 화 : +86-10-6275-1230
  · 팩 스 : +86-10-6275-1230
  · 이메일 : study@pku.edu.cn

Ⅱ. 기관소개

○ 연 혁

- 1898년 원·명·청 시대의 교육기관 국자감(國子監)을 대체하여 '경사대학당(京師大學堂)'으로 창설
- 1902년 경사대학당의 교육학원이 오늘날의 베이징사범대학교로 분리
- 1912년 중화민국 성립에 수반하여 국립 베이징대학으로 개칭
- 1917년 학장으로 취임한 차이위안페이(蔡元培)의 개혁으로 신문화 운동의 중심이 되어 근대 학술연구와 토론의 자유 학풍을 확립
- 1919년 5·4운동이 재학생들에 의해서 추진된 이후 학생운동의 중심적 역할을 수행

- 1920년 난징대학교에 이어 중국에서 2번째로 여학생 입학
- 1937년 중일전쟁중 칭화대학, 난카이(南開)대학과 함께 후난성 창사(長沙)에서 합병하여 창사임시대학교로 편성
- 1938년 윈난성(雲南省) 쿤밍(昆明)으로 옮겨 시난(西南) 연합대학으로 편성
- 1946년 연합대학 해산 후 각각의 학교로 분리
- 1952년 대학 재편성에 의하여 옌징(燕京)대학을 합병하고 칭화(淸華)대학과의 조정이 단행되어 문·이과계의 기초이론을 중심으로 한 종합대학으로 개편, 베이징 도심에서 옛 옌징대학 캠퍼스 자리로 옮김
- 1966~1976년 문화대혁명 기간 중 1970년까지 3년 동안 휴교조치
- 1977년 국가통일 입시제에 의하여 입학자를 선발
- 2000년 베이징의과대학교를 합병하여 베이징대학교 보건 캠퍼스를 조성
- 2005년 역학, 정보 부문 기반에서 공학부 복원

❍ 조 직
- 교육기구 : 대학 5개, 학부 및 대학원 64개
  · 전 공 : 학사 121개, 석사 261개, 박사 233개
- 행정기구 : 총무부, 인사부, 재무부 등 31개
- 연구소 및 실험실 : 129개
- 부속건물 : 도서관, 체육관, 부속중학 등 21개
  · 도서관(장서 약 940만권), 부속병원 10개

❍ 인 원(2016년 기준)
- 교 직 원 : 21,000명(전임교수 7,000명 등)
- 중국학생 : 40,000명(본과 15,000명, 석사 15,000명, 박사 10,000명)
- 유 학 생 : 3,600명(본과 1,600명, 석사 700명, 박사 300명, 연수 1,000명)
  · 한국인 유학생 : 본과 600명, 석사 120명, 박사 40명

❍ 국제관계학원
- 1960년 북경대학 정치학과가 설립된 후 1963년 국제정치학과로

개명, 1996년에 국제정치학과, 국제관계연구소, 아시아·아프리카 연구소의 합병을 통해 국제관계학원이 설립됨

- 국제관계학원에는 4개 학과 및 3개 연구소가 있음.
  · 학 과 : 국제정치과, 외교학 및 외사관리과, 비교정치학과, 국제정치경제학과
  · 연구소 : 국제관계 연구소, 아시아·아프리카 연구소, 세계사회주의 연구소, 기타 20개 연구센터
- 국제관계학원의 전공은 본과 3개, 석사 8개, 박사 6개가 있음.
  · 본 과 : 국제정치, 외교학, 국제정치경제학
  · 석 사 : 국제정치, 국제관계, 외교학, 국제정치경제학, 중공당사, 중외정치제도, 국제공공정책, 과학사회주의 및 국제공산주의 운동
  · 박 사 : 국제정치, 국제관계, 외교학, 국제정치경제학, 중외정치제도, 과학사회주의 및 국제공산주의 운동
- 규 모(2016년 기준)
  · 교 수 : 53명(정교수 29명, 부교수 23명, 강사 1명)
  · 학 생 : 1,023명(본과 505명, 석사 326명, 박사 192명)
  중국인 : 684명, 유학생 : 339명(33.1%)

Ⅲ. 기관교섭 관련

○ 어학연수 및 대학원 교섭은 온라인 신청과 이메일 교환으로 진행할 수 있음. 학교에서도 신청학생이 많고 언어소통의 이유로 전화 문의나 팩스 교환보다는 이메일 문의를 선호함. 또한 유학생 사무실에 근무하는 인원은 기본적으로 영어소통이 가능함.

○ 입학에 필요한 관련 정보는 '북경대학 국제합작부 유학생사무실' 홈페이지(http://www.isd.pku.edu.cn)에서 얻을 수 있음. 홈페이지 이용시 중문판과 영문판의 정보가 다소 상이할 수 있으니 중문판 사용을 권장함.

○ 기타 학교 및 해당학과 관련정보는 북경대 및 해당학과 홈페이지에서 얻을 수 있음. 해당학과 홈페이지에서는 전공 및 교수경력이

소개되어 있어 연구방향과 학과 선정시 도움이 됨. 대학원 면접 일자 및 합격자 발표 등 관련정보는 해당학과 홈페이지 참조.

❍ 유학생사무실 홈페이지를 통해 입학 전·후 필요한 정보를 얻을 수 있으므로 관심을 가지고 볼 필요가 있음. 홈페이지 하단에 있는 QR코드(ISDPKU, 北大留办微信)를 위챗으로 스캔후 공식계정에 등록하면 핸드폰에서도 쉽게 접근 가능함.

❍ 특히 작년 또는 재작년의 공지를 참고하면 특별한 경우가 아닌 경우 올해 주요일정이 어떻게 진행될지 예측할 수 있어 장기적인 계획 수립에 도움이 됨.

❍ 어학연수 신청 후 우편으로 입학통지서 등 관련서류 도착은 한달 정도 소요됨. 동봉되는 유학생 가이드북은 학교 등록 및 생활에 필요한 정보가 수록되어 있으므로 유용하게 활용됨. 홈페이지상의 ORIENTATION 항목을 통해서도 사전 참고가 가능함.

❍ 어학연수 등록시 학교측에서 그룹 채팅방(위챗)을 운영하여 학사 일정 및 생활정보 등을 추가로 전달함. 북경대 학생동아리에서는 유학생의 조기정착을 위해 일종의 언어교환 프로그램을 운용하여 신청시 1:1 중국인 학생을 매칭시켜줌. 신청안내는 합격자 통지시 개인 이메일로 전송됨.

❍ 온라인 신청시 여권은 일반여권을 사용하여야 함. 중국 교육부 규정상 관용여권으로 학위과정 신청이 제한되기 때문에 사전 어학연수시에도 일반여권으로 등록하는 것에 주의해야 함. 관용여권으로 등록하였다면 일반여권으로 비자 취득후 입학등록시 변경 가능함. 단, 학생카드, 인터넷 등록 등 초기 비밀번호 설정에 관용여권 번호가 사용되는 등 번거로움 발생.

❍ 비자는 학습과정이 6개월 미만시 X2비자, 6개월 이상은 X1비자를 발급받을 수 있음. 사전 어학연수시에는 X2비자를 발급받아 입국

하고 대학원과정 등록시 X1비자로 변경. 중간에 비자기한을 연장하거나 해외 출입이 필요한 경우 학교측 비자사무실을 통해 수속 가능. 접수비용 RMB 400, 1주일 소요

<어학연수>

○ 비학위과정에서 국외훈련시 지원가능한 과정은 한어진수와 전업진수과정으로 볼 수 있음. 한어진수과정은 크게 일반어학과정과 어학강화과정으로 구분되고, 전업진수과정은 보통진수과정과 고급진수과정으로 구분되나 보통진수과정은 학기별 등록이 가능, 고급진수과정은 1년 단위로 등록하기 때문에 보통진수과정만 가능.

○ 보통진수과정은 어학과정과 연계하여 전공과목을 편성하고 수강신청할 수 있으므로 학위과정 전에 개론수준의 수업을 중국어로 들을 수 있는 장점이 있음. 해당학부에 개설된 전공과목들의 교수들이 대부분 석·박사과정도 가르치는 경우가 많음.

○ 또한 주당 20시간의 어학을 이수해야 하는 규정하에 전공과목을 6개 이상 들을시 중간고사와 기말고사에서 부담감이 매우 크지만, 사전에 전공기초과정을 접하고 학사시스템에 먼저 적응할 수 있는 장점이 있음

○ 여름학기는 4주코스와 8주코스가 있고 온라인에서 신청 및 학비 납부가 진행됨. 과정 선택시 이어지는 학위과정 등록일을 고려하여 중간에 비자기간에 문제없도록 주의가 필요함.

○ 과정별 학비
- 일반어학과정 : 주 20시간, RMB 18,000 / 학기
- 어학강화과정 : 주 30시간, RMB 28,000 / 학기
- 보통진수과정 : 주 6~20시간, RMB 18,000 / 학기
- 여름 8주과정 : 주 20시간, RMB 10,000

<대 학 원>

❍ 대학원 신청과 입학시험이 타대학보다 빠른 편이므로 사전에 HSK성적 및 관련서류(개인진술서, 추천서 등)를 준비하여 기한내 신청을 하는 것이 중요. 대학원 과정은 유학원 등을 통한 대리수속 없고 본인이 온라인으로 신청하여야 함. 온라인으로 신청한 후에 유학생사무실로 필요한 서류를 우편송부 해야 함으로 기한준수가 중요함.

❍ 입학관련(2016년 국제관계학원 석사과정 기준)
- 국제관계학원 홈페이지 '통지공고' 및 개인 이메일로 송부
- 유학생은 별도의 필기시험 없이 서류전형과 면접시험으로 선발
- 서류전형 합격자 및 면접일정 공지 : 3월 16일
- 면접등록 : 3월 25일
- 면접시험 : 3월 26일
- 합격자 발표 : 4월 11일

❍ 면접시험(국제관계학 전공 기준)
- 면접시험의 형태는 국제관계학원 안에서도 전공마다 다름
  · 중외정치제도 전공은 면접만 50분, 타전공 논술 미실시 등
- 면접 전 논술시험(30분, A4 1장)
  · 3문제 : 국가란 무엇인가, 최근 국가의 권위는 어떠한가
  2차 세계대전 이후 평화체제 유지의 원인과 배경
  최근 중국이 국제관계에서 직면한 주요 도전과제
- 면접(20분)
  · 응시번호에 따라 순서가 정해지고 한명씩 입장
  · 국제관계학 전공교수 5명, 조교 2명
  · 자기소개, 영문 전공서적 중국어 번역, 중문 전공서적 낭독, 개인경력 질문, 연구주제관련 질문 등

❍ 합격자 발표
- 유학생 응시 58명, 합격 35명(한국인 11명)

- 전공별 합격자

전 공	응 시	합 격
중외정치제도	2	2
중공당사	2	2
국제정치	14	9
국제관계	16	8
외교학	6	3
국제정치경제학	15	8
공공관리석사	3	3
계	58	35

제1장 서 론

1.1 연구배경 및 목적

9.11 테러 이후, 테러리즘은 기존의 특징과 다른 양상을 보이며 뉴테러리즘으로 진화하고 있다. 뉴테러리즘은 사이버공간이라는 특수한 공간과 결합하면서 영향력 및 파급력이 확대되었다. 정보화시대의 발달은 사이버공간과 우리 실생활을 더욱 긴밀하게 연결해주었고 편리함과 이익을 가져다 주었지만 이와 동시에 잠재적인 위험은 더욱 증가하게 되었다.

이에 따라 전 세계는 사이버 테러에 대응하기 위해 국내 법제도를 정비하고 대응책을 마련하는데 다양한 노력을 기울이고 있다. 그러나 사이버 테러의 초국가적인 특징과 사이버공간이 가지는 특수한 성격 때문에 한 국가의 법제도 및 정책만으로는 충분히 사이버테러에 대응할 수 없다. 그러므로 각 국은 국제협력 및 공조를 위해 다자간, 양자간 협력을 추진하고 국제규범 마련에 적극적으로 참여하고 있다.

그러나 이러한 각 국의 대내외적인 노력에도 불구하고 아직 사이버테러에 대한 공통된 정의나 합의된 국제규범은 부재한 현실이다. 각 나라가 추구하는 국가 이익이 다르고 상이한 가치관에 따라 국제적인 합의는 요원하다. 사이버테러 대응에 있어서 국제협력의 필요성은 공감하지만 각 국의 전략 및 상황은 제약요인이 되고 있다.

그러므로 이러한 제약요인 및 한계를 분석하고 극복하는 것은

사이버테러 대응에 있어서 중요한 의의를 지닌다. 이는 국제협력을 제고하고 국제공조를 강화할 수 있는 정책 및 전략의 기반이 될 수 있기 때문이다.

그렇다면 왜 한국은 중국과의 협력이 필요한가? 한국은 주로 북한으로부터의 사이버위협 및 공격에 대응하기 위해 많은 노력을 기울여 왔다. 그리고 북한의 사이버공격은 주로 중국을 경유하여 진행되었다. 제3국을 경유한 사이버공격은 그 진원지를 파악하더라도 관할권의 문제로 인해 외교적인 역량이 대응에 필수적이다. 양국의 신뢰구축 및 제도적 뒷받침이 없으면 실질적인 사이버테러 대응에 취약점은 해결할 수 없다.

한편으로 중국은 한국과의 협력이 필요한가의 문제가 남는다. 중국은 미국과의 사이버공간에서 거버넌스 및 표준화 경쟁을 하고 있다. 중국은 사이버공간에서 한·미·일 동맹이 형성되는 것을 바라지 않는다. 또한 한국은 미국과의 높은 사이버협력 단계에 있는 나라이지만 ICT 발전지수가 높고 정보기술산업이 상당히 발달한 경제적으로 매력적인 나라이다. 사이버 관련 기술은 경제와 밀접하게 연결되어 있으며 사이버테러 대응 기술은 곧 정보기술산업의 수준을 반영한다.

그러나 한중 양국은 협력 필요성은 공감하지만 사이버테러 대응에 관한 법제도와 전략의 차이점과 공격주체에 대한 인식의 상이점 그리고 미국과 북한 변수로 인해 협력은 낮은 단계에서 진행중이다. 그러므로 구체적인 차이점에 대한 분석을 통하여 양국의 긴밀한 협력방안을 도모하고자 하는데 이번 연구의 목적이 있다.

1.2 선행연구검토

현재까지 사이버테러 대응에 관한 국제정치학적 연구는 대표적으로 세가지 관점에서 진행되고 있다.

첫째, 군사전략과 국가안보에 주목하는 국제정치학적 시각이다. 국가 행위자가 관여하는 전통 군사안보 전략의 관점에서 사이버테러에 대응하려는 시각이다. 일반적으로 핵안보 연구에서 비롯된 '사이버 억지'라는 개념으로 사이버테러에 대응하려는 것이다. 사이버테러 대응에 있어서도 전통 국제정치에서 논하던 세력균형이나 안보 딜레마 등과 유사한 현상이 발생할 것으로 예상할 수도 있다.[1)]

그러나 30여년 전 핵 시대와 재래전 시대의 상투적인 현실주의 국제정치관을 그대로 21세기 사이버테러 대응에 투영하려는 시도는 경계해야 한다. 사이버 테러대응의 문제는 전통 군사전략론의 시각에서 사이버 냉전이나 사이버 억지의 비유를 무분별하게 적용해서 대처할 일이 아니기 때문이다. 게다가 이러한 시각은 국가 행위자의 군사안보라는 근대 국제정치의 맥락에서 접근함으로써 사이버테러 대응이 지니는 탈근대 안보의 면모를 간과할 우려가 높다. 사이버테러 대응에서도 상대방에 대한 억지가 매우 중요하지만 핵무기를 보유한 국가 간의 대칭적 관계에서 기원한 핵 억지의 개념을 비대칭 전력을 핵심으로 하는 사이버테러 대응에 끌어오기에는 무리가 따른다. 특히 공격이 식별되고 공격자는 발각되며 이에 대한 철저한 보복이 따라야 한다는 핵 억지 전략의 기본전제를 사이버테러 대응 분야에 적용하기는 어렵다. 사

1) 김상배, "버추얼 창과 그물망 방패", 한울 아카데미, 2018. 2, pp.16-21.

이버테러대응 분야에서는 공격자, 심지어는 공격행위 자체를 식별하는 것이 쉽지 않기 때문이다.[2)]

이러한 주장들은, 사이버테러의 범인을 찾아 보복하거나 책임을 묻겠다는 단호함을 표명하는데는 효과가 있을지 몰라도, 실제로 발생하는 사이버테러에 대처하는 적절한 처방이 될 수는 없다. 무엇보다도 사이버 공간에서 발생하는 위협을 객관적으로 측정하고 이에 보복할 수 있다는 선형적 사고방식 자체가 논란거리이다. 인과관계를 밝힐 수 없거나, 혹은 밝힐 수 있더라도 매우 복잡한 인관관계에 기반을 두고 있어 공격의 주체와 보복의 대상을 명확히 판별할 수 없는 현상을 단순 마인드로 파악하는 오류를 범할 가능성이 크다. 기본적으로 사이버테러대응 문제는 국가라는 개념을 중심에 둔 군사안보 측면에서 접근할 전통안보 문제와는 다르다.[3)]

둘째, 국제규범과 국제기구를 강조하는 국제정치학의 시각이다. 이는 자유주의적 제도주의나 국제법 논의와 맥이 닿는다. 이와 관련하여 주목할 것은 전통적인 국제법의 틀을 원용하여 사이버테러를 이해하려는 움직임이다. 탈린매뉴얼이 그 일례로서 사이버테러로 인해 인명피해가 발생했을 경우 해당 국가나 해커집단을 응징하고 좀 더 적극적으로는 사이버테러의 배후지를 제공한 국가나 단체에 대해서도 책임을 묻겠다는 발상에서 발견된다. 전통적인 국제기구인 유엔 차원에서 사이버테러 대응 문제를 다루려는 시도도 최근 빠르게 진행되고 있다. 그 대표적인 사례가 2013년 6월 유엔 GGE에서 합의해서 도출한 최종 권고안이다. 이 권고안에서는 사이버공간에서도 기존의 국제법이 적용

2) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.16-21.
3) Ibid., pp.16-21.

될 수 있다는 점에 합의했다.[4]

그런데 사이버테러 대응 분야에 뒤늦게 뛰어든 국가 행위자들의 포맷인 '국가간' 의 틀에 입각해서 이 분야의 국제규범을 만들려는 시도는 한계가 있다. 즉, 탈지정학적이고 초국적인 특징을 가지고 있는 사이버테러 대응 문제는 국가간의 관계를 연구하는 국제정치 담론의 접근에 있어서 신중함이 요구된다. 따라서 전통적인 국제법과 국제기구의 형식에 의존한 탈린메뉴얼과 유엔 GGE의 방법으로 해결되기에는 한계가 있다. 그럼에도 최근 나토와 유엔 등을 중심으로 진행되고 있는 전쟁법과 국제법 적용 시도는 도구적으로 활용할 긍정적인 여지가 있다.[5]

사실 국제규범과 국제기구를 강조하는 시각은 비국가행위자들의 역할을 적극적으로 파악해온 자유주의 국제정치이론과 맥이 닿는다. 기본적으로 사이버테러와 공격은 국가행위자들이 아니라 체계적으로 조직되지 않은 네트워크 형태의 행위자들이 벌이는 게임이다. 다시말해, 사이버테러 대응 분야는 해커들과 테러리스트 같은 비국가행위자들의 주무대이며, 최근 모색되고 있는 사이버테러 대응분야 글로벌 거버넌스의 논의도 비국가 행위자들이 적극적으로 참여하여 해법의 마련에 기여할 가능성이 높다. 그러나 이러한 시각은 사이버 공격 자체나 사이버 위협의 해소 문제에 적극적으로 개입하기 시작한 국가의 영향력을 과소평가할 우려가 있다. 특히 최근 진행되고 있는 사이버테러 대응 국제규범의 형성은 민간 행위자들의 주도권이 발휘되었던 글로벌 인터넷 거버넌스의 틀보다는 유엔과 같은 전통 국제기구의 틀에 좀 더

4) 김상배, "버추얼 창과 그물망 방패", 한울 아카데미, 2018. 2, pp.16-21.
5) Ibid., pp.16-21.

의존하는 모습을 보이고 있다.[6)]

셋째, 관념의 구성적 역할을 강조하는 구성주의 국제정치이론의 시각이다. 사이버테러 대응에서 관념변수를 강조하는 것과 관련해서는 우선 사이버심리전에 대한 논의에 주목할 필요가 있다. 사이버 심리전은 "인터넷을 통해 특정 인물 또는 집단의 견해, 감정, 태도 및 행동을 자신의 의지대로 유도하기 위하여 실시하는 선전, 선동, 모략 및 유언비어 유포 등과 관련된 활동"을 의미한다. 사이버공격의 대상은 개인, 기업, 단체, 국가 등 다양하다. 이러한 사이버 심리공격이 만약 상대국의 사회불만세력과 결합한다면 그 결과는 예측하기 어렵다. 사이버공격의 기본적 성격이 버추얼하다는 점 때문에 사이버 심리전의 요소는 항상 주요 변수가 된다.[7)]

한편, 구성주의 국제정치이론 진영 일반은 여전히 사이버테러 대응 문제에 대해서 이렇다 할 연구 성과를 내놓지 못하고 있다. 그럼에도 구성주의 시각이 갖는 유용성은 사이버공격의 현실과는 별도로 진행되고 있는 사이버테러 대응의 개념과 그 상징적 차원을 보여줄 수 있다는데 있다. 코펜하겐 학파로 알려진 국제안보 연구자들이 제시한 안보화 이론이 일례이다. 안보화 이론에 의하면, 안보는 객관적으로 존재하기보다는 안보행위자에 의해서 현존하는 위협의 대상, 즉 안전이 보장되어야 할 안보의 대상이 무엇인지를 정치적으로 쟁점화하는 과정에서 구성된다. 이러한 시각에서 보면 사이버테러 대응은 전형적인 안보화의 사례이다. 사이버테러 대응 문제는 실제로 큰 재앙의 형태로 발생한 실재하는 위협이거나, 또는 검증 가능한 형태의 사건이라기 보

6) 김상배, "버추얼 창과 그물망 방패", 한울 아카데미, 2018. 2, pp.16-21.
7) Ibid., pp.16-21.

다는 아직까지는 전문가들이나 정치가들이 구성한 현실 속에서 버추얼하게 존재하는 위협이기 때문이다.[8)]

이러한 안보화에 대한 논의는 항시 '과잉 안보화'의 위험성을 안고 있다. 특히 기존의 논의들은 '국가간' 프레임을 과도하게 강조할 '과잉-현실주의화'의 위험을 안고 있다. 근대 국제정치학의 주류인 현실주의 담론은 국민국가가 주요행위자이기 때문에 국가간의 권력정치 과정에 주목한다. 오늘날에도 이렇게 현실주의 담론이 상정하고 있는 현실은 엄연히 존재한다. 세계화, 정보화 및 민주화 등의 변화가 그 예이다. 그러나 오늘날 이러한 변화는 단지 국가간의 제로섬 게임 양상이라기 보다는 좀 더 복합적인 모습이 전개되고 있다. 따라서 현실주의 담론에 지나치게 집착할 경우 담론이 현실을 왜곡할 수 있는 가능성을 배제할 수 없다.[9)]

이상에서 살펴본 바와 같이, 기존의 국제정치이론적 시각들은 사이버테러 대응 분야의 복합성을 제대로 설명하지 못하고 있다. 기존의 이론적 시각은 사이버 위협의 성격을 제대로 파악하지 못할 뿐만 아니라 새로운 안보위협이 국제정치의 영역과 만나는 접점이나 그 동학에 대한 분석적 안목도 결여하고 있다. 기본적으로 기존의 시각에서 나타나는 가장 우려스러운 부분은 '탈근대적 현실'을 배경으로 부상하는 사이버테러의 위협을 이해하려 할 때 전통안보의 문제를 다루었던 경험에서 도출된 '근대적 인식론'을 원용하려는 오류에서 발견된다. 따라서 새로운 안보 패러다임의 부상이라는 맥락에서 사이버테러의 독특한 성격을 이해하고, 이를 둘러싸고 벌어지는 갈등과 협력의 복합적

8) 김상배, "버추얼 창과 그물망 방패", 한울 아카데미, 2018. 2, pp.16-21.
9) Ibid., pp.16-21.

