2019 여름 | 제 19권 2호(통권74호)

ISSN 2466-2259

국가안보와 전략

NATIONAL SECURITY AND STRATEGY

INSS
INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

2019 여름 | 제19권 2호(통권74호)

국가안보와 전략

NATIONAL SECURITY AND STRATEGY

INSS
INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

국가안보와 전략

2019년 여름 | 제19권 2호(통권74호)

편집위원: 채재병(위원장, 전략연), 김일기(전략연), 유현정(전략연), 이수석(전략연),
김영호(국방대), 문경연(전북대), 박원곤(한동대), 손병권(중앙대),
정구연(강원대), 조동준(서울대), 조한승(단국대), 한인택(제주평화연)

발행처: 사단법인 국가안보전략연구원
발행인: 조동호
주 소: 서울특별시 강남구 언주로 120
인스토피아 빌딩 13-18층
전 화: (02)6191-1000, FAX:(02)6191-1111
E-mail: publication@inss.re.kr

인쇄일: 2019년 6월 25일
발행일: 2019년 6월 30일

* 국가안보전략연구원은 2016년 봄호부터 『국제문제연구』를 『국가안보와 전략』으로 제호를 변경해서 연속 발행합니다. 본지에 실린 내용은 집필자 개인의 견해이며 본 연구원의 공식입장이 아닙니다.

Contents 국가안보와 전략

2019 여름 제19권 2호(통권74호)

Ⅰ 사이버안보 위협, 대응 전략 그리고 한국적 함의 1

장노순 (한라대학교)

1. 문제 제기
2. 사이버안보의 특징
3. 사이버 위협과 대응전략
4. 한국 국가사이버안보전략의 전략적 함의
5. 결 론

Ⅱ 국제정치학적 관점에서의 사이버안보 논의와 국가차원의 대응전략 37

홍석훈 (통일연구원)

1. 서 론
2. 사이버안보의 중요성과 우리 정부의 대응체계
3. 국가차원의 사이버안보 강화를 위한 전략
4. 결 론

Ⅲ ‘중국 특색 국제정치이론’ 논의의 출현과 향후 전망 77

함명식 (지린대학교)

1. 서 론
2. 중국 특색 국제정치이론의 등장 배경, 전개 과정, 특징
3. 중국 특색 국제정치이론의 사례
4. 중국 특색 국제정치이론의 한계
5. 결 론

Ⅳ 트럼프 정부의 2017 대북 선제공격 위협의 실효성 평가 115
: 미국의 과거 선제공격 사례 시사점을 중심으로

박창권 (한국국방연구원)

1. 머리말
2. 미국의 선제공격 고려시 주요 고려요소 및 조치사항
3. 미국의 선제공격 사례
4. 미국의 선제공격 사례의 주요 특성과 시사점
5. 트럼프 정부의 대북 선제공격 위협의 실효성 평가
6. 결 론

I

사이버안보 위협, 대응 전략 그리고 한국적 함의

장노순 (한라대학교)

1. 문제 제기
2. 사이버안보의 특징
3. 사이버 위협과 대응전략
4. 한국 국가사이버안보전략의 전략적 함의
5. 결 론

Summary

사이버 공간은 안보 위협 측면에서 확장성과 복잡성이 크게 강화된 특징을 보여준다. 이에 따라 사이버안보의 위협이 전략적 목적에 따라 전통적인 방식과 다르게 제기되고 있다. 사이버전, 사이버 강압전략, 사이버 첩보활동, 공급망선도전략은 대표적인 유형이고, 이에 대한 대응 전략으로 적극적 방어전략, 사이버 강압대응전략, 사이버 방첩전략, 공급망안보전략이 강구되고 있다. 사이버전이나 사이버 첩보활동은 오랫동안 사이버안보 위협으로 강조되었고, 강압전략이나 공급망선도는 국제안보질서에 주요 위협 방식으로 최근 대두되고 있다. 이런 상황에서 한국 정부는 금년 초에 '국가사이버안보전략'을 발표했다. 이 전략에서 사이버안보 위협에 대한 대응 기조는 종합적이고 포괄적인 내용을 담고 있지만 억제와 예방전략을 채택하고 있다. 하지만 억제전략의 효과는 공개 천명만으로는 기대하기 어렵고, 그에 따른 구체적인 실행 의지와 역량이 필요하고 구체적인 실행의 경험도 담보되어야 한다. 국제사회와 우방국의 협조와 지원 없이는 매우 제한적인 효과만을 기대할 수 있다. 즉, 국가사이버안보전략의 발표는 국내 정책과 제도로 뒷받침되어야 하고, 대외적으로는 실질적인 대응 여건이 갖추어져야 한다.

| **주제어** | 사이버안보, 대응 전략, 사이버 강압, 공급망안보, 국가사이버안보 전략

1. 문제 제기

새로운 기술의 등장으로 무기 체계가 획기적으로 발전하게 된다면, 국제안보는 불확실성이 증대하고 국가 간 갈등과 분쟁의 가능성이 높아진다. 국가안보를 위협하는 무기는 기존의 세력분포에 변화를 초래하고, 그에 따른 안보전략과 국가 간 협력의 방식이 바뀐다. 정보통신기술의 빠른 발전은 안보 행위자들의 역량 강화, 비용 감소, 연계성 증대로 요약되고, 이로 인해 사이버안보환경을 새롭게 조성하고 있다.[1] 사이버 공간에서는 국가와 사회의 거의 모든 활동을 연계하면서 국가안보의 연관성이 다층적으로 연결되어 작동한다. 군사 작전, 경제활동, 사회 시스템의 유지, 개인의 생활은 사이버 공간을 배제하고는 기대하는 목적을 달성하거나 정상적인 운용이 불가능할 정도에 이르렀다. 정보통신 기술이나 네트워크는 재래식 군사력이나 핵무기처럼 특정 국가의 압도적인 우위를 보장하고 있지 않다. 글로벌 사이버안보환경은 완벽한 진공 상태라 하기 어렵지만, 사이버안보의 국제규범과 안보전략이 안정적인 방식으로 확보될 수 있을지는 아직까지는 진행형이라 할 수 있다. 그 여파를 충분히 가늠하기 어려운 불확실성이 높다.

국제안보질서를 주도하고 있는 미국은 사이버 위협에 가장 많이 노출된 강대국으로 이에 대한 심각성을 꾸준히 인식하고 이를 강조해왔다. 미국 의회와 정보기관, 백악관 등은 사이버 위협을 미국의 안보위협에 가장 심각한 요소로 간주한다. 미국 국가정보국은 2017년 전세계위협평가보고서(2017 Worldwide Threat Assessment)에서 미국의 안보 위협 요소로 사이버 위협을 가장 상위에 배치했고, 테러 혹은 대량살상무기의 위협보다 더 심각하게 평가했다. 중국과 러시아 역시 사이버안보의 중요성을 오래 전에 인식하고, 이에 대한 안보 및 기술발전 전략을 발전시켜왔다. 상당한 수준의 사이버 공격력을 보유한 것으로 추정되는 이란, 북한, 이스라엘은 사이버 공격을 통해 정치, 군사, 경제적 목적을 달성하기도 했다.

---

1) Bruce D. Berkowitz and Allan E. Goodman, *Intelligence in the Information Age* (Yale University Press, 2000), pp.13-18.

2000년대 들어서면서 사이버안보 위협의 심각성이 크게 주목을 받기 시작하였고, 중반에는 학술과 정책적 관심이 본격적으로 나타나기 시작했다.[2] 하지만 오래 전부터 미국방부 장관이었던 레온 파네타가 경고했던 사이버 진주만기습(Cyber Pearl Harbor)이나 사이버 9/11(Cyber 9/11)과 같은 재앙적인 사이버 공격이 벌어지지 않았다. 과거 핵무기 도래와 비교하면, 사이버안보 위협의 성격이 확연히 다르다는 점은 분명하다. 10여 년 전부터 심각한 사이버 공격이 현실화되는 사례들이 등장했고, 파괴 목적으로 사이버 무기가 활용된 명확한 공작활동이 성공을 거두었다. 사이버 위협의 방식과 범위는 전통적인 안보에서 결코 기대될 수 없는 수준으로 확대되고 있고, 한국을 포함한 선진 국가들은 이에 대한 전략과 정책을 만족할만한 수준으로 갖추지 못한 상태이고, 국제사회 역시 규범적 제도화에 빠른 진전을 보여주고 있지 못하다.

본 연구는 사이버안보의 위협이 전략적 목적에 따라 여러 방식으로 등장하고 있는 특징을 분석하고, 이에 대응하는 전략의 유형을 설명하려고 했다. 이런 사이버 위협과 대응 전략을 바탕으로 한국 사이버 전략의 방향을 모색하고자 했다. 국내에서의 네트워크 방어수단과 대응체계에 대한 논의보다는 잠재적인 사이버 위협세력의 공격을 억제하고 예방하기 위한 전략의 효과를 분석할 것이다.

2. 사이버안보의 특징

가. 사이버안보의 확장성

국제사회가 사이버공간에서 제기되고 있는 안보 위협과 관련해서 안보질서의 의미, 위협의 수단과 방식, 국제규범의 발전 등 커다란 변화를 이미 경험하고 있는 상황이다. 글로벌 사이버안보환경은 증폭적인 위협의 방식과 다양한 전략

2) Sharp Travis, “Theorizing Cyber Coercion,” *Journal of Strategic Studies*, Vol.7, No.7 (2017), pp.898-899.

적 목적으로 전통적인 안보위협의 일관성과 제한성을 유지하기 힘들다. 사이버 안보의 특징은 전통적인 안보와 비교하면 안보 위협의 확장성이다. 안보 확장성은 국가안보에 영향을 미치는 위협의 영역과 위협의 방식에서 전통 안보의 범위를 넘어서 확대했음을 지적한 것이다.

첫째, 비군사 영역의 안보 의미로 확장성이다. 비물리적 결과(non-kinetic)를 초래하는 국가안보의 위협으로 평가된다. 전통적인 국가안보의 위협은 군사 공격으로 물리적 파괴와 인명 손실의 엄청난 피해를 동반하는 결과를 전제하고 있다. 영토와 주권 보호는 군사 위협으로부터 방어하려는 가장 핵심적인 전략적 가치이다. 사이버 위협에 대한 초기 관심은 사이버 무기를 군사 무기로써의 활용에 집중되어 있었다. 일부에서 예상했던 것처럼, 사이버 역량의 확산은 사이버전의 양태로 이어지지 않았다. 아주 제한된 조건에서 저비용으로 군사, 정치 혹은 전략적 목적을 위해 사이버전 역량이 이용될 수 있지만, 광범위한 활용의 가능성은 높지 않다.[3] 사이버안보 위협은 그런 군사적 공격에 따른 파괴와 다른 차원의 안보 위협으로 제기되고 있다.

둘째, 외교의 강압적 수단으로 사이버 역량이 활용된다. 외교는 상대국가와 협상을 통해 상호의 요구를 타협하는 과정이고 방식이다. 국제정치에서 강압은 자국의 요구를 받아들이도록 상대방을 설득하기 위해 '피해를 줄 수 있는 힘'으로 정의될 수 있다.[4] 피해를 줄 수 있는 힘은 경쟁국가에게 위협을 하거나, 실제로 위협을 보여주는 낮은 수준의 행동까지를 포함한다. 강압이 상대방의 적대적인 대응을 초래하여 확전되는 상태가 전쟁이다. 외교의 강압 수단으로 경제제재, 외교 고립, 지원 중단 혹은 군사 공격의 위협 등은 상대방이 상당한 피해를 입을 수 있음을 설득하는 전통적인 방식이다. 강압은 무자비한 물리력의 사용과 대비된다. 막대한 군사력을 동원한 물리력은 상대방을 군사적으로 제압하고 적대국에 대해 정치적 해결방안을 강요하는 것을 목적으로 동원된다. 강압의

---

3) Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'?" *The Journal of Strategic Studies*, Vol.35, No.3 (June 2012), pp.401-428.

4) Thomas C. Schelling, *Arms and Influence* (Yale University Press, 1966), p.2.

궁극적인 목적은 강압의 대상국이 저항하거나 반격할 수 있는 군사력을 갖추고 있지 않다고 하더라도, 적대국과 무력 충돌보다는 자국의 요구에 양보하여 정치적 타협점을 모색하는 것이 더 유리하도록 인식을 바꾸는 것이다. 핵무기의 도래는 강압 전략의 효과를 확보하는데 기존의 어떤 무기체계보다 적절한 수단이다.

사이버 무기는 핵무기와 달리 사이버 강압의 효과를 확보하는 용도로 그 의미가 크게 증대하고 있다. 핵무기는 핵전쟁이나 재래식 무력충돌의 심각한 위험을 내포하고 있지만, 사이버안보 위협은 강압 외교의 수단으로 다양한 활용도를 보여주고 있다. 사이버 무기는 무력 충돌의 확전으로 이어질 가능성이 상대적으로 낮고, 상대방이 보복을 위해 비례성을 지키면서 적절하게 상응한 수단을 찾기도 어렵다. 이런 이유로 사이버 무기는 재래식 무기와 달리 강압의 수단으로써 그 활용 범위를 넓혀가고 있다. 특히 사이버 수단은 핵무기나 재래식 군사공격처럼 민간인의 심각한 피해를 부작용으로 일으키지 않기 때문에 활용될 여지가 높으면서도, 군사력 우위를 지닌 상대방의 보복을 피할 수 있다.[5)]

셋째, 디지털 기술의 이중 용도는 과거의 군사 수단으로 활용되는 기술에 비해 안보 위협의 대상과 범위가 월등히 넓다. 생화학 무기나 핵무기와 같이 이중 용도의 기술보다 일상생활에서 사이버 기술의 활용성이나 미래의 활용 잠재력은 안보 위협의 요인으로 작용할 가능성이 훨씬 높다. 산업 발전이나 사회의 안전으로 간주되었던 요소들이 국가안보의 심각성으로 평가될 여지가 넓어졌다. 네트워크나 컴퓨터 기술의 원천은 단순히 미래 산업 경쟁력만을 의미하지 않는다. 네트워크 장비나 소프트웨어는 첩보수집이나 사이버 공격의 수단이 된다. 개별 국가의 산업 기반이 되고 국제 연결성이 높다는 점에서 각 국가의 정책 선택이고 국가간 공조 문제가 대두되고 있다.

이런 관점에서 미국과 중국이 5세대 통신기술을 둘러싸고 벌이는 대립은 기술 패권 경쟁이다. 기술 패권은 사이버안보의 틀로 확장되어 자국의 정책을 정당화하고 있다. 국제 통신장비시장에서 수요자는 제품의 비용과 성능만을 고려

5) Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol.26, No.3 (2017), p.454.

하여 구매를 결정하지 않는다. 정보통신분야는 미래 산업의 근간이고, 사회 발전의 많은 영역에 영향을 미칠 수밖에 없기 때문에, 기술 패권국의 지위는 국가의 위상과 안보의 수준을 결정하게 된다. 기술 패권국은 기술적 우위를 바탕으로 타국가의 사이버 기반시설을 구축할 수 있다면 수출국의 안보 활용 가능성이 있고, 상대방의 국가안보 취약성은 높아진다.

나. 사이버안보의 복잡성

사이버안보의 복잡성은 사이버 위협의 행위자와 위협의 전략적 목적이 전통적인 안보의 성격에 비해 훨씬 복잡한 특성을 의미한다. 사이버안보는 국가의 독점적 지위가 전혀 허용되지 않는 영역이다. 사이버안보의 위협 수준에 따라 국가는 비국가 행위자가 쉽게 극복하기 어려운 치명적인 결과를 초래할 수 있는 역량을 갖추고 있다. 사이버안보에서 국가의 주도적 역할은 여전히 유효하다.[6] 그럼에도 불구하고, 사이버안보의 행위자가 국가 행위자에 국한되는 것이 아니고, 사이버 위협의 목적이 인명살상이나 시설 파괴와 같은 심각한 피해를 초래하는 결과에 한정되지 않는다. 결국 비국가 행위자의 관여, 사이버 활동의 애매한 목적, 국가의 불분명한 의도 등은 사이버안보의 복잡성을 높인다.

비국가 행위자들은 국가안보의 심각한 위협으로 중심적인 역할을 할 수 있다. 비국가 행위자는 재앙적 파괴력 보여주거나 군사적 위협의 수준으로 공격하는 기술력을 갖추기 어렵다고 하더라도 국가안보의 위협으로 인식될만한 위험을 조성할 수 있다. 비국가 행위자가 국가와 밀접하게 연계되어 활동한다면, 파급효과는 훨씬 강하게 나타날 여지가 있다. 전문 해커그룹이나 정부와 연계된 조직은 정부의 대리자로 사이버 공격을 주도하거나 국가와 공조하여 상대국가의 안보를 위협하는 핵심적인 역할을 담당한다. 사이버 공격자의 신원을 파악하기 위해 많은 시간이 필요하고 과정도 민감하고 복잡하지만, 비국가 행위자의 활동

6) James A. Lewis, *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (CSIS, 2018); Liff (2012), pp.422-423.

이 특정 정부와 연계되었다는 증거를 파악하기란 쉬운 일이 아니다.

또 다른 요소는 첩보활동과 공격행위가 밀접하게 연계되어 있다는 요소다. 사이버 첩보활동은 직접적인 손상이나 피해를 불러일으키는 위협이 아니다. 이러다 보니, 무력 공격과 달리 첩보활동을 규제하는 국제법이나 국제규범은 없다. 모든 국가가 첩보활동을 수행할 정당한 권한을 갖는다. 다만 상대 국가가 파악하지 못하도록 은밀하게 추진되어야 하지만, 설령 첩보 요원이 발각되더라도 개인 행위로 철저히 단절된다. 따라서 안보영역에서 첩보수집은 모든 국가의 공공연한 비밀 활동이다. 상대국가의 첩보활동은 군사 공격으로 인정되지 않고, 이를 빌미로 군사 보복이 정당화되기도 어렵다. 전통적인 안보에서 첩보활동과 무력 공격은 비교적 명확하게 구분이 되는 위협이다. 첩보활동은 군사공격의 효과를 극대화하는데 중요한 전략적 요소임에 분명하지만, 첩보활동만으로 무력 공격으로 오인되지 않는다는 점은 국제적으로 합의된 사항이라 볼 수 있다.[7] 그러나 사이버 공간에서 사이버 공격과 사이버 첩보활동(cyber espionage)은 그 경계가 구분하기 힘든 연속적인 과정에서 이루어진다. 일반적으로 사이버 공격은 사이버 첩보활동과 동일 과정으로 사전에 필요한 공격 요건을 갖춘 상태에서 가능하다. 기존의 군사안보에 적용된 관행이 사이버안보에서는 그대로 적용되지 않는다.

사이버안보에서 사이버 첩보활동은 상대방이 위협 행위로 오인되는 상황을 특히 피할 수 없다. 하지만 사이버 공간의 특성으로 사이버 첩보활동을 사전에 탐지하여 예방하고 방지하는 기술이나 전략적 방책이 가까운 장래에 안정적으로 관리할 수 있는 수준으로 발전하기 어렵다. 사이버 공간은 기본적으로 공격 우위의 안보구조이다. 사이버 공간의 영역별로 공격 우위의 정도와 수준이 다르지만, 민간 영역은 상대적으로 훨씬 취약하다. 정보통신기술의 발전으로 개인, 사회, 국가 사이의 공간적 거리가 무의미하다. 사회가 네트워크 의존성이 높아

7) 기술정보와 인간정보는 영토 침범 및 주권 침해와 관련해서 차이점이 있다. 인간정보와 달리 정찰비행기의 영공 침범은 용인되지 않는다는 점에서 사이버 활동은 기술정보의 제약을 공유하지 않는다.

진다는 것은 공격 우위의 영역이 확대되고 있다는 의미이기도 하다. 개인들의 활동, 사회와 국가의 운용 그리고 군사 활동이 네트워크로 연결되어 있기 때문에 사이버 위협의 대상은 거의 무한대로 확장되고 있다.[8] 사물인터넷이나 스마트시티 등을 구현하려는 미래 사회는 역으로 사이버 공격의 대상이 많아지고 있음을 의미한다. 네트워크로 연결된 모든 대상은 정보와 활동의 흔적을 남기게 되고, 이것은 개인, 사회, 국가를 위험에 빠뜨릴 수 있는 도구로 이용될 수 있다.

마지막으로 행위자와 관련해서 사이버안보의 복잡성을 높이는 요소는 정부의 의도나 상황 인지와 상관없이 사이버 공격에 연루된다는 점이다. 자국의 의도와 무관하게 특정 국가는 사이버 공격에 자국의 네트워크가 용이하게 이용될 수 있다. 전 세계가 인터넷으로 연결된 사이버 공간에서 공격자는 자신의 신원을 은폐하기 위해 여러 중간 경유지를 통해 공격의 최종 목표에 도달한다. 재래식 군사 분쟁에서는 다른 국가의 지리적 공간을 해당 정부의 인지를 피해 이용하기란 현실적으로 거의 불가능한 전략이다. 무력 공격의 지리적 위치가 분명하게 드러나고, 이같은 공격은 다른 정부의 허용 여부를 명확하게 판단하는데 무리가 없다. 사이버 공격은 공격자의 정체를 숨기기 위해 여러 국가의 네트워크를 경유함으로써 처음 시작된 지리적 위치나 공격자의 신원이나 정체를 단시간 내에 분명하게 밝혀내기 매우 어렵게 만든다.

특히 사이버 위협의 복잡성을 가중시키는 요소는 타국 정부가 자국 네트워크의 경유를 의도적으로 묵인하고 있는가를 판단하기 곤란하다는 것이다. 이점과 관련해서, 유엔의 정부전문가그룹(GGE)은 많은 논의를 통해 4차 회의에서 사이버 공격의 경유지로 정부가 배후 세력이거나 의도적으로 용인된 상황에서 이용된다면 해당 정부가 책임지도록 했다. 이 때문에 특정 국가가 사이버 공격자의 정체를 파악하기 위해 네트워크 경유 국가의 조사 협조를 거부한다면, 관련 국가가 경유를 묵인했는지 관계없이 공격자를 파악하는데 한계가 있다.[9] 잠재

---

8) 상업용 소프트웨어는 1천개의 코드 라인마다 20～30개의 버그(bug)가 일반적으로 존재하고, 5천만 개의 코드 라인이라면 100～150만개의 잠재적인 에러가 포함되어 있다는 평가가 있다. Marc Goodman, *Future Crimes* (Anchor Books, 2015), p.51.