면모를 분석하는 새로운 이론적 분석틀의 개발이 필요하다.[10]

개인 컴퓨터에서 발견되는 악성코드는 그냥 무시될 수 도 있겠지만 국가 기반시설을 통제하는 컴퓨터 시스템이 해킹을 당한다면 이는 국가적 차원에서 중대한 위험이 될 수 있다. 또한 이러한 해킹이 원자력 발전소 등 주요 산업시스템에 이루어질 경우 그 위험은 더욱 높아진다. 그리고 정치적 동기와 목적을 가진 테러집단의 수단으로 이용될 경우 그 위험성은 더욱 증폭된다. 심지어 해킹이 최근 국가간 사이버전쟁으로 전화될 가능성마저도 있다. 이러한 시각에서 보면, 사이버 안보의 문제를 개인안전이냐, 시스템 보안이냐, 국가안보냐 등으로 엄밀하게 구별하려는 시도 자체는 큰 의미가 없다. 대다수 사이버 위협은 처음에는 인터넷상의 해커나 범죄좌의 단속, 기업의 일상적인 정보보안, 이용자 개인의 보안 문제였을지라도 언제라도 그 규모와 목적이 커져 총체적 국가안보와 연계될 가능성이 있는 문제들이기 때문이다.[11]

사이버테러대응 분야는 영토성을 기반으로 하여 국가가 독점해 온 안보유지 능력의 토대가 잠식되는 현상을 보여주는 사례이다. 특히 사이버공간의 부상은 테러 네트워크나 범죄자 집단들에 의해 도발될 비대칭 전쟁의 효과성을 크게 높여놓았다. 결과적으로 사이버공간에서 등장한 새로운 위협은 국가에 의해 독점되어온 군사력의 개념뿐만 아니라 군사전략과 안보의 개념 자체도 그 기저에서부터 뒤흔들어 놓고 있다. 이러한 변화에 직면하여 기존의 지정학과 국가안보 중심의 국제정치학 시각은 시원스러운 해답을 제시하지 못하고 있다.[12]

---

10) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.16-21.
11) Ibid., pp.16-21.

최근 강대국들의 사이버공간에 대한 관여가 늘어나고 있고 점점 고전지정학 양상을 보이고 있다. 사이버 안보 게임의 이면에는 사이버 무기와 같은 기술변수가 존재하고 비국가행위자들의 개입요소가 커지면서 탈지정학적인 특징이 있다. 국제 사이버안보 이슈관련하여 강대국들은 사이버위협에 대한 인식이 다르기 때문에 자국의 안보화 과정이 다른 양상을 보이고 있다. 그렇기 때문에 어느 한 국가가 사이버테러의 대응 대책을 마련한다고 해서 각국에 적용하는 것은 한계가 있다. 그렇기 때문에 초국적인 특징을 지닌 사이버테러 대응 문제는 이해 당사국들의 긴밀한 협력을 통한 해법 모색이 필요한 것이다.[13]

최근에 사이버안보에서 두드러지게 나타나는 현상은 비국가행위자들이 시도하는 사이버 공격의 이면에 국가 행위자들이 깊숙이 관여하고 있다는 사실이다. 그러나 예전처럼 국가 행위자와 같은 어느 한 주체가 나서서 통제하고 자원을 동원하는 위계조직의 해법에 기댈 수는 없다. 오히려 국가 이외에도 지방자치단체, 기업과 개인 등의 이해당사자들이 각기 책임지고 자신의 시스템을 보호하는 분산적이지만 자율적인 거버넌스 모델이 효과적일 수 있다. 게다가 주변국이나 해외국의 정부 및 국제기구・단체 등과 적극적인 협력관계를 구축할 필요가 발생하고 있다. 복합 네트워크의 메커니즘을 빌려 발생하는 사이버테러와 공격은 단순히 일국 차원의 대응책 마련과 법제도의 정비 등으로 해결될 문제가 아니기 때문이다. 최근에는 초국적 위협으로 제기된 사이버테러와 공격의 문제에 대해서 국제협력이나 국가 간 협약과 같은 메커니즘으로 해결하려는 움직임도 적극 모색되고 있다.[14]

12) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.16-21.
13) Ibid., pp.16-21.

결국 중요한 것은 이 다양한 행위자들을 어떻게 엮어서 실제로 작동할 수 있는 메커니즘을 만드느냐의 문제이다. 궁극적으로 이러한 역할을 담당하는 것은 공익성의 담지자로서 국가 행위자일 수 밖에 없다. 다만 종전과 같은 위계모델로서의 근대 국민국가가 아니라 새로운 형태와 새로운 역할을 모색하는 국가모델을 찾아야 한다.

1.3 연구방법

본 연구를 위해 양국의 백서 및 기존 논문 자료를 바탕으로 하는 문헌조사 방법을 활용하여 양국의 법제도 및 정책 그리고 전략을 비교 분석하려 한다. 제2장에서는 사이버테러에 대한 개념과 이론적 배경을 분석하고 제3장과 제4장에서는 중국과 한국의 사이버테러에 대한 법제도 및 정책 그리고 전략을 살펴본다.

14) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.16-21.

제2장 이론적 배경

2.1 사이버테러의 개념 및 특징

1) 사이버테러의 개념

사이버테러(cyber-terror)는 사전적으로 사이버(cyber)와 테러(terror)가 결합된 용어이다.

사이버란 용어는 원래 그리스어 'Kyber(조타장치)'에서 유래한 것으로[15] 1947년 미국의 수학자 노버트 워너(N. Wiener)가 프로세스 제어기술의 연속적 형태를 나타내기 위해 사이버네틱스(cybernetics, 인공두뇌학)라는 용어를 새롭게 사용하면서 알려지기 시작했다. 사이버네틱스(그리스어 kubernectics)는 배의 키잡이 또는 조타수를 의미하는데 이는 당시 조타수들이 배의 운항에 관해 필요한 결정을 스스로 할 수 있는 자율성이 있었다는 특징을 차용한 것이었다.[16] 최근에는 정보통신기술과 관련된 행위를 포괄적으로 의미한다.

'사이버 공간(Cyberspace)'이라는 말은 1980년대 초반, 미국의 공상과학 소설가 윌리엄 깁슨(William Gibson)이 컴퓨터를 매개로 새롭게 생겨난 매트릭스 공간이라고 지칭하면서 알려지기 시작했다.[17] 사이버 공간은 현실에 존재하지 않는 가상(virtual)공간으로서 개인이나 기업, 국가 간에 컴퓨터 네트워크 시스템으로 연결되는 전자적 공간을 의미

15) 유동열, "사이버공간과 국가안보", 북앤피플, 2012, p.147.
16) 한희, "사이버 공간과 국가안보", 2014년 국가안보전략연구소 학술회의, 2014, p.8.
17) William Gibson, "Neuromancer", July 1, 1984, Ace Books.

한다.[18] 또한 사이버공간은 일반적으로 세가지 층위로 분류하는데 네트워크 인프라의 물리적 층위, 소프트웨어나 기술표준의 논리적 층위 및 지식이나 이념의 콘텐츠 층위로 구분한다.[19]

테러는 정치적·종교적·이념적 또는 민족적 목적을 가진 개인이나 집단이 그 목적을 추구하거나 그 주의 또는 주장을 널리 알리기 위하여 계획적으로 행하는 국가요인 등의 납치·암살, 국가 중요시설 등의 폭파, 항공기 등의 교통수단 납치·폭파, 폭발물·화생방 물질 등을 이용한 대규모 인명살상 등의 행위로서 국가안보 또는 외교관계에 영향을 미치거나 중대한 사회적 불안을 야기하는 행위로 이해된다.[20] 테러와 테러리즘은 흔히 동일한 의미로 사용되기는 하나, 테러는 폭력을 동반한 행위를 테러리즘은 주체인 단체, 행위, 나아가 그 정신 및 일련의 과정을 포괄하는 용어로 사용되기도 한다.[21]

사이버테러리즘의 대표적인 학자 도로시 데닝(Dorothy Denning)에 의하면, 사이버테러란 비국가행위자들이 자신들의 정치적·사회적 목적을 추구하고자 정부나 사회를 협박 또는 강제하기 위해 정보시스템을 대상으로 고도의 손상을 초래하는 컴퓨터 기반의 공격이나 위협을 뜻한다. 또한 사이버테러는 사이버공간이 테러행위를 수행하는 수단이 되기 때문에 사이버공간과 테러의 융합이며, 사이버테러리스트들은 인적·물적 재산을 대상으로 폭력행위를 저지르기 보다는 디지털 재산을 파괴 또는 방해하는 행위를 일으킨다.[22]

---

18) 이갑헌, “첩보에서 정보까지”, 형설출판사, 2010, p.321.
19) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.10-11.
20) 이황우, 한상암, “대테러 정책론”, 진명문화사, 1996, p.75.
21) 정준현, 지성우, “국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구”, 미국헌법연구, 2009, pp.218-219.
22) Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The

미국 연방수사국(FBI)은 사이버테러를 유사 국가단체나 비밀요원이 민간인에 대한 폭력으로 귀결되는 정보, 전산기기 시스템, 컴퓨터 프로그램, 그리고 데이터에 대한 계획된 정치적 공격으로, 그 산하기관인 국가기반시설보호센터는 컴퓨터 시스템이나 연결망을 활용한 공격을 통하여 폭력, 사망 그리고 파괴 및 공포를 조장한 다음 이를 바탕으로 정부에 정책을 변경하라고 강요하는 행위로 정의하고 있다.[23] 국제 전략문제 연구소(CSIS, The Center for Strategic and International Studies)는 에너지・교통・정부기관 등 주요 국가기반시설을 중단시키거나 정부 또는 시민들을 강제 또는 협박하기 위한 컴퓨터 네트워크 도구를 이용하는 것이라고 정의한다.[24]

사이버테러는 사이버 공간에서 소프트웨어와 네트워크를 활용한 테러행위라는 점에서 불특정 다수에 대한 물리적인 위협이나 폭력이 동반되는 일반적인 테러행위와는 구분할 수 있다.[25] 또한 기존의 테러리즘의 경우 정치적 목적이 본질적인 요소가 되고 있었던 것에 비해, 사이버테러는 정치적 목적뿐만 아니라 개인적 이유 등 다양한 목적 하에 이루어질 수 있기 때문에 어떠한 목적 하에 이루어진 행위라 할지라도 구성원 및 사회에 공포심이나 불안감을 조성시키는 행위는 모두 사이버테러에 포함될 수 있다.[26]

Internet as a Tool for Influencing Foreign Policy", Special Reports, 2001, pp. 20-21.

23) 오길영, "사이버테러의 대응체제의 문제점과 개선방향", 민주법학, 2014, p.467.

24) 조정은, "사이버테러 대응법제에 관한 연구", 토지공법연구, 2016, p.298.
" the use of computer network tools to shut down critical national infrastructures(e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population"

25) 윤해성, "사이버 테러의 동향과 대응방안에 관한 연구", 한국형사정책연구원, 2012, pp.64-65.

26) 곽관훈, "사이버테러 방지에 관한 일본의 법제도 및 시사점", IT와 법연구, 2014,

여기서 사이버테러 개념과 혼용되는 사이버전쟁과 사이버범죄도 살펴볼 필요가 있다.

사이버전쟁(cyber warfare)은 사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서, 컴퓨터 시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버체계를 파괴하고 아군의 사이버체계를 보호하는 것으로 정의할 수 있다.[27] 한편 Richard A. Clarke는 사이버전쟁이란 사전허락 없이 일국의 정부에 의해, 정부를 위하여 또는 정부의 지원을 받아 다른 국가의 컴퓨터·네트워크에 침투하거나 또는 컴퓨터 시스템에 영향을 주는 다양한 행위로서 그 행위의 목적이 컴퓨터·네트워크 또는 컴퓨터 시스템이 통제하는 대상에 데이터를 첨가·변경 또는 왜곡되게 하거나 또는 혼란·붕괴 내지는 손해를 입히는 것이라고 주장하였다.[28]

즉, 사이버전쟁이란 "국가 또는 그 요원이 자국의 이익을 위해 인터넷 등 사이버공간에서 정보기술을 이용하여 타국을 대상으로 적대적 행위를 가하고 이에 대하여 타국이 사이버공간에서 정보기술을 통해 방어하는 일련의 과정"을 의미한다고 볼 수 있다.

사이버전쟁의 핵심요소로 '국가간에 이루어지는 적대적 행위'이고, '인터넷 등 사이버공간에서 정보기술을 이용하여 이루어지는 행위'라는 점을 제시하고 있다는 점은 동일하다. 사이버전쟁은 전쟁의 일부

---

pp.263-264.

27) 김재윤, "사이버전 대책 및 개선방안", 2012년 국정감사 정책자료집, 2012, p.51.

28) 박기갑, "사이버전쟁 내지 사이버공격과 국제법", 국제법평론, 2010, p.41.

또는 전쟁의 전초과정으로 이루어지는 것이므로 그 개념정의에서 전쟁의 핵심요소인 '국가 간의 적대행위'란 요소를 빼놓을 수 없고, 기존의 전쟁과 달리 사이버공간에서, 기존의 무력수단이 아닌 사이버기술을 이용하여 이루어지는 분쟁이란 점에서 '사이버공간에서 정보기술을 이용하는 행위'란 요소도 개념정의에 필수적이란 면에서 위와 같은 일반적 정의는 타당성이 있다고 본다.[29]

사이버범죄(cyber crime)는 사이버공간에서 나타나는 제반 법규범 위반행위라고 포괄적으로 말할 수 있지만 아직 명확하게 정의된 바는 없다.[30] 즉, 사이버범죄란 일반적으로 인터넷 중심으로 한 사이버공간에서의 신종 범죄행위를 지칭하지만, 이러한 사이버범죄는 컴퓨터·네트워크 범죄(computer·network crime), 인터넷 범죄 (internet crime), 전자범죄(electric crime), 하이테크 범죄(high-tech crime)라는 용어 등으로 다양하게 사용되고 있어 그 개념이 명확하지 않다.[31]

사이버범죄는 단일현상이 아니라 정보네트워크와 통신테크놀로지에 의해 수행되는 것으로 가상공간이 주축이 되어 야기되는 것으로 컴퓨터범죄를 시작으로 하여 인터넷 범죄와 네트워크범죄를 거치고 최근에 디지털 기술과 결합함으로써 진화하고 있다.[32]

따라서 사이버범죄는 많은 유형의 범죄가 컴퓨터시스템을 이용하여 발생되고 기술의 꾸준한 발전과 동시에 이를 악용하여 발생하고

29) 김흥석, "사이버테러와 국가안보", 한국법학원, 2010, p.322.
30) 이성식, "사이버범죄와 시민의 역할", 정보화정책, 2006, p.70.
31) 윤영환, "사이버범죄의 실태와 대응방안", 한국행정과 정책연구, 2004, pp.157-158.
32) 이병종, "테크놀로지 발전에 따른 사이버범죄의 진화와 범죄현상의 조명 및 대응", 한국공안행정학회보, 2010, p.190.

있기 때문에 단적으로 정의하기란 매우 곤란하다.[33]

사이버범죄는 사이버공간에서 일어나는 범죄라는 점에서는 사이버테러와 같으나, 사이버범죄가 개인의 이익을 추구하는 것이라면, 사이버테러는 인터넷 공간을 이용하여 국가기관이나 다중에 영향을 미치는 민간영역에 대하여 정보통신기술을 활용한 공격행위로 사회적 혼란을 야기하거나 국가안보를 위협하는 목적을 가진 행위로 볼 수 있을 것이다.[34]

그러나 실제 사이버공간에서 발생한 불법행위에 대한 규제는 법규를 중심으로 이루어지기 때문에 실무상이나 학계에서 논의하고 있는 행위유형에는 차이가 있을 수밖에 없고 여기에서 사이버테러와 사이버범죄와의 구별의 혼란이 생기게 되는 원인이 될 수도 있다.[35]

따라서 사이버범죄는 기존의 컴퓨터를 활용하여 발생되는 범죄를 포함하여 사이버 공간에서 행해지는 모든 유형의 범죄를 포괄하는 것으로 정의되어야 한다.[36] 또한 사이버범죄는 국가를 초월하는 초국가적 특성을 띤다는 점에서 국가 간에도 적용될 수 있는 보다 포괄적이고 일반적인 의미로서의 정의가 필요하다.[37]

---

33) 조민상, “사이버침해 사례분석을 통한 위기대응방안”, 한국민간경비학회보, 2013, p.273.
34) 김태계, “사이버테러 범죄 대응에 관한 제도적 문제점과 대책”, 법과 정책연구, 2014, p.1342.
35) 조현빈, “현행법상 사이버테러의 규제 가능성에 대한 검토”, 한국위기관리논문집, 2008, p.26.
36) 조민상, “사이버침해 사례분석을 통한 위기대응방안”, 한국민간경비학회보, 2013, p.274.
37) 김영환, “사이버범죄에 대한 국가적 대응체계 구축의 이론적 함의-사이버테러형 범죄를 중심으로”, 한국 컴퓨터정보학회 논문지, 2009, p.166.

이렇듯 사이버테러를 하나로 정의하는 것은 한계가 있다. 사이버테러리즘의 용어 정의가 불분명한 근본적인 이유는 이 용어의 의미가 불분명한 테러리즘이라는 용어를 기반으로 하여 생성된 데다가 사이버라는 또 다른 불분명한 개념을 포함하여 만들어진 합성어라는 사실이다. 또한 사이버테러리즘에 대한 논의나 연구를 수행하는 전문가와 연구자들의 배경이 정보통신학・법학・행정학・사회학・범죄학・국제정치학・군사학 등 이질적인 다양한 분야를 포함하여 각기 서로 다른 의미로 사이버테러리즘에 접근하고 있기 때문이다.[38)]

그러나 사이버전쟁, 사이버테러, 사이버범죄의 개념을 구분하는 것은 사이버테러 대응에 있어서 중요한 의미를 가진다. 대응과정에 있어서 주된 적용규범이 달라질 수 있기 때문이다. 사이버전쟁의 경우는 전쟁의 한 부분을 구성하는 것이기 때문에 당연히 전쟁법이 문제된다. 사이버전쟁이나 사이버테러의 수준에 이르지 못한 사이버범죄의 경우에는 형사법만이 문제가 될 것이다. 이에 비하여 사이버테러의 경우는, 주로 형사법적 규율이 문제되겠지만, 경우에 따라서는 전쟁법이 문제되는 경우도 있을 수 있다. 이처럼 어떤 개념에 포섭되는가에 따라 법적규율이 달라질 수 있기 때문에, 사이버테러 대응 체계를 분석하는데 의미가 있다.

사이버테러대응은 1990년대 초반 컴퓨터 시스템의 장애나 인터넷이라는 물리망의 보호에 중점을 둔 컴퓨터 보안과 네트워크 보안의 의미로 이해되었다. 그러나 2000년대에 들어서면서 인터넷의 활용이 확산되고 논리적 층위에 대한 보호가 정보보호의 문제로 인식되기 시

38) 윤민우, “새로운 안보환경을 둘러싼 사이버테러의 위협과 대응방안”, 한국경호경비학회지, 2014, p.117.

작되었다. 2000년대 후반 이후 사이버공간에서 정치·사회·문화적 활동이 활발해지고 그 중요성이 강조되면서 사이버공간의 안전과 안보 문제에 대한 논의가 확대되었다. 특히 9·11 테러 이후 각 국은 사이버활동의 기반이 되는 시스템과 지식정보를 보호하려는 사이버테러 대응정책 수립을 위해 노력을 하였다.[39]

인터넷의 보급이 미미하던 시기 컴퓨터 보안과 정보보호는 컴퓨터 전문가나 소프트웨어 엔지니어들의 영역에 머물렀다. 주로 기술공학적인 연구를 통해 세계정치 현상의 하나로 사이버테러를 바라보거나 또는 뉴테러리즘의 새로운 기술적 형태로 인식되었다. 그래서 사이버테러는 주로 비국가행위자인 해커그룹이나 테러리스트들이 일으키는 비대칭 전력의 공격방식 중 하나로 간주되었다. 그러나 최근 국가 행위자들이 사이버테러의 공격과 방어에 직간접적으로 관련되면서 국제정치학적인 논의가 활발히 진행되고 있다.[40]

2) 사이버테러의 특징

사이버 공간의 확장속도가 예상을 뛰어넘고 그 확장범위가 지구 곳곳에 미치는 것만큼, 이에 비례해서 사이버테러 위협도 매우 빠른 속도로 늘어나고 있다. 사이버테러는 전통적 형태의 테러처럼 물리적 공간에서 수행되는 것이 아니라 네트워크로 연결된 사이버공간에서 수행되기 때문에 피해의 파급과 규모면에서 대단히 큰 영향력을 가지고 있다.[41] 즉, 사이버공간에서 행해지는 사이버테러는 해킹과 바이러스

39) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.10-11.
40) Ibid., p.16.
41) 정용기, “위험사회에서의 사이버 테러 대응방안”, 성균관법학, 2014, p.288.

같은 수단으로 목적하는 대상의 정보시스템에 영향을 주어 목적하는 결과를 기대한다는 점에서 시·공간적으로 제한을 받는 전통적인 물리적 테러리즘과 다른 특징을 나타낸다.[42]

APT(Advanced Persistent Threat) 공격

APT는 지인으로 위장해 특정 조직의 정보를 지속적으로 빼내는 방식으로 공격을 당한 조직은 보안 사고가 생기기 전까지 인지하지 못하는 경우가 대부분이며 APT는 불특정 다수가 아닌 특정한 목표를 겨냥해 오랜 기간 잠복하면서 기밀 정보를 빼내도록 설계된다는 점이 기존 해킹과 구별된다.[43]

3) 사이버공격 주요사건

2007년 에스토니아 사이버공격

2007년 4월 에스토니아의 주요 기관 홈페이지와 전산망이 디도스 공격을 받고 국가 전체에 걸쳐 전산망이 마비되었다. 이 사건은 수도 탈린에 있던 구소련의 참전기념 동상을 이전한다는 정책을 발표하고 러시아계 주민과 러시아로부터 거센 반발을 받은 후에 발생하였다.

2008년 터키 BTC 송유관 폭발

2008년 터키 동부지역에서 카스피해부터 지중해에 이르는 구간을 관통하는 송유관(길이 1,760km)이 폭발하였다. 당시 사건의 원인으로는 기기의 오작동 또는 테러조직의 소행이 거론되었다. 그러나 오랜 시간의 조사 끝에 6년이 지난 2014년 당시 사건이 악성코드 삽입을 통

42) 남길현, “사이버테러와 국가안보”, 국방연구, 2002, pp.168-169.
43) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, p.16.

한 사이버공격에 의한 것이었음이 밝혀지게 되었다. 공격의 배후로는 러시아가 지목되었다.[44]

2008년 조지아 사이버공격

2008년 러시아와 조지아간 전쟁 당시 러시아의 물리적 공격 이전에 조지아 대통령의 홈페이지 및 의회・국방부・외교부 등의 사이트가 사이버공격을 받아 전산망이 무력화된 사건. 사이버전력이 무력과 결합한 케이스로 주목을 받았다.

2010년 스턱스넷 사건

2010년 가을, 이란의 나탄즈 핵재처리 시설에 스턱스넷(Stuxnet worm)이라는 악성코드 공격에 의해 1,000개 이상의 원심분리기가 파괴된 사건이다.[45] 본래 스턱스넷 웜은 마이크로소프트의 윈도우 운영체제 결함을 이용하여 만들어졌다. 특히 지멘이 설계한 산업통제 시스템이 설치된 공장의 공정절차 운영체계를 붕괴시키는 기능을 지니도록 만들어졌다. 그러나 이란 스턱스넷 사건 이후, 스턱스넷 웜은 전 세계에 있는 약 44,000개의 컴퓨터들을 감염시키는 역할을 했고 미국과 독일을 비롯한 많은 컴퓨터에 피해를 입혔다.[46] BTC 송유관폭발 사건이

---

44) Bloomberg, “Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar”, Dec. 10, 2014, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

45) David Albright, Paul Brannan and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?”, Institute for Science and International Security Report, Dec. 22, 2010, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant.

46) Sharon Weinberger, “U.S. Also Vulnerable to Stuxnet Virus, Official Warns”, AOL News, 2010.12.07.

http://www.aolnews.com/2010/12/07/us-also-vulnerable-to-stuxnet-virus-official-warns

사이버공격에 의한 것임이 밝혀지기 전까지 스턱스넷 사건이 물리적 파괴를 가져온 최초의 사이버공격 사건으로 알려져 있었다. 해당 사건의 공격 배후는 미국과 이스라엘로 기정사실화 되어 있다.

2014년 우크라이나 대선개입 사건

2014년 우크라이나 대선 4일 전에 우크라이나 중앙선거관리위원회 컴퓨터에 대한 사이버공격으로 투표 검수 프로그램이 운영 불가 상태가 되었고, 선거 결과가 방송되기 40분 전에 악성바이러스가 제거되었다. 악성코드를 통해 실제 당선자가 아닌 극우정당 후보가 당선된 것으로 방송되도록 조작되어 있었다.[47]

2014년 소니해킹 사건

2014년 미국의 소니 영화사의 홈페이지가 해커집단에 의해 해킹 공격을 받은 사건이다. 이는 북한 김정은 위원장을 암살하는 내용의 영화 '더 인터뷰(The Interview)' 개봉을 앞두고 발생하였다.

2016년 미국 민주당 전국위원회 이메일 해킹사건

2016년 폭로전문 사이트 위키리크스가 민주당의 대선 후보인 Hillary Clinton의 캠프 선대본부장 John Podesta의 이메일 수천 건을 공개하면서 촉발되었으며, 위키리크스가 폭로한 이메일 해킹의 배후에 러시아가 있다는 미 당국의 발표에 따라 러시아의 미 대선개입 논란이 문제가 된 사건이다. 러시아가 미국 민주당 전국위원회의 이메일을 해킹하여 공개함으로써 미국 대선에 개입하려 한다는 의혹이 불거진 사건으로 미국연방수사국(FBI)이 공식적으로 수사에 착수하기도 하였

47) The Christian Science Monitor, "Ukraine election narrowly avoided 'wanton destruction' from hackers", Jun. 17, 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

다.[48]

2017년 워너크라이 랜섬웨어 공격

WannaCry는 전형적인 랜섬웨어 공격으로 사용자의 파일을 암호화한 다음, 이를 푸는 대가로 금전을 요구하였다. 2017년 5월 12일부터 유포가 되었고 전세계 100여개국에 확산되어 피해를 입혔다. 이 랜섬웨어는 미 국가안보국이 해킹당한 툴이 사용된 것으로 알려졌다.

48) The New York Times, “Sowing Doubt Is Seen as Prime Danger in Hacking Voting System”, Sept. 14, 2016. http://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html.

2.2 동맹안보딜레마 이론

1) 안보딜레마 이론

안보딜레마(security dilemma)란 자국의 안보를 위해 취한 조치가 다른 국가의 안보를 저해하게 되면서 의도하지 않았던 충돌이 벌어지는 국제정치 상황을 의미한다. 다른 국가를 공격하거나 침략할 의도에서가 아니라 자국의 안전을 확보하기 위해 군사력을 증강한 것이 주변의 다른 국가로 하여금 안보의 위협을 느끼게 되는 것이다. 안보딜레마는 비록 국가가 공격적 행위를 행하는 현상타파국가가 아닌 상황에서도 결과적으로는 경쟁이 나타나게 되는 국제정치의 상황을 설명한다.[49)]

안보딜레마는 냉전이 시작되고 미소 양진영의 첨예한 갈등구조가 전개되었을 때 논의가 시작되었다. 논의의 시작은 허버트 버터필드(Herbert Butterfield)와 존 헤르츠(John Herz)라고 할 수 있다. 1940년대 말부터 냉전은 국제정치 구조를 경직되게 만들었다. 이는 자유주의와 공산주의 진영간에 반세기 동안 지속적인 긴장관계를 형성하였다. 1·2차 세계대전 이후 많은 나라들에서는 전쟁의 경험을 통해 생존에 관한 안보담론이 지배했다. 이것은 다시 대외적으로 공격적인 양상으로 나타났고 다른 나라에게 생존에 관한 위협을 상승시키며 연쇄적인 악순환이 계속되었다..

버터필드와 헤르츠는 무정부상태인 국제정치에서 국가간에 생존

49) 하영선 외 15인, “변환의 세계정치”, 을유문화사, 2012, pp.188-189.

의 문제에서 비롯된 자구책이 주변국가를 위협하게 되는 안보딜레마를 지적하였다. 버터필드는 무정부상태의 국제정치에서 필연적으로 나타나는 '홉스적 공포(Hobbesian fear)'를 강조하였다. 이론인해 발생되는 불확실성이 안보불안을 야기시키는 원인이라고 설명하였다. 이러한 안보불안은 어쩔수 없이 인간사회에서 발생하고 수용할 수 밖에 없는 원죄 같은 비극이라고 주장하였다.[50]

이러한 관념이 구체적인 '안보딜레마'의 개념으로 수립된 것은 헤르츠에 의해서였다. 그는 사회적 상호작용에서 비롯된 안보문제의 구조적 딜레마에 초점을 맞추고, 이것이 개별국가차원에서 쉽게 해결할 수 없는 것이라는 점을 부각시켰다. 또한 20세기 초반에 여러 차례의 대규모 전쟁을 겪으면서 갈등구조로 빠져들 수밖에 없었던 국제정치의 '비극적 속성(tragedy)'을 강조하였고, 그로부터 적절한 해법을 모색하는 일이 얼마나 어려운가를 생생하게 논증하였다. 1950년대부터 핵무기와 이데올로기적 대립, 그리고 양극화 구도를 기반으로 구축되어온 전략적 접근방식이 국제정치의 안보딜레마 문제를 해결하는데 근원적인 한계를 지니고 있다는 점이 이로써 분명해졌다.[51] 이때부터 안보딜레마는 20세기의 비극적 냉전구조의 한 가운데에 자리잡고 있는 가장 핵심적인 퍼즐로 간주되기 시작했던 것이다.

1970년대 로버트 저비스(Robert Jervis)는 심리학적인 접근방법을 통해 안보딜레마 이론을 확립하였다. 저비스는 냉전시기 미소 양국의

---

50) Herbert Butterfield, "History and human relations", 1951, Macmillan.
51) John H. Herz, "Idealist Internationalism and the Security Dilemma", Jan, 1950, World Politics Vol.2, pp.157-159. ; Christian Hacke and Jana Puglierin, "John H. Herz: Banlancing Utopia and Reality", September, 2007, International Relations 21, pp.277-288.

힘겨루기 양상에 대하여 ‘억지(deterrence)모형’과 ‘상승작용(spiral) 모형’으로 비교하였다. 상승작용 모형은 두 행위자가 서로 의도하지 않았지만 불가피하게 전쟁으로 국면이 전개되는 안보딜레마의 구조가 나타난다고 하였다. 즉 안보딜레마가 발생하는 결정적인 요인은 안보상황을 잘못 판단하는 정책결정자들의 오인(misperception)에서 비롯된다고 강조하였다. 정책결정자들이 아무리 합리적인 판단을 내린다고 해도 상대국의 정책결정에 미치는 영향을 정확하게 파악하기 어려운 심리적 한계에 대하여 언급하고 있다.

저비스의 안보딜레마 이론은 국제정치의 갈등과 비극이 ‘의도하지 않은 결과’로서 나타난다는 점을 분명하게 보여주고 있는데, 이는 행위자의 자유의지 대신 구조적 한계로 말미암아 방어에 관한 욕구가 하나의 ‘딜레마’로 이어질 수밖에 없는 이유를 설명한다. 거시적 환경에 대한 심리적 인식의 한계가 구조적인 안보딜레마로 이어지는 모습을 그리고 있기 때문이다. 이런 점에서 그의 안보딜레마 개념은 국제정치의 ‘상호의존성(interdependence)’에서 야기되는 결과의 비합리적 측면을 잘 드러내고 있다. 개별 국가들이 좁은 의미의 합리성(rationality) 개념에만 치중할 경우 원래 의도했던 목표에서 벗어나 서로에게 더 나쁜 결과를 초래할 수 있다는 현실주의적 비관론으로 이어지고 있는 것이다.[52]

저비스는 안보딜레마를 완전하게 극복하는 것이 불가능하다고 보았다. 하지만 그 강도를 완화할 수 있다고 해석하였다. 안보딜레마의 강도는 일종의 변수로서 강화될 수도 있고 약화될 수도 있다고 보았

52) Robert Jervis, “Perception and Misperception in International Politics”, Princeton University Press, 1976, pp.54-67.

다. 이러한 안보딜레마의 강도에 영향을 주는 요인에 두가지 결정요인을 제시하였다. 하나는 ‘공격방어 균형’이고 또다른 하나는 ‘공격방어 구분 가능성’이다.

첫째, 공격방어 균형 변수는 방어보다 공격이 유리한 공격우위 상황과 방어가 공격보다 유리한 방어우위 상황으로 구분된다. 공격우위상황에서 상대국가가 기습적으로 공격을 할 경우 치명적일 수 있지만 방어우위상황에서는 치명타를 피할 수 있다. 따라서 공격방어 균형은 국가가 전략적 취약성을 결정하는데 영향을 준다.

둘째, 공격방어 구분 가능성은 상대국가가 취하는 행동에 대하여 공격과 방어가 구분이 가능한 상황과 불가능한 상황으로 나뉜다. 이러한 구분 가능성을 통해 상대국가가 공격우위의 국가인지 방어우위의 국가인지에 대한 의도성을 파악할 수 있게 된다.[53]

안보딜레마 이론에 대한 몇 가지 비판적 의견들도 존재한다. 먼저 미어세이머(John Mearsheimer)는 안보딜레마라는 개념 자체가 성립하지 않는다고 주장한다. 미어세이머는 국제사회의 무정부상태를 매우 위험한 상태로 간주하고 패권국을 제외한 모든 국가들을 현상타파국가로 분류했다. 안보를 확립하는 유일한 방법은 패권국이 되는 것이고, 따라서 패권국을 제외한 모든 국가들은 팽창을 추구한다는 것이 그의 주장이다. 즉 애초부터 현상타파 국가가 ‘의도치 않게’ 다른 국가의 안전을 저해한다는 안보딜레마의 명제는 미어세이머에게 성립하지 않는다.[54]

53) 이근욱, “왈츠 이후 : 국제정치이론의 변화와 발전”, 한울 아카데미, 2016, pp.56-58.
54) 이근욱, “왈츠 이후 : 국제정치이론의 변화와 발전”, 한울 아카데미, 2016, pp.56-58.

2) 동맹안보딜레마 이론

글렌 스나이더(Glenn Snyder)는 동맹 내부에서 발생하는 안보문제에 있어서도 민감한 딜레마 구조가 나타난다고 보았다. 스나이더는 군사동맹 관계에서 한 구성 국가는 항상 상대 동맹국가로부터 버림을 받거나 상대 동맹국가로 인해 원하지 않는 전쟁의 휘말릴 수 있는 위험에 항상 노출되었다고 지적하였다. 이는 '방기(abandonment)'와 '연루(entrapment)' 현상으로 구분되고 두가지 현상 모두 국가안보를 위해 바람직하지 않은 상황이기 때문에 국가는 이러한 상황을 회피하려는 성향이 나타난다고 하였다. 그러나 이를 동시에 회피하는 것은 불가능하게 되는데 한가지 위험을 회피하게 되면 다른 위험이 커지기 때문이다.

따라서 전통 안보딜레마가 적대 (adversary)관계에 있는 국가들 사이의 관계를 다룬다면, 스나이더의 개념은 '동맹(alliance) 안보딜레마'에 주안점을 둔다. 결국 어떤 국가든지 동맹을 체결하고 있다면 적국과의 안보관계 및 동맹국과의 안보관계를 동시에 다루어야 한다는 점에서 그는 '복합(composite) 안보딜레마'라는 개념을 제시한다.[55]

유사한 맥락에서 크리스텐슨(Thomas Christensen)과 스나이더(Jack Snyder)의 연구도 다극화 구조 속에서 나타나는 동맹국간의 갈등 및 안보딜레마 문제를 다루고 있다. 이들은 신현실주의의 구조적 이론에 대항하여 다극화 세계가 대단히 불안정한 모습을 보이는 이유로 국가 차원의 '함께 엮기(chain-ganging)'와 '부담 전가하기(buck-passing)'

55) Glenn H. Snyder, "The Security Dilemma in Alliance Politics.", World Politics , 1984, pp.477-479.

라는 두 가지 행태를 꼽는다. 첫 번째 현상은 반드시 필요하지 않은 세력균형을 달성하기 위해 무리하게 동맹관계를 구축하는 것을 일컬으며, 두 번째 현상은 헤게모니의 부상을 견제하는데 소모되는 비용을 제3자에게 전가하려는 행태를 말한다. '함께 엮기' 현상은 공격의 이익이 클 경우에, '부담 전가하기'는 방어의 이익이 클 경우에 주로 사용되는 전략인데, 이러한 이익은 대부분 주관적인 인식에 따라 결정된다.[56] 제1차 세계대전 당시에는 공격적인 인식이, 제2차 세계대전 당시에는 방어적인 인식이 지배함으로써 각각 '함께 엮기'와 '부담 전가하기'의 특징이 나타났다는 것이 이들의 설명이다.

냉전 시기에는 방기의 위험이 작았기 때문에 딜레마가 상대적으로 심각하지 않았다. 따라서 적대관계 안보딜레마가 주로 나타났지만 냉전 이후 국제정치구조가 다극화되면서 동맹국에 의한 방기의 위험이 커지면서 동맹 안보딜레마가 더욱 심각해진다고 보았다. 이러한 스나이더의 주장은 20세기에 나타난 갈등과 분쟁의 구조를 이해하는데 도움을 주었으며 안보딜레마 이론을 발전시키는데 기여하였다. 또한 크리스텐슨과 스나이더는 안보딜레마의 구조적 측면과 심리적 측면에서 동맹내부의 동학을 분석함으로써 기여하는 바가 크다. 동맹국간의 안보협력은 국제정치 구조가 자국에 유리한 상황인지 불리한 상황인지에 따라 다르게 전개된다. 이러한 설명은 안보딜레마의 내부 동학이 초기 이론에 비해 더욱 복잡하다는 점을 잘 나타내주고 있다.

56) Thomas J. Christensen and Jack Snyder, "Chain Gangs and Passed Bucks : Predicting Alliance Patterns in Multipolarity.", International Organization, 1990, pp.144-147.

2.3 안보화 이론

1) 주요내용 및 가정

코펜하겐 학파(Copenhagen School)는 기존의 전통안보 개념이 비군사적 위협들에 대해서 설명하는 것에 한계가 있다는 문제의식에서 출발하였다. 안보문제가 단순히 군사적 영역에만 머무르는 것이 아니라 비군사적인 영역에서도 발생할 수 있다고 보았다. 코펜하겐 학파는 안보문제가 다섯가지 분야에서 발생할 수 있다고 보았다. 정치, 경제, 군사, 사회, 환경에서 발생하는 안보문제는 위협을 받는 대상이 무엇인가에 의해 그 분야가 결정된다고 하였다.[57] 그러나 특정한 안보문제가 꼭 한분야에만 관련된 것이 아니기 때문에 위협의 속성 역시 그 분야에 따라 결정되는 것은 아니라고 보았다. 예를 들어, 군사영역에서 발생한 안보문제라도 군사적 위협뿐만 아니라 환경 또는 경제적 위협을 동반할 수 있다. 물론 코펜하겐 학파가 안보를 다섯가지 다른 분야에서 이해하려는 것은 안보문제의 위협을 좀더 심층적으로 분석하려는 의도가 담겨있다. 즉, 안보의 범주를 확장시킴으로써 다양한 형태의 위협과 복잡한 속성을 이해하려고 하는 것이다.

코펜하겐 학파가 군사적 영역과 비군사적 영역을 모두 포함하여 안보의 범주를 확장시켰지만 안보가 생존이라는 문제와 분리될 수 없는 것은 전통적인 국가중심의 안보론과 그 맥을 같이한다. 즉, 어떤 문제가 안보문제로 격상되려면 특정 대상에게 실질적인 위협이 존재해야 한다. 이러한 실존적 위협은 꼭 실존할 필요는 없으며 위협의 정도가

57) Barry Buzan, Ole Wæber, Jaap de Wilde, “Security : A New Framework for Analysis”, Lynne Rienner Publisher, 1998, pp.21-23.

지정된 대상의 생존을 위태롭게 할 만큼의 심각성이 인식되고 이해된다면 안보의 위협으로 간주될 수 있다.[58]

코펜하겐 학파는 안보화 행위자와 안보의 대상 그리고 수용자의 역할의 상호작용을 분석함으로써 특정한 문제가 안보적 위협으로 변화되는 과정을 설명한다.

안보화 행위자는 특정한 문제나 현상을 안보문제로 격상시키기 위해서 실존하는 위협이 지정된 안보대상의 생존을 위협한다고 주장하는 행위자를 뜻한다. 이를 위해 안보화 행위자는 실존적 위협을 묘사하고 소개하는 안보화 행위를 실천한다. 주로 이러한 안보화 행위자는 정부, 정치인, 관료, 로비스트 등 권력행사가 가능한 개인이나 집단을 일컫는다. 이는 특정한 문제를 안보위협으로 변화시키고 안보화된 문제를 해결하는데 필요한 비상조치의 도입을 정당화하기 위해서 권력이 필요하기 때문이다.[59]

안보의 대상은 실존적 위협에 노출되었거나 그로인해 생존을 위협받는 개인이나 집단 또는 사물이나 현상을 의미한다. 이러한 대상은 실존적 위협으로부터 자신의 생존을 요구할 권리를 가지면 코펜하겐 학파는 안보의 대상을 주권국가에만 국한시키지 않는다. 예를 들어, 군사적 분야에서 안보의 대상은 주로 국가를 의미하지만 국가 이외에도 정치적 독립체나 군대 그 자체도 대상이 될 수 있다. 정치 안보분야에서는 국가의 주권, 사상 또는 이념 등이 안보의 대상이 될 수 있다. 사

58) Barry Buzan, Ole Wæber, Jaap de Wilde, “Security : A New Framework for Analysis”, Lynne Rienner Publisher, 1998, pp.21-23.
59) Ibid., pp.21-23.

회적 안보분야에서는 안보의 대상을 거대한 규모의 집단 정체성으로 규정하고 있는데 집단 정체성이란 국가의 경계영역을 넘어서 기능할 수 있는 민족이나 종교 등을 의미한다.[60]

수용자는 안보화 행위자가 안보영역에서 다루기를 원하는 문제와 관련이 있거나 그 문제에 관심을 가지고 있는 이들을 의미한다. 수용자는 안보화행위자가 특정 문제를 안보문제로 격상시키는데 필요한 정치적인 지지를 제공하는 역할을 한다. 또한 안보문제를 해결하기 위한 비상조치의 도입에 있어서도 정치적 지지를 보냄으로써 안보화 행위자의 결정에 정당성을 부여하는 역할을 한다. 만약 안보화행위자가 이러한 과정에서 수용자의 지지를 받지 못하는 경우 그 문제는 안보문제로 격상될 수가 없다. 즉 안보문제의 실존적 위협은 안보화 행위자와 수용자간의 상호작용을 통해 구성되는 것으로 보는 것이다.[61]

코펜하겐 학파의 안보론의 핵심은 단순히 안보의 개념을 확장하는 것이 아니라 기존에는 안보적 사안이 아니었던 문제가 안보 영역으로 옮겨져 안보 문제로 다루어지는 과정을 분석하고 이해하는 것, 즉 '안보가 구성되어지는 과정'을 이해하는 것이다. 코펜하겐 학파에 따르면 특정 문제는 총 세 가지 수준에서 다루어질 수 있는데, 이는 비정치적(non-politicised), 정치적(politicised), 그리고 안보적(securitised) 수준이다. 먼저 비정치적 수준의 문제는 국가적 차원에서 다루어질 필요가 없거나 대중적 담론의 주제가 될 만한 무게를 지니지 않은 사안을 의미한다. 다시 말해, 문제의 심각성이 무겁지 않다고 여겨질 경우 그

60) Barry Buzan, Ole Wæber, Jaap de Wilde, "Security : A New Framework for Analysis", Lynne Rienner Publisher, 1998, pp.21-23.
61) Ibid., pp.21-23.

문제는 주로 비정치적 수준에 머물게 된다. 두 번째 정치적 수준의 문제란, 국가의 일반 정치 체계(normal political system)에서 다루어지는 사안을 의미하는데, 비정치적 수준에 머물던 문제의 위협이 점점 더 심각한 수준으로 발달하여 공론화되고 국가적 차원에서 다루어질 필요가 있다고 여겨질 때 비로소 정치적 문제로 거듭나게 된다. 정치적 수준의 문제는 주로 국가의 공공정책을 통해 관리된다. 이렇게 정치화된 문제가 특정한 대상의 생존을 실질적으로 위협하는 사안으로 여겨짐과 동시에 더 이상 국가의 일반 정치 체계에서는 해결할 수 없는 수준에 이르렀다고 판단될 때 그 문제는 안보 문제로 격상된다. 이미 정치화된 문제가 안보 문제로 거듭나는 과정에서 안보화 행위자는 문제에 대응하기 위해 자신이 도입하고자하는 비상조치(국가의 일반 정치체계의 역량을 벗어나는 정책이나 전략)의 정당성을 확보하게 된다.

실존적 위협에 대응하기 위한 비상조치의 정당성을 확보하는 것은 안보화에 있어 매우 중요하다고 볼 수 있다. 앞에서 서술한 바와 같이 비상조치는 흔히 국가의 일반 정치 체계의 원칙(rules)과 절차(procedures)를 넘어서는 정책이나 전략의 수행을 의미하기 때문에 대내외적인 반대를 불러일으킬 수 있다. 더군다나 그 비상조치가 문제시되고 있는 안보적 사안과 직간접적으로 관련된 행위자들의 희생을 필요로 하거나 받아들이기 어려운 어떠한 비용을 전제로 할 경우, 비상조치의 도입을 정당화하는 작업은 더욱 중요해진다. 따라서 안보화 행위자는 자신이 도입하고자하는 비상조치의 정당성을 확보하기 위해 첫째, 본 문제는 안보의 대상을 실제로 위협하고 있으며, 둘째, 국가의 일반적인 정치 체계에서는 다룰 수 없을 만큼 심각하고 시급한 수준의 안보적 사안이라는 점을 문제와 관련된 수용자들에게 효과적으로 전달

해야한다. 여기서 한 가지 집고 넘어갈 부분은 안보화 행위자가 비상조치의 도입을 정당화하는 과정에서 비상조치의 필요성을 강조하는 발언을 하는 것은 아니라는 점이다. 다시 말해 안보화 행위자는 구태여 '본 문제에 효과적으로 대응하기 위해서는 일반 정치 체계를 넘어서는 특별하고 긴급한 조치가 필요하다'고 직접적으로 말할 필요가 없다. 단지 문제의 실존적 위협을 알리고 그 심각성을 부각시키고 일반 정치 체계의 한계를 드러냄으로써 비상조치의 도입이 정당화될 수 있는 환경을 조성하는 것만으로도 충분하다.

이렇게 안보화 행위자가 수용자를 설득하는 과정이 안보화 전략의 핵심이라고 할 수 있는데, 이를 위해 안보화 행위자는 화행(speech act)을 사용한다. 화행이란 간단히 말해 특정 문제를 위협화하는 언어적 표현이다. 화행은 '생존' 이나 '실존적 위협' 그리고 문제의 '우선권(priority)' 등을 내포하는 수사적 구조의 발화(utterance)를 의미하며, '지금 당장 이 문제를 해결하지 못한다면 이를 바로잡을 기회를 놓치고 만다' 는 식의 담론을 형성하고 이를 수용자에게 효과적으로 전달하기 위한 수단으로 볼 수 있다. 안보적 담론의 핵심은 결국 특정 문제의 위협을 과장하여 최우선적 사안으로 비춰지게끔 만드는 것이라고 해도 과언이 아니다. 특히, 비군사적 분야에서 발생한 어떤 문제를 안보 문제로 격상시키기 위해서는 강력한 설득력을 지닌 화행을 통해 안보적 담론을 형성해야만 한다. 따라서 안보화 행위자는 특정 문제의 위협을 묘사함에 있어 '안보' 를 이야기함으로써 위협에 대한 공유된 이해와 인식 혹은 두려움을 자신과 수용자 간의 관계 속에 형성할 수 있게 된다. 이러한 맥락에서 코펜하겐 학파는 '안보'를 말하는 행위가 단순히 묘사의 기능을 넘어 실천적 기능을 가진다고 주장한다.

이렇듯 코펜하겐 학파가 이야기하는 화행은 언어적 표현에 국한된 개념이지만, 안보화가 단순히 언어의 사용에 의해서만 이루어질 수 있다고 보기는 어렵다. 즉, 안보적 언어를 사용하는 '발화 행위' 이외에도 위협에 대한 공유된 이해와 인식 혹은 두려움을 확산시킬 수 있는 다른 형태의 행위가 존재한다면 이 역시 안보화의 수단이 될 수 있다. 이러한 맥락에서 안보화 행위자의 일상적 실천(routinised practice)은 발화 행위만큼이나 강력한 안보화 수단이 될 수 있는데[62], 예를 들어 이슈화된 문제에 대한 정부의 입장 표명은 담화나 연설 등 직접적인 발화 행위를 통해서도 전달될 수 있지만 특정한 정책이나 전략의 수행에서도 들어날 수 있다.

2) 정치적 안보

코펜하겐 학파가 이야기하는 정치적 안보(Political Security)는 정치적 구성단위(political units)의 조직적 안정성(organisational stability)에 관한 것으로서 그 핵심에는 국가 주권에 대한 위협을 두고 있다.[63] 정치적 안보 분야는 국가 주권에 대한 비군사적 위협(non-military threats)에 주목하는데 이는 국가 주권에 대한 군사적 위협은 군사적 안보 분야에서 다루어질 수 있기 때문이다. 코펜하겐 학파를 대표하는 배리 부잔(Barry Buzan)은 정치적 위협은 국가의 조직적 안정성을 겨냥하는 위협이며 국가의 정체성(national identity)과 조직 이념(organising ideologies) 그리고 이를 표현하는 제도(institutions)에 대한 위협이라고 주장한다.[64] 더 나아가 부잔은 국가 역시 결국 정치적 구성단위이기

62) Matt McDonald, "Securitization and the Construction of Security", European Journal of International Relations, December 2008, pp.563-587.
63) Barry Buzan, Ole Wæber, Jaap de Wilde, "Security : A New Framework for Analysis", Lynne Rienner Publisher, 1998, p.141.

때문에 정치적 위협은 군사적 위협만큼이나 국가 주권에 심각한 위협이 될 수 있다는 점을 역설한다.