9) Paul Mozur and Jane Perlez, “China Is Reluctant to Blame North Korea, Its Ally,

적인 사이버 공격자의 우회 시도를 차단하거나 사전 탐지하기 위해서는 여러 국가들이 자국의 네트워크 시스템에서 벌어지는 상황을 감시하고, 의심되는 정보를 신속하게 공유하는 체계가 필요하다. 비협조 국가 혹은 갈등관계 국가들은 자국의 의도에 관계없이 외교 혹은 군사적 긴장 상태에 빠질 수 있고, 반대로 은밀하게 이를 전략적으로 이용할 수 있다.

요약하면, 사이버안보의 특징으로 확장성과 복잡성의 혼재는 재래식 군사안보와 달리 사이버안보의 회색지대가 넓게 자리 잡게 됐다는 점이다. 군사 강대국의 절대 우위와 안보 구조의 안정적 관인리가 어려워졌다. 사이버 위협의 방식과 목적 그리고 행위자들은 글로벌 사이버안보환경에서 각국의 대응 전략 마련을 어렵게 하고 있고, 반면에 잠재적인 도전세력이나 국가들의 사이버 활동은 다양한 방식의 비대칭적 전략으로 구체화되고 있다.

3. 사이버 위협과 대응전략

가. 사이버 위협의 유형

사이버 위협을 구분하는 방법은 피해의 구체성 여부, 피해의 심각성 정도, 혹은 위협의 목적과 행위자 등의 기준에 따라 다르다. 사이버전, 사이버 사보타지, 사이버 테러, 사이버 범죄, 헥티비즘, 사이버 심리전, 사이버 첩보활동 등 다양한 유형의 사이버 활동이 존재한다.[10] 여기에서는 사이버 활동의 목적에 따라 4 가지로 분류하였다. 기존의 사이버안보 연구에서 논의 되지 않는 공급망 안보(supply-chain security)을 포함함으로써 사이버안보 위협을 확장하려고 했다. 사이버전의 위협은 인명 및 시설 파괴를 목적으로 이루어지는 반면, 사이버 강압은 전쟁 수준에 미치지 못한 위협으로 사회 혼란과 피해를 초래한다.

---

for Cyberattack," *New York Times* (May 17, 2017).

10) Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013).

사이버 첩보활동은 직접적이고 가시적인 피해가 즉각적으로 나타나지 않고, 공급망안보 위협은 잠재적인 첩보활동과 기술패권의 우위를 보장하는 수단이 되는 것이다.

(1) 사이버전 전략

사이버 무기를 군사 목적으로 활용하는 전략이다. 가장 가능한 표적은 무기, 국가 통제 시스템, 정보통신 기반시설 등이 될 가능성이 있다.[11] 미국은 사이버 공격이 전쟁 수준으로 평가될만한 범주에는 화학시설, 응급지원서비스, 금융, 식량 및 농업 등 16개 분야의 국가기반시설을 포함하고 있다. 그러나 이런 범주로 확대하더라도 적어도 지금까지 공개된 사례에서 무력 전쟁과 유사한 수준으로 사이버전이 실제로 일어난 경우는 드물다. 사이버 공격이 시설 파괴를 목적으로 활용된 공개적인 사례가 2011년 스턱스넷(Stuxnet) 웜 공격이다. 미국과 이스라엘의 정보기관은 당시까지 유례를 찾을 수 없을 만큼 정교한 사이버 무기를 마련하여 이란의 핵시설을 파괴하려는 목적으로 활용하였다.[12] 사이버 공격이 무력 공격의 수준으로 평가되는 가장 심각한 위협의 사례였다. 심각한 사이버 위협이 현실적으로 등장할 수 있음을 인식하게 됐던 계기였다. 이런 사이버 위협 행위는 사이버 공격력을 갖춘 강대국들이 주도적으로 실행에 옮길 수 있다. 미국의 경우, 사이버 무기의 선제적 활용뿐만 아니라 사이버 위협에 대한 억지전략 차원에서도 사이버 수단을 포함하여 모든 가능한 수단을 활용하겠다고 선언했다.[13] 러시아는 재래식 군사 작전을 전개하면서 동시에 보조 수단으로 사이버 무기를 사용하여 상대방의 저항 역량을 약화시켰다. 러시아는 2008년 인접 국가인 조지아와 무력 분쟁을 일으켰을 때 선제적으로 사이버 공격을

11) James A. Lewis, *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (CSIS, 2018), p.17.

12) David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *New York Times* (June 1, 2012).

13) The White House, "International Strategy for Cyberspace," (May 2011). 하지만 사이버 보복의 한계를 인정하고 있다. The White House, "Expanding Our Ability to Combat Cyber Threats," (April 2015).

시도했다.

이란은 스턱스넷 공격의 보복으로 사이버전의 중요성을 인식하고 사이버 전력을 적극 강화시켰다. 이란 내 해커들은 사이버 공격을 당한 1년 뒤 2012년 세계 최대 정유회사인 사우디아라비아의 아람코 정유사를 해킹 공격을 하였다. 정유회사는 컴퓨터 1/3 이상이 복구가 불가능한 피해를 입었다. 사이버 공격이 기간시설이나 산업시설이 파괴되거나 완전 마비되는 결과는 사이버전의 수준으로 전통적인 무력공격의 범주로 충분히 간주될 수 있었다. 이런 피해에도 불구하고, 국제사회나 피해국들은 보복과 응징의 반격을 구체적이고 공개적으로 실행하지 못했다. 그 원인 중에는 특정 국가의 책임을 인정할만한 명확한 증거를 단시일 내에 제시하기 어려웠고, 정당성을 인정받는 보복 수단을 확보하지 못했으며, 반격에 따라 상대방의 추가 보복과 확전의 위험을 통제하기도 어려운 안보구조도 요인으로 작용했다. 사이버전 수준의 사이버 위협은 결국 사이버 공격력을 갖춘 강대국이 주도하고 있고, 사이버안보의 중요한 선례를 만들었다. 강대국들은 다른 한편으로 자국의 사이버 위험을 충분히 인식하고, 국제규범과 자국의 사이버안보전략을 통해 이를 예방하기 위해 시도하고 있다.

(2) 사이버 강압전략

사이버안보 위협은 외교 수단으로써 활용도가 크게 증대하고 있다. 사이버 공격의 수준이 무력 사용의 위협으로 평가된다면 사이버 공격자의 비용은 상대방의 보복과 반격으로 원래 기대했던 이익 이상으로 클 수 있다. 이를 피하면서도 자국의 안보 혹은 외교적 목적을 달성하기 위해서는 상대방의 보복 수단과 정도가 위협적이지 않도록 조절할 필요가 있다. 사이버 위협의 세력은 무력 충돌이나 반격의 임계점에 미치지 못한 사이버 활동을 전개할 강한 동기를 갖는다. 이는 '회색지대의 방어(defense in the gray zone)'에 해당한다.[14] 사이버안보에서 회색지대는 무력 충돌의 영역과 사이버 첩보활동 사이에서 이루어지는 사이

14) Lewis (2018), p.36.

버 활동을 의미한다. 전쟁 수준에 미치지 못한 사이버 활동은 사이버 위협 세력이나 국가가 자신들의 손실을 최소하면서도 정치적 목적을 달성하려는 효과적인 수단이었다.

사이버 강압전략은 이런 사이버전의 위험을 최소화하고 자국의 요구를 관철하기에 적절한 전략적 목적을 지닌다. 사이버 강압의 목적은 전통적인 안보위협의 목적과 다르다.[15] 즉, 상대방의 사회 혼란과 정권의 정당성 약화 등이 추구된다. 이같은 전략적 목적은 사이버 강압적 전략의 효율성을 가장 잘 반영하고 있다. 사이버 강압적 활동은 최근의 국제안보질서에서 그 효용성을 증명했고 전략적 가치가 충분히 인정되고 있다. 사이버 강압이 상대방의 사회 불안정과 정권의 정당성 훼손(집권능력)이 목적이라면, 사이버 강압의 요구 사항을 공개할 필요성이 없다.[16] 국가 간 분쟁이 이해관계를 조정하는 이슈가 아니라 정치 체제의 우위와 안정성 확보가 목적이라면, 공격자의 정체 혹은 공격자의 요구가 명확하게 드러나지 않는다고 하더라도 그 전략적 가치가 크게 줄어들지 않을 것이다. 이점은 전통적인 군사 분쟁이나 갈등과 사이버 강압적 활동이 커다란 차이가 있음을 보여준다.

사이버 강압전략의 대표적인 사례가 북한의 소행으로 의심되는 소니영화사의 해킹 사건이다. 북한은 김정은을 조롱하는 소니영화사의 영화에 대한 불만으로 해킹하여 사적 이메일을 공개했고, 영화를 인터넷에 공개하였다. 또한 이 영화 상영을 계획한 극장들에 대해서도 상영할 경우에 피해를 입히겠다고 협박하였고, 일반 극장들이 상영을 포기하도록 했다. 미국 오바마 행정부는 북한을 지목하여 공개적으로 보복을 천명한 첫 번째 사례이기도 하다. 명확한 증거는 아직 밝혀지지 않았지만, 북한은 2015년 1월 초에 인터넷 시스템이 다운되는 경험을 한다.[17] 사이버 강압의 또 다른 상징적인 사건은 러시아의 미국 대선 개입이다.

---

15) Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony," *Journal of Strategic Studies*, Vol.40, No.7 (2017), pp.898-911.

16) Erica D. Borghard and Shaw W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol.26, No.3 (2017), pp.262-263. 요구사항전달(communication)은 사이버 강압의 성패를 좌우하는 요소이지만, 자국의 요구를 공개할 필요가 없는 전략 목적은 요구사항전달의 요건이 중요하지 않다.

러시아는 해킹을 통해 얻은 정보를 공개하거나 가짜 뉴스를 확산시키거나 네트워크의 혼란 등으로 미국의 과정에 개입했다. 미국의 정치과정을 왜곡하려는 심각한 위협이었고, 러시아의 해킹은 대선 결과에 영향을 미쳤다는 것이 일반적인 평가이다. 트럼프 행정부 출범 이후, 미국과 중국 간 통상분쟁이 격화되었다. 미국에 반감을 가진 중국의 해커들은 미국의 기업, 정부 부처들을 겨냥해서 적대적인 공격을 가했고, 사이버 강압이 전략적 목적으로 활용됐다.[18] 민주당 대선후보인 힐러리 클린턴에 대한 러시아의 부정적인 인식은 힐러리 후보의 낙선을 유인하려는 사이버 활동으로 이어졌다.

(3) 사이버 첩보활동

사이버 활동이 사이버전이나 사이버 강압이라면 실질적인 피해가 발생한다. 시설 파괴, 혼란, 마비, 거부 등의 결과는 사이버 공격이 이루어졌음을 드러낸다. 이미 설명했듯이, 사이버 활동의 피해 결과가 표출되는 경우에 피해국의 보복과 국제사회의 비판 등의 위험이 뒤따른다. 네트워크와 국가기간시설을 파괴, 혼란, 마비, 손상하려는 외국의 정보기관이나 조직의 활동, 의도, 계획을 파악하여 대비하거나, 선제적으로 이를 제거하고 무력화하는 활동이 필요하다. 사이버 첩보활동은 사이버전이나 사이버 강압과 달리 정보를 수집하는 것이 주된 목적이다. 사이버 활동의 피해나 영향이 가시적으로 쉽게 드러나지 않거나 거의 탐지되지 않는다. 사이버 첩보활동은 기존의 정보수집과 비교해서 디지털 사회의 특징에 부합한 유용한 장점을 갖고 있다. 사이버 공간에서 첩보활동은 인간정보에 비해 첩보원의 노출이나 처벌 등의 위험이 적고, 첩보위성 등과 같은 기술정보에 비해 비용이 적게 요구되고, 인터넷에서 공개적으로 취합되는 다량의 정보는 광범위하게 활용되고 있다.

---

17) David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times* (January 18, 2015).

18) Nichole Perlorth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *New York Times* (Feb. 18, 2019).

사이버 첩보활동은 특성상 외부 공개되지 않지만, 기밀이나 민감한 정보가 누출된 이후에도 전혀 파악되지 않을 수 있다. 2014년 미국의 인사처에 대한 해킹으로 미국 정부 공직 진출자와 지원자들의 신상 정보가 2천만 건 이상이 유출되었다. 그 중에는 정보기관에 소속되어 해외에서 활동하는 요원들의 신상도 포함된 것으로 알려져서 정보 절취의 심각성이 제기됐다. 미국은 중국 정부 혹은 연관된 해커들 소행으로 결론을 내렸지만, 이에 대한 보복을 실행에 옮기지 않았다. 중국 소행의 증거를 공개하는 것은 미국의 첩보수집 방식을 노출해야 하고, 중국과의 사이버 확전 위험성을 우려했기 때문이다. 또한 미국과 중국 간 외교적 갈등을 야기했던 이슈는 경제 사이버 첩보활동이다.[19] 미국은 첨단기술을 절취하려는 중국의 해킹 활동을 안보영역의 첩보활동과 명백하게 구별하였다. 미국의 기업체와 연구소에서 개발하고 있는 첨단무기관련 기술이나 최신 산업기술이 유출된다면, 미국의 안보뿐만 아니라 산업적 피해가 엄청난 규모가 될 것이다.[20] 오바마 행정부는 중국의 첨단기술 해킹에 대해 비공식적인 접근 방식을 포기하고 공개적인 외교 문제로 다루기로 전환했다. 2015년 미국 오바마 대통령과 중국 시진핑 주석은 처음으로 양자 간 사이버 협약을 체결했다. 미국은 사이버 첩보활동의 위협을 제어하기 위한 사상 첫 양자 간 접근방식을 성사시킨 것이다.[21] 중국은 사이버 절취로 사이버 범죄 활동을 근절하기로 합의했고, 이를 지속적으로 감독하고 확인하기 위해 장관급 회의를 추진하기로 했다.

(4) 공급망선도전략

조셉 나이(Joseph Nye)는 사이버 공격의 3가지 핵심적 매개체로 네트워크,

---

19) 컴퓨터 보안업체 MaAfee는 사이버 범죄로 전 세계가 매년 많게는 1조억 달러의 손실을 입고 있다고 추산했다. Rich Dandliker, "Putting a Face on Intelligence Property Theft," *Symantec* (July 11, 2012).

20) U.S. National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (July 2018).

21) Ellen Nakashima and Steen Mufson, "U.S., China vow not to engage in economic cyberespionage," *Washington Post* (September 25, 2015). 중국의 사이버 절취 행위는 범죄와 안보위협의 이중적 성격을 포함하고 있다.

공급망, 내부자(insider)를 지목했다.[22] 이 중에 장비와 기술의 외부 의존성이 가장 높은 요소가 공급망이다. 이 때문에 최근 급부상하고 있는 이슈가 정보통신 장비와 기술을 제공하는 공급망보안 문제다. 정보통신 분야는 미국이 주도하고 발전시켜왔고, 패권적 지위를 누려왔다. 하지만 중국은 20여 년 전부터 정보통신 기술을 발전시켜 미국과의 국력 격차를 줄이고 중국의 산업과 국력을 선도하려고 추구해왔다. 네트워크 장비에서 중국의 5G 기술은 비용 및 기술적인 측면에서 미국을 일정 부분 앞서고 있다.[23] 정보통신 분야에서 미국은 기술패권을 장악해왔지만, 차세대 이동통신 분야에서 중국의 도전을 무시하기 어려운 단계에 이른 것이다. 정보통신 강국들은 적어도 외견상 산업경쟁력을 확보하기 위해 기술의 우위를 적극 추진하고 있다. 그러나 정보통신 기술과 장비는 단순히 산업의 경쟁력에 국한되는 문제가 아니라, 공급망을 통제하지 못한 국가는 안보의 취약점에 노출될 수 있다.[24] 완전한 검증과 통제가 불가능한 네트워크 장비의 구축은 장기적으로 백도어를 통한 첩보수집이나 제로 데이 공격(zero-day attack)의 위험에 빠질 수 있다. 파이브 아이즈(Five Eyes)로 불리는 미국과 정보공유의 4개 정보동맹국인 영국, 호주, 캐나다, 뉴질랜드는 중국 네트워크 제조업체인 화웨이와 ZTE의 통신 장비 도입을 두고 안보 및 외교적 고민에 빠져 있다.

미국은 2019년 국방수권법에서 연방정부가 중국의 화웨이와 ZTE 장비 구입을 제한하도록 규정했고, 향후 2년 내에 이들 기업의 기술사용을 금지했다. 미국 의회 역시 오래 전인 2012년 중국 정보통신기업의 위협을 조사한 보고서에서 화웨이와 ZTE 제품이 미국의 경제 및 국가안보에 위험이 되고 있다고 진단했다.[25] 이런 조치들은 중국의 정보통신 장비제조업체가 미국의 시장에서 점유

---

22) Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, no.3 (Winter 2016/17), pp.50-51.

23) U.S.-China Economic And Security Review Commission Report, *2018 Annual Report* (2018), pp.446-451.

24) 중국의 기술발전과 혁신이 빠른 속도로 이루어지면서 앞선 영역이 있다고 하더라도, 이런 기술 우위가 군사력으로 확보되기 어렵다는 지적도 있다. 이 경우 중국은 미국을 당분간 기술-군사력 격차를 줄이기 어렵다. Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet," *International Security*, Vol.43, No.3 (Winter 2018/19), pp.141-189.

율을 확대하기 어렵게 됐다. 미국은 이들 정보동맹국, 한국 등 우방국들에게 미국의 입장에 따라줄 것을 설득하고 있다. 첫 번째 관문이 미국의 4개 정보동맹국의 공동 보조 여부이다. 호주와 뉴질랜드는 잠재적인 안보 위험의 가능성이 제기되자 미국과 동일하게 화웨이 장비의 도입을 금지하려는 입장을 취했다. 그 근거로 중국의 네트워크 제조업체가 중국 정부의 통제를 쉽게 받고, 장비의 사이버 첩보수집 목적으로 용이하게 활용될 수 있으며, 2017년 개정된 중국의 사이버보안법은 단체나 개인은 국가정보활동에 협조하도록 규정한 내용 등이 제시됐다.[26] 초기의 단호한 입장에도 불구하고, 이들 국가는 중국과 통상 마찰과 자국의 경제적 이득 때문에 유동적인 태도를 보여주고 있다. 반면 캐나다는 중국 장비의 위협에 대해 충분히 감독하는 기술력을 확보했고 통제할 수 있다고 보고 미국과 다른 입장을 보였지만, 나중에 미국에 동조하는 모습을 보여주기도 했다. 영국은 중국 장비의 위험을 오랫동안 점검하기 위해 화웨이와 함께 공동으로 조사해왔지만 위협 증거를 확실하게 찾지는 못했다. 안보 위험의 우려를 불식시키려는 화웨이 노력 속에서 영국은 미국과의 공조를 주저하고 있다.

나. 사이버안보 위협의 대응 전략

사이버안보 위협에 대응하는 전략은 목적에 따라 4가지 유형으로 나누어 볼 수 있다. 대응의 수단, 갈등의 심각성, 파급 효과, 국제협력의 필요성 등 기준에서 다른 특징을 지닌다.

(1) 적극적 방어전략

사이버안보의 비대칭성은 사이버 공격력의 우위가 재래식 군사력처럼 확실한

---

25) House Permanent Select Committee on Intelligence, *Investigative Reportn the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (October 8, 2012).

26) Danielle Cave and Tom Uren, "Why Australia banned Huawei from its 5G telecoms network," *Financial Times*" (August 30, 2018).

안보구조를 보장하는 것이 아님을 의미한다. 북한처럼 사이버 방어력에 비해 사이버 공격력이 훨씬 강한 수준을 갖춘 국가가 있을 수 있다.[27] 상당한 사이버 공격력을 보유한 국가나 세력 혹은 개인이더라도 방어력이 열세인 경우 상대국가 혹은 집단의 사이버 공격으로 사회가 마비되거나 혼란에 빠질 수 있다. 수세적이고 방어적인 방식만의 사이버안보전략으로 자국의 네트워크와 국가기반시설을 보호하기 어렵다는 것은 분명해지고 있다. 재래식 군사안보에서처럼 사이버 공격에 대한 억제력의 효과를 높이기 위해서는 반드시 최소한의 상응한 응징의지와 보복의 역량을 갖추고 있어야 하는 것이다. 그리고 사이버 공격을 사전에 차단하기 위해 선제적이고 공세적인 전략과 수단이 필요하다. 사이버 공격의 반격은 재래식 군사력이나 사이버 수단을 활용하여 군사력을 약화시키거나 전쟁 수준의 분쟁에서 전략적 수단으로 활용 가능하다. 사이버안보에서 적극적 방어전략은 사이버 위협을 방지하기 위해 비례의 원칙에 따라 사이버 수단에만 의존하는 것이 아니다. 사전 예방의 조치는 사후의 대처에서 공세적인 시도가 가능하다.[28]

이런 사이버 공격수단과 억지전략은 트럼프 행정부의 사이버 전략에서 가장 분명한 특징이다. 미국은 사이버 공격의 심각성을 사전에 예방하기 위해 핵무기의 사용마저 고려할 정도이다.[29] 2018년 9월 발표된 미국의 사이버국방전략은 응징과 보복을 바탕으로 적극적인 사이버 억지전략을 추구할 것을 천명하고 있다. 2018년 공개된 국가사이버전략에서도 유사한 전략 기조를 공개했다. 즉, 사이버 공격자에게 '신속하게 대가를 치루는 투명한 결과'를 부과하겠다는 것이다. 잠재적 적대세력의 사이버 공격이 국가안보에 심각한 피해를 초래하는 경우, 미국은 이를 예방하거나 억제하는 전략은 재래식 군사안보와 동일한 전략을

27) Richard A. Clark and Robert K. Knake, *Cyber War* (HaperCollins Pub., 2010), pp.147-149.

28) Ellen Nakashima, "Pentagon Launches first Cyber Operation to Deter Russian Interference in Midterm Elections," *Washington Post* (October 23, 2018). 미국은 2016-17년 북한의 탄도미사일 시험을 저지하기 위해 사이버전과 전자전을 이용했다는 보도도 있다 (*New York Times*, March 4, 2017).

29) David E. Sanger and William J. Broad, "Pentagon suggests Countering Devastating Cyberattacks with Nuclear Arms," *New York Times* (Jan 16, 2018).