정치적 안보 개념을 이해하기 위해서는 우선 코펜하겐 학파가 의미하는 '정치'의 개념이 무엇인가를 분명히 할 필요가 있다. 먼저 코펜하겐 학파의 관점에서 본 정치의 개념은 '상대적으로 안정된 권위의 제도화(a relatively stable institutionalisation of authority)'를 의미하며, 이는 권위에 대한 승인(recognition)이나 지지(support) 혹은 정당성(legitimacy)을 부여하거나 거부하는 문제와 관련이 있다.[65] 이러한 맥락에서 정치적 구성단위란 실체적 영토 내에서 강압적 권력을 행사할 수 있는 권한을 가지고 다수로 이루어진 집단(들)을 통치하는데 필요한 정치논리에 따라 행동하는 조직체를 의미한다. 이러한 관점에서 볼 때, 정치적 구성단위는 근대 주권국가가 아닌 다른 형태로도 얼마든지 존재할 수 있다.[66]

정치적 안보란 따라서 정치적 구성단위의 생존이며, 더 정확히는 정치적 구성단위의 정체성과 이념 그리고 이를 나타내는 제도의 생존을 의미한다. 코펜하겐 학파는 정치적 구성단위를 주로 근대 주권국가로 보기 때문에 국가의 정체성과 그 근간을 이루는 이념, 그리고 이를 드러내는 국가 제도를 정치적 안보의 대상으로 규정한다. 따라서 국가가 그 지위 (statehood)를 유지하는 데에 필요한 구성적 요소를 위협하는 문제를 정치적 안보 위협으로 볼 수 있다. 이러한 맥락에서 부

64) Barry Buzan, "People, States and Fear : An Agenda for International Security Studies in the Post-Cold War Era", 2nd ed., Lynne Rienner Publisher, 1991, pp.118-119.
65) Barry Buzan, Ole Wæber, Jaap de Wilde, "Security : A New Framework for Analysis", Lynne Rienner Publisher, 1998, pp.141-143.
66) Ibid. p.143.

잔은 정부의 특정한 정책에 압력을 가하는 행위나 정부 타도, 분리주의(secessionism) 조성 등 국가의 정치적 권위를 약화시킬 수 있는 문제들은 모두 정치적 위협으로 구분될 수 있다고 주장한다.[67] 물론, 정부의 정책에 압력을 가하는 모든 행위를 실존적 위협으로 규정하기에는 무리가 있을 수 있다. 따라서 국가의 특정 정책에 압력을 가하는 행위가 국가주권, 국가정체성, 국가조직이념 등 국가 의 조직적 안정성에 필요한 핵심 요소들을 위협할 수 있다면 이는 정치적 안보 문제가 될 수 있다.

정치적 안보의 대상을 국가의 조직적 안정으로 본다면, 안보화 행위자는 당연히 정부가 될 수밖에 없다. 정부는 특정한 문제가 국가의 정치 체계를 위협하거나 국가와 정부에게 정당성을 부여하는 이념 등을 위협한다고 여길시 적절한 안보적 주장을 사용하여 해당 문제를 국가에 대한 정치적 안보 위협으로 격상시킬 수 있다. 더 나아가 정부는 특정한 비군사적 문제가 국민 다수의 생존을 위협할 수 있다고 판단할 경우 이를 안보적 사안으로 격상 시키고 그에 따라 대응할 수 있다.[68]

3) 사회적 안보

사회적 안보(Societal Security)는 특정 공동체의 정체성과 관련되었다. 한 사회의 본질적인 속성을 변화하는 환경과 잠재적 혹은 실존적 위협으로부터 보호하는 것을 의미한다.[69] 즉, 한 사회의 집단 정체

67) Barry Buzan, "People, States and Fear : An Agenda for International Security Studies in the Post-Cold War Era", 2nd ed., Lynne Rienner Publisher, 1991, pp.118-119.
68) Barry Buzan, "People, States and Fear : An Agenda for International Security Studies in the Post-Cold War Era", 2nd ed., Lynne Rienner Publisher, 1991, p.100.

성(collective identity)을 지키는 것이 사회적 안보라고 할 수 있다. 따라서 사회적 안보의 대상은 사회적 집단(collectives)과 그 집단의 정체성(collective identity)이다. 좀 더 추상적으로 '우리(we)' 라는 정체성이 위협받았다고 주장할 수 있는 다수로 이루어진 사회적 집단이라 할 수 있다. 이 점에서 사회적 안보는 정체성 안보(identity security)로도 이해될 수 있다. 한 가지 주의할 점은 한 국가의 인구(state population)를 사회적 안보의 대상으로 볼 수 없다는 것이다. 이는 한 국가의 인구가 항상 하나의 통일된 집단 정체성에 기초하는 것이 아니기 때문이다. 실제로 한 국가의 인구는 다양한 종교나 언어 혹은 인종에 의해 구성된 여러 다른 정체성을 가진 집단들로 이루어진 경우가 많다. 이 점에서 코펜하겐 학파는 사회의 개념을 국민(nation)의 개념과 항상 동일시하지 않는데 이는 코펜하겐 학파가 주목하는 '사회'의 개념이 영토나 제도에 구속된 집단을 의미하는 것이 아니라 동일한 정체성을 공유하는 공동체를 의미하기 때문이다. 따라서 사회적 위협(Societal threat)은 이미 구성된 '우리(we)'라는 집단 정체성을 와해시키거나 그러한 집단 정체성이 형성되는 것을 방해하는 사물, 현상 또는 행위로 간주할 수 있다.[70]

사회적으로 위협에 노출된 집단 공동체 또는 사회는 자체적으로 대응하거나 해당문제를 국가차원의 문제로 격상하여 정치적 안보 또는 군사적 안보분야로 확장시켜 대응한다.[71] 이러한 과정에서 안보화 행위자는 위협에 노출된 사회 또는 국가(정부)가 될 수 있다. 특히 '우리'

69) Ole Wæver, Barry Buzan, Morten Kelstrup, Pierre Lemaitre "Identity, Migration and the New Security Agenda in Europe", Pinter Publisher, 1993. p.23.
70) Barry Buzan, Ole Wæber, Jaap de Wilde, "Security : A New Framework for Analysis", Lynne Rienner Publisher, 1998, p.121.
71) Ibid, p.122.

와 ‘그들’이라는 용어를 주로 쓰는 정치인, 언론 또한 강력한 안보화 행위자가 될 수 있다.[72]

4) 소결

1980~1990년대에 부상한 이른바 코펜하겐 학파의 안보이론은 탈냉전기의 안보문제를 새로운 시각으로 다루었던 대표적인 시도였다. 이들은 구성주의 시각에서 기존에 지엽적으로 다루어졌던 비전통안보 문제들에 좀 더 적극적으로 접근하였고 탈냉전 이후의 안보연구가 국가 중심의 군사안보 연구를 넘어서 새로운 지평을 여는데 기여하였다.[73]

안보화 이론에 따르면 안보란 현존하는 위협이 무엇인가에 대한 사회적 합의를 상호작용을 통해 주관적으로 구성되는 정치적 담론이라고 할 수 있다. 이러한 과정에서 안보화는 비안보문제도 안보문제의 지위와 우선성을 부여해서 안보문제로 구성하는 과정이다. 즉, 일반적인 상황에서는 직접적인 위협으로 간주되지 않는 문제도 안보 행위자가 중대한 위협으로 부각시키고 비상상황으로 상정하여 조치하는 정치적 행위로 볼 수도 있다.

특히 사이버테러는 그 위협의 실체와 효과가 아직 명시적으로 입증되지 않았고 아직까지는 전문가들이나 정치가들이 구성한 현실 속에서 존재하는 위협의 성격이 강하다. 일각에서는 사이버테러에 대한 대응 논의가 다소 과장된 것이 아니냐는 회의론이 제기되고 있는 것도 이러한 이유가 있기 때문이다. 결국 사이버테러 대응에 대한 담론은

72) Ibid, p.124.
73) 김흥석, “사이버테러와 국가안보”, 한국법학원, 2010, p.322.

형성과정에 있어서 단순히 중립적인 의도 보다는 각기 입장에 따라서 다르게 구성될 수 밖에 없는 정치적인 과정이며, 그렇기 때문에 힘 있는 자가 주도하는 권력정치의 일면을 보인다.[74]

코펜하겐 학파의 대표적인 학자 한센(Lene Hansen)과 니센바움(Helen Nissenbaum)은 이러한 안보담론에 대하여 세가지 특징을 지적하였다. 첫째, 과잉안보화(Hypersecuritization)이다. 사이버테러 대응에 대한 안보담론은 과장스럽게 느껴질 정도로 아직 발생하지 않은 사항들에 대하여 그 규모 및 파장을 부각시키고 있다. 둘째, 안보의 일상화(Everyday Security Practice) 경향이다. 이러한 안보담론은 과잉안보화의 시나리오를 더욱 실감나고 그럴듯하게 보이기 위해 대중들의 경험, 느낌, 요구, 이익에 호소하는 경향이 강하다. 셋째, 기술적이고 전문적인 담론(Technification)이다. 주로 일반대중에게 잘 알려지지 않은 비밀정보와 고도의 전문지식을 독점한 전문가들에 의해서 독자적 공간을 형성하는 방식으로 생산되는 담론이라는 것이다.[75]

74) 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2, pp.76-77.
75) Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, International Studies Quarterly 53, 2009, pp.1163-1168.

제3장 중국의 사이버테러 대응 전략

3.1 사이버테러 대응의 역사

중국은 사이버(cyber)라는 표현대신 네크워크(网络)나 정보(信息)라는 용어를 사용한다. 이는 정보통신기술 산업발전과 정보자원, 기반시설, 법적요소 등을 바탕으로 현대화와 정보사회로의 전환을 목적으로 한다. 또한 중국 인민군은 네트워크 전쟁과 네트워크 보호, 정보보호 등으로 개념을 분류해 전략을 수립하고 있다. 이 개념은 나토가 사용하는 컴퓨터 네트워크 작전 개념과 유사하지만 컴퓨터 네트워크 공격의 역량을 강조하는 것이 다르다. 이러한 개념을 바탕으로 중국은 사회, 경제, 군사 영역의 정보화를 추진하고 있다.[76)]

중국은 1992년 전자산업부를 신설하여 사회·경제 영역에서 현대화 전략을 추진하기 시작하였다. 개혁 개방의 확대 속에 경제구조의 체질개선을 위해 과학기술 발전과 경제를 결합하는 것이 중요하다고 인식한 것이다. 전자부와 산업부를 통합한 전자산업부는 해외기업의 국내진출을 통해 국영전자기업의 안정적인 기술발전을 도모하고 이를 통해 경쟁력을 강화할 수 있도록 지원하였다.

이후 1998년 정보산업부를 신설해 전자산업, 우전부, 텔레비전부를 통합하여 정책결정, 규제, 인허가 조직을 일원화 하였다. 이를 통해 정보통신산업발전을 위한 정책집행의 효율성을 제고할 수 있었다.

76) 박용숙, “중국의 네트워크 안전법에 대한 일고찰”, 강원법학 53, 2018, pp.39-73.

2002년 중국은 ‘국민경제 및 사회 발전에 관한 제10차 5개년 정보화 핵심사업계획’ 하에 정보화 발전을 통한 공업화를 도모하였다. 전자상거래 산업을 확대하고 소프트웨어 산업발전 지원 및 첨단기술제품에 대한 외국인 투자를 장려함으로써 경제 구조개혁을 진행하였다.[77]

2008년에는 공업정보화부를 신설하여 지식·기술 집약형 첨단산업 및 정보통신·인터넷 산업 등의 발전을 주도하기 시작했다.[78]

사회·경제 영역 뿐만아니라 안보영역에서도 정보화 발전전략이 진행되었다. 2013년 이전까지 중국은 국방·군사분야의 현대화에 초점을 맞추고 있었으나, 2013년부터 중국 인민군은 사이버 공간을 경쟁공간으로 인식하기 시작하며, 군사력의 다양화를 목표로 전략을 새롭게 수립하였다.

또한 사이버 공간에서 상대국의 공격이 있을 경우에는 보복공격을 하여 주권을 지키는 적극적 방어전략을 강조하였다다. 이후 2015년 국방백서에서는 “중국은 사이버공격의 가장 큰 피해국으로, 사이버공간에서 심각한 위협에 직면해 있기 때문에, 사이버안보를 위한 군사력을 증대하고 전쟁능력을 강화해야한다.”고 명시하였다.[79]

이같은 기조를 바탕으로, 사이버전쟁 발생시 효율적 대응을 위해 중앙군사위원회 총참모부내 사이버작전 전담부서를 신설하였다. 시

77) 중국 국민경제 및 사회발전에 관한 제10차 5개년 계획 요강, 《中华人民共和国国民经济和社会发展第十个五年规划纲要”》, 2001.
78) 중국 국민경제 및 사회발전에 관한 제11차 5개년 계획 요강,《中华人民共和国国民经济和社会发展第十一个五年规划纲要”》, 2006.
79) 중국 2006-2020년 국가 정보화 발전전략,《2006-2020年国家信息化发展战略》, 中共中央办公厅, 2006.5.8。

진핑 군사중앙위원회 위원장과 팡펑후이 중앙군사위원회 총참모장이 직접 지시하는 사이버작전 전담부서 중 제3부서는 해외조직, 군수지원부, 과학기술정보부 등을 관리한다. 또한 제4부서는 공식적으로는 전파방해와 레이더 전략을 담당하지만, 실질적으로는 군의 사이버전략 추진과 기술발전을 담당하는 것으로 알려져 있다.[80]

사이버 영역의 발전으로 광범위한 영역에서 국내외 디지털 정보교류가 활발해졌으며 중국 지도부는 이러한 발전이 사회적 불안정성을 야기할 수도 있기 때문에 사이버공간의 취약성에 대한 우려를 나타내었다. 따라서 2000년대 초반부터 중국공산당 상무위원회, 중앙군사위원회 및 국무원은 정보화 전략수립과 정책집행을 적극적으로 이행하기 시작하였다. 특히 2014년에는 '중앙 네트워크 안전 및 정보화 영도소조(中央网络安全和信息化领导小组)'를 신설하여 정보화 관련 정부부서를 일원화 하였고, 안전한 인터넷 구축을 통한 사이버공간내 사회주의 가치를 공고화하기 위해 노력하고 있다.

2014년 이전까지 운영된 '국가정보화영도소조(国家信息化领导小组)'는 경제구조의 현대화를 위한 정보통신 산업발전에 중점을 두고 정책의 방향을 제시하였다. 그러나 중국을 대상으로 한 국외 사이버공격이 증가하자 중국지도부는 기존의 영도소조를 확대해 새로운 네트워크 및 정보화 영도소조를 신설하였다. 사이버 위협이 사회적·경제적 위협은 물론 국방전략 위협으로 확대될 가능성이 높아지자 정보화 관련 부서를 네트워크 영도소조 산하로 재편하고 일원화된 통합 지도 체제를 완성한 것이다.[81] 2018년 3월 국가기구 개편안에 따라 중앙 네트

80) 조윤영, 정종필, "사이버안보를 위한 중국의 전략- 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로", 21세기정치학회보, 2016, pp.151-177.

워크 및 정보화 영도소조는 중앙 네트워크 및 정보화 위원회로 개편되었다.

또한 중국은 사이버안보 관련 조직 개편은 물론 사이버안보법 제정을 통하여 사이버공간을 통제하는 제도적 기반을 마련하였다. 2015년 제정한 사이버안보법은 제1장 제1조에서 “사이버주권과 국가안전 수호”를 가장 먼저 명시하고 제2조에서는 “중국 영토내 네트워크 구축, 운영, 보호, 사용, 관리·감독 등에 적용한다”고 명시함으로써 국내 사회 안정과 경제이익을 보호하기 위해 국가가 사이버공간을 포괄적으로 통제할 수 있는 법적근거를 마련하였다.[82]

81) 주문호, 권헌영, 임종인, “주요국 사이버보안 거버넌스 분석과 정책적 시사점”, 정보보호학회논문지, 2018, pp.1259-1277.
82) 박용숙, “중국의 네트워크 안전법에 대한 일고찰”, 강원법학 53, 2018, pp.39-73.

3.2 사이버테러 대응 법

2015년 6월 2일, 중국은 제12기 전국인민대표대회(全国人民代表大会, 이하 전인대)에서 사이버안보법 초안을 발표하였다. 같은해 6월 24일 제12기 전인대 제15차 상무위원회에서 제1차 심의가 이루어졌다. 1년 뒤인 2016년 6월에는 제2차 수정안이 발표되었으며 제21차 상무위원회에서 제2차 심의를 진행하였다. 2016년 10월 31일 제24차 상무위원회에서 제3차 수정안을 최종적으로 심의하여 11월 7일 제12기 전인대 제24차 상무위원회에서 최종 통과되었다. 2017년 6월부터 시행되고 있다.

사이버안보법은 전체 7장, 79개 조문으로 구성되어 있다. 제1장은 총칙, 제2장은 정보통신망 안전 지원 및 촉진, 제3장 정보통신망 운행 안전, 제4장 정보통신망 정보 안전, 제5장 모니터링 경보와 응급조치, 제6장 법률책임, 제7장 부칙으로 구성되었다.

본 법은 중국에서 처음으로 법률의 형식으로 국가의 정보통신망 보안등급 보호제도를 규정하였다는 것에 의미가 있다.[83] 그러나 아직 보안등급 보호제도에 대한 구체적인 방법과 표준에 관한 규정이 정해지지 않은 상태이다. 따라서 앞으로 상당 기간은 기존의 보안등급 보호제도에 의해 운영될 수밖에 없을 것이다.

제21조[84]

83) 박용숙, “중국의 네트워크 안전법에 대한 일고찰”, 강원법학 53, 2018, pp.39-73.
84) 第二十一条
国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、

국가는 정보통신망 보안등급 보호제도를 시행한다. 정보통신망 사업자는 정보통신망 보안등급 보호제도에 의거, 다음의 안전 보호 의무를 이행해야 한다. 교란·파괴 및 불법침입으로부터 정보통신망의 안전을 보호하고, 정보통신망 데이터의 유출, 도난, 왜곡을 방지한다.

1. 내부 안전관리 제도 및 조작 관련규정을 제정하고 정보통신망 안전 책임자를 지정하여, 정보통신망 안전 보호에 대한 책임을 구체화한다.

2. 컴퓨터 바이러스 및 정보통신망 공격, 침입 등 정보통신망 안전을 위협하는 행위에 대한 기술적 조치를 취한다.

3. 정보통신망 운영 상태에 대한 기록 및 감시, 보안사고 발생 시 기술적 조치를 취하고, 규정에 의건 관련 정보통신망 일지를 최소 6개월 보존한다.

4. 데이터분류, 중요 데이터백업 및 보안설정 등에 관한 조치를 취한다.

5. 법률·행정 법규에 규정된 기타 의무를 이행한다.

본 법 제21조에 근거하여, 국가는 정보통신망 보안등급 보호제도를 실시하여 정보통신망 사업자의 책임 하에 보안등급을 받아야 한다. 이는 공안부로부터 등급확정 신고증명을 받아야 하는 것을 의미한다. 실제 검사 평가는 공안부가 지정한 기업에서만 진행이 가능하다. 그리고 운영자는 검사를 자체 진행하거나 보안서비스 기구에 위탁해서 할 수 있으며 매년 최소 1회 실시하여야 한다.

사실, 정보통신망 보호제도는 본 법에 의해 처음 규정된 것은

篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。

아니다. 이미 공안부, 국가비밀유지국, 국가비밀번호 관리국 국무원 정보화 업무 사무처 등의 기관이 2007년에 제정한 정보보안등급보호관리방법(信息安全等级保护管理办法)은 정보 시스템의 보안보호 등급을 5등급으로 나누어, 정보시스템을 운영·사용하는 조직은 정보시스템보안등급보호실시 가이드라인 (信息系统安全等级保护定级指南)에 따라 구체적으로 등급보호 업무를 실시 할 것을 규정하고 있다.[85]

본 법을 정보통신망 사업자가 이행하지 않을 경우에는 관련 주관부서가 시정명령을 하고 경고를 준다. 만약 불이행 또는 시정을 거부여 정보통신망 보안이 위협되는 결과가 초래될 경우 벌금에 처한다. (1만 위안 이상 10만 위안 이하)

사이버테러 대응 관련한 법률에서 핵심 정보인프라시설은 무엇이고 어떻게 보호하는지에 대한 규정을 고찰할 필요가 있다. 본 법 제34조와 제39조를 통해 핵심 정보인프라시설 보호에 관련 내용을 살펴본다.

제34조[86]
본 법 제21조의 규정 외에 핵심 정보인프라 시설의 운영자는 다음과 같은 안전보호 의무도 이행하여야 한다.
1. 전문안전관리 기구를 설치 및 안전관리 책임자 지정. 해당 책임자와 주요 직위에 있는 인원에 대한 신원조사 실시.

85) 박용숙, "중국의 네트워크 안전법에 대한 일고찰", 강원법학 53, 2018, pp.39-73.
86) 第三十四条
除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。

2. 정기적으로 종사자에게 사이버보안 교육, 기술훈련 및 평가 실시.
3. 중요 시스템과 데이터베이스에 대한 재난 대비 백업자료 준비.
4. 사이버 안보 사건 발생 대비 비상대책안 수립 및 정기 훈련 실시.
5. 법률 및 행정법규에서 부여하는 기타 의무의 이행.

본 법에서 핵심 정보인프라 시설이라 함은 공공 통신과 정보서비스, 에너지, 교통, 수리(水利), 금융, 공공 서비스, 전자정부 등 중요 산업과 영역 등에서 일단 기능이 파괴되거나 데이터가 유출되어 국가 안보, 경제, 국민 생활 및 공공이익에 심각한 위협을 초래할 가능성이 있는 시설이다.

이러한 핵심 정보인프라 시설을 건설할 때 업무의 안정성과 지속적인 운행이 가능한 성능을 확실하게 보장하여야 한다. 또한 안전관련 기술적인 조치가 이루어질 수 있도록 계획되고 건설되어야 한다. 또한 핵심 정보인프라 시설 안전보호 업무를 책임지는 부서는 해당 업계와 영역에서 안전 모니터링 경보와 통보 시스템을 확실하게 확립해야 한다. 규정에 의거 정보통신망 안전 모니터링 경보 정보를 발송해야 한다.

제39조[87]
국가 사이버 안보 및 정보화 담당 부처는 핵심정보인프라시설의 보

87) 第三十九条
国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

호를 위해 다음 조치를 취하는 것에 대해 유관부서를 총괄 조정해야 한다.

1. 핵심 정보인프라 시설의 안전도에 대한 표본 검사를 진행하고, 개선 조치를 시행한다. 필요시 네트워크 안전 서비스 기관에 위탁하여 안전도 평가를 실시할 수 있다.
2. 핵심 정보인프라 시설의 운영자가 정기적으로 사이버 안전 대응 훈련을 진행하도록 하고 사이버침해 사건에 대한 대응 및 협조 능력을 제고한다.
3. 유관 부처, 핵심 정보인프라 시설 담당자와 관련 연구기관 및 네트워크 안전 서비스 기관 간에 사이버안전 관련 정보공유를 촉진시킨다.
4. 사이버 침해 사고 관련 긴급조치 및 기능복구 등에 대한 기술 지원과 협조를 제공한다.

또한 국가 정보화 담당 부처는 관련부문과 협조해서 정보통신망 안전 위험평가를 실시하고 긴급대응체계를 확립해야 한다. 또한 보안사고 긴급대응 대책을 마련하고 정기적인 예방연습을 실시하여야 한다. 핵심 정보인프라 시설 안전보호에 관한 업무책임 부서 또한 관련 업계 및 영역과 보안사고 긴급대책을 제정하고 정기적인 훈련을 실시한다. 정보통신망 보안사고 긴급대책은 사건 발생시 위협정도 및 영향범위 등을 고려하여 보안사고 등급을 분류하고 이에 상응하는 조치를 규정하도록 되어있다.

3.3 사이버테러 대응 제도

3.3.1 사이버안보 전략

2016년 12월 27일 중국은 ‘국가 사이버안보 전략(国家网络空间安全战略）’을 발표하였다. 시진핑 국가주석이 조장을 맡고 있는 중앙네트워크안전 정보화 영도소조가 승인하고 국가인터넷정보 판공실에서 발표하였다.[88)]

이 전략은 중국이 수립한 최초의 사이버안보 전략으로 사이버안보에 대한 중국의 시각을 알 수 있다. 전략의 전문을 보면 기회와 도전, 목표, 원칙, 전략임무 네 부분으로 구성되어 있다.

국가의 사이버안보를 지키는 것은 소강사회(小康社会)로 발전하고, 개혁을 촉진시키며, 법치사회를 구현하고, 공산당의 주요 통치 전략을 엄중히 실현하고, 중국의 ‘이백년’목표를 달성하며, 위대한 중화민족을 부흥시켜 중국의 꿈을 실현시키는 일이다. 또한 시진핑 주석의 국제 인터넷 통치체계 변혁을 위한 네 가지 원칙[89)] 및 사이버공간 운명공동체 설립을 위한 다섯가지 제안사항[90)]을 관철시키기 위함이다. 이를 실현하기 위하여 사이버공간의 발전과 사이버안보에 관한 중국의 주된 입장 천명, 사이버안보 구현의 가이드라인을 설정, 사이버공간에

88) 중국 사이버안보 및 정보화 판공실 홈페이지, “중국 국가사이버안보전략 전문”, “国家网络空间安全战略全文”, 2016. 12. 27
http://www.cac.gov.cn/2016-12/27/c_1120195926.htm
89) ① 인터넷 주권 존중, ② 평화안전 수호, ③ 개방협력 촉진, ④ 질서 구축
90) ① 글로벌 네트워크 인프라의 가속화, ② 인터넷 문화교류 및 공유 플랫폼 건설, ③ 인터넷 경제 혁신 발전 추진, ④ 인터넷 안전보장, ⑤ 공평하고 정의로운 인터넷 거버넌스 체계 구축

서 국가주권과 이익의 수호, 사이버공간의 안전과 발전을 추구하기 위하여 본 전략을 제정한다.[91]

첫 번째 '기회와 도전'에서는 사이버안보 환경에 대한 중국의 인식이 반영되어 있다. '기회' 관련해서 '중대한 기회'로 명명하고 있으며 사이버공간은 정보전달의 새로운 수단, 새로운 생산공간, 경제발전의 새로운 원동력, 문화번영의 새로운 촉매, 국가통치의 새로운 플랫폼, 교류협력의 새로운 접점, 국가의 주권이 적용되는 새로운 영토라고 규정하고 있다.[92]

---

91) 信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。网络空间安全（以下称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全。维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现"两个一百年"奋斗目标、实现中华民族伟大复兴中国梦的重要保障。为贯彻落实习近平主席关于推进全球互联网治理体系变革的"四项原则"和构建网络空间命运共同体的"五点主张"，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益，制定本战略。

92) 一、机遇和挑战

（一）重大机遇

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。

信息传播的新渠道。网络技术的发展，突破了时空限制，拓展了传播范围，创新了传播手段，引发了传播格局的根本性变革。网络已成为人们获取信息、学习交流的新渠道，成为人类知识传播的新载体。

生产生活的新空间。当今世界，网络深度融入人们的学习、生活、工作等方方面面，网络教育、创业、医疗、购物、金融等日益普及，越来越多的人通过网络交流思想、成就事业、实现梦想。

经济发展的新引擎。互联网日益成为创新驱动发展的先导力量，信息技术在国民经济各行业广泛应用，推动传统产业改造升级，催生了新技术、新业态、新产业、新模式，促进了经济结构调整和经济发展方式转变，为经济社会发展注入了新的动力。

文化繁荣的新载体。网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化创新创造，丰富了人们精神文化生活，已经成为传播文化的新途径、提供公共文化服务的新手段。网络文化已成为文化建设的重要组成部分。

社会治理的新平台。网络在推进国家治理体系和治理能力现代化方面的作用日益凸显，电子政务应用走向深入，政府信息公开共享，推动了政府决策科学化、民主化、法治化，畅通了公民参与社会治理的渠道，成为保障公民知情权、参与权、表达权、监督权的重要途径。

交流合作的新纽带。信息化与全球化交织发展，促进了信息、资金、技术、人才等要素的全球流动，增进了不同文明交流融合。网络让世界变成了地球村，国际社会越来越成为你中有我、我中有你的命运共同体。

国家主权的新疆域。网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。尊重网络空间

또한 이와 동시에 심각한 도전 관련하여 정치적 안정, 경제안보, 문화안보, 사회안전, 사이버 공간에서의 국제경쟁의 내용이 담겨 있다.[93]

① 정치적 안정

인터넷의 보급은 정치적 안정에 부정적 영향을 끼친다. 정치적 안정은 국가발전과 국민행복을 위한 기본적인 전제조건이지만 인터넷을 이용한 타국에 대한 내정 간섭과 정치제도 공격, 사회 불안을 선동하고 타국의 정권에 대한 전복, 인터넷에 대한 대규모 감시통제, 사이버스파이 행위 등은 국가 정치적 안정과 인터넷 사용자 정보보안을 해친다고 주장한다.[94]

② 경제안보

사이버공격은 경제안보를 위협한다. 인터넷과 정보시스템은 주요기반시설과 경제 전반 및 사회의 중추 신경과 같은 역할을 하게 된다. 사이버공격으로 시스템에 심각한 보안사건이 발생할 시, 에너지・교통・통신・금융 인프라와 같은 주요기반시설이 마비되고 재난상황이 발생함으로써 국가경제안보와 공공의 이익에 심각한 손상이 발생한다.[95]

主权，维护网络安全，谋求共治，实现共赢，正在成为国际社会共识。

93) 网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

94) 网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。

95) 网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

③ 문화안보

인터넷상 유해정보는 문화안보를 저해한다.[96]

④ 사회안전

사이버테러와 불법범죄가 사회안전을 해친다.[97]

⑤ 국제경쟁

사이버공간에서 국제경쟁이 급속히 확대되고 있다. 국제사회에서는 사이버공간의 전략자원에 대한 쟁탈, 규범 설정력 강화, 전략제정권과 전략적 고지 선점, 전략주도권 추구 등 경쟁이 나날이 격해지고 있다. 일부 국가는 사이버안보 전략을 강화하고, 국가간 사이버 군비경쟁은 치열해지고 있다. 이로인해 세계 평화는 새로운 도전에 직면하고 있다.[98]

사이버공간에서 기회와 도전이 병존하고 있는 상황이지만 기회는 도전보다 크다.[99]

두 번째 목표에서는 다음과 같이 주장한다. 국가안보적 시각에

---

96) 网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

97) 网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

98) 网络空间的国际竞争方兴未艾。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。

99) 网络空间机遇和挑战并存，机遇大于挑战。必须坚持积极利用、科学发展、依法管理、确保安全，坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及13亿多中国人民，造福全人类，坚定维护世界和平。

서 전략은 창의, 협력, 상생, 개방, 공유의 발전이념을 철저히 시행한다. 위협 및 위기에 대한 의식을 강화하고 국내외 정세도 함께 살펴야 한다. 사이버공격에 적극적으로 예방, 방어, 대응하고 사이버공간에서 평화, 안보, 개방, 협력, 질서를 촉진한다. 또한 국가의 주권, 안보, 발전이익을 수호하여 사이버강국 건설이라는 전략 목표를 실현해야 한다.[100]

세 번째 원칙에서는 네 가지 원칙을 제시한다.

① 사이버공간의 주권존중 및 수호

사이버공간에서 주권 침해는 용납되지 않는다. 각국이 자주적으로 발전경로와 정보통신망 관리 방식, 인터넷 공공정책을 선택하고, 각국 주권 범위내의 사이버 문제는 각국의 국민이 스스로 결정하는 것으로, 각국은 자국의 사정에 근거하고 국제적 경험을 참고하여 사이버공간과 관계된 법률과 법규를 제정하고 법에 의해 조치를 취하며, 자국

---

100) 二、目标

以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

和平：信息技术滥用得到有效遏制，网络空间军备竞赛等威胁国际和平的活动得到有效控制，网络空间冲突得到有效防范。

安全：网络安全风险得到有效控制，国家网络安全保障体系健全完善，核心技术装备安全可控，网络和信息系统运行稳定可靠。网络安全人才满足需求，全社会的网络安全意识、基本防护技能和利用网络的信心大幅提升。

开放：信息技术标准、政策和市场开放、透明，产品流通和信息传播更加顺畅，数字鸿沟日益弥合。不分大小、强弱、贫富，世界各国特别是发展中国家都能分享发展机遇、共享发展成果、公平参与网络空间治理。

合作：世界各国在技术交流、打击网络恐怖和网络犯罪等领域的合作更加密切，多边、民主、透明的国际互联网治理体系健全完善，以合作共赢为核心的网络空间命运共同体逐步形成。

有序：公众在网络空间的知情权、参与权、表达权、监督权等合法权益得到充分保障，网络空间个人隐私获得有效保护，人权受到充分尊重。网络空间的国内和国际法律体系、标准规范逐步建立，网络空间实现依法有效治理，网络环境诚信、文明、健康，信息自由流动与维护国家安全、公共利益实现有机统一。

의 정보체계와 자국 영토상의 사이버 활동을 관리할 수 있다. 각국은 자국의 정보체계와 정보자원을 침입, 간섭, 공격, 파괴로부터 보호한다. 각국은 국가안보와 이익에 유해한 정보가 자국의 망에 전파되는 것을 예방, 저지, 처벌하며, 사이버공간의 질서를 지킨다. 어떤 국가도 인터넷의 패권을 주도 하거나 이중 기준을 가져서는 안 되며, 타국의 내정에 간섭하는데 인터넷을 이용하지 말아야 하고, 타국의 국가안보에 위해가 되는 사이버 활동에 종사하거나, 종용, 지원해서는 안 된다.[101]

② 사이버공간의 평화적 이용

사이버공간의 평화적 이용은 인류공공의 이익과 부합한다. 각국은 <유엔헌장>을 존중하여야 하고, 정보기술이 국제사회의 안보, 안정과 충돌되지 않도록 해야 한다. 사이버공간에서 군비 경쟁은 공동으로 저지하여 충돌을 막아야 한다. 국가간 사이버 안보에 대한 이익을 존중하고, 조화로운 사이버공간을 구축해야 한다. 국가 안보의 명목으로 기술적 우위를 이용한 타국의 인터넷과 정보시스템을 통제하거나 데이터를 수집 및 절취하는 것에 반대한다. 타국의 안보를 희생하여 자국의 절대적 안전을 도모해서는 안 된다.[102]

---

101) (一) 尊重维护网络空间主权

网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

102) (二) 和平利用网络空间

和平利用网络空间符合人类的共同利益。各国应遵守《联合国宪章》关于不得使用或威胁使用武力的原则，防止信息技术被用于与维护国际安全与稳定相悖的目的，共同抵制网络空间军备竞赛、防范网络空间冲突。坚持相互尊重、平等相待，求同存异、包容互信，尊重彼此在网络空间的安全利益和重大关切，推动构建和谐网络世界。反对以国家安全为借口，利用技术优势控制他国网络和信息系统、收集和窃取他国数据，更不能以牺牲

③ 사이버공간에서의 법치주의 실현

사이버공간에서 법치주의를 전면적으로 추진하고 법률에 따라 인터넷을 관리한다.[103]

④ 사이버안전과 발전

정보화 발전이 없으면, 사이버안전도 보장되지 않으며 현재의 안전까지도 잃게 될 것이다.[104]

마지막으로 전략적 임무에서는 아홉가지 사항을 강조한다.

① 사이버공간에서의 주권수호

중국의 주권 범위 내에서 헌법과 법률·법규에 따라 인터넷 상 활동을 관리하고 국가의 정보기반시설과 정보자원을 안전하게 보호한다. 경제·행정·과학기술·법률·외교·군사적 조치를 포함한 모든 수단을 동원하여 사이버공간상 국가의 주권을 강력히 수호한다. 인터넷을 통한 정권 전복이나 국가 주권을 파괴하는 일체의 행위에 대하여 강력히 반대한다.[105]

② 국가안전보장강화

---

103) (三) 依法治理网络空间

全面推进网络空间法治化，坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。依法构建良好网络秩序，保护网络空间信息依法有序自由流动，保护个人隐私，保护知识产权。任何组织和个人在网络空间享有自由、行使权利的同时，须遵守法律，尊重他人权利，对自己在网络上的言行负责。

104) (四) 统筹网络安全与发展

没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是一体之两翼、驱动之双轮。正确处理发展和安全的关系，坚持以安全保发展，以发展促安全。安全是发展的前提，任何以牺牲安全为代价的发展都难以持续。发展是安全的基础，不发展是最大的不安全。没有信息化发展，网络安全也没有保障，已有的安全甚至会丧失。

105) (一) 坚定捍卫网络空间主权

根据宪法和法律法规管理我国主权范围内的网络活动，保护我国信息设施和信息资源安全，采取包括经济、行政、科技、法律、外交、军事等一切措施，坚定不移地维护我国网络空间主权。坚决反对通过网络颠覆我国国家政权、破坏我国国家主权的一切行为。

인터넷을 이용해 국가에 반대하여 분열, 반란, 정권 전복을 선동하는 모든 행위를 예방하고 저지하며 법에 의거 처벌한다. 인터넷을 통한 국가 기밀 절취 또는 유출은 국가 안보를 저해하는 행위로서 경계하고 저지하며 법에 따라 처벌한다. 국가 외부 세력이 인터넷을 통해 국가에 침투, 파괴, 전복, 분열시키는 활동에 대해서도 방어 및 저지하고 법에 의거 처벌한다.[106]

③ 주요정보기반시설 보호

국가의 주요정보기반시설은 국가 안보, 경제, 국민 생활에 영향을 끼친다. 여기에는 공공통신, 라디오, TV 전송 서비스 등의 정보네트워크 뿐만 아니라, 에너지, 금융, 교통, 교육, 과학연구, 수리, 공업제조, 의료위생, 사회보장, 공공사업, 국가 기관 핵심정보 시스템, 주요 인터넷 애플리케이션 시스템 등이 포함된다. 가용한 모든 필요 조치를 하여 주요정보기반시설과 주요정보가 공격 및 파괴당하지 않도록 식별・방어・감시・조기경보・대응・복구 등의 과정을 고려한 주요정보기반시설 보호제도를 마련하여 실시한다. 또한 관리, 기술, 인력, 예산의 투자 확대를 통해 법률에 근거한 종합 대책을 마련하고 주요정보기반시설의 방어를 강화한다.[107]

---

106) (二) 坚决维护国家安全

防范、制止和依法惩治任何利用网络进行叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治利用网络进行窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力利用网络进行渗透、破坏、颠覆、分裂活动。

107) (三) 保护关键信息基础设施

国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。

关键信息基础设施保护是政府、企业和全社会的共同责任，主管、运营单位和组织要按照法律法规、制度标准的要求，采取必要措施保障关键信息基础设施安全，逐步实现先评估后使用。

④ 사이버문화 건설 강화

인터넷상 이데올로기와 문화 건설을 강화하고 사회주의 핵심 가치관을 강력히 증진하고 실천해야 하며, 각국 국민들이 중국의 우수한 문화를 이해할 수 있도록 하고 중국 국민들이 각국의 우수한 문화를 이해할 수 있도록 하며, 사이버 문화의 번영과 발전을 함께 추진하고 인문적 정신세계를 풍요롭게 하며 인류문명 진보를 촉진한다.[108]

⑤ 사이버테러 및 사이버범죄 단속

사이버공간에서 테러 및 스파이 행위에 대한 차단 능력을 강화하고 이를 엄격하게 단속한다. 종합적인 관리, 근원지 차단 및 법률적 통제를 지속한다. 온라인 금융 사기, 절취, 총기·마약 판매, 개인정보 침해, 음란 정보 전파, 정보 탈취, 지식재산권 침범 등 불법 범죄 행위를 엄격히 단속한다.[109]

加强关键信息基础设施风险评估。加强党政机关以及重点领域网站的安全防护，基层党政机关网站要按集约化模式建设运行和管理。建立政府、行业与企业的网络安全信息有序共享机制，充分发挥企业在保护关键信息基础设施中的重要作用。

坚持对外开放，立足开放环境下维护网络安全。建立实施网络安全审查制度，加强供应链安全管理，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性，防止产品服务提供者和其他组织利用信息技术优势实施不正当竞争或损害用户利益。

108)（四）加强网络文化建设

加强网上思想文化阵地建设，大力培育和践行社会主义核心价值观，实施网络内容建设工程，发展积极向上的网络文化，传播正能量，凝聚强大精神力量，营造良好网络氛围。鼓励拓展新业务、创作新产品，打造体现时代精神的网络文化品牌，不断提高网络文化产业规模水平。实施中华优秀文化网上传播工程，积极推动优秀传统文化和当代文化精品的数字化、网络化制作和传播。发挥互联网传播平台优势，推动中外优秀文化交流互鉴，让各国人民了解中华优秀文化，让中国人民了解各国优秀文化，共同推动网络文化繁荣发展，丰富人们精神世界，促进人类文明进步。

加强网络伦理、网络文明建设，发挥道德教化引导作用，用人类文明优秀成果滋养网络空间、修复网络生态。建设文明诚信的网络环境，倡导文明办网、文明上网，形成安全、文明、有序的信息传播秩序。坚决打击谣言、淫秽、暴力、迷信、邪教等违法有害信息在网络空间传播蔓延。提高青少年网络文明素养，加强对未成年人上网保护，通过政府、社会组织、社区、学校、家庭等方面的共同努力，为青少年健康成长创造良好的网络环境。

109)（五）打击网络恐怖和违法犯罪

加强网络反恐、反间谍、反窃密能力建设，严厉打击网络恐怖和网络间谍活动。

坚持综合治理、源头控制、依法防范，严厉打击网络诈骗、网络盗窃、贩枪贩毒、侵害公民个人信息、传播淫秽色情、黑客攻击、侵犯知识产权等违法犯罪行为。

⑥ 네트워크 관리 시스템 개선

사이버안전 관련 법규 체계를 완비하고 행정 감독관리, 산업계 자율성 강화, 기술보장, 일반인에 대한 감독, 사회교육과 결합된 사이버 통치 체계 구축을 가속화한다.[110]

⑦ 네트워크 보안 강화

빅데이터, 클라우드 컴퓨팅 등 기술 혁신을 지원하며, 국가 사이버안전을 보장하기 위한 산업 기반을 강화한다. 사이버안전 인재 양성 프로젝트를 실시하고, 사이버안전학과의 건립을 강력하게 추진한다. 최고의 사이버안전 학부와 창의혁신단지를 건립하여, 인재 육성과 창의혁신적 기업발전에 이로운 보안 생태계를 구축한다.[111]

---

110) (六) 完善网络治理体系

坚持依法、公开、透明管网治网，切实做到有法可依、有法必依、执法必严、违法必究。健全网络安全法律法规体系，制定出台网络安全法、未成年人网络保护条例等法律法规，明确社会各方面的责任和义务，明确网络安全管理要求。加快对现行法律的修订和解释，使之适用于网络空间。完善网络安全相关制度，建立网络信任体系，提高网络安全管理的科学化规范化水平。

加快构建法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的网络治理体系，推进网络社会组织管理创新，健全基础管理、内容管理、行业管理以及网络违法犯罪防范和打击等工作联动机制。加强网络空间通信秘密、言论自由、商业秘密，以及名誉权、财产权等合法权益的保护。

鼓励社会组织等参与网络治理，发展网络公益事业，加强新型网络社会组织建设。鼓励网民举报网络违法行为和不良信息。

111) (七) 夯实网络安全基础

坚持创新驱动发展，积极创造有利于技术创新的政策环境，统筹资源和力量，以企业为主体，产学研用相结合，协同攻关、以点带面、整体推进，尽快在核心技术上取得突破。重视软件安全，加快安全可信产品推广应用。发展网络基础设施，丰富网络空间信息内容。实施“互联网+”行动，大力发展网络经济。实施国家大数据战略，建立大数据安全管理制度，支持大数据、云计算等新一代信息技术创新和应用。优化市场环境，鼓励网络安全企业做大做强，为保障国家网络安全夯实产业基础。

建立完善国家网络安全技术支撑体系。加强网络安全基础理论和重大问题研究。加强网络安全标准化和认证认可工作，更多地利用标准规范网络空间行为。做好等级保护、风险评估、漏洞发现等基础性工作，完善网络安全监测预警和网络安全重大事件应急处置机制。

实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境。办好网络安全宣传周活动，大力开展全民网络安全宣传教育。推动网络安全教育进教材、进学校、进课堂，提高网络媒介素养，增强全社会网络安全意识和防护技能，提高广大网民对网络违法有害信息、网络欺诈等违法犯罪活动的辨识和抵御能力。

⑧ 사이버공간 방어력 향상

사이버공간은 국가 주권이 적용되는 새로운 공간이다. 중국의 국제적 지위에 부합하는 사이버 강국으로서의 사이버공간 방어 능력을 갖춰야 한다. 사이버안전 방어 수단을 크게 발전시키고 인터넷 침입을 즉시 탐지・대응하여 국가 사이버안전을 강력하게 지원 및 보호해야 한다.[112]

⑨ 사이버공간에 대한 국제협력 강화

상호존중과 신뢰를 바탕으로 국제사회에서 각국의 양자・다자간 사이버안전 대화・교류 및 정보교류를 강화하며, 국가간 차이점을 효과적으로 관리, 통제해야 한다. 인터넷 주소와 루트 DNS 서버 등 기초 자원 관리의 국제화를 추진한다.

UN이 주도적인 역할을 수행하도록 지원하고 모든 국가들이 보편적으로 수용 가능한 사이버공간의 국제 규범과 국제 반테러 조약 제정을 추진한다. 사이버 범죄 단속을 위한 사법 공조 체제를 완비하며, 정책법률・기술혁신・표준규범・긴급대응・주요 정보기반시설 보호 등의 영역에서 국제 협력을 심화한다. 개발도상국과 낙후지역에 대한 인터넷 기술 보급과 기반시설 건설 지원 및 원조를 강화하여 디지털 격차를 완화하기 위해 노력한다. “일대일로(一带一路)”의 건설을 장려하고 국제 통신 상호접속서비스와 상호교류를 증진하여 원활한 정보 실크로드를 구축한다. 세계인터넷대회(世界互联网大会)와 같은 전 세계 인터넷 공유・공동관리 플랫폼을 구축하여 힘을 합쳐 건강한 인터넷

---

112) (八) 提升网络空间防护能力

网络空间是国家主权的新疆域。建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络入侵，铸造维护国家网络安全的坚强后盾。

발전을 도모한다.[113]

3.3.2 사이버테러 대응에 대한 인식

사이버위협에 대한 인식은 사이버 안보 전략의 핵심적인 구성요소이다. 인식은 전략의 이념, 거버넌스 구조 및 사이버역량에 영향을 미치기 때문이다. 중국은 사이버위협을 국내와 국외로부터 발생한다고 인식한다.[114]

국내 사이버테러 위협은 소수민족이나 분리주의 종교집단에 의해 행해지는 가능성을 높게 보고 있다. 이러한 정치적인 목적을 가진 사이버테러 위협은 중국 공산당 지도부에 민감하게 받아들여지고 있다. 중국 공산당 지배와 정권의 정치적, 이념적 정통성을 비판하고 부정하기 때문이다.[115]

또한 중국은 국외 사이버테러의 주요 위협은 미국에 의한 사이버첩보 행위로 인식한다. 2013년 스노든 사건을 통해 미국 NSA의 사이

---

113) (九) 强化网络空间国际合作

在相互尊重、相互信任的基础上，加强国际网络空间对话合作，推动互联网全球治理体系变革。深化同各国的双边、多边网络安全对话交流和信息沟通，有效管控分歧，积极参与全球和区域组织网络安全合作，推动互联网地址、根域名服务器等基础资源管理国际化。

支持联合国发挥主导作用，推动制定各方普遍接受的网络空间国际规则、网络空间国际反恐公约，健全打击网络犯罪司法协助机制，深化在政策法律、技术创新、标准规范、应急响应、关键信息基础设施保护等领域的国际合作。

加强对发展中国家和落后地区互联网技术普及和基础设施建设的支持援助，努力弥合数字鸿沟。推动“一带一路”建设，提高国际通信互联互通水平，畅通信息丝绸之路。搭建世界互联网大会等全球互联网共享共治平台，共同推动互联网健康发展。通过积极有效的国际合作，建立多边、民主、透明的国际互联网治理体系，共同构建和平、安全、开放、合作、有序的网络空间。

114) 조현석, “중국 사이버안보 전략의 통합적 접근”, 한국위기관리논집, 2017 vol.13, p.94.

115) 조현석, “중국 사이버안보 전략의 통합적 접근”, 한국위기관리논집, 2017 vol.13, p.94.

버감시 프로그램이 폭로되면서 중국의 외교부 대변인은 중국이 사이버 공격의 희생자라는 것을 다시한번 보여준다고 주장했다.[116]

중국은 사이버전쟁에 대하여 현실적인 위협으로 인식하지 않았다. 그러나 2009년 미국의 사이버사령부 설립과 2011년 미국 국방부 사이버안보전략 발표는 중국이 사이버전의 위협을 보다 현실적으로 인식하는 계기가 되었다. 또한 2010년 이란 스턱스넷 사건이 2014년 미국과 이스라엘의 사이버공격이라는 사실이 보도되면서 중국의 인식변화에 영향을 주었다.[117]

116) Amy Chang, “Warring State: China's Cybersecurity Strategy”, Center for a New American Security, 2014, p.28.
117) Adam Segal, “The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age”, New Public Affairs, 2016 ; 조현석, “중국 사이버안보 전략의 통합적 접근”, 한국위기관리논집, 2017 vol.13, p.95.