적용해야 한다고 여기는 것이다. 그러나 사이버 공세전략은 모든 국가가 채택할 수 있는 선택 방안이 아니다. 상대방의 네트워크에 침투할 수 있는 해킹 기술력을 갖추고 있거나, 군사 보복에서도 상대방이 오히려 확전을 우려하여 물러설 수 있는 압도적 우위를 확보하고 있어야 한다. 사이버 공격에 대한 보복의 정당성은 사이버안보에서 특히 어렵다는 점을 고려하면 사이버 공세전략은 공개적으로 수용하기 힘들다. 잠재적 적대세력을 대상으로 사이버 공세전략을 천명하고 그에 필요한 보복 역량이 신뢰를 받는다고 하더라도, 상대방의 추가 반격과 확전의 위험이 있다. 사이버 방어의 제약이 많고 반격의 피해가 예상된다면 사이버 보복은 여전히 조심스러운 전략이 된다.

(2) 사이버 강압의 방어전략

러시아, 중국, 북한 등이 강압 목적의 사이버 활동을 적극 실행하고 있고, 상당한 효과를 보았다. 사이버전과 달리, 국가 간 분쟁에서 적용되는 비례의 원칙은 사이버 강압의 대응 전략에서는 그대로 답습하기 힘들다. 강압의 대상과 목적은 각 국가마다 정치체제와 산업의 발전 수준에 따라 다양한 특징을 지니고 있기 때문에 동일한 방식이 사이버전에 비해 더욱 어렵다. 특히 민주주의 국가가 타국의 정치과정에서 혼란을 조성하고 결과를 왜곡하기 위한 사이버 공격은 정당성을 갖기 어렵다. 따라서 다른 수단의 대응전략이 필요하다. 우선, 사이버 보복의 천명이다. 사이버 공격에 따른 피해를 공개하는 것은 자국의 정치 혹은 산업의 혼란을 일으키는 부작용이 발생할 수 있고, 적절한 대응 수단이 없을 뿐만 아니라 제재를 위한 국제규범도 부족한 상황에서 비공개적이거나 수동적인 방어에 집중했었다. 하지만 사이버 강압의 공격에 대해 보복의 의지를 공개적으로 밝힘으로써 잠재적인 공격 세력에게 악의적인 사이버 활동을 자제하도록 유인하려는 것이다. 즉, 사이버 대응전략을 공개하고, 잠재적 공격자들이 사이버 공격으로 얻을 수 있는 이득을 상회하는 심각한 손실을 감당해야 한다는 것을 예견하게 한다. 사이버 강압의 응징과 보복 방침을 공개 표명하는 전략은 사이

버안보전략에서 커다란 변화이다.

그러나 사이버 강압에 대한 회색지대 방어전략은 사이버 반격의 전략 천명만으로 부족하다. 유사입장국과의 공조, 국제법 허용의 비례적 대응, 형사처벌, 경제 제재, 국제사회의지지 등이 있다. 회색지대의 사이버 활동은 국제규범의 미발달, 적절한 대응수단의 부재, 피해의 심각성 등이 애매한 환경에서 사이버 억지전략을 더욱 어렵게 한다. 또 다른 방식은 사이버 방식이 아닌 수단으로 경제제재, 외교적 압박 등 공격국가 혹은 공격의 후견국에게 실질적인 제재를 취하려고 한다. 미국처럼 압도적인 국력과 경제력을 바탕으로 단독으로 전개하는 것은 가능하다. 상대방의 사이버 강압전략에 맞서 민주주의 국가가 상응한 수단으로 대응하기에는 국내 정치의 민주적 정당성을 확보하기 힘들기 때문에 사이버 수단이외 전략과 수단을 동맹국으로부터 지원받는 협력이 필요할 수 있다.[30] 하지만 미국이 회색지대의 사이버 공격을 효과적으로 통제하고 있는지는 아직까지는 명확하지 않다. 러시아가 독일 등 유럽 국가들을 상대로 국내 정치 과정에 개입하려고 시도를 했지만, 미국에서 훨씬 치명적인 영향을 미쳤다는 점에서 사이버 강압의 대응 전략이 쉽지 않음을 보여준다. 오바마 대통령은 이임을 앞두고 러시아의 사이버 개입에 대해 외교적 보복을 가했다. 다수의 러시아 외교관을 추방하고 러시아 외교 시설을 2곳을 폐쇄하는 조치를 취했다.

이같은 사이버 강압전략에 맞서는 방식은 사이버 피해국이 단독으로 대응하는 전략만으로 효과가 제한적이고, 억지 효과는 더욱 불확실하다. 회색지대의 사이버 방어전략은 기존의 안보전략과 마찬가지로 여러 조건이 충족되지 않는다면 효과를 담보하기 어렵다. 이들 요건 중에서 사이버 공격자를 파악하고 효과적으로 제재를 가하기 위해서는 국제사회의 지지와 협력이 필요하다. 사이버 공격자의 정체를 파악하기 위해서는 독자적인 사이버 역량이 충분히 갖추고 있거나, 다른 국가들의 지원이나 협력이 있다면 사이버 강압의 대응 전략이 실효성 있는 추진이 가능하다. 이 때문에 유사입장국과 협정을 통해 공동으로 대응

30) Reuters, "With an Eye on Russia, U.S. Pledges to Use Cyber Capabilities on Behalf of NATO," *New York Times* (October 3, 2018).

하거나, 국제규범을 통해 제재하는 접근 방식이 동반되어야 한다. 국제사회의 협조와 제재의 정당성을 확보하는 국제규범이 최소한 유사입장국들의 공조 속에서 지지받아야 한다.[31]

(3) 사이버 방첩활동

사이버 활동은 정보를 수집하는 수단으로 일반화됐고, 그 중요성이 계속 증대되는 경향이 있다. 약소국이나 개인 혹은 집단이 국력이나 사이버 역량의 열세를 극복하고 비대칭적인 전략을 구사하는데 유용하다. 사이버 첩보활동은 국가안보 혹은 국익 향상에 도움이 되고, 효과적으로 활용된다면 산업 발전에도 기여할 수 있다. 사이버 첩보활동은 크게 두 가지 측면에서 전략적인 가치가 높다. 하나는 재래식 안보의 첩보활동과 차이이고, 둘째는 사이버 첩보활동과 공격 행위와의 구분이 애매한 점이다. 사이버 방첩활동은 이런 사이버 첩보활동과 공격을 사전에 탐지하는 것이다. 목적과 대상이 다를 수 있지만 활동 수단과 방식은 동일하다. 사이버 첩보활동은 재래식 안보영역의 첩보활동과 구분이 될 정도로 폭넓게 활용된다.

재래식 군사영역에서 첩보수집활동이나 정보기관의 활동은 비공개적으로 추진되고, 첩보수집이 노출되면 그에 따라 외교적 갈등의 원인이 된다. 그럼에도 군사 충돌의 확전으로 발전되는 경우는 거의 없다. 하지만 사이버 첩보활동은 그 표적이 제한이 없을 정도로 광범위하게 전개된다. 국제규범이나 관행으로 허용되는 첩보활동의 범위와 기준이 애매하기 때문에 사이버 방첩활동도 마찬가지로 용인되는 범위가 그만큼 넓어진다. 첨단기술에 대한 사이버 첩보활동은 안보 위협으로 받아들여져야 하는 것인지, 아니면 범죄 행위로 간주되어야 하는

31) 사이버 위협에 대해 강대국들은 상호 이익을 도모하기 위해 국제규범화가 불가피할 것이라는 주장도 있지만(James W. Forsyth, Jr., and Billy E. Pope, "Structuring Causes and Cyber Effects," *Strategic Studies Quarterly*, Vol.8, No.4 (Winter 2014), pp.113-130), 사이버 위협의 양태와 변화가 아직 불확실성이 높고 자국의 이익과 국제규범 사이에 간극을 쉽게 해소하기 어렵다는 주장도 있다(Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly*, Vol.9, No.2 (Summer 2015), pp.78-95).

것인지 하는 문제이다. 즉, 첨단기술이 국가안보 영역으로 간주된다면 첩보활동의 범주이고 산업 영역이라면 범죄로 취급받는다. 비국가 행위자나 국가 기관이 산업기술이나 무기 기술을 절취했다면, 그것은 기존의 관행으로 허용되어야 하는가 하는 점이다.

사이버 첩보활동의 효용성은 첩보를 수집하려는 사이버 활동이 사이버 공격의 사전 준비 작업과 구분이 어렵다는 점에서도 증대된다. 이 두 가지 행위는 동일하다. 사이버 공격은 사이버 첩보활동처럼 사전에 상대방의 네트워크나 컴퓨터 시스템에 침투하고 있어야 한다. 그렇다면 해킹을 통해 상대방의 네트워크에 침투하려는 활동은 공격 행위로 간주될 것인지, 아니면 첩보활동의 일환이라고 볼 것인가이다. 만약 사이버 공격의 시작으로 인정된다면, 그에 상응한 보복과 응징은 정당성이 높아진다. 사이버 활동이 시설파괴 혹은 강압을 위해 전개되기 위해서 사이버 방첩활동과 동일한 노력을 해야 한다. 다만 사이버 방첩활동은 적대 세력의 정보기구에 비중을 두고 있지만, 기밀을 절취하려는 대상이 확대됐다는 점에서 방첩의 활동도 확장되는 것이다. 사이버 방첩활동은 사이버 활동과 유사한 특징을 장점으로 최대한 활용하는 시도이다.

사이버 방첩활동은 다른 유형의 방첩활동이나 첩보수집활동의 어려움을 극복하고 외교적 갈등을 최소화하는 사이버 전략이다. 공세적 사이버 방첩활동은 국내외의 해커와 적대 세력의 사이버 활동, 의도, 계획을 파악하여 선제적으로 방어하거나 사이버 위협의 피해를 약화시킨다.[32] 사이버 방어는 재래식 군사안보와 달리 제아무리 기술력을 높이고 다양한 수단을 마련했다고 하더라도 완벽한 수준에 이를 수 없다. 사이버 방첩활동은 공세우위의 사이버 공간 특징에서 방어전략으로 중요성이 날로 증대하고 있다. 사이버 방첩활동은 국내 사이버 보안의 소극적인 노력을 포함하여, 해외에서 사이버 위협 세력들의 활동, 위협 수단의 발전, 유

32) 미국 국가정보장 산하에 국가방첩안보센터(NCSC)는 방첩, 사이버위협, 안보의 3개 영역을 관장한다. 안보 수준의 사이버위협에 대처하기 위해 사이버 방첩활동을 임무로 삼고 있다(NCSC 홈페이지, https://www.dni.gov/index.php/ncsc-home). 미국은 오바마 행정부 시절인 2016년 국가방첩전략에서는 방첩의 목적으로 기술, 경제, 과학 분야에서 국익에 심대한 영향을 미치는 외국 정보기관 혹은 조직들의 활동을 파악, 약화시키는 것임을 분명히 했다. (NCSC, *National Counterintelligence Strategy 2016*)

통, 활동의 목적과 계획 등을 파악하는 적극적인 역할이 강조되는 것이다.[33]

(4) 공급망안보전략

공급망안보전략(Supply-chain security strategy)은 첨단기술의 국가안보적 가치를 강조하고, 이에 대한 국가의 통제와 관리를 경제적 논리보다 안보적 기준에서 보호하는 전략이다. 네트워크 장비와 정보통신기술은 산업 경쟁력 우위와 국가안보의 확보라는 양면성을 띤다. 정치적 이념의 구분이 명확했던 국제안보환경에서 첨단기술의 개발과 발전은 군사 강대국의 지도력을 추종하면 심각한 안보 위협에 노출되지 않았다. 군사 및 이념적 대결이 크게 약화된 국제안보구조에서 기술력 우위를 차지하려는 강대국들의 경쟁은 복잡한 국제문제를 야기하고 있다. 엄밀하게 얘기하면, 네트워크 장비는 군기지에 설치된 군사 시설이나 무기가 아니다. 하지만 군사 활동의 핵심적 요소가 되었다는 점에서 안보 위협의 수단으로 활용될 여지가 매우 높다. 이는 핵물질이나 핵기술의 확산과 유통을 감시하고 통제하려는 국제사회의 지속적인 노력과 비교하면 충분히 납득 할만하다. 유사한 사례로 생화학 기술과 물질은 산업과 군사 목적으로 이용 가능하기 때문에 거래와 생산 및 비축을 통제하는 국제규범 역시 국제안보적 시각에서 다루어지고 있다.

강대국은 국제안보구조의 급격한 변화를 초래하는 무기의 기술과 원료를 통제하여 국제분쟁을 예방하고 강대국의 국제안보 주도권을 확보하려고 국제법이나 국제규범의 구축을 적극 추진하는 경향이 있다. 핵무기나 생화학무기는 파괴력이나 비인도적인 피해 때문에 강대국들의 합의가 이루어졌고, 국제사회의 구성원들은 자발적 혹은 비자발적으로 유인됐다. 그러나 정보통신기술과 제품은 다른 무기체계와 전혀 다른 성격으로 강대국 간 합의와 여타 국제사회가 동참하는 방식은 정보유통, 사이비 공간의 관리, 사이버 공간의 군사화, 통신장비의 표준화와 규제 등 해결해야 하는 이슈들이 많다.[34] 미국과 중국은 각각 유사입

33) Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (Wiley, 2004).
34) GGE, Sanghai Cooperation Organization, Budapest Convention, ITU 등 사이버 공간

장국과 함께 공동보조를 취하고 있지만, 자국의 경제적 가치를 최우선시하는 국가는 국가안보를 강조하는 우방국의 공조 요청을 쉽게 수용하기 어렵다. 경제적 가치와 국가안보를 비교하는 전략적 평가가 정보통신 장비와 기술의 도입을 결정하는 기준으로 작용한다. 많은 국가들은 네트워크 장비의 비용과 성능만을 고려해서 도입을 결정할 것이다. 문제는 패권적 지위에 있는 미국과의 안보협력을 유지해야 하는 국가들의 전략 선택이다.

미국의 입장을 지지하는 국가들은 중국의 통상 보복과 제재를 우려해야 하기 때문에 전략 선택을 더욱 어렵게 한다. 중국과의 경제 혹은 외교적 의존성이 높지 않다면, 미국의 유사입장국들은 부담이 줄어들 것이다. 반면에 미국의 국가안보 지원에 심각하게 의존하지 않은 국가는 경제적 가치만을 고려해 중국 기업의 네트워크 제품을 도입할 수 있다. 아프리카와 동남아 지역 국가들은 경제 원조와 차관을 받으며 제공되는 정보통신 기반구축을 막연한 국가안보의 가치 때문에 포기하기 어렵다.

4. 한국 국가사이버안보전략의 전략적 함의

한국 정부는 오랫동안 준비한 '국가사이버안보전략'을 완성했다. 2019년 4월 발표된 '국가사이버안보전략'은 사이버 공간에서 안보위협을 대처하기 위해 관련 부처들의 정책 방향을 종합하고 있다. 한국의 국가사이버안보전략은 억지전략 채택을 공식적으로 명기했고, 그 실효성을 담보하기 위해 전술, 수단, 의지를 제시했다. 이에 대해 사이버 위협의 유형에 따라 한국의 편익을 기준으로 사이버안보전략의 기대되는 효과를 가늠해 보았다. 즉, 사이버안보 위협에 대응하려는 전략의 기대효용은 한국의 역량, 의지, 성공가능성 기준에서 평가해 볼 수 있다.

의 관리와 안보 위협을 해소하려는 국제 협상은 국가들 간 진영으로 나뉘어져 있고, 국제규범의 제도화 과정은 여전히 불확실성이 높고 오랜 논의를 지속하고 있다 (Josepn S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, Belfer Center, Harvard Kennedy School (November 2014), pp.5-11.

첫째, 사이버전의 심각한 위협을 방지하려는 사이버 억지전략을 채택할 것인가 여부이다. 정부는 사이버 억지전략 차원에서 보복과 응징 의지를 공식적으로 천명함으로써 얻는 효과를 고민해야 한다. 사이버 억지전략의 성공은 적대 세력이 상대국가의 보복 위협을 신뢰해야만 하고, 이를 결정하는 요소는 크게 네 가지이다. 사이버 보복 의지, 보복 역량, 보복의 성공 가능성(분쟁 비용), 그리고 갈등 이슈이다.[35] 보복 역량은 군사, 외교, 경제, 형사 처벌 등 다양하게 강구될 수 있지만 공격용 사이버 무기의 전략적 의미는 크다. 보복 의지는 국내외 정치적 비용과 확전의 위험에 의해 영향을 받는다. 보복의 성공 가능성은 표적의 접근성이나 손실을 입힐 수 있어야 한다는 의미이다. 따라서 한국의 국가사이버안보전략은 사이버공격 대응역량 강화 차원에서 포괄적·능동적 수단 강구를 위해 국제규범이 허용한 수단 마련이나 사이버전에 대비하여 다양한 전력체계 보강 및 핵심기술 확보를 공언했다.[36] 이런 전략 표방은 국내외에서 구체적인 정책과 전술로 실행에 옮겨지기에는 귀속(attribution) 문제, 확전의 위험, 비대칭적 안보 취약점, 국제규범의 미비 등으로 한계가 분명하다. 결국 전략 선언은 향후 실행과 관련해서 전략적 딜레마를 해결해야 한다. 사이버 보복 의지를 천명하고 효과적인 집행 여부는 국내외에서 국가 평판과 직결되어 있다. 쉽게 실행하기도 어려운 역량과 의지를 드러낸 것은 국제안보환경에서 국가 억지전략의 신뢰성을 저해하거나 다른 국가와의 안보의존성을 높일 수 있다. 또한 억지전략의 실행은 상대방을 보복할 만큼 안보위협의 심각성이 있는가에 달려있다.

사이버 억지전략은 보복과 응징을 위한 수단 마련이 전제되어야 한다. 이는 공격형 사이버 무기를 보유하고 있음을 인정하는 신호로 해석될 수 있다. 억지

35) Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (Cambridge University Press, 2017), pp.28-34.

36) 사이버안보전략의 이같은 핵심 내용은 특정 유형의 사이버 공격에 대해 무력과 사이버 무기를 동원한 보복도 선택될 수 있음을 암시하는 것이다. 하지만 전쟁 수준에 미치지 못한 사이버 공격에 대응하는 전략은 명확한 국제규범이 존재하는 것도 아니고, 포괄적이고 능동적인 수단도 국제 사회의 협력 없이는 매우 제한적인 효과만을 기대할 수 있다. 2018년 발표된 미국의 국가사이버안보전략에서도 미국의 안보와 국익을 위해 모든 수단이 활용될 수 있음을 천명했지만, 유사입장국이나 협력 대상들과의 공조가 필요하다는 점을 명확히 하고 있다 (The White House, "National Cyber Strategy of the United States of America" (September 2018)).

의 긍정적인 효과와 달리, 자칫 잠재적 적대세력이 사이버 무기를 적극 개발하고 방어망을 강화하도록 유인하는 부작용을 불러일으킨다. 더욱이 사이버 무기는 공격과 방어가 동일한 과정으로 개발되고 활용되기 때문에 설령 방어력을 향상시키는 코드의 개발이라 할지라도 사이버 공격의 수단으로 쉽게 전환이 가능하다. 이런 이중용도의 사이버 무기 특징은 자국의 사이버안보를 더욱 불안정하게 만들 수 있다.[37] 만약 사이버 억지전략의 천명이 공격용 사이버 무기를 개발하겠다는 의지 표명으로 주변 국가들이 인식한다면, 사이비 군비경쟁이나 사이버 확전의 불확실성을 높일 수 있다. 이같은 부작용을 충분히 고려하여 국가사이버전략의 실질적인 집행은 정밀하게 대비되어야한다.

둘째, 사이버 강압의 대응으로 해커 처벌, 경제 제재, 국제 사회의 공조 등을 활용하는 전략이다. 전쟁 수준에 미치지 못한 사이버안보 위협에 대한 한국의 독자적인 대응전략은 현실적으로 효과를 기대하는 것이 아직은 무리이다. 억지전략 차원에서의 보복을 취할 정도로 위협 이슈의 중요성(stake)이 크지 않다. 설령 중요성이 인정된다고 하더라도, 동북아 지역, 한미 안보동맹, 아세안 지역포럼, 혹은 기존의 국제조약이나 규범을 활용하여 제재하는 방안에 의존할 수밖에 없다. 사이버 강압의 대응 전략은 사이버 강압을 시도한 국가에게 편익보다 비용을 높일 수 있다면 성공적인 결과로 이어질 수 있다. 그러나 한국의 입장에서는 국내정치적 비용(domestic audience costs)을 고려해야 한다. 사이버 억지전략에 비해 사이버 강압의 대응전략은 좀 더 쉽게 선택될 수 있지만, 명백한 증거 제시와 실효적인 응징 수단이 불충분한 여건에서 공개적인 보복 다짐은 국내 정치적 비용이 무시될 정도로 쉽게 실행될 수 없다. 물론 한국 정부의 무대응은 정부에 대한 국민의 신뢰 저하와 사회 불안으로 유권자의 불만과 정치적 비판으로 이어질 수 있다.

국제기구와 지역안보협력체에서 이슈화하는 방안은 충분히 가능하다. 사이버 활동의 근거지인 국가와 사법 및 정보공유를 추진하여 공격자의 신원을 밝히는

37) Guy-Philippe Goldstein, "Cyber Weapons and International Stability", *Military and Strategic Affairs*, Vol.5, no.2 (2013), pp.126-127.

작업도 중요하다. 공격자의 정체를 객관적으로 밝힐 수 있다면, 그것은 당장의 응징으로 이어지지 않는다고 하더라도 향후의 위협을 줄이는 효과는 있을 것이다. 미국의 최근 전략 변경에서 볼 수 있듯이, 공격자의 정체를 공개하고 구체적인 처벌과 응징을 분명하게 시도하는 노력은 장기적으로 전략적 효과를 제공할 수 있다. 현재까지의 한국 정부의 대응은 국내 네트워크 시스템의 보안을 향상시키는 대책이나 대응 체계를 마련하는데 주안점을 두었다. 한반도에서 군사적 긴장이 고조된다면 사이버 위협의 수준이나 빈도가 증대할 가능성이 높다. 시설 파괴의 목적이 아니더라도 사회적 불안과 혼란이 조성될 수 있는 영역에서는 한국의 보복을 약화시킬 수 있기 때문이다. 한국은 사이버 반격보다는 경제제재 혹은 외교적 압박이 안정적인 상황 관리를 위해 좀 더 현실적인 접근법이 될 것으로 보인다.

셋째, 사이버 방첩활동은 한국 정부가 한국의 역량과 주체성을 갖고 추진할 수 있는 전략이다. 특히 북한과 관련해서 지금까지 축적된 한국의 경험과 정보는 결코 적지 않다. 그 동안 북한의 소행으로 의심되는 많은 사이버 공격에 직면하면서 한국 정부는 상당한 정보를 갖게 되었고 공격자의 정체를 파악하고 방어하는 기술력을 높였을 것이다. 이를 활용하면 사이버 방첩활동은 모든 사이버 위협을 완전하게 해소할 수는 없지만 예방하거나 사이버 보복의 수단으로 사이버 전략의 핵심 역할을 담당할 수 있다. 미국이 2014년 미국의 소니영화사 해킹에 대한 보복으로 북한에 사이버 보복을 취했을 때 한국 정부의 지원이 있었고, 미국의 국가안보국은 적어도 2010년에 북한의 네트워크에 침투해 있었다.[38] 적극적인 사이버 방첩활동의 필요성을 보여준 사례였다. 또한 미국의 정보기관 조직 개편은 이런 관점에서 시사하는 바가 크다. 사이버 첩보활동이 각국의 첩보수집 수단으로 활용되고 있고, 사이버 공격을 사전에 차단하기 위한 전략으로 사이버 방첩활동의 중요성이 강조되고 있다. 미국 CIA는 조직 창설 이후에 가장 커다란 조직 개편을 통해 사이버 활동의 중요성을 반영하고 있다. 사이버국

38) David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times* (January 18, 2015).

(Cyber Directorate)을 신설하고, 사이버 첩보수집, 분석, 공작을 포괄하는 새로운 활동의 방향을 수립했다.[39]

정보수집, 공작, 방첩 등의 정보활동에서 사이버 영역을 독립적인 조직으로 구축하여 종합적이고 체계적이며 상호 유기적인 활동이 되도록 조직 개편을 고려해 볼 시기이다. 사이버 방첩활동은 국내에 국한되는 방어적인 보안 활동이 아니라, 해외에서 활동하는 적극적인 방어전략의 차원에서 조직 정비, 인력 확충 및 예산 지원이 필요하다. 사이버 방첩활동은 외부의 사이버 공격자를 파악하고 진상을 조사하는 활동의 기본이 되기도 하다. 미국은 2018년 9월 그 동안 북한의 소니영화사 혹은 랜섬웨어 등 미국과 전 세계를 대상으로 사이버 공격을 주도했던 해커와 조직의 정체를 공개하고 형식적이지만 제재 조치를 취했다. 미국의 이런 조치는 비밀의 정보수집 방식을 노출시키는 부작용이 있었지만, 자국민과 우방에 미국의 기술력을 과시하려는 의도도 있었다.[40] 기술의 발전으로 과거에 비해 사이버 공격자의 귀속 문제를 점진적으로 개선해나가고 있다.

넷째, 한국은 2018년 12월 세계 최초로 5세대(5G) 이동통신시대를 열었다. 비록 기업용 상용화 서비스이지만, 획기적인 네트워크 서비스가 이루어지게 됐다. 이동통신장비 시장에서 비용과 성능을 따진다면, 중국의 화웨이가 유리한 입장에 있다. 중국은 당연히 자국 기업의 제품을 판매함으로써 정보통신분야의 주도권을 확보하려고 노력하고 있다. 2018년 5G 네트워크 장비의 시장 점유율은 화웨이가 1위(28%)를 차지했다.[41] 통신 장비 도입에 관한 한국의 정책 방향을 결정하는 주요 요인은 중국의 통신장비가 사이버 첩보활동에 활용된다는 명확한 증거, 미국과의 안보동맹 차원에서 제기되는 전략 공조, 중국 정부의 통상 및 외교 압박 등이다. 미국과 미국 우방국들이 중국의 화웨이나 ZTE의 정보통신 장비가 사이버 간첩활동으로 활용되고 중국 정부와 연계성이 드러난다면,

---

39) Andy Greenberg, "Cyberespionage is a Top Priority for CIA's New Directorate," *Wired* (March 9, 2015).

40) Elllen Nakashima and Devlin Barrett, "U.S. Charges North Korean Operative in Conspiracy to Hack Sony Pictures, Banks," *Washington Post* (September 6, 2018).

41) James A. Lewis, *How 5G Will Shape Innovation and Security*, CSIS (December 2018), pp.4-8.

5G 시설 구축을 전면 차단할 수 있는 근거가 마련되는 것이다. 한국에서 중국의 통신 장비(LTE)가 부분적으로 도입되어 활용되고 있다는 점에서 5G 장비 도입을 전면 금지하는 방식이 수용될 수 있을지 회의적이다. 중국 제품의 안보 위협 가능성이 지속적으로 제기되고 있지만, 실제로 화웨이 장비가 정보 절취에 직접 관련되어 있다는 증거는 명확하지 않다. 중국 기업의 전산 장비에 의혹이 일어나거나 해킹의 사례가 발생한 사례들은 다수 있다. 그럼에도 미국에 대한 중국과 러시아의 최근 사이버 공격들은 중국 기업의 장비에 의존하지 않았다는 점이다.[42]

한국이 선택 가능한 방안은 크게 네 가지 방향이다. 우선, 화웨이 등 중국 정보통신 업체의 한국 정보통신 기반시설 구축에 참여를 전면 허용하는 방안이다. 전면적이지는 않더라도 적절한 감시와 통제 장치를 마련하여 허용하는 방안이다. 영국이나 독일이 최근 보여주고 있는 태도이다. 국내 기업이 선호하고 중국과의 사이버안보협력의 실마리를 이어가는 계기를 마련할 수 있다. 미국의 안보 및 외교적 압박을 어떻게 극복할 것인가가 관건이다. 둘째 방안은 한국의 통제 업체별로 자율적으로 중국 정보통신업체와의 협력 체제 구축을 일임하는 것이다. 국내 통신업체의 독자적인 결정은 장기적으로 중국 기업의 설비 유입을 인정하는 것이고, 중국과 미국의 입장을 절충하는 효과가 있다. 셋째, 한국의 5G 기반시설 구축을 연기하고, 그 기간 중국의 정보통신 장비를 도입하는데 따른 국가안보의 위험성을 평가하고 그에 따라 결정하는 방안이다. 물론 국내 보안업체와 정부가 합동으로 조사하는 방식과 해외 기관에 맡기는 방법이다. 추후 결과에 따른 갈등을 회피할 수 있다. 한국에서는 5세대 이동통신 도입의 일정이 가시권에 있는 상황에서 미룰 수 없다. 마지막으로 호주, 뉴질랜드, 일본과 미국처럼 중국의 정보통신업체가 기반시설 구축을 전면 불허하는 방안이다. 미국과 사이버안보협력을 강화하는 효과를 얻을 수 있다. 하지만 국내 통신서비스업체의 불만과 중국의 압박이 문제이다. 한국 정부가 미국 입장과 동일하게 공조하기에는 국내여론과 지지가 충분하게 형성되어 있지 못하다. 또한 통신업체가 비용과 기술

42) James A. Lewis, "ZTE, the Telecom Wars, and Cyber Spies," *CSIS Briefs* (June 2018), pp.2-3.

지원 등의 많은 경제적 비용을 부담하며 정부의 방안을 수용하기에도 용이하지 않다.

5. 결 론

사이버 공간에서 일어난 활동이나 장비 혹은 인적 자원은 국가안보의 핵심적인 요소이고, 관련 요소들이 다양한 목적으로 활용되고 있다. 한국처럼 정보통신 강국의 면모를 갖춘 국가에서는 사이버안보에 관한 국가전략이 시급히 마련되어야 하고, 이를 바탕으로 사이버 위협의 사건에 대해 체계적이고 일관성이 있는 신호를 대내외에 알려야 한다. 이를 위해 한국 정부는 미국과 유사한 사이버안보 지침과 법제화의 필요성을 적극 검토하고 구체화하는 작업이 필요하다. 하지만 한국은 미국과 같은 국제사회에서의 위상과 사이버 역량을 갖추지 못하고, 한반도와 주변의 안보구조에서 독자적인 조치와 대응만으로 효과를 기대하기 어렵다. 한국은 국제기구에서 금융지원 제재, 군사지원 제한, 관련 인사의 출입국 금지 등 미국과 유사한 방식의 제재 수단이나 국제 공조 체제를 동원하기에 한계가 있다.

한국 정부의 전략 선택폭이 제한적이고 효과를 담보하기에도 어려운 요소가 많지만, 사이버 억지효과를 거두기 위해서는 오랜 시간이 소요되더라도 분명한 증거를 통해 공격자의 신원을 밝히는 노력을 해야 한다. 특히 사이버 강압의 위협에 대해서는 지속적인 노력을 통해 공개적인 제재 조치를 취해야 한다. 비록 조사 기간이 수년이 걸리거나 제재의 단기적인 실효성이 없다고 하더라도, 이런 조치는 사이버 공격자가 사이버 활동에 더욱 주의하도록 경각심을 줄 수 있다. 사이버안보에 관한 국제사회의 합의점은 사이버 공격으로 인명살상이나 시설파괴가 발생한다면 군사 공격과 동일 수준으로 대응의 정당성이 인정된다는 점이다. 아직까지 그런 수준의 사례가 거의 없었기 때문에, 무력충돌의 보조 수단으로 사이버 무기가 동원되는 경우가 아니라면 사이버전의 가능성이 높지 않다.

이 경우는 한미 안보동맹의 틀 내에서 공동보조를 취해 나가는 것이 바람직할 것으로 보인다.

잠재적인 사이버 공격을 예방하기 위해 시급히 정비해야 하는 전략은 사이버 방첩활동이다. 국내의 정부 네트워크나 국가기반시설에 대한 사이버 보안 수준이 아니라, 해외에서 사이버 방첩활동을 적극 지원하는 것이 필요하다. 사이버 첩보활동이 국가, 단체, 개인 등이 정치, 종교 혹은 범죄의 목적으로 전개되고 있고, 드러나지 않는 사례를 감안한다면 일상적이고 실질적인 위협이다. 국내의 정치 환경과 국민의 회의적 시각을 고려하는 방첩활동이 되어야 하겠지만, 해외 지역에서의 사이버 방첩활동은 적극적인 방어 전략차원에서 추진되어야 한다. 국내 활동은 입법부의 통제를 받아들이는 방향에서 투명성을 높이고, 해외에서는 정보활동의 기밀성을 최대한 보장받도록 제도 정비가 필요하다.

정보통신 기술 및 장비 도입은 국가안보의 기준에서 정부의 정책적 판단이 요구된다. 그러나 현안으로 중국 화웨이의 설비를 국내에 도입을 허용하는 문제는 한국 정부의 개입이 쉽지 않는 구조이다. 외견상 개별 통신업체의 판단에 맡기면서 국가는 사이버 방첩활동과 국가안보의 확보를 위해 엄격한 감시와 통제를 실시하는 것이다. 외국산 통신장비의 안보위협이 객관적이고 구체적인 증거가 확보되기 전까지 정책 결정은 미루는 것이 바람직하다. 미국이 제기한 의혹이 공식적이고 명확한 위협으로 드러난다면, 이를 반영하는 정책으로 수정하면 된다. 파이브 아이즈 국가들은 자국의 역량과 상호 정보 공조를 통해 외국산 통신장비의 위험을 감시해 나갈 것이고, 한국은 이를 지켜보며 편승하는 전략이 필요하다. 한국의 사이버안보를 위협하는 주요 대상이 예측되는 동북아의 안보환경에서 한국 사이버안보전략의 실행은 중국의 협조가 절실하다. 우리가 지나치게 선도적인 입장에 서는 것은 막대한 경제적 피해 이외에도 전략적 손실이 크다.

참고문헌

1. 단행본

Berkowitz, Bruce D. and Allan E. Goodman. *Intelligence in the Information Age* (Yale University Press, 2000).

Clark, Richard A. and Robert K. Knake. *Cyber War* (HaperCollins Pub., 2010).

Goodman, Marc. *Future Crimes* (Anchor Books, 2015).

House Permanent Select Committee on Intelligence. *Investigative Reportn the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (October 8, 2012).

Lewis, James A. *How 5G Will Shape Innovation and Security*, CSIS (December 2018).

Lewis, James A. *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (CSIS, 2018).

NCSC. *National Counterintelligence Strategy 2016*, (https://www.dni.gov/index.php/ncsc-home, NCSC).

Nye, Joseph S., Jr. *The Regime Complex for Managing Global Cyber Activities*, Belfer Center, Harvard Kennedy School (November 2014).

Rid, Thomas. *Cyber War Will Not Take Place* (Oxford University Press, 2013).

Schelling, Thomas C. *Arms and Influence* (Yale University Press, 1966).

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World* (Wiley, 2004).

Sechser, Todd S. and Matthew Fuhrmann. *Nuclear Weapons and Coercive Diplomacy* (Cambridge University Press, 2017).

U.S. National Counterintelligence and Security Center. *Foreign Economic*

Espionage in Cyberspace (July 2018).

U.S.-China Economic And Security Review Commission Report. *2018 Annual Report* (2018).

2. 논문

Borghard, Erica D. and Shaw W. Lonergan. "The Logic of Coercion in Cyberspace," *Security Studies*, Vol.26, no.3 (2017).

Brian M. Mazanec. "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly*, Vol.9, No.2 (Summer 2015).

Cave, Danielle. and Tom Uren. "Why Australia banned Huawei from its 5G telecoms network," *Financial Times* (August 30, 2018).

Dandliker, Rich. "Putting a Face on Intelligence Property Theft," *Symantec* (July 11, 2012).

Forsyth, James W., Jr., and Billy E. Pope. "Structuring Causes and Cyber Effects," *Strategic Studies Quarterly*, Vol.8, No.4 (Winter 2014).

Gilli, Andrea. and Mauro Gilli. "Why China Has Not Caught Up Yet," *International Security*, Vol.43, No.3 (Winter 2018/19).

Goldstein, Guy-Philippe. "Cyber Weapons and International Stability", *Military and Strategic Affairs*, Vol.5, No.2 (2013).

Greenberg, Andy. "Cyberespionage is a Top Priority for CIA's New Directorate," *Wired* (March 9, 2015).

Lewis, James A. "ZTE, the Telecom Wars, and Cyber Spies," *CSIS Briefs* (June 2018).

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'?" *The Journal of Strategic Studies*, Vol.35, No.3 (June 2012).

Mazanec, Brian M. “Why International Order in Cyberspace Is Not Inevitable,” *Strategic Studies Quarterly*, Vol.9, No.2 (Summer 2015).

Mozur, Paul and Jane Perlez. “China Is Reluctant to Blame North Korea, Its Ally, for Cyberattack,” *New York Times* (May 17, 2017).

Nakashima Ellen. “Pentagon Launches first Cyber Operation to Deter Russian Interference in Midterm Elections,” *Washington Post* (October 23, 2018).

Nakashima, Ellen and Steen Mufson. “U.S., China vow not to engage in economic cyberespionage,” *Washington Post* (September 25, 2015).

Nakashima, Elllen and Devlin Barrett. “U.S. Charges North Korean Operative in Conspiracy to Hack Sony Pictures, Banks,” *Washington Post* (September 6, 2018).

Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol.41, No.3 (Winter 2016/17).

Perlorth, Nichole. “Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies,” *New York Times* (Feb. 18, 2019).

Reuters. “With an Eye on Russia, U.S. Pledges to Use Cyber Capabilities on Behalf of NATO,” *New York Times* (October 3, 2018).

Sanger, David E. “Obama Ordered Wave of Cyberattacks Against Iran,” *New York Times* (June 1, 2012).

Sanger, David E. and Martin Fackler. “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say,” *New York Times* (January 18, 2015).

Sanger, David E. and William J. Broad. “Pentagon suggests Countering Devastating Cyberattacks with Nuclear Arms,” *New York Times* (Jan 16, 2018).

Sharp, Travis. “Theorizing Cyber Coercion: The 2014 North Korean

Operation Against Sony," *Journal of Strategic Studies*, Vol.40, No.7 (2017).

The White House. "Expanding Our Ability to Combat Cyber Threats," (April 2015).

The White House. "International Strategy for Cyberspace," (May 2011).

Abstract

Cybersecurity Threats, Counter Strategies and South Korea's Cyber Strategy

Noh-soon Chang (Halla University)

Cyberspace has been facilitating the expansiveness and complexity of national security. Under such a condition, cybersecurity threats which differ from traditional ones can be made diversely for its strategic purposes such as Cyber warfare, cyber coercion, cyber espionage, and supply network dominance. The counter strategies to prevail over malicious cyber operations are developed and applied with active cyber defense, counter cyber coercion, cyber counterintelligence, and supply network security strategies, respectively. Early this year, South Korea revealed the National Strategy for Cybersecurity that is based on deterrence and prevention. But this strategy can be expected to achieve its aims only by domestically introducing the policies and laws that cope with cyber attacks and maintain government performance, and internationally demonstrating its capabilities and willingness to do with allies and partners.

Key Words: Cybersecurity, Counter Strategy, Cyber Coercion, Supply Network Security, National Strategy for Cybersecurity

투고일: 2019.05.16 심사일: 2019.05.31 게재확정일: 2019.06.05.

Ⅱ

국제정치학적 관점에서의 사이버안보 논의와 국가차원의 대응전략

홍석훈 (통일연구원)

1. 서 론
2. 사이버안보의 중요성과 우리 정부의 대응체계
3. 국가차원의 사이버안보 강화를 위한 전략
4. 결 론

Summary

사이버위협은 개인의 단위뿐 아니라 국가적 단위로 확대되고 있다. 과학기술의 발달과 사이버 영역의 확대는 과거와 달리 광범위한 영역에서 상호이익을 창출하면서도 개인의 재산권 침해와 정보유출의 위협이 증가하고 있고, 국가를 중심으로 국제적 수준의 위협으로 인식되기도 한다. 무엇보다도 국가안보의 관점에서 사이버 공간의 위협은 새로운 수준의 대응방안을 요구하고 있다.

한국은 IT 기술력을 바탕으로 높은 수준의 국제 경쟁력을 가진 것으로 알려져 있으나, 사이버 공간의 확대와 접근 용이성, 보안 취약성, 행위자의 불명확성 등으로 인해 국가적 차원의 사이버위협이 증가하고 있다. 최근 청와대 국가안보실의 '국가사이버안보전략' 발표는 사이버안보의 중요성을 다시금 강조하는 계기가 되고 있다. 그러므로, 본 논문은 국가차원에서 진화하는 사이버 공간의 안보위협과 이에 대한 우리의 사이버 안보전략을 살펴보고, 향후 사이버위협을 통합적이며 효과적으로 방어하고 예방할 수 있는 국가 차원의 대응방안을 논의하고자 한다.

| **주제어** | 사이버안보, 사이버위협, 보안 취약성, 사이버안보 대응체제, 사이버안보 강화전략

1. 서 론

사이버위협은 개인의 단위뿐 아니라 국가적 단위로 확대되고 있다. 개인이 사용하는 정보통신은 국가단위의 교통, 통신, 자원분야, 국방, 금융 등의(ICBM: Internet of Things, Cloud, Bigdata, Mobile) 인프라와 연결가능하게 되었으며 국경을 초월하여 국제적 수준의 정보까지도 접촉, 교류가능하게 된 것이다. 이러한 과학기술의 발달과 사이버 영역의 확대는 과거와 달리 광범위한 영역에서 상호이익을 창출하면서도 개인의 재산권 침해와 정보유출의 위협이 증가하고 있고, 국가를 중심으로 국제적 수준의 위협으로 인식되기도 한다. 무엇보다도 국가안보의 관점에서 사이버 상의 위협은 새로운 수준의 대응방안을 요구하고 있다.

국가적 인프라 시설에 대한 사이버공격(Cyberattacks)은 이미 현실화 되고 있다. 이미 알려진 스턱스넷(stuxnet) 등의 경우는 군사적 영역까지 확대되었다는 것을 보여준다. 사이버공격 기제인 악성코드가 이란 핵시설을 마비시켰으며, 세계분쟁지역에서 사이버테러가 빈번하고 발생하고 있으며 사이버전쟁으로 확대되는 양상을 보이고 있다. 우리나라에서도 2017년 5월 2일 국방부 검찰단은 2016년 9월에 우리군 인터넷망과 인프라넷망이 북한 해커 조직에 의해 해킹당한 사실이 있음을 밝혔다.

한국에서 사회적 수준의 사이버 위협의 경험도 빈번하다. 2013년 3월 20일 '방송・금융전산망 해킹사건이 발생하여 KBS, MBC, YTN과 농협, 신한은행 등 전산망 마비 사태가 발생하였으며, 2014년 12월 15일'원전반대그룹(Who Am I) '이 한국수력원자력을 해킹하고 악성코드를 통해 원전 제어시스템을 파괴하겠다고 협박함으로써 우리 사회는 큰 충격을 받았다. 2010년 이후 국내원전에 대한 해킹시도가 무려 1840여회에 이른다는 국정감사 자료도 보도되었다.[1)]

또한, 북한의 핵능력 강화와 사이버전 능력의 향상 뿐만 아니라 해외의 사이버전 강화는 한반도 안보를 위협하는 중요한 요인으로 인식되고 있다. 특히, 북

1) 『서울신문』, 2014.12.20.

한은 1990년대 동구 사회주의권 몰락과 경제적 난관에 부딪혀 재래식 전력 증강이 힘들어지자 핵개발과 상대적으로 비용이 적게 드는 사이버전 능력 배양에 심혈을 기울여 온 것으로 파악된다. 물론, 남북관계 진전과 북미 비핵화 협상을 통한 한반도 평화체제가 가시화된다 하더라도, 국내외 사이버위협은 개인과 사회적 차원을 넘어 국가안보의 중요이슈로 부상할 것으로 예상 된다.

사이버 공간에서 한국은 IT 기술력을 바탕으로 높은 수준의 국제 경쟁력을 가진 것으로 알려져 있으나, 사이버 공간의 확대와 접근 용이성, 보안 취약성, 행위자의 불명확성 등으로 인해 국가적 차원의 사이버위협은 증가하고 있다. 최근 4월 3일 청와대 국가안보실에서는 대한민국 정부 최초로 '국가사이버안보전략'을 발표하고 국가 전반에 걸친 사이버위협에 대응하기 위한 정책 방안을 제시하였다.[2] 이처럼 사이버안보 분야에 대한 관심과 제고가 다시금 중요한 이슈로 부각되고 있다. 그러므로 본 논문은 정보통신의 발전으로 인한 사이버 공간의 안보위협 증가와 이에 대한 국제정치학적 관점에서의 사이버안보 개념과 대응 논의들을 살펴보고자 한다. 또한, 국가차원에서 우리 정부의 사이버안보 대응체계를 분석하고, 향후 사이버위협을 통합적이며 효과적으로 방어하고 예방할 수 있는 국가차원의 대응방안을 논의하고자 한다.