3.3.3 사이버테러 대응과 국제협력

1) 중미 사이버테러 대응 협력

2013년 6월과 2015년 9월 중미 정상회담에서 시진핑 주석과 오바마 대통령은 사이버범죄 협력과 테러정보 공유 등에 관한 일정부분의 합의에 이르렀다.[118]

사이버테러 대응과 관련한 중미관계에서 세 가지 관점이 존재한다.[119] 중국학자는 미국이 사이버공간의 관리 및 기술적 우위를 활용하여 사이버안보의 전략적 우위를 유지하려고 한다고 주장한다.[120] 또한 최근 미국은 억지개념의 사이버전략 우위를 활용하여 국제제도를 형성하고 사이버공간에서의 우방을 확보하는데 주도권을 놓지 않는다고 생각한다.[121] 비록 오바마정부 시기 미국의 종합적인 국력이 다소 쇠퇴하였지만 사이버안보 분야에서 상대적인 전략적 우위는 오히려 명확하게 증대되었다. 또한 미국은 새로운 사이버안보 질서를 구축하려 하고 사이버분야에서의 핵심적 지위를 유지하고 있다.[122] 그러나 종합적으로 보면 사이버안보 문제에서 중국과 미국의 이익은 많은 차이점이 존재한다. 이러한 차이점은 사이버안보의 목표와 기술적인 측면 뿐만아니라 국제사이버공간의 규범 문제에서도 나타난다. 이것은 미국이 앞으로 국제사이버안보 분야에서 중심을 유지하는 것이 쉽지 않다는 것을 보여준다. 스노든 사건 이후 많은 국가들은 사이버공간의 비대칭적인

118) 刘宁、郎平，“不同议题下的中美网络安全关系：合作、竞争与冲突”，战略决策研究，2017年第2期，p.3.
119) Ibid.，p.4.
120) 吴则成，“美国网络霸权逻辑与中国防御性网络安全战略构建”，湖南师范大学社会科学学报，2014年4期，pp.34-35.
121) 蔡翠红，“美国网络霸权对中国国家安全的影响及对策”，国际问题研究，2014年1期，pp.43-51.
122) 沈逸，“美国国家网络安全战略的演进及时间”，美国研究，2013年3期，pp.49-50.

우위가 국가이익을 실현하는 수단이 될 수 있다고 인식하게 되었다. 또한 점점 더 국가들은 사이버주권화를 추구하게 되고 사이버공간의 지정학적인 의미는 더욱 명확히 드러나게 되었다.[123]

두 번째 시각은 다자협력주의이다. 다자협력주의는 사이버안보가 전통적인 국가안보와는 다르다고 생각한다. 사이버공간은 다양한 행위자들과 국가 및 각 단체들 그리고 민간상업기구 등이 존재한다. 사이버안보에 적절한 조치를 하기위해서는 정부, 민간, 비정부기관 등이 공동 협력하여야 한다. 또한 사이버안보의 이익은 이러한 이익상관자들에게 분배가 되기때문에 국가는 사이버공간에서 이미 유일한 행위자가 아니다. 국가, 사회 그리고 시장이 사이버공간의 서로 다른 부분에서 상호협력하고 있는 것이다.[124] 이렇기 때문에 국제 사이버안보협력도 다양한 참여자와 평등한 협상의 원칙하에 진행되어야 한다. 그리고 국가와 국제사회는 비정부행위자들의 참여를 확대할 수 있도록 노력해야한다. 이러한 다양한 참여자의 이익이 보장될 수 있어야지만 사이버 위협의 근원을 차단할 수 있다. [125] 다자주의협력의 핵심관점은 사이버안보 협력의 모델을 구축하고 다원화된 사이버안보 규범을 형성하려는 것이다.[126] 그러나 현실을 고려하면 다원주의는 사이버공간을 국가주권을 넘어서는 존재로 인식하는 면이 존재한다. 국제 사이버안보에서 국가는 여전히 중요한 행위자이고 다양한 행위자가 국가를 대

123) 李恒阳, “斯诺登事件与美国网络安全政策的调整“, 外交评论, 2014年3期, pp.123-124.
124) 蔡翠红, “国家-市场-社会互动中网络空间的全球治理”, 世界经济与政治, 2013年9期, pp.90-112.
125) Neil Weinstock Netanel, “Cyberspace Self-Governance : A Skeptical View form Liberal Democratic Theory”, California Law Review, Vol.88, 2000, pp.395-400.
126) Scott J. shackelford, “Toward Cyberspace : Managing Cyber-attacks through Polycentric Governance”, American University Law Review, pp.1273-1364.

체할 수는 없다.[127] 최근 사이버기술 및 관련 규정의 제정과 관련해서 주요 사이버 강국들의 경쟁이 심화되고 있으며 주요 협력 또한 국가간에 이루어지고 있다.[128]

세 번째는 국제제도의 시각이다. 이러한 종류의 연구는 국제사이버공간의 규범과 제도를 만드는 것에 중점을 둔다. 그러나 최근 국제 사이버공간의 규범 마련은 아직 초기단계이고 실질적인 사이버 위협이 존재함에도 불구하고 국제사회의 합의에는 이르지 못하고 있다.[129] 일부 학자들은 관념, 제도, 조직인 사이버안보를 보장하고 국제 사이버안보규범이 일종의 사회규범으로서 국제사회에 확산될 수 있고 최종적으로 국제규범으로 형성될 수 있다고 믿는다.[130] 그러나 현실적인 측면에서 UN, ITU와 국제사이버범죄협약은 국제사회가 교류할 수 있는 플랫폼을 제공하고 있지만 사이버공간의 규범측면에서 합의를 이끌어내지 못하고 있다. 이런 측면에서 제도 수립 및 조직 설립은 더욱 어려운 문제로 남아있다.[131] 부다페스트 사이버범죄협약은 국제 사이버안보협력의 큰 진전을 가져왔지만 여전히 일부국가는 의문을 가지고 있다. 일부 학자들은 이공약이 선진국의 기준하에 만들어졌으며 선진국의 이익을 보호하고 개도국의 사이버안보 상황은 반영되지 않은 것으로 본다.[132] 또한 중국은 상하이협력기구 회원국들과 함께 UN에 '정보보호국제행동준칙'을 제출하였고 이는 국제사이버공간 규범 마련에

---

127) James A. Lewis, "National Perception of Cyber Threats", strategic Analysis, Vol. 28, 2014, pp.566-576.
128) 刘宁、郎平, "不同议题下的中美网络安全关系：合作、竞争与冲突", 战略决策研究, 2017年第2期, p.7.
129) 郎平, "全球网络空间规则制定的合作与博弈", 国际展望, 2014年6期, pp.138-152.
130) Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity", The American Journal of International Law, Vol.110, 2016, pp.425-479.
131) 王孔祥, "网络安全的国际合作机制探析", 国际论坛, 2013年9月, pp.1-6.
132) 于志刚, "缔结和参加网络犯罪国际公约的中国立场", 政治论坛, 2015年9月, pp.91-107.

일정한 원칙을 제시한 것이지만 미국과 유럽국가는 기본적으로 반대 입장을 표명하고 있다. 비록 일부학자들은 사이버안보문제에 국제기준이 마련될 수 있다는 낙관적인 의견을 보였지만 누구의 기준에 따라 규범이 제정되는가 하는 문제는 여전히 남아있다.[133] 스노든 사건이 발생되고 난 후 국제사회는 좀더 다자적이고 민주적이며 투명한 국제규범 마련에 대한 요구를 하고 있지만 사이버안보 체계는 미국과 유럽 등 선진국의 영향을 벗어나기가 쉽지 않은 현실이다. 이렇듯 국제 사이버안보 규범 제정은 강대국들간의 게임으로 진행되고 있다.[134]

사이버안보에서 중미관계에는 협력, 경쟁 그리고 갈등의 양상을 모두 보이고 있다. 예를 들어, 사이버범죄에 대응에 있어서 중미 양국은 효과적인 대화와 협력을 이행하고 있으며 사법 공조에 관한 내용도 '중미 합동사법협력 협의회'라는 틀안에서 실질적인 협력이 진행되고 있다. 그러나 사이버안보의 다른 분야에서는 양국간의 대립과 경쟁이 보다 뚜렷하다. 2014년 미 법무부는 미국 산업기밀 절취 관련하여 중국 장교 5명을 기소하였고 2013년 6월 중미 정상회담 이후 확립된 양국의 사이버안보의 신뢰는 후퇴하였다.[135]

사이버안보에서 중미관계를 보면 한 나라가 상대국에게 취하는 행동이 매우 민감하게 작용하고 즉각적인 반응을 가져온다. 2011년 미국이 국제사이버공간전략을 발표한 후 중국은 즉각적으로 반응하였다.

---

133) Harvey Rishikof and Kevin Lunday, "Corporate Responsibility in Cybersecurity : Building International Global Standards", Georgetown Journal of International Affairs, Vol.12, 2011, pp.17-24.
134) 蒋丽、张小兰、徐飞彪, "国际网络安全合作的困境与出路", 现代国际关系, 2013年9月, pp.52-58.
135) 刘宁、郎平, "不同议题下的中美网络安全关系：合作、竞争与冲突", 战略决策研究, 2017年第2期, p.8.

이러한 국가간의 경쟁의 일면에는 사이버공간에 대한 주도권확보와 전략적 우위를 추구하는 모습을 볼 수 있다.[136] 또한 미국이 사이버안보 정책을 국가전략으로 여기고 사이버사령부를 창설하려는 것은 중미 양국의 사이버안보 경쟁은 심화될 것이다. 이러한 경쟁관계는 '투키디데스 함정'에 쉽게 빠질 수 있다.[137] 또한 중미 양국은 사이버기술 역량을 지속적으로 강화하려고 경쟁할 것이다.

물론 사이버안보의 모든 분야에서 경쟁적인 것은 아니다. 경쟁을 하지 않거나 경쟁의 정도가 낮은 부분도 있다. 예를 들어, 사이버범죄, 사이버테러 등의 분야에서 양국은 공동으로 대응하려고 한다. 공공성이 있는 이슈와 관려해서는 경쟁보다는 협력의 요구가 더 큰 것이 현실이다.[138]

중미 양국의 협력은 양국이 처한 취약성을 반영하는 것이다. 상호의존의 관점에서 보면 취약성의 정도가 국가가 선택할 수 있는 대안과 비용을 결정한다.[139] 사이버안보 문제에 있어서 중미 양국의 상호의존도는 특히 높은 편이고 협력외에 다른 대안은 많지 않다. 즉, 국제협력만이 자국의 사이버위협을 해결할 수 있는 수단이다. 사이버공간의 특징인 다양성, 익명성, 공격우위 문제는 일국의 대응을 어렵게 하고 사이버안보 문제를 복잡하게 만들고 있다. 그렇기 때문에 국제협력이 이를 해결할 수 있는 효과적인 방법이다. 사이버범죄 대응에 있어서

136) 蔡翠红，“网络空间的中美关系：竞争、冲突与合作”美国研究，2012年3期，p.107.
137) 檀有志，“跨越修昔底德陷阱：中美在网络空间的竞争与合作”，外交评论，2014年5期，p.19.
138) 刘宁、郎平，“不同议题下的中美网络安全关系：合作、竞争与冲突”，战略决策研究，2017年第2期，p.8.
139) 罗伯特·基欧汉，约瑟夫·奈，“权力与相互依赖”，门洪华译，北京大学出版社，2014年，p.13.

중미양국은 이익을 같이하고 윈윈하려는 목표를 설정하여 협력의 길로 충분히 갈 수 있다.[140]

중미 양국의 갈등은 사이버안보 목표와 대응조치의 차이점에서 비롯된다. 이는 상호대립과 심지어 상호 공격에까지 이르게 한다. 우선 양국은 발전정도가 다르기 때문에 추구하는 사이버안보의 목표도 다르다. 이러한 목표는 국내 사이버안보 관련법에 반영되어 있다. 미국은 전세계적인 인터넷 개방에 역점을 두고 중국은 사이버공간의 주권 문제에 더 관심을 가지고 있다. 이러한 목표의 차이점은 때론 긴장국면을 유발하기도 한다. 다음으로 최근 사이버전에 관한 논의가 활발해지면서 사이버는 정치·군사적으로 이용될 가능성이 높아졌고 이러한 사이버공간의 군사화는 중미 양국의 갈등을 쉽게 야기할 수 있다.[141]

이러한 협력, 경쟁, 갈등의 정도를 기준으로 사이버안보의 중미 관계를 살펴보면 크게 두 가지로 구분할 수 있다. 첫째, 협력요인이 높고 경쟁과 갈등 요인이 낮은 경우이다. 중미 양국은 자국의 사이버안보를 위해 비록 일정정도의 경쟁과 갈등이 있음에도 사이버범죄, 사이버테러 등의 공공성이 높고 국가에 영향을 주는 어젠다에 대하여서는 협력의 필요성이 크게 작용한다. 여기서 공공성은 두가지로 구분할 수 있는데 하나는 사이버 공간이 제공하는 다양한 정보교환과 공유 등 인터넷의 장점을 지키는 것이다. 또 다른 하나는 사이버범죄나 테러 등 사이버공간에서 비롯된 위협에 대응하는 것이다. 이러한 문제에 관련

---

140) Harvey Rishikof and Kevin Lunday, “Corporate Responsibility in Cybersecurity : Building International Global Standards”, Georgetown Journal of International Affairs, Vol.12, 2011, pp.17-24.
141) 刘宁、郎平, “不同议题下的中美网络安全关系：合作、竞争与冲突”, 战略决策研究, 2017年第2期, pp.9-10.

하여 양국의 이견은 거의 없고 협력의 필요성에 대한 합의는 이미 이루어졌다.

둘째 협력요인은 낮고 경쟁과 갈등요인이 높은 경우이다. 양국은 사이버안보의 국내법, 사이버기술, 국제규범, 사이버공간의 군사화 등의 분야에서 경쟁이 어느정도 나타났고 갈등의 가능성도 존재한다. 양국이 추구하는 사이버안보 목표는 시각의 차이가 뚜렷하다. 미국은 자유롭고 개방적인 사이버공간을 만드는데 그 목표를 두고 중국은 사이버공간의 주권수호에 목표를 둔다. 또한 양국의 국내법이 일정부분 사이버안보법의 공백을 메우지만 법적인 측면에서 어떻게 사이버안보 협력을 이끌어낼 수 있는가에 대한 문제는 여전히 남아있다.

또다른 문제는 중미 양국이 사이버안보분야에서 경쟁하는 것이 갈등으로 바뀌는가의 문제이다. 사이버전의 경우 그 가능성의 일면이 있다. 그러나 만약 사이버공간이 정치군사화의 수단이 된다고 하더라도 갈등을 조정할 수 있는 여지는 남아있다. 국제규범의 제정 측면에서 보면 아직 초기단계로 볼 수 있는데 각 국은 기술, 군사안보 그리고 대책 세가지 방면에서 주요 논의를 진행하고 있다.[142] 중미 양국도 예외는 아니다. 한편으로 사이버안보 기술과 규범 측면에서 양국은 주도권 경쟁을 하고 있다. 그러나 이와 동시에 기술과 규범의 문제는 외부효과의 특징을 가지고 있기 때문에 양국 모두 서로를 경쟁구도 밖으로 배척할 수는 없다. 이러한 측면에서 보면 양국의 경쟁은 사이버공간에서의 전략적 우위의 주도권 쟁탈을 위한 것으로 볼 수 있다. 중국은 미국에게 주도당하는 것을 피하고 좀 더 많은 발언권을 얻으려하는

142) 郎平, “全球网络空间规则制定的合作与博弈”, 国际展望, 2014年6期, p.138.

측면이 강하다.[143]

중미 양국의 사이버안보 분야에서 협력, 경쟁, 갈등의 양상은 비교적 명확하게 드러난다. 사이버범죄, 국내 사이버안보법, 사이버 기술, 국제규범, 사이버 군사화 등 다섯가지 측면에서 중미관계를 살펴본다.

최근 중미 양국의 협력은 사이버범죄에 대한 대응과 위협정보 공유분야에서 주로 이루어지고 있다. 이 문제는 공공적인 성격이 강하여 양국의 이익이 일치하는 면이 크다. 중미 양국은 사이버범죄로 인한 경제적 손실이 크고 사이버의 초국적인 특성으로 일국의 국가가 대응하는데 한계가 있다. 2015년 이후 중미 양국은 사이버범죄 대응관련 협력에서 실질적인 진전을 이루었다. 사이버범죄 관련 합동사법협력협의회와 고위급 회담 기제가 그 예이다. 2015년 12월에 사이버범죄관련 고위급 회담이 처음으로 진행되었고 '사이버범죄 대응 관련 지침'에 상호합의하였다. 2016년 6월, 양국은 중국 베이징에서 두 번째 고위급 회담을 하였고 '사이버범죄 대응 관련 핫라인 운용 방안'에 합의하고 관련분야의 포괄적인 의견일치를 보았다. 2016년 12월에는 세 번째 고위급 회담을 열었다.[144]

세차례의 고위급회담에서 두가지 특징을 볼 수 있다. 하나는 중미 양국이 적합한 협력방식을 계속 찾으려 노력한다는 것이고 또다른 하나는 양국의 협력과제가 점점 확대된다는 것이다. 두 번째 회담에서 사이버공간의 국제규범에 관한 논의가 진행되었고 세 번째 회담에서는

143) 刘宁、郎平，“不同议题下的中美网络安全关系：合作、竞争与冲突”，战略决策研究，2017年第2期，pp.11-12.
144) Ibid., p.12.

사이버테러 이슈가 추가되었다는 것이다. 비록 양국의 의견차가 존재하지만 이러한 대화기제는 상호소통 및 교류의 장을 제공해준다.[145]

사이버안보 관련해서 중미 양국은 협력보다 경쟁과 갈등의 양상이 더 나타난다. 최근 양국은 네 가지 분야에서 주로 경쟁과 갈등을 보이고 있다. 국내사이버안보법, 사이버기술, 사이버 군사화, 국제규범 문제이다. 이러한 문제들은 협력요인이 약하고 배타성은 큰 분야로 특히 국내 사이버안보법과 사이버군사화 분야에서는 특히 갈등이 심화되고 있다.

먼저 국내 사이버안보법을 살펴보면, 미국의 국내입법은 정부와 개인간의 정보와 책임을 분명하게 구분하고 이를 통해 사이버안보를 강화하려 한다. 2013년 4월 미국은 '2013년 연방정보보호 수정안'을 발의하였고 정부가 지속적으로 정보감시통제권을 가지고 위협에 대한 평가 권한을 가진다는 내용이다.[146] 오랜기간의 논의 끝에 2015년 6월 오바마 정부는 상원에서 '미국자유법안'을 상원에서 통과시켰다.[147] 같은 해 10월에는 '사이버안보 정보공유 법안'을 통과시켰다.[148] 두 법안은 인터넷을 운용하는 개인 영역에서도 일정부분의 사이버 안전조치를 취해야 한다는 것을 명확히 했고 정부의 역할 또한 명확하게 규정하였다. 중국의 사이버안보법은 상대적으로 진전이 늦었으나 십여년의 우여곡절 끝에 2015년에 입법단계에 들어갔다. 2016년 11월 중국은 사이

145) 刘宁、郎平, "不同议题下的中美网络安全关系：合作、竞争与冲突", 战略决策研究, 2017年第2期, p.12.
146) House Republicans, "Federal Information Security Amendments Act of 2013", Apr 13, 2013.
147) Congress, "US Freedom Act of 2015", Apr 28, 2015..
148) United States of Senate, "Cybersecurity Information Sharing Act of 2015", Mar 3, 2015.

버안보법을 통과시켰고 2017년 6월 1일 부로 시행하였다. 중국의 사이버안보법은 두가지 특징이 있다. 하나는 사이버 주권을 강조하여 국가주권원칙이 사이버공간에 적용되는 것이다. 또 다른 하나는 국가의 관리 및 통제를 강조하는 것이다. 즉 국가가 국내외에서 오는 사이버위협 및 위험에 대해 상응하는 조치, 감시, 예방를 취하고 국가기간시설에 대한 보호를 하는 것이다.[149]

중미 양국의 사이버안보법에는 크게 두가지 차이점이 있다. 하나는 중미 양국이 사이버안보 문제를 대하는 태도가 다르다. 미구그이 '사이버안보 정보공유 법안'을 보면 미국정부는 주로 불법 침입과 기밀절취를 주요 문제로 본다. 따라서 미국정부는 정부와 민간영역의 정보공유를 통해 민간부분의 사이버안전문제 개선하는 것을 강조한다. 중국은 사이버주권을 강조하고 외부 침입을 중요하게 여긴다. 사이버안보법을 보면 중국은 영토내에 있는 인터넷에 대해 지속적인 감시 및 통제를 할 것이다. 중미 양국의 사이버 운영 기본이 다른 것을 고려했을 때 미국은 중요기반시설 대부분이 민간에서 운용하지만 중국의 국내기반 대부분은 공공부문에서 운용한다. 따라서 현실적으로나 법률적으로 보나 이러한 부분은 양국 사이버안보 협력에 자연스럽게 장애가 되고 있다. 2010년에 일어난 구글 사건에서도 중미 양국은 사이버안보 딜레마를 실질적으로 경험했다.

두 번째는 중미 양국의 사이버 안보는 구체적으로 무엇을 의미하는가이다. 중미 양국은 모두 자국 인프라의 안전과 자국민의 사생활 보호를 강조하고 있다. 하지만 구체적으로 보면 양측의 지향점은 일치

149) 刘宁、郎平，“不同议题下的中美网络安全关系：合作、竞争与冲突”，战略决策研究，2017年第2期，pp.13-14.

하지 않는다. 미국은 인터넷 운영 관련 민간부문의 상업적 이익을 더욱 강조하는 반면 중국은 상업적 이익 외에도 사이버 안보에서 자국의 정치적 군사적 이익을 더욱 중시하고 있다. 2016년 12월 27일 중국은 '국가사이버안보 전략'을 발표하였다. 이 전략은 중국 사이버안보의 행동 강령일 뿐만 아니라 동시에 중국 사이버안보환경의 현실을 보여준다. 중미 양국의 사이버안보 환경이 다르기 때문에 양측은 안보이익에 대한 관점이 상이하고 이로인해 입법에 차이를 가져오게 된다. 이것은 양국 사이버안보 협력이 앞으로 순탄하지 않고 갈 길이 멀다는 것을 의미한다.[150]

두 번째는 기술적인 측면이다. 미국은 세계 정상급 도메인 13개 중 10개를 가지고 있다.[151] 동시에 미국은 다른나라와 비교할 수 없는 정보산업과 대부분의 핵심설비를 가지고 있다. 하드웨어 방면에서 미국의 시스코 시스템스는 네트워킹 교환기의 생산 판매에서 거의 독점을 하고 있다. 소프트웨어 부분을 보더라도 전세계 90%이상을 차지하는 컴퓨터 운영체제는 마이크로소프트사가 만든 것이다. 페이스북과 트위터와 같은 SNS 분야에서도 미국은 일정한 독점적 지위를 가지고 있다. 2016년 2월 미국 백악관은 '사이버안보 국가 행동계획'을 발표하였다. 이 계획의 내용은 주로 어떻게 사이버안보 수준을 향상시키는가에 대한 것이었고 사이버안보분야 예산도 확대되었다.[152] 2016년 4월 19일 열린 사이버안보 및 정보화 좌담회에서 중국의 시주석은 사이버안보를 지켜야하고 이를 위해 사이버 기술 방면에서 혁신이 필요하다고 강조하였다. 또한 최근 중국의 핵심기술은 외국에 제약을 받고 있

150) 刘宁、郎平, "不同议题下的中美网络安全关系：合作、竞争与冲突", 战略决策研究, 2017年第2期, p.14.
151) Internet Assigned Numbers Authority, "Root Servers".
152) The White House, "Cybersecurity National Action Plan", Feb 09 2016.

는데 이는 사이버안보에 큰 우려라고 하였다. 중국은 인터넷 후발주자로서 새로운 기술을 받아들이고 투자를 확대하는 등의 방법으로 사이버 기술 수준을 더욱 강화해야 한다고 강조하였다.[153] 2016년 7월, 중국은 '국가정보화발전전략 요강'을 발표하였다. 발전전략요강에는 3단계 전략계획을 수립하여 핵심기술이 사람에 의해 제약받는 상황을 철저하게 변화시키고 기술과 산업을 발전시켜 사이버안보의 확고한 보장을 전략목표로 설정하였다.[154] 사이버 선진기술이 없다면 사이버안보도 없다는 것이다. 이것은 미국은 사이버안보 기술면에서 우위를 지속적으로 유지하려고 하고 중국은 계속 추월전략을 계속 시행할 것을 의미한다. 당분간 중미 양국은 사이버안보기술 측면에서 경쟁은 심화될 것이다.

세 번째로 국제 사이버안보 규범이다. 이 어젠다는 여전히 중미 양국에 중요한 문제이다.. 최근 국제 사이버규범의 제정은 여전히 초기단계이고 합의를 이루지 못하였다. 2001년 부다페스트 사이버범죄 협약은 국제사회가 이룬 큰 진전이라고 할 수 있다. 그러나 이 협약은 서방국가의 주도하에 제정되었다. 일부학자들은 이 협약이 서방국가의 이익추구를 반영한다고 한다. 중국의 입장에서 보면 협약은 중국의 사이버안보 요구가 반영되지 않았고 중국은 아직 가입하지 않았다.[155] 2011년 5월 미국 백악관은 국제사이버전략을 발표하였고 미국은 사이버공간의 자유, 번영, 안전을 위해 최선을 다할 것을 명확하게 주장하였다. 미국은 자국의 이점을 활용하여 전세계에 사이버공간 규칙을 반영하려고 한다. 중미 양국은 이 문제에서 첨예하게 대립하고 있다.