2. 사이버안보의 중요성과 우리 정부의 대응체계

가. 사이버안보의 중요성 증대

(1) 사이버 공간의 안보개념 확대

전통적 국가안보의 핵심은 국민의 생명과 안전을 보호하고 외부로 부터의 침입에 따른 피해를 방지하는 데 있었다. 그러나 최근 과학기술의 발전은 안보적 위협

2) 청와대 국가안보실에서는 2019년 4월 3일 '국가사이버안보전략'을 발표하고 국민을 위한 사이버안보의 3대 기본 원칙과 6개 전략과제 및 66개 소과제를 제시하고 있다: https://www1.president.go.kr/articles/5893(검색일: 2019. 5. 1).

에 대한 공격의 주체와 수단이 다양화되고, 가시적 피해와 위협의 구체성이 모호해 지고 있다.[3] 21세게 정보통신의 발전은 글로벌화(globalization)와 자본주의(capitalism) 확대를 추동시키고 있다. 이로 인해 과거 국가 간 국가 행위자에 의한 상호관계가 이루어졌다면, 이제는 사이버 공간을 통해 국경과 시간을 초월하여 개인과 개인이 직접 소통하고 교류하면서 새로운 정치・경제적 상호관계를 형성하고 있다.

이처럼, 정보기술의 발달로 사이버공간은 급격하고 팽창하게 되었고, 2000년대 이후 인터넷망의 확산으로 정치, 사회, 문화 활동이 급증하게 되었다. 더욱이 미국 9.11 테러 사건 이후 테러의 공포감이 커지면서 사이버공간의 테러로부터 보호하려는 정책적 연구로 확대되었다. 과거 냉전시대 국가간 군사적 안보영역에 집중되었다면, 냉전시대 이후 전통적 안보개념에서 사이버공간을 포함한 포괄적 안보영역으로 확대되고 있다는 점이다.

사이버(cyber) 용어는 1947년 미국의 수학자 노버트 워너(N. Wiener)가 프로세스 제어기술의 연속적 형태를 나타내기 위해 사용한 '사이버네틱스(cybernetics)'에서 출발하였으며, 사이버공간(cyber space)은 깁슨(W. Gibson) 소설의 『뉴로맨서(Neuromancer, 1984)』에서 컴퓨터가 생성한 이미지를 현실로 받아들이게 되는 상태를 지칭하였다.[4] 사이버공간은 물리적 제한에 관계없이 네트워크상에 구축된 가상의 공간으로 개인과 사회, 국가에 걸친 정보인프라와 실생활에 사용되는 정보 전반에 통용된다.

안보(security)는 라틴어 'Securitas'에 기원을 두고 있는데, 불안, 근심, 걱정으로부터 자유로움을 의미한다.[5] 안보란 위협의 존재와 주체의 행동이 전제되어 있는 것으로, 냉전시대 까지 개인과 사회는 안보의 대상으로 취급하지 않고 국가를 대상으로 그 안전을 고민해 왔다. 그러나 냉전이후 '인간안보'라는 의미가 포함되면서 안보개념도 확산되고 있다.

---

3) 유호근・설규상. 2017. "사이버안보 체계: 거버넌스 형성의 문제와 한국" 『한국정치외교사논총』, 제38권 2호,(2017), pp.237-238.
4) 조성렬, 『전략공간의 국제정치-핵, 우주, 사이버 군비경쟁과 국가안보』(서울: 서강대학교 출판부, 2016), p, 377.
5) 이성만 외, 『국가안보의 이론과 실제』 (서울: 오름, 2013), p.18.

이러한 사이버 공간의 자유성과 초월성은 국가 간 상호협력과 경제적 이익을 창출하는 순기능으로 작용하지만, 광범위한 사이버 공간은 공격과 침해의 기제로 활용될 가능성이 크다. 이러한 사이버 상의 위협은 국가안보 문제 영역으로 확대되어 자국의 사이버 시스템을 마비・파괴 시키거나 막대한 경제적 손실, 그리고 사회적 혼란을 도모할 수 있기 때문에 국가차원의 다양한 법적・제도적, 기술적 방안과 대응조치를 마련하고 있다.

이처럼 21세기 정보기술의 발전은 국가안보를 위협하는 새로운 유형의 안보영역으로 사이버분야를 고민하게 되었다. 국가안보에 주축을 이루었던 전통적 분야인 군사영역을 넘어서 사이버 역량(cyber power)이 중요한 안보 요소로 등장하게 된 것이다. 기존 연구에 있어, 사이버안보 연구는 비전통 분야로 분류되어 대부분 사이버시스템 침해 방지와 보안에 그 주안점을 두었다. 이런 이유로 대응방안 역시 기술적 요소와 법적 조치 방안에 집중되어 있었다.[6] 즉 사이버 시스템 침해 방지와 보안에 주안점을 두었기 때문에 기술적, 법적 조치에 집중하였고, 사이버 위협의 주체에 대한 국제법이나 사법공조와 같은 법적 구속력으로 통제가능하다는 입장이었다.

그러나 21세기 사이버 위협의 주체와 공격의 방법이 다양화 되면서 이러한 전통적 방법의 대응책만으로 사이버 위협을 막는다는 것은 한계가 있다. 실례로 2007년 에스토니아, 2008년 조지아(그루지아), 2010년 이란 경우와 같이 국가적 차원의 사이버 공격은 기존의 사법적 대응방안으로 처벌이라 예방이 힘든 상황이기 때문이다. 또한 국내 정부, 언론, 금융기관의 해킹사건과 디도스(DDos: Distributed Denial of Service) 공격 등은 국가 간 전략적 차원에서 국가차원에서 실행되었으며 안보적 차원의 위협이 가시화 되었다. 그러므로 사이버 위협은 국가・안보차원의 연구가 필요하게 되었다.

---

6) 유호근・설규상, 앞의 글, p.240.

[표 1] 사이버공격으로 인한 주요 피해 사건

year	Operation Country	Contents of damage caused by cyber attack
2016	Russia	US Democratic National Committee (DNC) Information Disclosure
2015	China	US federal officials 21.5 million information outflows
2014	Russia	US White House Computer network Penetration
2014	North Korea	US Sony Pictures attack • Information leak
	USA	North Korea Labor Newspaper Website Paralysis
2013	North Korea	Korean Broadcasters • Financial Institutions 3.20 • 6.25 Cyberterror
2012	Iran	US financial firm attacks Israeli government
2011	North Korea	Korea NH Agricultural Cooperation Network Paralysis
2010	USA	Iran Stuxnet nuclear uranium facility destruction
2008	Russia	Gurusia homepage tampering, DDoS attack paralysis
2007	Israel	Syria's air defense network neutralized
2007	Russia	Estonian DDoS attack Internet paralysis
2001	USA	Iraq information system, command communication network disablement
1993	USA	Disabling Serbian network infrastructure
1991	USA	Iraq war information network, disturbance of air defense network, psychological war

출처: 함승현・박대우 2017, p. 1669[7)]

사이버안보는 인터넷망을 근간으로 민간・공공부문과 연결되어 있으며, 전통적 안보에서 다루는 군사안보 분야 보다 훨씬 다양한 분야와 공격기제, 그리고 공격 주체를 가지고 있다. 국가안보 수준에서 사이버안보는 개인, 기업, 사회단체, 정부기관의 주체를 포함하고, 국가정보망의 방어체계, 국가 재산권, 공공인프라 분야와 개인의 인적, 물적, 지적재산권을 포함한다. 즉, 국가 사이버안보(National Cybersecurity)는 사이버공격, 사이버테러, 사이버전쟁에 대응하는 국가 차원의 대응전략과 방안이 필요한 것이다.[8)]

---

7) 함승현・박대우, "국가 사이버안보를 위한 정책 연구"『한국정보통신학회논문지』 제21권 9호, (2017), p.1669.

8) 사이버전쟁이란 사이버공격 및 사이버테러를 통하여 군사적 목적달성을 위한 국가인프라파괴, 지휘통제전, 군사정보전, 정보전, 미디어심리전, 해킹전, 경제정보전 등의 국가와 국민의 안전을 위해를 가하는 물리적・전자적・경제적・정신적・인적 전쟁수행을 말한다(함승현, 박대우 2017, 1667). 김소정・김규동은 사이버공격, 전쟁 등이 개념적 이해 없이 혼재되어 있음을 지적한다. 사이버공간에서 일어나는 위협 사례들은 소위 "사이버 오퍼레이션(cyber operation)"개념 정의한다. "사이버 오퍼레이션"은 국가와 국제사회에 대한 위협 수준은 대규모 사이버범죄로 인한 경제적 피해와 사회적 불안정에서부터 국가 중요시설과 국가정보에 대한 위협, 군사적 사이버 공격으로 인한 전쟁의 가능성까지의 범위를 포함하는 등 폭넓고 심각하게 제기된다고 말한다(김소정・김규동, "UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의"『정치・정보연구』 20(2), (2017), p.89.).

사이버안보를 위한 국제적 차원의 논의와 협력은 다양한 수준에서 진행되고 있다. 1997년 G8은 테러리스트들의 통신과 연락망을 공유하는 국제형사경찰기구(INTERPOL)와의 협조 하에 상설 비상연락망을 설치하였다.[9] 경제협력기구(OECD), 국제전기통신연합(ITU), 북대서양조약기구(NATO) 등이 사이버안보를 위한 조치와 대응전략을 협의해 왔다. 특히 NATO는 2007년 에스토니아 사이버 공격 사건을 계기로 군사안보분야를 사이버안보 영역으로 확대하여 2008년 'NATO 사이버 방어정책'을 수립하였으며, 국가주권 원칙을 존중하고 국제・지역・국내적 수준에서 구조 및 역량의 중복 회피, 신뢰에 기초한 사이버 공간의 안보 정책의 세 축으로 채택하였다.[10] 이후 나토(NATO)는 사이버 방위를 나토방위계획과정에 일부로 통합시키고 (2012년), 사이버위협과 도전에 대한 민간부분과 협력을 진작시키고 EU(유럽연합)와 사이버 방위에 관한 기술협정을 체결하였다(2016년).

또한, 사이버안보에 대한 국제규범 논의에 있어 정부 간 기구 논의로는 UN GGE(GGE: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security)가 대표적이다.[11] 소다자적 차원에서는 유럽안보협력기구(OSCE: Organization for Security and Co-operation in Europe)의 신뢰구축조치 프로세스와 상하이협력기구(SCO: Shanghai Cooperation Organization)'가 있다.

(2) 국제정치학적 관점에서 사이버안보 논의

사이버안보는 국제정치학과 정책결정론에서 새롭게 대두되고 있는 도전적 분

9) 유호근・설규상, 앞의 글, p.246; Nazhi Choucri, Stuart Madnick and Jeremy Ferwerda, "Institutional for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development* Vol. 20, No. 2., (2014), p.109.

10) 유호근・설규상, 앞의 글, p.247.; Catalin-Ionut Nastasiu, "Cyber Security Strategies in the Internet Era," *Scientific Research and Education in the Air Force* NO. 2(2016) p, 621.

11) 김소정・김규동, "UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의" 『정치・정보연구』 제20권 2호, (2017), p.90.

야이다. 또한 국가안보, 경제, 인권, 시민 사회와 국제규범과 같이 다양한 분야에서 사이버안보 문제가 중요한 쟁점으로 부각되고 있으며, 사이버공간이 영토 주권처럼 방어의 경계선이 명확하지 않지만 국가안보 분야와 산업기밀과 개인의 정보유출 등 사이버 공격 대상이 급증함에 따라 국가적 차원의 안보대상으로 활발한 논의가 이루어지고 있다.

첫 번째, 국제정치학 분야에서 현실주의적 입장(Realists' Approaches)을 살펴보자. 먼저, 안보대상에 대한 인식이다. 주체와 대상이 변화함에도 불구하고 안보의 본질은 안보의 위협과 그 대응이라는 본질적 구조에 집중하는 것이 현실주의적(realism) 접근방법이다. 왈츠는 3가지 이미지(levels of analysis) 분석방법 중에서 국가를 하나의 행위자(unit)로 보고, 국제정치를 구조적 입장에서 분석한다.[12] 국제정치는 국제체제(international-system) 수준에서 논거 되고 있으며, 국가는 행위자 주체라고 본다. 이러한 현실주의적 이론은 최근까지 국가를 단위로 전제하고 안보의 위협을 분석해 왔다.

또한, 현실주의자들은 국제체제의 무정부 상태를 지적한다. 이러한 무정부 상태는 국가안보딜레마를 야기시킨다고 본다. 국가가 자신의 안보를 지키지 위해서는 모든 조치를 취해야 하며, 의도와 상관없이 다른 국가에게는 안보 위협의 존재로 인식되는 상충관계를 만든다. 결국, 국제관계는 제로섬 게임의 성격을 갖게 되고 사이버공간에서의 국가안보 상충관계는 곧 사이버안보 딜레마 성격을 가지게 된다는 입장이다.

사이버공간에서 안보위협에 대한 급증은 국제안보질서의 구조적 측면에서 분석하는 입장에서, 과거 냉전 구조적 국제체제 무정부 상태에서는 국제안정성을 결정하는 요인들이 초강대국이 참여한 전쟁과 강대국들 사이의 관계이었으나,[13] 냉전체제 붕괴 이후 정보발달로 인해 국제안보질서의 수평적으로 평준화시키는 경향이 증대되고 있어 군사력 강화를 통한 공격력 확보 보다는 네트워크

12) Kenneth N. Waltz, *Man, the State, and War* (New York: Columbia University Press, 1959).
13) John Mearsheimer, *The Tragedy of Great Power Politics* (W.W. Northon & Company, 2001).

에 기반을 둔 사회시스템을 방어해야 하는 문제가 발생하게 되었다고 보는 입장이다. 미어샤이머(J. Mearsheimer)의 공격적 현실주의는 과거 냉전시대의 초강대국들간의 헤게모니 추구에 따라 핵공격이나 선제타격의 방법을 통해 국제질서가 유지될 수 있었다고 한다면, 사이버공간의 확대는 지휘, 통제, 통신, 첩보시스템 등 군사핵심 기간시설의 범위를 수정하도록 요구하고 있다. 결국, 초강대국들은 사이버공격 수단을 활용하여 상대국가의 정보시스템을 마비시키거나 혼란을 유도하기 위한 사이버전략을 마련하여 국가안보 위협에 대비하고 있다는 분석이다.[14]

국가안보 차원에서 사이버안보를 포함하여 하드파워인 핵과 재래식 무기를 활용한 군사작전뿐만 아니라 정보시스템 유지와 외부 사이버공격에 의해 정보파괴, 훼손 등을 당하지 않고 경제, 행정시스템이 원활하게 기능할 수 있게 하는 구조적 방어능력이 국가안보의 핵심요소가 되고 있음을 주장한다.[15] 사이버공간에서의 공격을 통해 초강대국의 안보 혹은 사회시스템이 파괴되는 사례가 발생하고 있기 때문이다.

이러한 분석 틀에서 사이버안보와 관련하여 가장 위협적인 사이버공격 유형으로 사이버전이다. 사이버전의 개념 규정은 사이버안보를 논의하는 출발점이며, 사이버전의 개념은 광범위하게 정의되어 사용되고 있다. 나이는(Nye) 사이버전이 재래식 전쟁과 차별화하고, "사이버공간 이외에서 물리적 폭력을 확장하거나 동등한 파급효과를 불러일으키는 사이버 행위"라고 규정하고 직접적인 정치 및 군사적 목적을 위해 비물리적(non-kinetic) 수단을 활용한 컴퓨터 네트워크 공격이나 심리전 목적의 공격을 배제한 것으로 규정되기도 한다.[16] 사

14) 장노순, "초국가적 행위자의 사이버공격과 핵공격에 관한 비교연구: 국제안보질서의 안정성을 중심으로"『한국정치학회보』39집 5호 (2005), p.271.

15) Alfred A. Jones, "Information Security: Planning for the Deluge," *The Information Revolution and National Security Dimensions and Direction* (The CSIS Press, 1996), pp.15-23.

16) Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5(5) (2011), p.9; 장노순·한인택, "사이버안보의 쟁점과 연구 경향,"『국제정치논총』53(3) (2013).

이버전의 공격자는 국가 혹은 비국가 행위자로 제한하고 있지는 않지만, 전시일 경우는 사이버전의 공격 주체는 국가일 수밖에 없고 사이버공격은 곧 사이버전쟁에 해당된다.

최근 냉전기의 억지전략 경험을 사이버 공간에 적용하여 '사이버 억지(cyber deterrence)'의 개념을 발전시키고 있다. 2013년 발간된 '탈린 매뉴얼(Tallinn manual)'은 북대서양조약기구(NATO) 산하 사이버방위협력센터(Cooperative Cyber Defense Center of Excellence)의 후원 하에 기존의 국제법 틀 안에서 사이버 공격 및 그와 관련된 여러 행위를 법적으로 해석하려는 시도이다. 탈린 매뉴얼은 사이버 공격으로 인한 교란, 파괴적 효과를 야기하는 '무장공격(armed attacks)'에 대한 국가가 자위(self-defense) 차원에서 법적 대응법을 제시하고 있다. 오바마 행정부도 이러한 취지에서 2012년 인명 살상이나 국가안보에 위해를 야기할 수도 있는 즉각적 또는 지속적 위협을 저지하기 위해 군사작전을 실행하도록 지시하는 명령을 만들었다.[17]

현실주의적 입장에서는 핵무기 출현과 같이, 사이버위협은 새로운 무기체계를 구축하는 것으로 기존의 안보체제를 수정해 나가고 있음을 지적한다. 사이버 공간에서 국가 행위자 주체 개념이 약화 된다 하더라도 여전히 국가가 주도하여 사이버 공격을 효과적으로 방어해야 한다는 구조적 접근법을 활용하고 있다. 국가안보를 위해 전통적 군사안보 전략에만 집중하는 것이 아니라, 안보체제 내부의 정보시스템 방어와 유지 등 행정시스템이 원활하게 기능할 수 있게 하는 구조로 전환하고 있음을 지적한다. 과거 핵위협의 대응은 강대국이 국제안보질서의 구조적 측면에서 공격적 현실주의에 기반한 것에 비해, 최근 강대국은 초국가적 사이버공격에 대비하여 방어적 현실주의에 입각한 전략을 채택하고 있다고 분석한다. 정보통신 기술 발달과 사이버 공간의 급격한 발전은 공격의 주체와 공격의 목적이 다양하기 때문에 헤게모니를 가진 초강대국이 유일 패권주의를 주장하는 것이 아니라 다자주의적 접근방법을 수용할 가능성 크며, 과거 전

17) 김상배, 『사이버 안보의 국가전략: 국제정치학의 시각』(사회평론, 2017), pp.32-33.

쟁 억지론과 달리 '억제-보상'이라는 포괄적 억지전략의 수정을 그 대안으로 삼고 있다.

두 번째, 신자유주의적 입장(Neoliberalists' approaches)은 사이버위협을 막고 자유로운 사이버공간의 활용을 위한 국제적 협력을 강조한다. 사이버안보는 전통안보와 구별되는 특징을 가진다. 정보통신 발달로 사이버공간의 확대는 사이버 안보 위협 행위자 수준이 국가단위를 초월한다는 것이다. 왈츠의 왈츠는 3가지 이미지(levels of analysis) 분석 방법에서 첫 번째, 두 번째 수준의 개인과 사회(국내수준)가 사이버안보의 주체로 등장하기 때문이다. 현실주의적 입장에서는 국가를 중심으로 행위자 모델을 상정하고 있지만, 신자유주의적 입장에서는 국가 보다는 개인과 사회가 행위자 모델이 될 수 있으며, 국가 정책 역시도 국내적 요소로 인해 전략변화가 일어난다는 기본 가정에서 출발한다.[18]

사이버안보는 군사적 분야의 위협을 포함하여, 사이버의 초연결성은 개별 컴퓨터와 인터넷 서버를 매개로 한 모든 사물과 공간으로 확장되어 적용해야 한다는 것이다.[19] 또한, 사이버 공간의 초국가성으로 인해 위협 주체가 비국가 행위자일 수 있고, 사이버 위협이 비군사적 영역에서 일반사회 영역까지 확장됨에 따라 국가 간의 협력을 통해 사이버안보를 확보하는 것이 필수적이라는 관점이다.

사이버공간을 두고 강대국들 간에 이해가 충돌하고 사이버 위협이 민간인의 피해가 우려되는 가운데 사이버 공간을 규율하기 위한 국제협력의 필요성이 지속적으로 제기되어 왔다.[20] 사이버안보의 국제규범과 관련한 논의들은 이러한 신자유주의적 관점에서 발전되고 있다. 국제사회에서 사이버 공간의 질서를 회복하기 위한 논의들은 이러한 입장에서 최근 부상하고 있다. 물론 사이버 공간에서의 위협과 대처방안에 대한 주체화 방안에 대한 명확한 개념 정립은 되어 있지 않지만, '사이버 범죄'에 대응하기 위한 국제공조체제를 수립하려는 의도

---

18) Andrew Moravcsik, "Taking Preferences Seriously: A Liberal Theory of International Politics." *International Organization* Vol. 51, No. 4(1997).

19) 조화순・권웅, "한국과 미국의 사이버안보 거버넌스: 사이버위협의 안보화 관점에서의 비교"『정보사회와 미디어』제18권 2호 (2017), p.98.

20) 이상현, "국제규범론으로 보는 사이버 안보,"『사이버 안보의 국가전략』(서울: 사회평론, 2017), pp.66-67.

에서 출발하였다.[21] 국가 관계에서 사이버안보 문제는 중요한 사안으로 거론되고 있으나, 사이버 공간에 대한 국제규범이나 법적 통제 장치에 대한 논의는 미약한 것이 사실이다. 개인적 차원의 사이버 범죄에 관해 유럽 사이버범죄협약(The Council of Europe Convention on Cybercrime) 있으나 유럽 중심의 30여 개 국가만이 비준하였으며, 중국과 러시아는 이에 반대하는 입장이다.

또한, 사이버 공간에 대한 자유성에 대한 논의이다. 기본적으로 사이버 공간의 초국가성으로 인해 인터넷 자유권과 정보콘텐츠(information content)와 정보 인프라(information infrastructure)의 권한 문제가 대두된다. 신자유주의적 관점에서 본다면 사이버 공간의 활동은 국가안보에 피해가 되지 않는다면 적극적으로 자유롭게 보장되어야 하며, 경제적 이익 역시 사이버 행위 주체에게 돌아가야 할 사안이기 때문이다. 사이버 관련 안건들은 국가 간 입장차이가 커서 규범에 대한 합의가 쉬운 것은 아닐 것이다.

과거 사이버 안보의 규범을 창출하기 위한 노력은 1990년대부터 2000년 초반까지 '사이버 범죄'에 대한 국가 간 공조체제를 마련하는 데 집중되었다. 국가 주체 행위자 간의 협력 차원이 아닌 국가 대 비국가 행위자의 협력관계이어서 비교적 용이 하였으며, 사이버 범죄에 대한 초국가적 협력의 공동의 이익이 발생하는 사안이었기 때문이었다. 사이버 범죄에 관련한 개인적 차원을 대상으로 국가 간 협력이 이루어 졌기 때문에 가시적 성과를 보였다. 앞서 언급한 유럽평의회(Council of Europe) 주도로 사이버범죄협약이 2001년 채택되고, 2004년 발효되었다. 여기에 유럽평의회 회원국 이외에 호주, 도미니카, 일본, 미국 등 다른 지역의 국가들도 자발적으로 참여하였다. 또한, G8 도빌 정상회의(2011.5.27-28) 인터넷 관련 규범체계 수립 및 사이버 공간 사용을 위한 행동규범 개발(Norms of Behavior)을 촉구하기도 했다. 미국과 대비되는 접근 방식으로 중국이 주도하는 '상하이협력기구(SCO: Shanghai Cooperation Organization)'가 있다. 2001년 중국, 러시아, 카자흐스탄 등의 국가들이 참여하는 협력기구로 에

21) 조화순・김민제, "사이버공간의 안보화와 글로벌 거버넌스의 한계," 『법학연구』 제16권 제2호 (2016).

너지, 경제, 문화 영역에서 협력을 강화 하는데 있었다.

[표 2] 사이버 공간을 보는 시각

구분	영미권 국가	중국, 러시아 등 (사회주의권)
사이버 공간에 대한 입장	중립적인 공간	국가 주권이 미치는 공간
규제(개입)	민간중심	국가중심
인터넷 거버넌스 모델	다양한 이해관계자 참여 필요 (Multi-stakeholder Model)	국가 중심의 논의 필요 (새로운 규범, 국제기구 등)

출처: 이상현, 『사이버 안보의 국가전략』(서울: 사회평론, 2017), p.68.

마지막으로 구성주의 논의와 글로벌 거버넌스론적 입장(Constructivists' & Global Governance's approaches)에서의 사이버안보 논의이다. 사이버안보의 개념은 사회 구성원 간의 결과물이라는데 중점을 두는 구성주의적 논의도 주목해야 한다. 사이버공간에서 행위자 간 인식의 문제로 인해 사이버안보가 결정된다는 사회 구성적 개념이다. 웨버(Ole Waver)는 "안보화를 안보와 관련된 담론이 사회적으로 형성되는 과정으로 정의하는데, 안보를 객관적으로 실재하는 조건이 아닌 현존하는 위협에 대한 사회 합의를 주관적으로 구성하는 정치적 담론과 그 담론에 따른 결과물로 규정"하고 있다.[22]

구성주의적 시각에서 안보란 사회구성권 간에 오랜 기간 동안 어떠한 행위와 사건이 공통의 위협으로 인식되는 '사회적 공유(Shared idea)'과정을 거쳐서 만들어지는 개념이다. 즉, 사이버안보의 개념도 어떠한 사건이나 행위들이 사회구성원 간에 공통의 위협으로 인식하는 사회적 과정을 통해서 생성된다는 것이다. 안보는 그 주체가 무엇을 안보적 조건(being secured condition)으로 인식하고 개념화하느냐의 문제로, 궁극적으로 주체가 어떠한 사회적 조건과 환경에 놓여 있는가를 고민하고 선택하는 문제로 간주한다.[23]

22) 조화순・권웅, 앞의 글, p.102.
23) 박인휘, "새로운 이분법의 기로에 선 한국의 안보: 북핵문제와 남북미 관계," 박인휘 외 엮음, 『탈냉전사의 인식』 (서울: 한길사, 2012), p.185.

따라서 위협이라는 것은 특정의 단일한 차원과 내용으로 존재하지 않고, 개인적 차원에서든, 사회적 차원에서든, 지역적 차원에서든 다양한 위협들이 필연적으로 경쟁 한다. 그러므로 다양한 위협들 중 무엇을 중요한 위협으로 인식하는 것이 중요한 문제가 되며, 즉 '경쟁하는 위협'은 본질적으로 서로 경쟁하는 위협들 간 정치적 우선순위의 문제를 제기하게 된다. 무엇을 안보문제 혹은 위협으로 확정한다는 것은 특정 유형의 위협해소 문제를 정책적으로 선별해야 한다는 논리이다.[24)]

구성주의적 시각에서도 사이버안보를 정책적으로 선별하여 국가 혹은 사회 내부에서 우선순위로 올려놓고, 이를 실천하는 과정으로 설명한다. 사이버안보에 대한 위협 인식과 이를 국가 또는 사회의 안보 범주에 포함하여 적극적으로 확대・방어 정책을 전개시키는 것의 일련의 과정은 '사회구성적 논의'라는 것이다. 이러한 구성주의적 시각에서 사이버안보의 개념은 사회적으로 구성되어온 결과물로써 사이버안보 거버넌스 개념을 이해하는 단초를 제공한다.[25)]

'거버넌스(governance)'의 개념은 매우 다양한 분야에서 사용되고 있다. 먼저 비교정치학에 있어 거버넌스는 민주주의 발전에 미치는 영향과 정치경제학적 측면에서 분석되고 있다. 국제정치학적 접근법에 있어서는 세계화, 정보화 확산으로 정치행위자의 다양성이 지적되면서 정책결정과정과 이행과정에서의 다양한 주체들에 대한 관여와 지방의 역할 등이 강조되고 있다. 또한, 거버넌스 개념은 시민의식 성장과 시민사회의 발전은 자율적 통치(self-governing)를 근간으로 다양한 주체들이 정치에 참여하는 것을 말한다. 즉 정치 행위에 있어 상이한 주체들이 위계적으로 연계되는 것이 아니라 다양한 복합적 관계를 가지는 '네트워크'개념과 연결되어 있다. 그러므로 정치 행위자 간의 관계와 행위자 내부의 관계도 거버넌스의 대상이 된다. 결국, 거버넌스 개념은 민주주의 발전뿐만 아니라 정치・경제적 측면에서도 정책망(policy network), 네트워크 이론을 활용하고 있다. '국가와 사회'의 위계적 접근을 탈피하여 다양한 사회적 행위자와

24) 나용우, "초연결융합시대와 사이버안보: 사이버공간의 안보화와 한국의 사이버안보 강화 방안," 『Journal of North Korea Studies』 제3권 2호 (2017), pp.29-51.
25) 조화순・권웅, 앞의 글, p.102.

국가와의 수평적 관계를 제시하며 '상호조정과 협의'에 관심을 기울이는 영역까지 확대된 것이다.[26]

결국, 거버넌스의 개념은 민주주의와 시장경제를 중심으로 정보화와 지역화의 발전으로 다양한 비정부 단위들이 국가 행위 또는 정책 결정에 참여하는 형태를 말한다. 그리고 다양한 주체들이 위계적으로나 무정부적으로 연결되는 것이 아니라 협력적 네트워크 중심으로 정치질서를 산출하는 현상으로 해석될 수 있다. 이러한 거버넌스 논의는 사이버 공간에서의 '글로벌거버넌스' 입장으로 표현되어 분석하는 경향이 있다.

글로벌거버넌스의 관점에서 사이버공간은 국가만이 관여하는 장소가 아니라 초국경 행위자들이 자신의 자유와 활동을 위해 국가와 개인, 사회가 서로의 자율적 통제를 기반으로 사이버위협을 최소화하는 것에 집중한다. 즉, 사이버 공간에서 상호 이익을 기반으로 네트워크 형성하고 자유적인 상호조정과 협의를 통해 갈등을 조정하고 상대방에 대한 피해를 막는다는 것이다. 최근 미국과 영국은 사이버안보 문제를 개인과 공공부분의 동반자(public-private partnerships) 관계를 기본 축으로 접근하고 있다. 사이버안보의 대상 역시 사이버 공간을 사용하고 있는 개인(시민)과 사업자 인터넷 그 자체를 구성하는 세가지 요소를 동시에 고려해야한다고 주장한다.[27] 이러한 논의들은 사이버안보가 국가에만 치중하는 것이 아니라 사회구성원 모두에게 적용되는 사안임을 말해 준다. 따라서 시민사회의 발전으로 과거 전통적 안보의 개념으로 사이버 공간을 국가가 지배하는 것에 대한 비판적 관점에서 출발한다.

2000년대에는 미국의 9.11 테러 사건 등을 경험하면서 사이버공간에서의 단순한 사이버 범죄 문제 사안에 그치지 않고 국가적 차원의 사이버 공격과 안보의 문제로 확장하여 인식하기 시작했다. 또한, 이러한 논의들은 글로벌 차원의 거버넌스 구축을 요구하기 시작하였다. 2003년 이라크 전쟁, 2007년 에스토니

---

26) 서창록, 『한반도 평화번영의 거버넌스 구축을 위한 이론적 틀』(서울: 통일연구원, 2006).
27) Madeline Carr, "Public-private partnerships in national cyber-security strategies," *International Affairs* Vol. 92, No.1(2016).

아 디도스 공격, 2008년 조지아에 대한 사이버 공격 등에서 사이버 공간이 전쟁의 수단으로 활용되었기 때문이다. 이러한 위기감은 사이버 안보와 관련한 글로벌 차원의 '국제레짐' 추진에 대한 논의로 발전되었다.

2013년 UN의 '국제안보 관점에서 정보통신분야의 발전에 관한 정부전문가그룹(GGE: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security)'의 최종보고서는 사이버안보에 관한 의미 있는 시도였으며, 제64차 UN 총회에서 GGE의 최종보고서가 채택되었다. 이 보고서는 정보통신기술이 국제안보를 해치는 수단으로 악용되어 국제안보 위협요소가 될 가능성에 대한 국가들의 우려를 기초로 작성되었으며 국가가 대리인을 이용하여 국제위법행위를 범하지 않고, 자신의 영토가 ICT(Information and Communication Technology)를 불법적으로 사용하는 비국가 주체가 이용되지 않도록 규정하였다.[28] 즉, 핵심 내용은 사이버 공간에서 국가 행위가 기존의 국제법 적용 대상이 될 수 있고, 전통적 안보협력 조치로 투명성, 신뢰구축 방안 등을 확대하기로 한 것이다.[29]

그러나 사이버안보에 대한 국제규범에 대한 안보적 의미는 미국을 중심으로 하는 서구적 시각과 중국과 러시아를 중심으로 비서구적 시각으로 대비되고 있다. 미국을 중심으로 하는 사이버안보의 국제규범화는 국내 정보 자유화와 경제적 사이버 범죄와 같은 경제적 분야에 중심을 둔다. 그러나 중국과 러시아를 중심으로 하는 비서구적 접근방식은 국제안보 수준에서 사이버 위협을 통제하고 억지해야 한다는 것이다. 즉 서구적 입장은 자발적인 사이버안보의 협력을 통해 정보의 자유로운 소통과 경제적 이익을 추구하는 것인데 반해, 비서구적 그룹의 방식은 정부의 철저한 정보 통제와 외부의 이념적 공격으로 인식되는 정보 차단을 주요 골자로 삼고 있다.

---

28) 조화순・김민제, 앞의 글, p.85.

29) 장노순・한인택, "사이버안보의 쟁점과 연구 경향,"『국제정치논총』 제53권 3호(2013); Detlew Wolter, "The UN Takes a big step forward on Cybersecurity," *Arms Control Today* 43 (September 2013).

[표 3] 국제정치학에서 사이버공간을 바라보는 시각

구분	현실주의	자유주의	구성주의
사이버 공간을 바라보는 입장	국가 주권이 미치는 공간	중립적인 공간	중립적인 공간
규제	국가 중심	민간 중심	사회구성원 합의
거버넌스 모델	국가 중심의 국제기구	다양한 주체가 참여하는 국제기구	상호주관성 인정, 다양한 주체 참여
사이버안보 주체	국가단위	다양한 주체	사회적 합의, 정치적 과정

출처: 저자 정리

정리하자면, 전통적 안보개념으로서의 사이버안보 접근은 자칫 개인의 정보 활동 자유와 경제적 이익 창출을 가로 막는 제재 요인으로 작용하기 쉽다는 지적도 있다. 또한, 전통적 안보관으로 인해 새롭게 발전하는 사이버 공간의 사회, 문화 교류를 막고 국가의 통제와 패권국가 간의 경쟁만을 양상 한다는 점도 부각 되고 있다. 하지만 새롭게 진행되고 있는 사이버공간의 위협을 방지하고 개인의 사이버공간의 자유로운 향유와 경제적 이익을 창출하기 위한 국가 차원의 대응전략 마련도 요구되고 있다. 나아가 국가 간 사이버 공격을 막을 수 있는 안보적 차원의 사이버 능력배양과 모든 국가가 합의할 수 있는 사이버 규범체계 수립도 시급한 상황이다.

나. 사이버위협에 대한 한국의 대응체계

한국에서 일반적 보안업무는 1961년 '중앙정보부법'에 의해 중앙정보부가 이를 수행하기 시작하였으며, 동법의 제3조 제2항과 대통령령으로 규정된 '보안업무규정'(1964) 및 '정보 및 보안업무 기획・조정 규정'(1981) 등에 의거하여 냉전 종식 시기까지 군사・외교안보적 관점에 초점을 두었다.[30] 1980년대 컴퓨

30) 박종재・이상호, "사이버 공격에 대한 한국의 안보전략적 대응체계와 과제" 『정치・정보연구』, 제20권 제3호, (2017), p.82.; 『2015국가정보보호백서』(2015).

터의 등장과 전산업무 발생은 1988년 '전산업무보안관리지침'이 제정・시행되었으며, 1989년 6월 국가안전기획부는 산업보안을 보안업무에 포함시켜 산업기밀 보호활동을 수행하기 시작하였다.

또한, 1986년 제정한 '정보망 보급과 확장과 이용촉진에 관한 법률'은 보안 및 정보보호를 위한 법률 규정이었지만, 1980년대 기본적으로 정보화를 촉진하기 위한 것이어서 해킹이나 바이러스 침해 등 사이버 위협에 적극적이지는 않았다. 우리 정부는 컴퓨터의 확산과 전산망의 확대로 인해 증가하는 사이버 범죄를 규정하고 처벌하는 '정보촉진 기본법'(1995년)을 제정하고, '정보통신망 이용촉진 등에 관한 법률'(1999년)로 개정하여 정보화 침해에 대한 대응규정을 마련하였다.

2000년대 들어 정보통신의 의존도와 통신망 확산으로 인해 '정보통신 기반보호법'이 제정되고, 2003년부터 정보화 역기능 방지를 위한 국가기관이 설립되기 시작하였다.[31] 2005년 '국가사이버안전관리규정'(대통령훈령 제141호)을 통해 국가사이버안보 활동의 체계가 구체화 되었다. 2007년 '전자정부법'과 '정보통신기반보호법'이 개정되어 각급 행정기관장이 해당 정보통신망에 대한 보안조치를 시행하고 국가정보원장이 그 안정성을 확인하게 하는 등 2000년대 들어 사이버 침해와 방어를 위한 정부차원의 법적 노력들을 강구하기 시작하였다.

그러나 2009년 7월 정부, 금융기관 등에 대한 디도스(DDoS) 공격이 발생하여 주요사이트의 서비스 장애 및 마비 사태가 나타났다. 사이버 공격 주체가 북한으로 밝혀지면서 국가차원의 사이버안보 인식과 대책 방안에 대한 관심이 높아졌다. 이러한 계기로 '정보화촉진기본법'이 전면 개정되어 '국가정보화에 관한 법률'이 제정되고, 2010년 '국방정보화 기반조성 및 국방정보자원 관리에 관한 법률'이 제정되어 국방정보본부 산하에 사이버사령부가 신설되어 국가차원의 사이버안보 대응체계가 대폭 강화되었다.

---

31) 사이버테러 대응역량 강화를 위해 (구)한국정보보호진흥원(KISA) 내부에 '인터넷침해사고대응지원센터,' 국가정보원 산하에 '국가사이버안전센터,' 국방부 기무사령부에 '국방정보전대응센테'등이 설립되었다 (박종재・이상호 (2017), p.83).

이러한 노력에도 불구하고 2011년 3월 4일 '디도스 공격'과 농협전산망 장애 사건이 발생하자, 정부는 사이버위협이 국가안보와 직결된다는 인식 하에 '국가 사이버안보 마스터플랜'을 범정부 차원의 청사진을 마련하고, 사이버 공간을 새로운 영역으로 포함하여 국가차원 대응제계를 5대 분야(예방, 탐지, 대응, 제도, 기반) 중심의 전략과제를 선정하여 추진하게 된다.[32] 이후 2013년 사이버위협이 발생하자 '국가 사이버안보 종합대책'을 추가로 수립・시행하게 된다.[33]

우리 정부는 2014년 '사이버위협 정보 분석・공유 시스템'(C-TAS: Cyber Threats Analysis System)을 구축하여 주요 민간 사이버업체들과 연계하여 사이버위협 정보를 공유하고 연계하여 대응하는 시스템을 고도화하였다(미래창조과학부 2014). 또한 행정・공공기관에 대한 사이버 공격을 방어하고자 '범정부 로그분석 시스템'(nSIMS: National Security and Information Management System)도 마련하였다. 금융권 사이버 보안을 강화하기 위해 2015년 금융보안기구인 '금융보안원'을 신설하였다.

사이버안보에 대한 법제도적 대응책을 살펴보자면, 국가 사이버안보는 군사분야 영역을 넘어서 중요 정보시스템, 공공 인프라, 개인정보 보호 등 여러 분야를 포함하기 때문에 정부는 다양한 법률을 제정하고 이를 수행하고 있다. 기본적으로 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'과 '국가사이버안전 관리규정'(대통령 훈령)을 기본으로 다양한 법령이 존재한다. 이를 수행하는 기관으로는 크게 국가 및 공공부문은 국가정보원이 담당하고, 민간부분에는 과학기술정보통신부, 민간 정보통신 기반시설은 행정안전부, 정보보호 산업 육성은 산업통상부가 담당하는 구조로 편성되어 있다.[34]

먼저, 공공부문에 대한 사이버 안보는 대통령 훈령인 '국가사이버안전 관리규정' 및 '국가 위기관리 기본지침'등에 근거한다.[35] 이와 관련하여 대통령실이

32) 박종재・이상호, 앞의 글, p.83.
33) '사이버안보 종합대책'은 사이버 안보 강국을 위해 4대 전략을 수립,시행하기 위해 사이버 안보 컨트롤 타워는 청와대가 맡고, 실무총괄은 국정원, 미래부와 국방부 등 중앙행정기관이 소관분야를 담당하는 대응체계를 마련하였다.
34) 박종재・이상호, 앞의 글, p.85.
35) 『2015국가정보보호백서』(2015), p.44.

컨트롤타워 역할을 수행하고 국가정보원이 실무를 총괄하며, 분야별로 민관군이 책임기관을 지정해 관련 활동을 수행하는 체제로 구성되어 있다. 국가적 차원의 사이버안보 활동을 위해 2004년 설치된 국가사이버안전센터(NCSC: National Cyber Security Center)는 국가 사이버안전 정책 수립, 전략회의 및 대책회의 운영, 사이버위기 경보 발령, 사고 조사・분석 및 대응 복구 등 총괄기관 역할을 담당하고 있으며, 군의 사이버안보와 정보보안 업무는 '보안업무규정'(제43조) 등에 의거하여 국방부장관에게 위임되어 있어 국방부장관은 별도의 사이버안보 업무를 수행하고 있다.[36)]

민간부분의 사이버 분야는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 근거하여 일정 규모 이상의 정보통신서비스 제공자(ISP)는 정보보호 최고책임자를 지정하여 과학기술정보통신부 장관에게 신고하고 정보통신망 보호를 위한 보호조치를 강구해야 한다.[37)] 정보통신부 장관은 정보보호 지침을 수립하여 고시하고 정보보호 안전진단 수행기관을 관리・감독하며, 정보보호 관리등급 부여 및 관리체계 인증업무를 수행한다. 사이버 침해 사고 관련 정보의 수집・전파, 침해사고의 예보 및 경보, 침해사고에 대한 긴급조치 등을 수행하며, 필요한 경우 한국인터넷진흥원(KISA)이 이를 수행하도록 한다는 것이다.

또한, 사이버 침해사고가 정보통신의 발전으로 확산되고 그 공격 패턴도 ATP(Advanced Persistent Threat) 방식을 활용하여 특정 기관의 시스템 취약점을 장기간 분석하여 공격하고 있다. 이와 같은 사이버 침애 예방・대응을 위해 우리 정부는 행정기관 각 부처와 에너지, 금융, 의료 등 국가 주요 정보통신시스템에 대한 보안관제센터를 운영하고 있다. 사이버 보안관제는 공공부문과 한국전력 및 KT・LGU+・SK텔레콤 가입자 대상의 에너지・금융 등 민간부문 관제센터로 구분하여 실시하고 있다.[38)]

---

36) 박종재・이상호, 앞의 글, pp.86-87.
37) 『2015국가정보보호백서』(2015), p.45.
38) 박종재・이상호, 위의 글, p.89.

요약하자면 한국의 사이버안보는 국가정보원을 중심으로 컨트롤타워로 이루어져 있으며, 국군사이버사령부가 사이버전쟁을 대비하여 활동하고 있다. 정부기관의 사이버시스템은 행정자치부가 민간분야는 인터넷진흥원(KISA)를 중심으로 과학기술정보통신부가 사이버보안을 맡고 있다.