153) 国家互联网信息办公室，“习近平总书记在网络安全与信息化工作座谈会上的讲话”，2016年4月19日.
154) 国务院新闻办新闻发布厅，“国家信息化发展战略纲要”，2016年7月27日.
155) 于志刚，“缔结和参加网络犯罪国际公约的中国立场”，政法论坛，2015年9月，pp.91-107.

2014년 중국의 주도로 세계 인터넷 컨퍼런스가 개최되었다. 이 대회는 새로운 국제 사이버 협력의 플랫폼이라 할 수 있다. 2015년 1월 중국은 상해협력기구 회원국들과 함께 유엔에 '정보보호 국제행동 준칙'을 제출하였다. 이것은 사이버안보 규범에 대한 원칙을 준용한 건의이다.[156]

중국은 국제사이버규범에 관한 논의는 사이버주권을 존중하는 전제에서 시작되어야 한다고 주장한다. 2015년 12월 중국 절강성 이우시에서 제2회 세계 인터넷 컨퍼런스가 개최되었다. 중국은 다시한번 정보보호 국제행동 준칙을 천명하였다. 사이버공간의 자유, 번영, 안보는 계속 지켜나가야 하고 국가의 역할도 강조하였다.[157] 반대로 미국은 개방적이고 자유로운 정보이동이 가능한 사이버공간을 구축하는데 노력한다. 또한 미국은 사이버선진국으로 중국이 제창하는 사이버주권에 반대하는 입장이다.

아직 국제사회에 합의된 사이버협약의 부재한 상황에서 중미양측이 어느정도 수용할 수 있는 국제협약을 어떻게 제정하는가가 양국에도 매우 중요하다. 당분간 중미양국은 규범제정 분야에서도 경쟁이 심화될 것으로 보인다. 일부학자들은 사이버주권과 사이버자유가 중미양국 갈등의 근원이라고 여긴다.[158] 그러나 다른 한편으로 중미 양국의 사이버안보기술과 규범제정에서의 경쟁이 꼭 갈등을 일으킨다고는 할 수 없다. 물론 중국이나 미국 모두 인터넷에서 상대를 완전히 배제할 수 없고 양측은 발언권과 주도권을 최대한 쟁취하려고 하는 것이다.

156) 中国外交部, "信息安全国际行为准则", 2015年3月5日.
157) 储殷, "网络全球治理正在进入中国时代, 中国信息安全, 2016年1期, p.45.
158) 蔡翠红, "网络空间的中美关系：竞争、冲突与合作", 美国研究, 2012年第3期, p.107.

네 번째는 사이버군사화이다. 이 이슈는 중미 양국의 갈등요소가 제일 큰 영역이다. 사이버안보문제에서 미국 국방부는 특히 적극적이다. 2011년 7월 미국 국방부는 '국가행동전략'을 발표하였고 사이버안보를 국가안보전략에 분명하게 포함시켰다. 또한 선제공격의 사이버억지 정책도 실행할 것이라 했다.[159] 2012년 9월 뎀프시 미국 합참의장은 '연합작전구상 : 2020년 연합작전부대'를 발표하면서 전세계의 통합작전 개념과 사이버안보가 통합작전에서 가장 중요한 목표 중 하나라고 주장하였다.[160] 2014년 미국 국방부는 '4개년 국방 검토'를 발표하였고 미국은 지속적으로 세계 리더의 역할을 유지하고 사이버안보를 강화한다는 내용이 담겨있다. 동시에 협력국가들과의 관계를 공고히 하고 공동으로 사이버위협에 대응해 나갈 것이라고 주장하였다.[161] 2015년 4월 미국은 국방부 사이버전략의 새로운 버전을 발표하였다.[162] 이 전략은 군 내부망의 보호, 사이버공격의 반대, 국가 이익의 보호, 사이버 후방지원의 내용을 담고 있다. 이것은 사이버가 이미 미군의 중요한 공격무기에 포함되었다는 것을 보여준다. 2016년 6월 미 국방부는 '정보전장하 작전전략'을 발표하였고 사이버안보 관련 통합대응의 중요성을 강조하였다.[163] 미군은 통합작전의 개념을 사이버공간에도 적용하려고 하고 있다. 미국을 중심으로 사이버공간은 신속하게 군사화되고 있다. 게다가 미국은 국내에서 중국위협론을 퍼뜨리고 중국이 주

---

159) The Department of Defense, "Department of Defense strategy for Operating in Cyberspace", July 2011.
160) Association of The United States Army, https://www.ausa.org/events/ilw-rogers-strategic-issues-forum.
161) The Department of Defense, "The 2014 Quadrennial Defense Review", Mar 4, 2014.
162) The Department of Defense, "The Department of Defense Cyber Strategy", Apr 17, 2015.
163) The Department of Defense, "The Department of Defense Strategy for Operations in the Information Environment", Jun 2016.

요 사이버위협이라고 선전한다. 2011년 5월 중국 국방부는 사이버청군을 창설하였다. 2015년 중국은 전략지원 부대를 창설하고 정보화작전 능력을 향상시키려고 하였다. 또한 사이버안보에서 군과 민간의 융합 문제는 새롭게 관심을 가질만 하다. 국가간 사이버전은 국내의 군사역량 뿐만아니라 민간부분의 역량도 중요하기 때문이다. 미국이 민군 합동 역량은 중국에게 적지않은 부담을 주는 것이 사실이다. 2016년에 중국도 사이버 민군 합동 개념을 도입하기 시작했다.[164] 사이버군사화는 전통적인 군사안보와 유사하여 중미양국의 갈등을 쉽게 촉발시킬 수 있다.

164) 新华社，“关于经济建设和国防建设融合发展的意见”，2016年7月21日。

제4장 한국의 사이버테러 대응 전략

4.1 사이버테러 대응의 역사

1980년대부터 추진해온 국가 정보화와 함께 역기능이 나타나면서 정보보호에 대한 법률과 제도가 정비되기 시작하였다. 1981년에는 '정보 및 보안업무 기획·조정규정'(대통령령)이 제정되었고 이는 국가통신보안 업무에 대한 기획과 조정의 절차와 방법을 규정하였다.[165] 1986년에는 정보화에 관한 최초의 법률로 정보화에 관한 국가적 시책과 제도를 규정한 '전산망 보급확장과 이용촉진에 관한 법률'이 제정되었다. 이 법은 전산망 보호에 관한 일부 규정이 포함되어 있지만, 정보보호의 중요성을 인식하거나 이에 초점을 맞춘 법률이라 할 수는 없다.[166]

1994년 체신부를 확대개편하고 과학기술처·공보처·상공자원부의 정보통신기능을 통합하여 정보통신부를 출범시켰다.[167] 1995년에 제정된 '정보화촉진 기본법'은 정보화 촉진에 관한 내용 및 정보보호에 관한 기본적인 규정이 일부 마련되었다. '형법'이 개정되면서 전자기록 위작, 변작죄, 전자기록에 대한 비밀침해죄 등이 규정되었다.[168] 1996년 한국 정보보호센터(KISA)가 설립되었다. 1999년에는 을지연습시 사이버전 모의훈련이 최초로 실시되었다. 또한 '전산망 보급확장과 이용촉진에 관한 법률'이 '정보통신망 이용촉진 등에 관한 법률'로 개편되었다.

---

165) 국가정보원, "2018년 국가정보보호백서", 2018, p.6.
166) Ibid., p.91.
167) Ibid., p.6.
168) Ibid., p.91.

그리고 ‘국가 정보통신보안 기본지침’과 ‘전자서명법’이 제정되었다.[169]

한편, 1999년에는 인터넷 보급이 본격화되고 인터넷 전자상거래가 활발해지면서 정부는 개인 및 기업의 정보유통과 중요정보를 보호하기 위해 ‘전자서명법’을 제정하였다. 또한 ‘전산망 보급확장과 이용촉진에 관한 법률’을 ‘정보통신망 이용촉진 등에 관한 법률’로 전면개정하면서 정보화의 역기능에 대한 규정을 정비하였다.[170]

2000년대에는 정보통신 시스템에 대한 국가와 사회의 의존도가 점차 높아졌다. 이에 따라 정보보호 법제를 재정비하여야 할 필요성이 커지게 되었다. 따라서 관련 법률들이 제정되거나 기존의 법률이 전면개정되기 시작하였다.[171]

2001년 ‘정보통신기반 보호법’이 제정・공포되었다. 이 법은 금융・통신・에너지 등 국가와 사회의 중요한 정보통신기반시설을 보호하기 위한 특별한 체계를 주요 내용으로 한다. 또한 컴퓨터를 활용하여 타인의 재산을 침해하는 온라인 사기행위에 대한 처벌 관련 형법규정도 신설되었다.[172] 그리고 한국정보보호센터(KISA)가 한국정보보호진흥원으로 승격되었다.[173]

또한 ‘정보통신망 이용촉진 등에 관한 법률’은 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’로 명칭을 변경하였으며 정보보호와

169) 국가정보원, “2018년 국가정보보호백서”, 2018, p.6.
170) Ibid., p.91.
171) Ibid., p.92.
172) Ibid., p.92.
173) Ibid., pp.6-7.

관련된 규정을 대폭 강화하였다. 동법은 2003년 ‘1·25 인터넷 대란’이 발생되고 침해사고 대응과 관련된 규정을 크게 보완하였으며,[174] 한국정보보호진흥원 산하 인터넷침해사고대응지원 센터가 설립되었다. 2004년에는 국가사이버안전센터가 설립되었고 ‘국가위기관리 기본지침’(대통령 훈령) 및 국가사이버위기관리 매뉴얼이 제정되었다.[175]

2005년에는 ‘국가사이버안전관리규정’이 대통령 훈령으로 발령되었다. 이는 국가안보를 위협하는 사이버공격으로부터 국가정보통신망 보호를 위해 사이버안전에 관련된 조직 및 운영에 대한 사항을 체계적으로 정립하였다.[176]

2007년에는 기존의 ‘전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률’을 ‘전자정부법’으로 전면 개정하였으며 전자정부를 구현하기 위한 관련 법제의 정비가 진행되었다.[177]

2000년대 후반부터 지식정보사회 구현이 정보화정책을 추진하는데 중요하게 인식되었다. 중요 정보자원을 지식화하고 정보의 공동이용을 활성화하는 것은 국가경쟁력의 제고와 삶의 질 향상에 기여한다고 보았다. 한편 국민생활 및 사회 전반에서 정보통신기술에 대한 의존도가 높아지면서 사이버위협은 사회 안정과 국가안보의 문제로 연결되는 가능성이 높아졌다. 따라서 사이버공간에 대한 보호를 위해 지속적으로 노력해야 한다는 인식이 확대되었다.[178]

---

174) 국가정보원, “2018년 국가정보보호백서”, p.92.
175) Ibid., pp.6-7.
176) Ibid., p.92.
177) Ibid., p.92.
178) Ibid., pp.92-93.

2009년에는 ‘정보화촉진 기본법’을 ‘국가정보화 기본법’으로 전면 개정하였다. 또한 정보보호산업의 활성화를 촉진하기 위한 제도적 기반으로 ‘정보통신 산업진흥법’을 제정하였다.[179] 2009년 7.7 DDos 사건 이후 국가 사이버위기 종합대책이 수립되었다. 그리고 한국 정보보호진흥원, 한국 인터넷진흥원, 정보통신 국제협력진흥원을 통합하여 한국인터넷진흥원(KISA)이 출범하였다.[180]

2010년에는 ‘국방정보화 기반조성 및 국방정보자원관리에 관한 법률’이 제정되었다. 또한 ‘전자정부법’이 전면 개정을 통해 국방정보화와 행정정보화를 촉진하였고 이와 동시에 정보보호에 관한 부분을 개선하였다. 그리고 군에서는 사이버사령부가 설립되었다.[181] 2011년에는 3.4 DDos 사건이 발생하였고,[182] ‘개인정보보호법’이 제정되었다. 개인정보보호법은 관계 법령 가운데 개인정보보호 규정을 개정하여 개인정보보호를 대폭 강화할 수 있었다. 한편, ‘지식재산 기본법’의 제정은 지식재산권 보호를 강화하기 위해서 정보보호의 중요성을 증대할 수 있는 제도적 기반을 마련하였다.[183]

2013년 3.20 사이버테러 및 6.25 사이버공격이 발생하면서 국가 사이버안보 종합대책이 수립되는 계기가 되었다. 또한 정보보호 최고책임자 협의회가 출범하였으며,[184] 청와대를 중심으로 하는 ‘국가사이버안전관리규정’이 개정되었다. 2014년에는 한국수력원자력 해킹 사고

179) 국가정보원, “2018년 국가정보보호백서”, 2018, pp.92-93.
180) Ibid., pp.6-7.
181) Ibid., p.7.
182) Ibid., p.7.
183) Ibid., pp.92-93.
184) Ibid., p.7.

가 발생하였고[185] 2015년에는 ‘정보보호산업의 진흥에 관한 법률’이 제정되었다. 동법률을 통해 정보보호산업의 발전과 일자리 창출 등의 환경이 조성될 것을 기대할 수 있게 되었다.[186] 그리고 국가 사이버안보 태세 강화 종합대책이 발표되었으며, 2016년에는 ‘국가사이버안보법안’이 국무회의를 통과하였다.[187] 또한 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’이 개정되어 스마트폰 응용프로그램 개발자나 개발회사의 접근권한으로부터 이용자를 보호할 수 있도록 하고, 정보 통신서비스 제공자 등의 개인정보 분실·유출 등에 대한 징벌적 손해배상을 도입하였다.[188] 2017년에는 기존 정보보호 관련 법률의 시행과정에서 나타난 문제점들을 해결하고자 하는 법령 개정이 추진되는 한편, ‘4차 산업혁명위원회의 설치 및 운영에 관한 규정’을 제정하여 4차 산업혁명을 본격적으로 준비하고 역기능에 대처하는 체계를 본격적으로 구축하기 시작하는 등 정보보호 환경을 개선하고자 하는 제도적 차원의 노력이 계속 이루어졌다.

185) 국가정보원, “2018년 국가정보보호백서”, 2018, p.7.
186) Ibid., pp.92-93.
187) Ibid., p.7.
188) Ibid., p.93.

4.2 사이버테러 대응 법

경찰청 사이버안전국의 통계에 따르면, 2018년 전체 사이버범죄는 149,604건이 발생했으며, 2017년도(131,734건)에 비해 약 13.6% 증가하였다. 해당 발생건수는 최근 5년 내 최고치(2016년 153,075건)에 근접한 수준으로, 주춤 했던 증가 추세가 다시 이어지고 있다.[189]

해킹, 악성프로그램 유포 등 정보통신망에 불법적으로 침입하는 방식으로 저지른 범죄(정보통신망 침해범죄)는 전년대비 8.5% 감소한 반면, 인터넷사기, 사이버금융범죄 등 정보통신망을 이용해 저지른 범죄(정보통신망 이용범죄)는 15.3% 증가했다. 사이버음란물, 사이버도박 등 법이 금지하는 재화를 생산・유포하는 범죄(불법컨텐츠 범죄) 또한 8.1% 증가하였다.[190]

유형별 비중에서는 인터넷사기(11만 2,000건)가 전체 사이버범죄(14만 9,604건) 발생건수의 74.9% 로 가장 큰 비중을 차지하였다. 다음으로 명예훼손・모욕(1만 5,926건)이 전체 사이버범죄의 10.6%를 차지하였으며, 이외에 사이버금융범죄(5,621건), 저작권침해(3,856건), 사이버도박(3,012건) 등의 세부 유형이 사이버범죄의 주종을 이루고 있다.

경찰청 사이버안전국에서 분류한 사이버 범죄의 유형은 크게 세 가지로 분류된다. 정보통신망을 침해한 범죄와 정보통신망을 이용한 범죄 그리고 불법컨텐츠 범죄이다.

189) 경찰청, “2018년 사이버위협 분석 보고서”, p.4.
190) Ibid., p.4.

1) 정보통신망 침해 범죄[191]

정당한 접근 권한 없이 또는 허용된 접근 권한을 넘어 컴퓨터 또는 정보통신망(컴퓨터 시스템)에 침입하거나 시스템·데이터 프로그램을 훼손·멸실·변경한 경우 및 정보통신망(컴퓨터 시스템)에 장애(성능저하·사용불능)를 발생하게 한 경우[192]를 말한다. 주로 해킹, 서비스거부공격, 악성프로그램 3개 유형으로 나누고 이에 해당되지 않는 기타유형이 있다.

해킹은 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 행위[193]로 계정도용[194], 단순침입[195], 자료유출[196], 자료훼손이 포함된다. 서비스거부공격은 정보통신망에 대량의 신호, 데이터를 보내거나 부정한 명령을 처리하도록 하여 정보통신망에 장애(사용불능, 성능저하)를 야기한 경우이다. 악성프로그램은 정당한 사유 없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하는 경우를 말한다. 기타 정보통신망 침해형 범죄[197]는 정보통

---

191) 경찰청 사이버안전국 홈페이지.
http://cyberbureau.police.go.kr/prevention/sub2.jsp?mid=010201.

192) 고도의 기술적인 요소가 포함되며, 컴퓨터 및 정보통신망 자체에 대한 공격행위를 수반하는 범죄로, 정보통신망을 매개한 경우 및 매개하지 않은 경우도 포함

193) 컴퓨터 또는 네트워크와 같은 자원에 대한 접근제한(Access Control) 정책을 비정상적인 방법으로 우회하거나 무력화시킨 뒤 접근하는 행위.(사이버범죄 매뉴얼의 정의)고도의 기술적인 요소가 포함되며, 컴퓨터 및 정보통신망 자체에 대한 공격행위를 수반하는 범죄로, 정보통신망을 매개한 경우 및 매개하지 않은 경우도 포함

194) 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 타인의 계정(ID, Password)을 임의로 이용한 경우. 현재는 게임계정도용과 일반계정도용을 분리, 집계하고 있으나, 구분의 실익이 없으므로 계정도용으로 단순화

195) 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 컴퓨터 또는 정보통신망에 침입한 경우

196) 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 컴퓨터 또는 정보통신망에 침입 후, 데이터를 유출, 누설한 경우

197) 기타 정보통신망 침해형 범죄의 예

신망 침해형 범죄 중에서, 위 중분류 3개 항목(해킹, 서비스거부공격, 악성프로그램) 어디에도 유형별로 분류되지 아니하거나, 이전에는 없었던 신종 수법으로 정보통신망을 침해하는 범죄인 경우이다.

2) 정보통신망 이용 범죄[198]

정보통신망 이용 범죄는 정보통신망(컴퓨터 시스템)[199]을 범죄의 본질적 구성요건에 해당하는 행위를 행하는 주요 수단으로 이용하는 경우로 전통적인 범죄를 행하기 위하여 컴퓨터 시스템을 이용하는 범죄이다. 주로 인터넷 사용자간에 행해진다. 그 유형으로 인터넷 사기, 사이버금융 범죄, 개인위치 정보 침해, 사이버 저작권 침해, 스팸메일, 기타 정보통신망 이용 범죄가 있다.

인터넷 사기는 정보통신망(컴퓨터 시스템)을 통하여, 이용자들에게 물품이나 용역을 제공할 것처럼 기망하여 피해자로부터 금품을 편취(교부행위)한 경우이다.[200] 직거래사기[201], 쇼핑몰사기[202], 게임사

---

* 컴퓨터 등 장애 업무방해 (형법 제314조 제2항)
정보통신망(컴퓨터 네트워크)을 통하여, 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 업무를 방해한 경우. 단, 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 물리적인 방법으로 손괴하여 업무방해한 경우 사이버범죄에서 제외(망치로 컴퓨터 손괴 등)

* 타인 명의 공인인증서 발급 (전자서명법 제31조 제3호)
정보통신망(컴퓨터 네트워크)을 통하여, 타인의 명의로 공인인증서를 발급 받거나 발급 받을 수 있도록 한 경우

198) 경찰청 사이버안전국 홈페이지.
http://cyberbureau.police.go.kr/prevention/sub2_2.jsp?mid=010202.

199) 컴퓨터 시스템이란, 하나의 장치 또는 서로 접속되거나 서로 관련되어 있는 장치들의 그룹으로서, 이 중 하나 또는 그 이상의 장치가 프로그램에 의하여 자동적인 데이터처리를 수행하는 것(EU 사이버범죄 조약 제1조 정의)

200) 단, 온라인을 이용한 기망행위가 있더라도, 피해자와 피의자가 직접 대면하여 거래한 경우 등은 사이버범죄 통계에서 제외
※ on-line에서 기망행위 후, off-line에서 만나 현금·물품 편취는 제외
※ off-line에서 기망행위 후, on-line에서 대금을 송금 편취는 제외

201) 직거래사기 : 정보통신망(컴퓨터 시스템)을 통하여, 물품 거래 등에 관한 허위의 의사

기[203] 등이 있다. 사이버금융범죄는 정보통신망을 이용하여 피해자의 계좌로부터 자금 이체받거나, 소액결제가 되게 하는 신종 범죄를 말한다. 피싱[204], 파밍[205], 스미싱[206], 메모리해킹[207], 몸캠피싱[208] 등이 있다. 개인·위치정보 침해는 정보통신망(컴퓨터 시스템)을 통하여, 디지털 자료화되어 저장된 타인의 개인정보를 침해, 도용, 누설하는 범죄로, 정보통신망(컴퓨터 시스템)을 통하여, 이용자의 동의를 받지 않거나 속이는 행위 등으로 다른 사람의 개인·위치정보를 불법적으로 수집·이용·제공한 경우도 포함한다.[209] 사이버 저작권 침해는 정보통신망(컴퓨터 시스템)을 통하여, 디지털 자료화된 저작물 또는 컴퓨터프로그

표시를 게시하여 발생한 대금 편취 사기.

202) 쇼핑몰사기 : 정보통신망(컴퓨터 시스템)을 통하여, 허위의 인터넷 쇼핑몰 등을 개설하여 발생한 대금 편취 사기.

203) 게임사기 : 정보통신망(컴퓨터 시스템)을 통하여, 게임 캐릭터 및 아이템 등 인터넷 게임과 관련하여 발생한 대금 편취 사기

204) 피싱(Phishing) : 개인정보(Private data)와 낚시(Fishing)의 합성어
① 금융기관을 가장한 이메일 발송 ② 이메일에서 안내하는 인터넷주소 클릭, 가짜 은행사이트로 접속 유도 ③ 보안카드번호 전부 입력 요구 등의 방법으로 금융정보 탈취 ④ 피해자 계좌에서 범행계좌로 이체

205) 파밍(Pharming) : 악성코드에 감염된 피해자 PC를 조작하여 금융정보를 탈취하는 경우
① 피해자 PC가 악성코드에 감염 ② 정상 홈페이지에 접속하여도 피싱(가짜) 사이트로 유도 ③ 보안카드번호 전부 입력 요구 등의 방법으로 금융정보 탈취 ④ 피해자 계좌에서 범행계좌로 이체

206) 스미싱(Smishing) : 문자메시지(SMS)와 피싱(Phishing)의 합성어
① '무료쿠폰 제공' 등의 문자메시지 내 인터넷주소를 클릭하면, ② 악성코드가 스마트폰에 설치되어 ③ 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인 금융정보 탈취

207) 메모리해킹 : 피해자 PC 메모리에 상주한 악성코드로 인하여 정상 은행사이트에서 보안카드번호 앞·뒤 2자리만 입력해도 부당 인출하는 수법
① 피해자 PC가 악성코드에 감염 ② 정상적인 인터넷 뱅킹 절차(보안카드 앞·뒤 2자리) 이행 후, 이체 클릭 ③ 오류 반복 발생(이체정보 미전송) ④ 일정시간 경과 후, 범죄자가 동일한 보안카드 번호 입력, 범행계좌로 이체

208) 몸캠피싱 : 음란화상채팅(몸캠) 후, 영상유포하겠다고 협박하여 금전을 갈취하는 행위
① 타인의 사진을 도용하여 여성으로 가장한 범죄자가 랜덤 채팅 어플 또는 모바일 메신저를 통해 접근 ② 미리 준비해둔 여성의 동영상을 보여주며, 상대방에게 얼굴이 나오도록 음란행위 유도 ③ 화상채팅에 필요한 어플이라거나, 상대방의 목소리가 들리지 않는다는 등의 핑계로 특정파일 설치를 요구, 다양한 명칭의 apk파일로 스마트폰의 주소록이 범죄자에게 유출 ④ 지인의 명단을 보이며, 상대방의 얼굴이 나오는 동영상을 유포한다며 금전 요구

209) 속이는 행위(피싱)로 타인의 개인정보를 수집한 경우에도 사기의 실행의 착수에 나아가지 않은 경우 개인정보침해에 해당(정보통신망법 제49조의2 제1항)

램 저작물에 대한 권리를 침해한 경우이다. 스팸메일은 정보통신망(컴퓨터 시스템)을 통하여, 법률에서 금지하는 재화 또는 서비스에 대한 광고성 정보를 전송하는 경우 및 이와 관련 허용되지 않는 기술적 조치 등을 행한 경우이다.[210] 기타 정보통신망 이용형 범죄는 정보통신망(컴퓨터 시스템)을 이용하여 행하여진 범죄 구성요건의 본질적인 부분이 컴퓨터 시스템 또는 정보통신망(컴퓨터 시스템)에서 행해진 범죄 중, 위 5개 유형으로 분류되지 아니하는 경우이다.[211]

3) 불법컨텐츠 범죄

불법컨텐츠 범죄는 정보통신망(컴퓨터 시스템)을 통하여, 법률에서 금지하는 재화·서비스 또는 정보를 배포·판매·임대·전시하는 경우이다. 사이버음란물, 사이버도박, 사이버 명예훼손·모욕, 사이버스토킹 및 기타 불법컨텐츠 범죄로 구분한다.