[표 4] 2009년 이후 북한으로 추정되는 국내 사이버 공격

일 시	사 건
2009년 7월 7일	35개 주요 정부기관 및 금융기관을 겨냥한 디도스(DDoS) 공격
2011년 3월 4일	국회·행정안전부·통일부와 은행·증권사에 대한 좀비PC 공격
2011년 4월 2일	농협 전산망 마비
2012년 6월 9일	중앙일보 신문제작시스템 파괴
2013년 3월 20일	주요 방송사 및 금융기관 서버·PC 악성코드 유포
2013년 6월 25일	청와대·국무조정실·정당 전산망 공격
2014년 8월	대학병원 전산망 서버 장악
2014년 12월 15일	한수원 조직·설계도 해킹
2015년 11월	금융보안업체 인증서 해킹
2016년 1월 27일 2016년 2월 18일	청와대 국가안보실 및 방송사를 사칭한 대통령 음해 E-mail 전파
2016년 7월 28일	'인터파크' 대형쇼핑몰 해킹

출처: 정구연・이기태, 『과학기술의 발전과 북한의 새로운 위협』(통일연구원, 2016), p.61.[39]

사이버안보 분야에서 우리 정부의 국제적 협력으로는 러시아(2014년 5월), 호주(2014년 8월), 인도(2015년 1월), 일본(2015년 10월), 중국(2015년 10월), 사우디(2016년 1월), EU(2016년 6월), 체코(2016년 6월), 독일(2016년 6월), 미국(2016년 6월) 등과 사이버정책 협의회를 개최하였고, 상호 간 사이버협력과 국제 사이버안보를 위한 협력을 도모하였다.[40] 또한 UN정보안보 정부전문가 그룹(GGE)과 국가 간 사이버안보 규범문제를 5차에 걸쳐 논의해 왔다.

한국은 2013년 10월 서울에서 각국 관료와 국제기구 대표들이 참여하는 제3차 사이버스페이스 총회를 개최하였다. 이 회의에서 사이버 공간의 국제협력 강

39) 정구연・이기태. 『과학기술의 발전과 북한의 새로운 위협: 사이버 위협과 무인기 침투』(통일연구원, 2016), p.61.
40) 함승현・박대우, 앞의 글, p.1668.

화와 문제 이슈들에 대한 공동기반 마련을 논의하고 사이버보안, 국제안보, 사이버범죄, 역량강화 등의 합의내용을 도출한 '서울 프레임워크 및 공약'을 부속문서로 채택하여 의장요약문을 발표하기도 하였다.[41]

최근 4월 3일 청와대 국가안보실에서 발간한 '국가사이버안보전략'은 우리 정부가 최초로 국가 차원의 사이버위협 전반에 걸친 대응방안을 발표한 것으로 그 의미가 크다. 이번 '국가사이버안보전략'은 날로 증가하는 사이버공간의 보안 취약성・위협성 증대를 인식하고 사이버안보의 중심이 국민이라는 것을 밝히고 있다.[42] '국가사이버안보전략'은, 1) 국민 기본권과 사이버안보의 조화; 2) 법치주의 기반 안보활동 전개; 3) 참여와 협력의 수행체계 구축으로 하는 3대 기본원칙과 6개 전략과제(1. 국가 핵심 인프라 안정성 제고; 2. 사이버공격 대응역량 고도화; 3. 신뢰와 협력 기반 거버넌스 정립; 4. 사이버보안 산업 성장 기반 구축; 5. 사이버보완 문화 정착; 6. 사이버안보 국제협력 선도)를 제시하고 66개 소과제를 구체적으로 기술하고 있다.

이러한 청와대의 '국가사이버안보전략' 발표는 국가 차원에서 사이버안보를 재정비하고 종합적 대응체제를 마련하려는 정부의 사이버안보 강화정책 추진 노력이 주목받고 있다. 앞서 언급했듯이 미국과 영국, 일본 등 사이버 강국들은 국가 상위기관의 연계와 협력 및 정부 조직 간 정보 공유가 확대되고 있다는 점을 고려하였을 때 국가안보실의 사이버안보 컨트롤타워 역할을 제안하였다는 점은 높이 평가받을 수 있다. 하지만 향후 정부가 구체적 실행 방안을 담은 '국가 사이버안보 기본계획'과 '국가 사이버안보 시행계획'을 수립・추진해야 할 과제가 남아 있다. '국가사이버안보전략'을 구체적으로 실행하기 위해서는 국가 사이버안보 기본법 제정과 국가 차원의 사이버안보를 통제할 수 있는 '컨트롤타워' 논의가 필요한 시점이기 때문이다.

---

41) 유호근・설규상, 앞의 글, p.255.
42) 청와대 국가안보실, 『국가사이버안보전략』 (서울: 2019년 4월).

3. 국가차원의 사이버안보 강화를 위한 전략

가. 사이버위협에 대한 우리의 대응과제

앞서 언급한 것처럼, 국제정치학에서 사이버안보를 바라보는 시각은 다양하다. 먼저 사이버위협에 대한 인식의 문제가 중요하다. 현실주의적 입장에서 과거 전통안보에서는 사이버 공간에 대한 방어기제나 안보문제를 고민하지 못했다. 정보통신의 발전은 사이버공간에서 개인 간 활발한 교류가 증진되고 경제적 상호이익을 창출하는 순기능을 파생시켰다. 하지만 최근 한반도와 국제적 차원의 사이버공격이 현실화되면서 사이버안보에 대한 현실주의적 인식이 중요한 사안으로 제고되고 있다. 013년 3.20사이버공격, 2014년 한수원 해킹사건, 2016년 국방망해킹 등 한국에서 발생한 사이버공격 이외에 2014년 11월 소니픽처스해킹 사건으로 인해 북・미 간 안보적 긴장상황을 연출하였다고 볼 수 있기 때문이다.

미국 오바마 대통령은 북한의 해킹 공격을 '사이버 반달리즘'으로 간주하고 '비례적 대응' 차원에서 미국은 북한 인터넷을 마비시키는 보복공격을 단행하였고, 북한 정찰총국과 관련자의 제재를 포함하는 행정명령을 발동하였다. 미국 하원에서 지난 6월 '사이버 억지・대응법안'이 통과 되었고, 상원도 '사이버 공격제재 법안'을 발의하였다.[43]

이러한 일련의 사이버공격과 위협은 우리 정부에게도 국가안보의 심각한 위협으로 인식되었고 현실주의적 대응전략을 고민하게 되었다. 사이버공격에 대한 체계적인 대응 및 대비 체제를 마련하기 위해 과거 '사이버안보비서관'을 신설(2015년 3월) 하였고, 사이버위협에 대한 기술적 능력과 한반도 주변국과 국제사회의 사이버안보 규범화와 협력에 대한 중요성이 강조 되었다. 그러나 북한의 대남 사이버공격에 대한 정부 차원의 적극적 대응은 제한적이었다. 또한 지난 2018년 7월 26일 청와대는 대통령비서실과 국가안보실 조직운영 개편안을

43) 『중앙일보』, 2018.9.14.

통해 ‘청와대 사이버 안보비서관’ 제도를 없애고, 사이버안보와 정보융합을 합쳐 ‘사이버정보비서관’으로 통합하여 운영하게 되었다. 이처럼 사이버안보와 정보융합의 유사성을 기준을 가지고 ‘사이버정보비서관’ 통합운영은 사이버안보 대응체제를 약화시키는 결과를 초래할 것이라는 우려도 제기되고 있다.

우리나라에서 사이버안보 문제는 제도적 차원에서 일반법의 부재가 지적된다. 북한 사이버 공격 대응법안은 국회에 계류되어 있고, 정부의 통합적인 컨트롤타워의 부재가 지적되고 있다. 최근 발전된 정보사회 도래는 사이버안보는 새로운 국가안보의 분야로 인식되고 있기 때문에 법치행정의 측면에서 큰 문제가 될 수 있기 때문이다.[44)]

사이버안보에 대한 법적근거가 명확하지 않으면 사이버침해를 막기 힘들뿐 아니라, 국가사이버안보 문제가 민간부분의 제한을 동반할 가능성도 크기 때문이다. 한국의 현행 사이버안보관련 법률은 공공・민간분야 적용범위와 대응체계가 분산되어 관리하고 있으며 대응체계 완결성의 문제도 지적된다. 공공부문에서도 2005년 대통령훈령으로 제정된 ‘국가사이버안전관리규정’에 의해 지금까지 규율되고 있다는 것은 중요한 문제점으로 지적될 수 있다.

사이버안보를 위한 공공부문의 최고규범이 대통령훈령이라는 것은 해당 규범의 정당성과 효력에 대해서도 이견이 발생할 수 있기 때문이다. 현실주의적 입장에서 사이버위협이 전통적 안보로 취급된다 하더라도, 자유주의적 입장에서는 사이버 공간의 자유와 개인 이익보장이 침해되어선 안되기 때문이다. 또한, 공공부문 사이버안보 업무를 국가정보원이 담당하고 있으나 이에 대한 법률적 근거 조항이 부재하다는 것은 사이버안보가 시민사회의 자유성을 제한한다는 비판을 받을 수 도 있기 때문에 사이버공간의 법적 체계가 완비되어야 한다는 지적이다. 따라서 국가적 차원의 사이버안보에 대한 적극적 보호 활동과 관리에 대한 법률제정이 요구되고 있다.

---

44) 김재광, “사이버안보 위협에 대한 법제적 대응방안”『법학논고』58, (2017), p.164.

사이버위협은 시공을 초월하는 특성을 갖고 있기 때문에 사이버보안 대응체계를 공공・민간부문으로 엄격히 구별하여 관리하는 것은 한계가 있어 보인다. 앞서 기술하였듯이 국정원, 국방부, 경찰청과 대검찰청, 과학기술정보통신부가 분야별 분권화되어 있어 사이버위협에 대한 통합된 대응체계를 유지・발전시키기에는 어려움이 있다. 자유주의적 입장에서 우리 정부가 사이버보안을 국가의 일반보호시스템과 구별하지 않고 있어 정보보안에 대한 과잉 대응 소지가 있다는 점이다.[45]

또한, 정보통신의 발전으로 사이버위협은 날로 증대되고 있으며 이에 대한 우리 정부의 대응체계 구축에도 불구하고 국내에서 디도스사건 등 사이버공격과 그 피해가 재발되고 있다. 그 이유로 중앙 행정기관과 비교해 지방 기관들의 백신 S/W 도입율이 저조하고 정보보호 인식도 부족한 상황이다. 또한 사이버침해사고에 대한 처벌이 관대하다는 것이다. 현행 '정보통신망법'에서는 사이버침해행위에 대한 처벌로 최고 5년 또는 5천만원 이하 벌금으로 규정되어 있고, '정보통신기반보호법'에서는 10년 이하 징역 1억 원 이하 벌금으로 규정되어 있다. 이는 유럽연합이 정부전산망에 대한 사이버 공격에 최고 5년 이상의 형량을, 미국은 상습적 사이버 범죄자나 네트워크 침해로 인한 사망사고 유발범에게 무기 또는 20년 이하의 징역과 대비된다.[46]

국가 차원에서 사이버전에 대한 준비상황 역시 체크해야 한다. 국가 차원에서 사이버 공간에서 자국의 이익을 위해 사이버공격을 수행하고 있으나, 각국의 사이버 능력을 비교・분석할 근거와 기준이 없어 사이버 역량을 측정하기도 힘들고 사이버 공격 기제와 피해 상황을 파악하는 것도 극히 제한적이다. 북한으로 추정되는 사이버 공격은 남한의 안전과 경제를 위협하고 있다. 그러므로 우리 정부는 사이버안보에 대한 대응정책을 발전시키고 국가사이버안보를 위한 아젠다 발굴에 힘써야 할 것이다.

---

45) 백영호, 『공공부문 정보시스템 보안통제 취약성 점검 방안연구』(감사원 감사연구원, 2015), p.48.; 박종재・이상호, 앞의 글, p.94.

46) 김태계, "사이버테러 범죄 대응에 관한 제도적 문제점과 대책," 『법과 정책연구』 제14권 제3호, (2014), 1371-1372; 박종재・이상호, 위의 글, p.96.

나. 국가차원의 사이버안보 추진전략 모색

결국, 사이버공간에 대한 자유성과 사이버위협에 대한 국가차원의 안보전략도 동시에 고려되어야 한다. 사이버안보 강화를 위해서는 우선 법・제도적 추진체계의 개선이 필요하다. 사이버침해는 국내인프라와 정보자산 뿐만 아니라 군사적 안보 수준까지 확대 되고 있다. 날로 발전되는 사이버침해를 대비하려면 사이버안보에 대한 관련법 제정과 추진체계의 정비가 시급하다.

현재 국가사이버안보를 규정하고 총괄하는 법률이 부재하고 국가적 차원의 사이버안보의 정책 수립과 실행을 위한 원칙과 용어의 정립도 필요한 상황이다. 현재 사이버안보 관련 법제는 대통령훈령인 '국가사이버안전관리규정'이 전부이고 산재한 규정들도 일상적인 정보 보호 수준이라는 우려가 제기되기 때문이다. 결국 사이버안보 법률 제정을 통하여 효과적으로 사이버위협에 대처하고 국가권력이 정보보호를 위한 구실로 민간부문의 권리를 침해하는 우려도 막을 수 있을 것이다. 사이버위협에 대응하는 '국가사이버안보 기본법(가칭)'이 제정이 필요하다. 일본은 이미 2014년 '사이버시큐리티'법을 제정하고 통합적 대응체계를 갖추었는데, 내각 관방장관을 본부장으로 하고 '사이버 시큐리티 전략본부'를 설치해 국가안보 전략의 수립과 민관 주요기관의 보안체계 강화를 위한 통합적 협력을 전개하고 있다.[47]

이와 함께 사이버위협에 대응하고 관리할 수 있는 사이버안보 추진체계의 정비도 요구된다. 비록 사이버안보 비서관 직제가 폐지되어 사이버안보 컨트롤타워 부재 우려가 있으나, 사이버위협에 대해 청와대를 근간으로 최상위 컨트롤타워를 만들고 국가정보원, 과학기술정보통신부, 국방부, 경찰청, 대검찰청 등의 정부기관들이 긴밀하게 협력하는 국가사이버안보 대응체계의 완결성을 높여야 한다.

또한, 국가사이버안보 관리시스템이 기존 안보시스템과 재난 관리시스템과 연동하여 강화되는 통합시스템이 필요할 것이다. 사이버공격과 위해는 시간과

47) 『전자신문』, 2015.8.18.; 박종재・이상호, 위의 글, pp.99-100.

물리적 공간의 제약을 넘어서기 때문에 초기 대응시간과 확산을 막는 것이 매우 중요다. 따라서 향후 법률에 따라 사이버대응시스템을 갖추고 군사안보시스템(데프콘(DEFCON)과 국가기반시설 보호체계 관리시스템(국내인프라: 정보통신기반시설)과 긴밀하게 연계되어야 한다.

현재 국가사이버안보 합동 대응은 현실적으로 평시에 국가정보원을 중심으로 민관군 합동대응팀을 구성하고 있지만, 급속하게 발전하는 사이버위협에 대응하려면 국가차원의 사이버안보 합동대응 기능을 강화하고 관련 부처와의 긴밀한 협력과 대응 매뉴얼의 정립이 필요하다. 이와 함께 사이버침해 수사체계를 보다 효율적으로 정비하고 사이버수사 전담조직과 예방시스템 구축에도 집중해야 할 것이다. 이를 위해 관련기관들과 민간 전문가 집단이 효율적으로 사이버공격 정보 분석과 대응책을 마련해야 할 것이다..

사이버안보의 국제규범화 논의와 국제적 협력이 필요하다. 최근 정보통신의 발전과 글로벌화는 개인 간, 국가 간 접촉과 상호이해관계가 복잡해지고 의존성도 증대되고 있다. 사이버안보의 특수성으로 인해 개별 국가 내부적으로 대응이 불가능하고 주변국, 국제적 협조가 필요하다. 이러한 현실은 주요 국가들의 국제관계에서 안보핵심의제로 사이버보안이 거론되기 시작했다. 한국은 IT강국으로 발달된 인프라와 인터넷 활용을 통하여 서구선진국들과 유사한 사이버환경이 조성되어 있으나 정보보호 분야의 산업이 뒤처져 있고, 상대적으로 사이버위협에 노출될 여지가 크다. 또한 우리 정부는 국가사이버안보에 상대적으로 미흡한 법제적, 재정적 대응체계를 가지고 있으며 정부의 일방적 방어활동에 의존하고 있다.[48] 이러한 사이버안보 환경을 개선하기 위해서는 국제적 사이버안보 규범과 협력에 동참하여 발전된 사이버안보 매뉴얼과 대응체제를 논의・공조해야 할 것이다. 즉 국가사이버안보전략을 국제적 규범과 협력에 양자・소다자・다자적 논의에 참여하여 대내외 전략을 수립하고 대응기준을 마련해야 할 것이다. 물론 국가 간 상호 호혜주의에 입각하여 사이버공간의 평화를 논의해야 한다.

---

48) 김소정・김규동, 앞의 글, pp.112-113.

우리 정부는 2000년대 들어와 새로운 사이버위협에 대응하기 위한 사이버안보 수행체계를 마련해 왔지만, 민간과의 사이버안보 협력은 제한적이라는 견해가 강하다. 2009년 출범한 한국인터넷진흥원(침해사고대응팀:CERT)이 국내외 사이버침해 사고 대응과 정보공유, 분석센터 등과 비상연락망을 구축하고 조기경보체계를 운영하여 민간분야와 협조하는 체계를 갖추고 있다.[49] 하지만 수평적, 유기적체계라기보다 민간분야 사이버침해사고 예방 및 대응을 지원하는데 주안점을 두고 있다. 따라서 우리 정부는 사이버안보를 강화하는 데 보다 효율적으로 대응하기 위해 이해 당사자들의 참여와 협력을 통해 사이버침해를 예방하고 조속하게 처리해야 할 것이다.

급속한 정보통신 환경의 발전은 사이버안보에 대한 국민들의 참여와 인식이 중요하다. 사이버침해에 대한 대응과 처벌도 중요하지만, 이에 대한 예방책이 보다 중요한 사안이기 때문에 정부의 힘만으로는 부족하다. 그러므로 정부와 국민들의 적극적 참여가 요구된다. 사이버침해에 대한 예방책으로 정보공유 시스템을 합리적으로 구성함으로써 시스템의 취약점과 사이버공격의 방어능력을 향상시킬 수 있다. 특히 사이버보안 전문가 양성을 통해서 웹(web), 시스템, 네트워크 해킹 등을 막고 향후 사이버공간의 순기능을 증진시킬 수 있는 전문가그룹 양성에 정부가 '빅 픽쳐(big picture)'를 그려야 할 것이다.

따라서 이러한 국가와 민간차원의 협력을 위해서는 국가차원에서 사이버안보를 위한 거버넌스(governance)적 접근이 필요하다. 사이버 공간에서 주체의 다양성과 상호연결성이 확대되고 비대칭전력으로써 안보적 파급효과 또한 크기 때문에 사이버안보의 국가 중심적 접근방법을 초월하여 보다 다양한 주체가 참여하고 상호소통과 관리를 필요로 한다. 이러한 다양한 주체를 포함하는 수평적, 전문적 접근법이 '거버넌스' 접근법이라고 말할 수 있다. 시민의식 성장과 시민사회의 발전은 자율적 통치(self-governing)를 근간으로 다양한 주체들이 정치에 참여하는 거버넌스 개념은 상이한 주체들이 위계적으로 연계되는 아니

49) 유호근・설규상, 앞의 글, p.256.

라 다양한 복합적 관계를 가지는 '네트워크'개념과도 연결되며 상호조정과 통제를 요구한다.[50]

미국의 경우 사이버안보의 거버넌스적 접근법을 활용하고 있다. 미국은 2013년 초 주요기반시설에 대한 사이버공격이 발생하자 오바마 행정부는 사이버안보 전략의 재정비차원에서 행정명령(Excutive Order, EO) 13636호와 정책지침(Presidential Policy Directive) 21호를 공표하였는데, 행정명령 13636호는 사이버보안 프레임워크 개발을 주요 내용으로 정책지침 21호는 국토안보부 등 주요기반시설 보호와 관련된 중앙부처의 역할과 의무를 명확하게 규정하기 위해서 도입되었다.[51] 2015년 2월 민간부문과 사이버위협정보 공유를 촉진을 추진하는 행정명령 13691호를 발표하였고, 2015년 12월 민관 사이버위협정보 공유를 주요 내용으로 하는 사이버보안법(Cybersecurity Act of 2015)이 통과되면서 민간부문을 포함하여 정보공유체계 구축과 사이버안보 추진체계와 관련된 연방정부의 권한과 책임을 규정하는 법정토대가 마련되었다.[52]

이처럼 사이버위협 이후 국가사이버안보 대응방안에 있어 미국 행정부는 사이버위협을 강하게 인식하고 민관 정보공유 체계를 사이버안보 거버넌스 강화 정책으로 추진하면서 의회 입법을 통한 사이버안보 거버넌스를 컨트롤할 수 있는 제도적 장치를 마련하고 있다. 그러나 한국은 정부는 상대적으로 일방적인 사이버안보 대응체계를 유지하고 있고, 여·야당의 사이버위협의 안보화 수준에 대한 의견 차이를 좁히지 못하고 있어 법률제정을 통한 사이버안보 거버넌스 구축에 한계를 보이고 있다. 따라서 우리 정부는 향후 사이버거버넌스 구축에 대한 인식을 높이고, 국회차원의 합의를 통해 제도적 사이보안보체계를 마련해야할 것으로 본다. 마지막으로 사이버전을 대비한 군사분야 사이버능력 배양도 중요한 사안이다.[53] 사이버공격은 지능화되고 조직적인 방법으로 발생하고 있

50) 홍석훈·나용우, "한반도 평화번영을 위한 새로운 로컬 거버넌스의 모색: 남북교류협력에 있어 지방자치단체의 역할을 중심으로"『세계지역연구논총』 36(1), (2018), p.188.
51) 조화순·권웅, 앞의 글, pp.105.; 송은지·강원영, "미국 오바마 정부 2기의 사이버보안 강화 정책, Internet & Security Focus", (한국인터넷진흥연구원: 2014).
52) 조화순·권웅, 위의 글, pp.105-106.
53) 조성렬은 사이버안보역량 강화를 위해 적성국들이 국내 사이버공간을 침투하지 못하도록

다. 북한의 사이버위협뿐만 아니라, 사이버 공격주체는 개인, 집단, 정보기관, 정부 단위와 같이 다양하기 때문에 국가안보 차원에서 사이버공격에 대한 안보무기체계와 기술력확보도 매우 중요하다. 사이버안보무기와 사이버방호체계 구축이 필요한 것이다. 사이버무기와 대응체계가 실시간 작동하도록 AI(Artificial Intelligence)을 활용한 사이버공격・방어 자가 학습 및 기술의 집적화를 이루어야 하고, 첨단 ICT기술의 발전과 사이버응용 범위의 확대에 따른 Iot(Internet of Things), AI, Drone 등을 활용한 맞춤형 기술개발 연구를 위한 조직과 재정이 지원되어야 한다.[54]

4. 결 론

사이버 공간의 초국가성과 행위자 확대는 정보의 활성화와 경제적 이익 창출의 긍정적 측면과 사이버 공간의 사이버 해킹, 사이버 테러, 사이버 범죄 등과 같은 부정적 측면의 문제들이 논의되어 왔다. 정보통신기술이 발전함에 따라 과거 냉전시대의 전통적 안보 개념에서 인간안보 개념으로 확대되고, 2000년 대 이후 사이버 위협은 국제안보의 주요 이슈로 등장하게 되었다. 새로운 정보통신의 발전 환경은 새로운 안보 위기를 조성하고 있고, 이에 대한 대안을 찾기 위해 광범위한 연구가 진행되고 있다. 여기에 국제정치학적 관점에서 사이버안보는 다각적 분석과 그 대안을 제시하고 있다.