사이버음란물은 정보통신망(컴퓨터 시스템)을 통하여, 음란한 부호·문언·음향·화상 또는 영상을 공공연하게 배포·판매·임대하는

---

210) 법률에서 금지하는 재화·서비스 전송의 경우이나, 이에 관련하여 허용되지 않는 기술적 조치에 대한 처벌 규정도 있는 점 감안하여, 불법 콘텐츠 범죄 항목이 아닌 정보통신망 이용 범죄로 포섭

211) 기타 정보통신망 이용형 범죄의 예

* 컴퓨터 등 사용사기 (형법 제347조의2)
정보통신망(컴퓨터 시스템)을 통하여, 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게함으로써, 재산상 이득을 편취하는 경우

* 전자화폐 등에 의한 거래 행위 (전자금융거래법 제49조 제1항 제7호, 9호)
정보통신망(컴퓨터 시스템)을 통하여, 다른 가맹점의 이름으로 전자화폐 등에 의한 거래를 한 경우
정보통신망(컴퓨터 시스템)을 통하여, 가맹점이 아닌 자가 가맹점의 이름으로 전자화폐 등에 의한 거래를 한 경우

* 정보통신망 인증 관련 위반 행위 (정보통신망법 제74조 제1항 제1호)
정보통신망(컴퓨터 시스템)을 통하여, 정보통신망의 인증을 받지 아니한 자가 그 제품이 표준에 적합한 것임을 나타내는 표시와 비슷한 표시를 한 제품을 판매 또는 판매 목적으로 진열한 경우

것으로 정보통신망법상 금지 규정만 있고 처벌 규정이 없다. 그러나 경찰청 사이버안전국에서는 심각한 사회적 문제가 되는 현실을 고려, 정책적 고려에 따라 사이버범죄로 포함하고 있다. 일반음란물[212]과 아동음란물[213]로 구분한다.

사이버도박은 정보통신망(컴퓨터 시스템)을 통하여, 도박사이트를 개설하거나 도박행위(또는 사행행위)를 한 경우이다. 주로 스포츠토토, 경마·경륜·경정 등의 인터넷시스템을 이용하여 도박을 행한다. 그러나 이또한 정보통신망법상 금지 규정만 있고 처벌 규정이 없고 심각한 사회적 문제가 되는 현실을 고려해서 사이버범죄에 포함되고 있다.

사이버 명예훼손은 정보통신망(컴퓨터 시스템)을 통하여, 다른 사람의 명예를 훼손하는 경우로 정보통신망법 제44조의 7 제1항 제2호의 적용을 받는다. 사이버모욕은 정보통신망(컴퓨터 시스템)을 통하여, 공연히 사람을 모욕하는 경우를 뜻한다.

사이버스토킹은 정보통신망(컴퓨터 시스템)을 통하여, 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 경우로 정보통신망법 제44조의7 제1항 제3호에 해당된다. 기타 불법 콘텐츠 범죄[214]는 위 4개 항목으로 분류

212) 일반음란물 : 정보통신망(컴퓨터 시스템)을 통하여, 일반 보통인의 성욕을 자극하여 성적 흥분을 유발하고 정상적인 성적 수치심을 해하여 성적 도의 관념에 반하는 내용의 표현물을 배포·판매·임대·전시하는 경우

213) 아동음란물 : 정보통신망(컴퓨터 시스템)을 통하여, 아동·청소년 또는 아동·청소년으로 명백하게 인식될 수 있는 사람이나 표현물이 등장하여 성교 행위, 유사 성교 행위, 일반인의 성적 수치심이나 혐오감을 일으키는 행위, 자위 행위를 하거나 그 밖의 성적 행위를 하는 내용의 표현물을 배포·판매·임대·전시하는 경우 (아동·청소년의 성보호에 관한 법률 제2조 정의 참조)

되지 않은 경우이다.

4.3 사이버테러 대응 제도

한국의 사이버안보 컨트롤타워 기능은 청와대 국가안보실에 있다. 이를 위하여 사이버안보 비서관을 국가안보실에 두고 있으며, 유관부처 차관급이 참석하는 사이버안보정책조정협의회를 통해 사이버안보 분야의 주요 정책을 수립조정하고 있다.[215]

1) 국가정보원

국가정보원은 ‘국가정보원법’, ‘정보통신기반보호법’, ‘전자정부법’ 등 관계법령에 근거 하여 국가 정보보안 업무의 기획·조정 및 보안정책 수립·시행 등 국가·공공기관에 대한 사이버안보 업무를 총괄하고 있다. 특히 2005년 1월 제정한 ‘국가사이버안전관리규정’(대통령훈령 제316호, 2013. 9. 2. 개정)에서 국가의 사이버안전과 관련된 정책 및 관리에 대하여 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하도록 규정하였다.[216]

국가정보원은 2003년 1.25 인터넷대란 발생 등을 계기로 국가

214) 기타 불법 콘텐츠 범죄의 예
* 청소년유해매체물 미표시·영리목적 제공, 청소년 유해 매체물 광고, 공개전시
- 정보통신망(컴퓨터 시스템)을 통하여 유통되는 매체물 중에서, 청소년 유해 매체물 미표시·영리목적 제공 또는 광고·공개 전시하는 경우(정보통신망법 제73조 제2, 3호)
* 허위주민번호 생성, 이익을 위해 사용 (주민등록법 제37조 제1호)
- 정보통신망(컴퓨터 시스템)을 통하여, 거짓의 주민등록번호를 만들어 자기 또는 다른 사람의 재물이나 재산상 이익을 위하여 사용한 경우
* 허위주민번호 생성 프로그램 타인 전달·유포 (주민등록법 제37조 제4호)
- 정보통신망(컴퓨터 시스템)을 통하여, 거짓의 주민등록번호를 만드는 프로그램을 다른 사람에게 전달하거나 유포

215) 국가정보원, “2018년 국가정보보호백서”, 2018, p.53.

216) Ibid., p.55.

차원의 사이버공격에 대한 종합적·체계적인 예방·대응을 위해 전담 조직을 운영하라는 당시 노무현 대통령의 특별 지시에 따라 2004년 2월 국가사이버안전센터(NCSC, National Cyber Security Center) 를 발족하였다.[217]

국가정보원은 국가 사이버안전 정책 수립, 국가 사이버안전 전략회의 및 대책회의 운영, 국가·공공기관 정보시스템의 보안대책 수립·지원, 각급기관 정보통신망 보안진단·평가 등 안전성 확인, 사이버공격에 대한 국가차원의 탐지·대응체계의 구축 운영, 국가안보를 위협하는 사이버공격에 대한 조사·분석 및 검·경·군 기무사와의 공조, 사이버위기 경보 발령, 공공분야 주요정보통신 기반시설 보호업무, 국가·공공기관용 암호장비 등 보안시스템의 개발·보급, 사이버안보 관련 해외 정보·보안기관과의 정보협력 등을 통해 사이버안보 총괄기관의 역할을 담당하고 있다. 또한 정보공유 활성화 및 공조체계 강화를 위해 국가사이버 안전센터에 유관기관이 참여하는 '민·관·군 사이버위협 합동대응팀'을 운영하고 종합판단·정보공유·합동분석·합동조사 등 4개 분야의 합동업무를 수행하고 있다.[218]

2) 경찰청 사이버안전국

경찰청 사이버안전국은 1997년 컴퓨터범죄수사대 창설에서 시작되었다. 1999년 사이버범죄수사대로 개편하고 2000년 사이버테러 대응센터로 확대되었다. 2014년 6월 사이버안전국으로 확대 개편하였다. 그동안 사이버안전국은 인터폴 IT 범죄수사 협의체 회의 및 국제 사이버테러 대응 공동심포지엄을 개최하는 등의 활동을 하였다. 그리고 2005

217) Ibid., p.55.
218) 국가정보원, "2018년 국가정보보호백서", 2018, pp.55-56.

년 10월 영국 하이테크범죄 대책단과 협력약정 체결을 시작으로 동년 11월 프랑스 정보통신기술범죄 대응센터, 2006년 11월 미국 FBI 사이버수사부, 2007년 독일 연방범죄수사청 중대범죄조직국과 협력약정을 체결하였다.[219]

3) 과학기술정보통신부

과학기술정보통신부는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '국가정보화 기본법', '전자서명법', '정보통신기반 보호법', '정보보호산업의 진흥에 관한 법률' 등 관계 법령에 근거하여 정보보호 업무를 수행하고 있다. 특히 민간 정보보호에 관한 정책의 수립·조정, 주요정보통신기반시설의 지정권고 및 총괄, 민간 분야 침해사고 예방·대응체계의 구축 및 운영, 전자인증 관련 정책의 수립·조정, 정보보호산업 관련 주요 정책의 수립 등 민간 정보보호 및 정보보호 산업 업무를 총괄하고 있다.[220]

정부는 2013년 3월 행정안전부·지식경제부·방송통신위원회에 나뉘어 있던 정보보호에 관한 업무를 미래창조과학부로 이관함으로써 사이버보안 위협에 대한 선제적 대응체계를 만들었으며, 2017년 문재인 정부 출범에 따라 과학기술정보통신부로 개편하였다.[221]

4) 한국 인터넷진흥원

한국인터넷진흥원(KISA, Korea Internet and Security Agency)은 '정보통신망 이용촉 진 및 정보보호 등에 관한 법률' 제52조에 의거하

219) 경찰청 사이버안전국 홈페이지.
http://cyberbureau.police.go.kr/bureau/sub3.jsp?mid=040300.
220) 국가정보원, "2018년 국가정보보호백서", 2018, p.57.
221) Ibid., p.57.

여 정보통신망의 고도화 및 안전한 이용 촉진, 정보통신망의 이용에 따른 역기능 분석 및 대책연구, 인터넷주소자원 관리 등을 목적으로 설립된 인터넷 및 정보보호 진흥기관이다. 한국 인터넷진흥원은 민간 분야 사이버 침해 사고 예방 및 대응, 개인정보보호 및 피해 대응, 정보보호산업 및 인력양성, 정보보호 대국 민서비스, 국가도메인(.kr/.한국) 서비스, 불법스팸 관련 고충처리 등의 업무를 수행한다. 또한 인터넷 진흥과 정보보호의 조화를 통해 국가의 글로벌 경쟁력을 확보하고 사회의 미래가치 창출을 선도하고자 노력하고 있다.[222]

특히 인터넷 침해사고를 예방하고 대응하기 위하여 365일 24시간 인터넷 이상 징후를 실시간 모니터링하고, 디도스(DDoS) 대응시스템 및 사이버대피소를 구축·운영하며, 주요 취약점을 모니터링하여 보안권고문을 배포하고 있다. 피싱(phishing)·파밍(pharming)·스미싱(smishing) 등 전자금융 사기에 대한 국민들의 피해 예방 및 대응 활동을 전개하고 있다. 그리고 사이버위협에 선제적으로 대응하기 위하여 국내외 관계기관과 '글로벌 사이버보안 협의체'를 구축하여 공조체계를 강화하고 있다.[223]

5) 인터넷침해대응센터

인터넷침해대응센터(KISC, Korea Internet Security Center)는 2003년 12월 인터넷침해사고대응지원센터로 개소하고, 2009년 한국인터넷진흥원이 통합 출범함에 따라 인터넷 침해대응센터로 명칭을 변경하였다. 인터넷침해대응센터는 국내 인터넷 침해사고 사전예방 및 침해사고 발생시 신속대응으로 피해를 최소화하기 위하여 다양한 업무를

222) 국가정보원, "2018년 국가정보보호백서", 2018, p.68.
223) Ibid., p.68.

수행하고 있다. 특히 종합상황실을 통해 국내 주요 통신사업자 및 보안관제업체와 연계하여 365일 24시간 인터넷트래픽의 이상 징후를 모니터링하고, 보안 취약점 및 악성코드 등 보안위협에 대한 정보를 수집·분석하고 있다. 한편, C-TAS를 통해 상시적으로 침해사고 정보를 공유하여 침해사고로 인한 사회적·경제적 손실을 최소화하고자 노력하고 있다.[224]

224) 국가정보원, '2018년 국가정보보호백서', 2018, p.69.

제5장 결 론

전 세계는 사이버 테러에 대응하기 위해 국내 법제도를 정비하고 대응책을 마련하는데 다양한 노력을 기울이고 있다. 그러나 사이버테러의 초국가적인 특징과 사이버공간이 가지는 특수한 성격 때문에 한 국가의 법제도 및 정책만으로는 충분히 사이버테러에 대응할 수 없다. 그러므로 각 국은 국제협력 및 공조를 위해 다자간, 양자간 협력을 추진하고 국제규범 마련에 적극적으로 참여하고 있다.

그러나 이러한 각 국의 대내외적인 노력에도 불구하고 아직 사이버테러에 대한 공통된 정의나 합의된 국제규범은 부재한 현실이다. 각 나라가 추구하는 국가 이익이 다르고 상이한 가치관에 따라 국제적인 합의는 요원하다. 사이버테러 대응에 있어서 국제협력의 필요성은 공감하지만 각 국의 전략 및 상황은 제약요인이 되고 있다.

한국은 주로 북한으로부터의 사이버위협 및 공격에 대응하기 위해 많은 노력을 기울여 왔다. 그리고 북한의 사이버공격은 주로 중국을 경유하여 진행되었다. 제3국을 경유한 사이버공격은 그 진원지를 파악하더라도 관할권의 문제로 인해 외교적인 역량이 대응에 필수적이다. 양국의 신뢰구축 및 제도적 뒷받침이 없으면 실질적인 사이버테러 대응에 취약점은 해결할 수 없다.

한편으로 중국은 미국과의 사이버공간에서 거버넌스 및 표준화 경쟁을 하고 있다. 중국은 사이버공간에서 한・미・일 동맹이 형성되는 것을 바라지 않는다. 또한 한국은 미국과의 높은 사이버협력 단계

에 있는 나라이지만 ICT 발전지수가 높고 정보기술산업이 상당히 발달한 경제적으로 매력적인 나라이다. 사이버 관련 기술은 경제와 밀접하게 연결되어 있으며 사이버테러 대응 기술은 곧 정보기술산업의 수준을 반영한다.

한중 양국은 협력 필요성은 공감하지만 사이버테러 대응에 관한 법제도와 전략의 차이점과 공격주체에 대한 인식의 상이점 그리고 미국과 북한 변수로 인해 협력은 낮은 단계에서 진행되는 한계가 있다. 이에대한 지속적인 연구는 과제로 남는다.

제6장 참고문헌

국내자료

[1] 경찰청, “2018년 사이버위협 분석 보고서”, 2018.
[2] 곽관훈, “사이버테러 방지에 관한 일본의 법제도 및 시사점”, IT와 법연구, 2014.
[3] 국가정보원, “2018년 국가정보보호백서”, 2018.
[4] 김상배, “버추얼 창과 그물망 방패”, 한울 아카데미, 2018. 2.
[5] 김영환, “사이버범죄에 대한 국가적 대응체계 구축의 이론적 함의-사이버테러형 범죄를 중심으로”, 한국 컴퓨터정보학회 논문지, 2009.
[6] 김재윤, “사이버전 대책 및 개선방안”, 2012년 국정감사 정책자료집, 2012.
[7] 김태계, “사이버테러 범죄 대응에 관한 제도적 문제점과 대책”, 법과 정책연구, 2014.
[8] 김흥석, “사이버테러와 국가안보”, 한국법학원, 2010.
[9] 남길현, “사이버테러와 국가안보”, 국방연구, 2002.
[10] 박기갑, “사이버전쟁 내지 사이버공격과 국제법”, 국제법평론, 2010.
[11] 박용숙, “중국의 네트워크 안전법에 대한 일고찰”, 강원법학 53, 2018.
[12] 오길영, “사이버테러의 대응체제의 문제점과 개선방향”, 민주법학, 2014.
[13] 유동열, “사이버공간과 국가안보”, 북앤피플, 2012.
[14] 윤민우, “새로운 안보환경을 둘러싼 사이버테러의 위협과 대응방안”, 한국경호경비학회지, 2014.
[15] 윤영환, “사이버범죄의 실태와 대응방안”, 한국행정과 정책연구, 2004.
[16] 윤해성, “사이버 테러의 동향과 대응방안에 관한 연구”, 한국형사정책연구원, 2012.
[17] 이갑헌, “첩보에서 정보까지”, 형설출판사, 2010.
[18] 이근욱, “왈츠 이후 : 국제정치이론의 변화와 발전”, 한울 아카데미, 2016.
[19] 이병종, “테크놀로지 발전에 따른 사이버범죄의 진화와 범죄현상의 조명 및 대응”, 한국공안행정학회보, 2010.
[20] 이성식, “사이버범죄와 시민의 역할”, 정보화정책, 2006.
[21] 이황우, 한상암, “대테러 정책론”, 진명문화사, 1996.
[22] 정용기, “위험사회에서의 사이버 테러 대응방안”, 성균관법학, 2014.
[23] 정준현, 지성우, “국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구”, 미국헌법연구, 2009.
[24] 조민상, “사이버침해 사례분석을 통한 위기대응방안”, 한국민간경비학회보, 2013.
[25] 조윤영, 정종필, “사이버안보를 위한 중국의 전략- 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로”, 21세기정치학회보, 2016.

[26] 조정은, “사이버테러 대응법제에 관한 연구”, 토지공법연구, 2016.
[27] 조현빈, “현행법상 사이버테러의 규제 가능성에 대한 검토”, 한국위기관리논문집, 2008.
[28] 조현석, “중국 사이버안보 전략의 통합적 접근”, 한국위기관리논집, 2017 vol.13.
[29] 주문호, 권헌영, 임종인, “주요국 사이버보안 거버넌스 분석과 정책적 시사점”, 정보보호학회논문지, 2018.
[30] 하영선 외 15인, “변환의 세계정치”, 을유문화사, 2012.
[31] 한희, “사이버 공간과 국가안보”, 2014년 국가안보전략연구소 학술회의, 2014.

국외자료

[1] Adam Segal, “The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age”, New Public Affairs, 2016.
[2] Amy Chang, “Warring State: China's Cybersecurity Strategy”, Center for a New American Security, 2014.
[3] Association of The United States Army, https://www.ausa.org/events/ilw-rogers-strategic-issues-forum.
[4] Barry Buzan, “People, States and Fear : An Agenda for International Security Studies in the Post-Cold War Era”, 2nd ed., Lynne Rienner Publisher, 1991, pp.118-119.
[5] Barry Buzan, Ole Wæber, Jaap de Wilde, “Security : A New Framework for Analysis”, Lynne Rienner Publisher, 1998, pp.21-23.
[6] Bloomberg, “Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar”, Dec. 10, 2014,
[6] Christian Hacke and Jana Puglierin, “John H. Herz: Banlancing Utopia and Reality”, September, 2007, International Relations 21.
[7] Congress, “US Freedom Act of 2015”, Apr 28, 2015.
[8] David Albright, Paul Brannan and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?”, Institute for Science and International Security Report, Dec. 22, 2010.
[9] Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”, Special Reports, 2001.
[10] Glenn H. Snyder, “The Security Dilemma in Alliance Politics.”,

World Politics , 1984.
[11] Harvey Rishikof and Kevin Lunday, “Corporate Responsibility in Cybersecurity : Building International Global Standards”, Georgetown Journal of International Affairs, Vol.12, 2011.
[20] Herbert Butterfield, “History and human relations”, Macmillan. 1951.
[21] House Republicans, “Federal Information Security Amendments Act of 2013”, Apr 13, 2013.
[22] Internet Assigned Numbers Authority, “Root Servers”.
[23] James A. Lewis, “National Perception of Cyber Threats”, strategic Analysis, Vol. 28, 2014.
[24] Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, International Studies Quarterly 53, 2009.
[25] Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity”, The American Journal of International Law, Vol.110, 2016.
[26] Matt McDonald, “Securitization and the Construction of Security”, European Journal of International Relations, December 2008, pp.563-587.
[27] Neil Weinstock Netanel, “Cyberspace Self-Governance : A Skeptical View form Liberal Democratic Theory”, California Law Review, Vol.88, 2000.
[28] Ole Wæver, Barry Buzan, Morten Kelstrup, Pierre Lemaitre “Identity, Migration and the New Security Agenda in Europe”, Pinter Publisher, 1993. p.23.
[29] Robert Jervis, “Perception and Misperception in International Politics”, Princeton University Press, 1976.
[30] Scott J. shackelford, “Toward Cyberspace : Managing Cyber-attacks through Polycentric Governance”, American University Law Review.
[31] Sharon Weinberger, “U.S. Also Vulnerable to Stuxnet Virus, Official Warns”, AOL News, 2010.12.07.
[32] The Christian Science Monitor, “Ukraine election narrowly avoided ‘wanton destruction’ from hackers”, Jun. 17, 2014.
[33] The Department of Defense, “Department of Defense strategy for Operating in Cyberspace”, July 2011.

[34] The Department of Defense, “The 2014 Quadrennial Defense Review”, Mar 4, 2014.
[35]) The Department of Defense, “The Department of Defense Cyber Strategy”, Apr 17, 2015.
[36] The Department of Defense, “The Department of Defense Strategy for Operations in the Information Environment”, Jun 2016.
[37] The New York Times, “Sowing Doubt Is Seen as Prime Danger in Hacking Voting System”, Sept. 14, 2016.
[38] The White House, “Cybersecurity National Action Plan”, Feb 09 2016.
[39] Thomas J. Christensen and Jack Snyder, “Chain Gangs and Passed Bucks : Predicting Alliance Patterns in Multipolarity.”, International Organization, 1990.
[40] United States of Senate, “Cybersecurity Information Sharing Act of 2015”, Mar 3, 2015.
[41] William Gibson, “Neuromancer”, July 1, 1984, Ace Books.
[42] 蔡翠红，“网络空间的中美关系：竞争、冲突与合作”美国研究，2012年3期.
[43] 蔡翠红，“国家-市场-社会互动中网络空间的全球治理”，世界经济与政治，2013年9期.
[44] 蔡翠红，“美国网络霸权对中国国家安全的影响及对策”，国际问题研究，2014年1期.
[45] 储殷，“网络全球治理正在进入中国时代，中国信息安全，2016年1期.
[46] 郎平，“全球网络空间规则制定的合作与博弈”，国际展望，2014年6期.
[47] 李恒阳，“斯诺登事件与美国网络安全政策的调整“，外交评论，2014年3期.
[48] 刘宁、郎平，“不同议题下的中美网络安全关系：合作、竞争与冲突”，战略决策研究，2017年第2期.
[49] 罗伯特·基欧汉，约瑟夫·奈，“权力与相互依赖”，门洪华译，北京大学出版社，2014年.
[50] 沈逸，“美国国家网络安全战略的演进及时间”，美国研究，2013年3期.
[51] 檀有志，“跨越修昔底德陷阱：中美在网络空间的竞争与合作”，外交评论，2014年5期.
[52] 王孔祥，”网络安全的国际合作机制探析“，国际论坛，2013年9月.
[53] 吴则成，“美国网络霸权逻辑与中国防御性网络安全战略构建”，湖南师范大学社会科学学报，2014年4期.
[54] 于志刚，“缔结和参加网络犯罪国际公约的中国立场”，政治论坛，2015年9月.
[55] 蒋丽、张小兰、徐飞彪，“国际网络安全合作的困境与出路”，现代国际关系，2013年9月.

[56] 国家互联网信息办公室，“习近平总书记在网络安全与信息化工作座谈会上的讲话”，2016年4月19日.
[57] 国务院新闻办新闻发布厅，“国家信息化发展战略纲要”，2016年7月27日.
[58] 新华社，“关于经济建设和国防建设融合发展的意见”，2016年7月21日.
[59] 中国外交部，“信息安全国际行为准则”，2015年3月5日.
[60] “中华人民共和国国民经济和社会发展第十个五年规划纲要”，2001.
[61] “中华人民共和国国民经济和社会发展第十一个五年规划纲要”，2006.
[62] “2006-2020年国家信息化发展战略”，中共中央办公厅， 2006.5.8.
[63] “国家网络空间安全战略全文”，2016. 12. 27.