따라서 최첨단의 정보통신 발전 환경은 새로운 안보 위기를 조성하고 있고, 국가 차원에서의 사이버안보 강화전략은 꼼꼼하게 마련되어야 한다. 하지만 안

하거나 침투 하더라도 피해를 최소화할 수 있은 '소극적 사이버방호(Passive Cyber Defense)' 및 사이버공격주체가 이용하고 있는 해외 사이버공격 거점을 색출하고 해당국 정부에게 폐쇄를 요청하는 등 사이버공격에 대한 능동적이고 원천적으로 차단하는 '적극적 사이버 방호(Active Cyber Defense)'와 함께 사이버공격 주체를 색출한 뒤 이에 대한 적절한 대응공격을 가하는 '사이버공격능력'을 확보해야 함을 지적하고 있다(조성렬, 『전략공간의 국제정치: 핵, 우주, 사이버 군비경쟁과 국가안보』 (서강대학교 출판부, 2016), pp.513-517.

54) 함승현・박대우, 앞의 글, p.1671.

보패러다임 중심의 사이버안보 접근은 자칫 개인의 정보활동 자유와 경제적 이익 창출을 가로막는 제재 요인으로 작용하기 쉽다는 의견도 중요하다. 전통적 안보관으로 인해 새롭게 발전하는 사이버 공간의 사회, 문화 교류를 막고 국가의 통제와 패권국가 간의 경쟁만을 양상 한다는 점도 부각되고 있다. 신자유주의적 입장은 사이버공간은 전통적 지리, 행위자 특성을 초월하기 때문에 사이버공간은 전통적 안보개념이 통용될 수 없으며 개인의 자유와 이익에 집중해야 한다. 사이버안보가 중요한 사안이지만, 사이버위협을 국가가 과장하거나 제재하려는 수단으로 활용되는 것도 경계해야 한다.

그러므로 국내 학계의 사이버안보 연구를 위한 확대방안이 논의되어야 한다. 국내 학계에서 사이버 공간에 대한 정치학적 연구는 정책 중심에 편중되어 있어, 이론적 측면의 사이버안보 연구가 필요한 상황이다. 또한, 사이버안보는 그 특성상 다양한 분야를 포함하는 개념으로 발전되고 있다. 사이버안보는 개인과 사회, 국가를 포괄하며 사이버전에 대비하는 군사적 대응방안과 개인의 정보보호와 경제적 이익을 보호하는 지협적 안전 개념까지 포괄하고 있으며, 기술적 분야에서 법・제도적 분야까지 그 연구영역이 방대하다. 그러므로 사이버 연구의 학제 간 융합 연구가 절실하다.

미래지향적 사이버안보 대응방안으로 사이버 공간의 각 주체들이 자유와 상호이익을 창출할 수 있어야 하며, 자율적 통제를 통해 사이버위협을 막아야 한다는 논의이다. 이러한 발상은 글로벌거버넌스 구축에 집중하게 되었으며, 사이버 공간의 국제규범과 국제레짐을 만들어야 한다는 입장도 주목해야 한다. 이러한 사이버공간의 자유성은 최근 청와대 국가안보실에서 발표한 '국가사이버안보전략'에서도 정부가 사이버공간의 안전을 보장하여 국민 모두가 안심하고 사이버 공간을 자유롭게 향유하는 데 그 이정표를 두고 있다는 것은 중요한 시사점을 내포하고 있다.

물론 우리 정부는 북한으로 추정되는 공공기관의 사이버공격과 군방망 해킹까지 다양한 사이버테러를 경험하였다. 이에 대한 방어와 피해확산을 막기 위해 조직체제 정비와 제도적, 기술적 대응능력을 향상시켜 왔다. 그러나 체계화・

통합된 사이버안보 법률이 부재한 상황이다. 즉 사이버침해에 대한 대응체계가 분권화되어 있어 국가 컨트롤타워에 의한 즉각적인 대처가 힘들고, 사이버침해 예방에 있어 정부 중심의 운용으로 인해 민간부문과의 정보공유, 민간 전문가 그룹의 참여, 사이버안보 거버넌스 구축 등이 제한되어 있다. 또한, 사이버안보는 전통적 군사안보와 연동하여 우리군의 사이버전 방어·공격 능력을 발전시켜야 하나, 과거 댓글 사건과 국방망 해킹사건 등으로 인해 국민들의 불신을 우려를 낳고 있다.

따라서 사이버안보 추진전략으로 국민과의 협의를 통한 사이버안보 법률제정이 시급하다(국회, 국가사이버안보법안 계류). 사이버안보의 중요성을 인식하고 법률에 의거한 국가차원의 통합적 대응체계를 만들어야 하기 때문이다. 무엇보다도 기술적 능력을 향상시키기 위해서는 사이버 전문가를 양성하고 이에 대한 재정적 지원이 담보되어야 한다. 하지만, 어떠한 경우에도 사이버안보가 정치적 쟁점이 되어 개인의 프라이버시를 침해하거나 사이버공간의 자유를 침해해서는 안 된다. 사이버안보에 대한 민·관의 협력과 이해가 필요하며 공공부문과 민간부문의 통합적 매뉴얼과 컨트롤타워가 마련되어야 한다. 결국 법·제도 구축을 통하여 사이버안보 거버넌스를 구축해야 한다. 사이버안보는 사이버 공간의 각 주체들이 자유와 상호이익을 창출할 수 있어야 하며, 자율적 통제를 통해 사이버위협을 방어하는 지향점을 찾아야 하기 때문이다.

다음으로, 우리의 강점을 발전시켜 나가야 한다. 전반적으로 한국은 IT 기술에서 강점을 가지고 있어 기술적 기반을 바탕으로 보안상의 취약점을 적극적으로 개선해나갈 수 있다는 이점이 있다. 더불어 북한을 비롯한 타국의 사이버위협에 대한 취약점 보완해 나가면서, 사이버 반격 능력을 키워 나가야할 것이다. 따라서 취약한 사이버안보을 강화하기 위해서는 보안산업에 대한 국가적 관심과 육성책을 마련해야 한다. 사이버안보를 위한 장기적 고급 인력양성을 통해서 미래를 준비할 수 있기 때문이다.

나아가 사이버안보에 관한 국제규범과 국제협력에 적극적으로 참여하여 사이버공간의 순기능을 확대시키고, 사이버위협에 대한 국제적 공동대응과 처벌을

도모해야 할 것이다. 먼저 우방국들과 협력체계를 기반으로 국제적 사이버안보 역량 강화가 중요하다. 기술교류 활성화, 공동의 전문 인력양성 등의 세부적 계획을 통해 국제적 사이버안보역량 강화가 가능할 것이다. 한국은 '가교국'(bridge state)으로서의 이점을 갖고 있다. 개인, 민간기업, 국제기구 등의 다양한 행위자 참여하는 '다자 당사자주의적 플랫폼' 운용에 적합한 행위자로서의 입지를 가지고 있다. 이러한 특성에서 사이버안보 규범화 문제에 있어서도 한국의 위상은 제고될 수 있다.

이번 청와대 국가안보실 '국가사이버안보전략' 발표를 통해 정부의 강한 사이버안보 대책마련 의지를 표명한 만큼 빠른 시일 내에 우리 정부의 구체적이고 실효성 있는 사이버안보 방안이 제시되어야 한다. 즉, 사이버안보 '컨트롤타워'의 재정립과 효율적 민관군의 사이버안보 거버넌스 구축이 추구되어야 할 과제이다. 현재 제도적 측면에서도 '국가사이버안전관리규정'이 대통령 훈령으로 이루어져 있어 제도적 정립이 시급하다는 점이 지적되고 있다. 향후, 우리 정부의 사이버안보체계는 전통적 안보와 재난관리체계와 연계하여 관리되어야 할 것이다.

참고문헌

1. 단행본

김상배.『사이버 안보의 국가전략: 국제정치학의 시각』. 서울: 사회평론, 2017.

박인휘 외.『탈냉전사의 인식』. 서울: 한길사, 2012.

백영호.『공공부문 정보시스템 보안통제 취약성 점검 방안연구』. 감사원 감사연구원, 2015.

이성만・김용재・이정석.『국가안보의 이론과 실제』. 서울: 오름, 2013.

서창록,『한반도 평화번영의 거버넌스 구축을 위한 이론적 틀』. 서울: 통일연구원, 2006.

정구연・이기태.『과학기술의 발전과 북한의 새로운 위협: 사이버 위협과 무인기 침투』. 서울: 통일연구원, 2016.

조성렬.『전략공간의 국제정치: 핵, 우주, 사이버 군비경쟁과 국가안보』. 서울: 서강대학교 출판부, 2016.

청와대 국가안보실,『국가사이버안보전략』. 서울:청와대, 2019년 4월.

Jones, Alfred A. “Information Security: Planning for the Deluge” *The Information Revolution and National Security Dimensions and Direction*, 15-23., The CSIS Press, 1996.

Mearsheimer, John J., *The Tragedy of Great Power Politics,* W.W. Northon & Company, 2001.

Waltz, Kenneth N., *Man, the State, and War,* New York: Columbia University Press, 1959.

Obama, Barack. *‘Remarks by the President on securing our nation’s cyber infrastructure’*, Washington DC: The White House, 29 May 2009.

2. 논문

김소정・김규동. 2017. “UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의”『정치・정보연구』제20권 제2호, pp.87-122.

김슬기・박대우. 2017. “사이버보안 전문가 양성을 위한 연구”『한국정보통신학회논문지』21(6) pp.1137-1142.

김재광. “사이버안보 위협에 대한 법제적 대응방안”『법학논고』제58권 (2017), pp.145-177.

나용우. “초연결융합시대와 사이버안보: 사이버공간의 안보화와 한국의 사이버안보 강화 방안,”『Journal of North Korea Studies』제3권 2호 (2017), pp.29-51.

박종재・이상호. “사이버 공격에 대한 한국의 안보전략적 대응체계와 과제”『정치・정보연구』제20권 제3호 (2017), pp.79-114.

유호근・설규상. “사이버안보 체계: 거버넌스 형성의 문제와 한국”『한국정치외교사논총』제38권 제2호 (2017), pp.237-270.

송은지・강원영, “미국 오바마 정부 2기의 사이버보안 강화 정책”,『Internet & Security Focus』(한국인터넷진흥연구원: 2014).

장노순. “초국가적 행위자의 사이버공격과 핵공격에 관한 비교연구: 국제안보질서의 안정성을 중심으로”『한국정치학회보』제39권 제5호 (2005), pp.263-281.

장노순・한인택. “사이버안보의 쟁점과 연구 경향”『국제정치논총』제53권 제3호 (2013) pp.579-618.

조화순・권웅. “한국과 미국의 사이버안보 거버넌스: 사이버위협의 안보화 관점에서의 비교”『정보사회와 미디어』제18권 제2호 (2017), pp.97-120.

조화순・김민제. “사이버공간의 안보화와 글로벌 거버넌스의 한계”『정보사회와 미디어』제17권 제2호 (2016), pp.77-98.

함승현・박대우. “국가 사이버안보를 위한 정책 연구”『한국정보통신학회논문

지』 제21권 제9호 (2017), pp.1666-1673.

Carr, Madeline. “Public-private partnerships in national cyber-security strategies,” *International Affairs* Vol. 92, No. 1 (2016).

Choucri, Nazhi., ed. “Institutional for Cyber Security: International Responses and Global Imperatives,” *Information Technology for Development* Vol. 20, No. 2 (2014).

Hansen, L., & Nissenbaum, H. “Digital disaster, cyber security, and the Copenhagen School”. *International Studies Quarterly*, Vol. 53 No. 4 (2009).

Moravcsik, Andrew. “Taking Preferences Seriously: A Liberal Theory of International Politics.” *InternationalOrganization* Vol. 51, No. 4 (1997).

Nye, Joseph S. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* Vol. 5, No. 5 (2011).

Wolter, Detlew. “The UN Takes a big step forward on Cybersecurity,” *Arms Control Today* 43 (September 2013).

3. 기타자료

국방부. 『보도자료(정보화기획관실 정보기획과)』, 2018.8.9.

미래창조과학부. “국가 사이버안보 종합대책으로 사이버 안심국가 초석 다져” 『보도자료(정보호정책과)』, 2014.11.17.

방송통신위원회. “정부, 국가 사이버안보 마스터플랜 수립” 『보도자료(네트워크정책국)』, 2011.8.8.

『서울신문』, 2014.12.20.

『중앙일보』, 2018.9.14.

『전자신문』, 2015.8.18.

https://www1.president.go.kr/articles/5893(검색일: 2019. 5. 1)

Abstract

Cybersecurity Debates from International Relations' Perspectives and National Cybersecurity Strategies

HONG Sukhoon (Korea Institute for National Unification)

Cyber threats are spreading not only to individual units but also to national units. The development of science and technology and the expansion of the cyber domain are increasing threats of personal property rights infringement and information leakage while creating mutual benefits in a wide range of fields. Above all, the threat of cyberspace from a national security perspective calls for a new level of response.

Korea is known to have a high level of international competitiveness based on its IT technology. However, cyber threats at the national level are increasing due to expansion of cyberspace, accessibility, security vulnerability, and uncertainty of actors. Recently, the announcement of the 'National Cybersecurity Strategy' from the National Security Office of the Cheong Wa Dae has been reemphasizing the importance of cybersecurity. Therefore, this paper would try to examine the security threats of the cyber space evolving at the national level and our cyber security strategies. In addition, this paper tries to discuss national countermeasures to prevent cyber threats in an integrated and effective manner.

Key Words: Cyber Security, Cyber Threat, Security Vulnerability, Cyber Security Response System, Cyber Security Strengthening Strategy

투고일: 2019.05.20 심사일: 2019.06.08 게재확정일: 2019.06.08.

Ⅲ

‘중국 특색 국제정치이론’ 논의의 출현과 향후 전망

함명식 (지린대학교)

1. 서 론
2. 중국 특색 국제정치이론의 등장 배경, 전개 과정, 특징
3. 중국 특색 국제정치이론의 사례
4. 중국 특색 국제정치이론의 한계
5. 결 론

Summary

현재 국제정치학계를 지배하고 있는 서구 국제정치이론의 주류는 중국의 부상을 현 국제질서에 도전하는 중대한 위협으로 간주하고 있다. 이와 같은 서구의 견제를 극복하고 자국의 부상에 정당성을 부여하기 위해 중국은 '중국 특색의 국제정치이론'을 창출하려는 노력을 기울여왔다. 본 논문은 중국 국제정치학계와 일부 서구 학자들이 중국 특색의 국제정치이론에 몰두하는 배경, 논의의 전개 과정, 이론적 특징을 살펴보고 이를 현재 진행중인 중국 외교정책에 대입해 중국 특색의 국제정치이론이 서구 국제정치이론으로부터 독립된 형태의 이론으로 발전할 수 있을지 여부를 조사했다. 연구 결과 중국 특색 국제정치이론 주창자들이 중국의 전통적 가치, 규범, 역사적 경험의 강조를 통해 서구 국제정치이론과 차별적인 이론의 수립이 가능함을 주장하고 있음에도 불구하고 중국 정부의 외교 정책이 자국의 이익을 중시하는 기존 강대국 외교와 아무런 차이점이 없다는 점에서 독자적인 중국 특색 국제정치이론이 지향하는 '이상'과 현실 사이에 적지 않은 모순이 존재하고 있음을 발견했다.

| **주제어** | 중국, 중국 특색 국제정치이론, 서구 국제정치이론, 천하관, 일대일로

1. 서 론

개혁 개방 이후 중국의 경제는 역사적으로 전례를 찾기 힘들 정도의 성취를 이룩했고 이를 바탕으로 정치, 외교, 군사 분야에서도 국제무대의 주요 행위자로 부상했다. 중국의 급속한 성장을 바라보는 세계의 시각은 중국의 부상이 미국 중심의 국제정치경제 질서에 변화를 가져올 것이라는 우려의 시선과 기존 질서를 대체하는 새로운 모델을 창출할 것이라는 기대감으로 나누어져 있다. 전자가 미국을 중심으로 하는 서방 세계의 시각을 대변하는 것이라면 후자는 중국처럼 경제적으로 개발도상국의 지위에 있거나 정치적으로 권위주의 체제를 유지하는 국가의 입장을 반영하고 있다. 지속적인 성장을 위해 아직 서구 세계의 협력과 도움을 필요로 하는 중국의 입장에서 서방 세계가 던지는 의혹의 시선을 잠재우는 것은 중국 정부가 풀어야 할 하나의 난제로 지목되어 왔다. 아울러 기존 서구 중심의 질서로부터 소외되어 온 국가들이 중국에 표출하는 우호적인 시각을 끌어안고 이들의 계속적인 지지를 확보하는 것 또한 중국 정부가 외면할 수 없는 중요한 과제임이 분명하다.[1)]

서구 사회가 중국의 부상을 바라보는 우려의 시각은 중국위협론으로 축약될 수 있다. 미국이 주도하는 현 국제질서가 강조하는 핵심 규범과 가치인 자유민주주의, 다원성, 시장경제, 인권중시와 궤도를 달리하는 중국의 권위주의, 일당지배, 국가주도 발전 정책, 인권 탄압은 중국위협론의 물적 토대로 작용해왔다. 이에 맞서 중국은 서구 사회가 자신만의 기준과 잣대로 중국을 평가한다며 이를 희석시킬 수 있는 새로운 논리를 마련해왔다. 오늘 날 '중국 특색'을 강조하며 횡행하는 다양한 논리가 중국의 이러한 시도를 뒷받침하고 있다. 예를 들어, 중국은 '중국 특색의 경제발전론',[2)] '중국 특색의 민주주의',[3)] '중국 특색의 소프

1) 2018년 9월 3-4일 베이징에서 개최된 중국·아프리카 협력포럼 정상회의는 중국의 개발도상국 외교정책이 불러일으키는 아프리카의 기대와 우려를 동시에 보여주었다. https://news.joins.com/article/22953849(검색일: 2018. 9. 1)

2) 중국 경제발전 모델의 지속가능성에 대한 상반된 입장을 살펴보기 위해선 아래 연구를 참고할 수 있다. Scott Kennedy, "The Myth of the Beijing Consensus," *Journal of Contemporary China*, Vol. 19, No. 65 (April 2010), pp.461-477; Suisheng Zhao, "The

트파워'[4] 등을 지속적으로 내세우며 중국이 추구하는 발전노선에 대한 서구 세계의 비판을 부인하고 있다. 중국 고유의 길을 강조하며 서구의 경계심을 약화시키려는 중국의 노력은 '중국 특색의 사회주의 이론'과 맥이 닿아 있다. 세계 2위의 경제 대국으로 성장하는 과정에서 중국은 중국 특색의 사회주의라는 논리를 바탕으로 사회주의 경제 체제에 자본주의 요소를 결합하는 전략에 대해 이데올로기적 당위성을 부여했다. 중국 경제의 빠른 성장을 뒷받침하는 수정주의 이데올로기를 둘러싸고 전개됐던 광범위한 학문적 논의가 오늘 날 강대국으로 부상하는 중국이 스스로를 방어하는 다양한 논리를 개발하는 시도에 자신감을 부여했을 것으로 추정된다.

중국 특색의 사회주의 이론이 사회주의 원칙을 상당 부분 포기하고 자본주의 경제를 받아들이는 정책 전환을 합리화시키는 논리적 기제로 활용됐다면 오늘 날 배회하는 중국 특색의 강조는 중국이 비서구 사회를 대변하는 새로운 이론을 제시하며 미래 미국의 패권을 대체할 수 있는 국가로서의 지위를 확보하려는 전략적 의도가 반영되어 있다.[5] 현재 중국 국제정치학계와 일부 서구 학자들은 중국의 장구한 역사적 경험, 풍부한 문화유산, 다양한 철학 사조를 근간으로 '중국 특색의 국제정치이론'을 창출하고 이를 확산시키는 작업을 진행 중이다.

China Model: Can It Replace the Western Model of Modernization?" *Journal of Contemporary China*, Vol. 19, No. 65 (April 2010), pp.419-436.

3) 이정남, "민주주의에 대한 중국의 인식: 비교 역사적 관점을 중심으로," 이정남 편, 『민주주의와 중국』(서울: 아연출판부, 2012), pp.48-59; 판웨이 저, 김갑수 역, 『중국이라는 새로운 국가모델론』(서울: 에버리치홀딩스, 2010). 중국 정치체제의 효율성과 관련된 주장은 2장에 나타나고 있다; Qiushi, http://english.qstheory.cn/politics/201109/t20110924_112513.htm (검색일: 2019. 3. 2)

4) 중국 소프트 파워가 작동하는 논리와 실증적 사례를 알기 위해서는 다음의 연구를 참조할 수 있다. Timo Kivimaki, "Soft Power and Global Governance with Chinese Characteristics," *Chinese Journal of International Politics*, Vol. 7, No. 4 (Winter 2014), pp.421-447; Myungsik Ham, Elaine Tolentino, "Socialisation of China's Soft Power: Building Friendship through Potential Leaders," *China: An International Journal*, Vol. 16, No. 1 (February 2018), pp.45-68.

5) 중국이 강대국으로 부상하면서 중국 최고 지도자들은 서구 세계에 맞설 수 있는 중국 특색의 담론이 필요함을 지속적으로 강조해왔다. Xinhua News, "Hu Jintao Calls for Enhancing 'Soft Power' of Chinese Culture," http://news.xinhuanet.com/english/2007-10/15/content_6883748.htm(검색일: 2018. 9. 1); 光明日报, "构建中国特色话语体系 增强国际影响力话语权:深入学习习近平总书记系列重要讲话精神笔谈," http://theory.people.com.cn/n/2015/1114/c40531-27815447.html(검색일: 2018. 9. 7)

중국을 중심으로 한 비주류 국제정치학계의 이런 접근법은 서구 국제정치이론의 패러다임 중 국제체제가 강제하는 구조적 요인 또는 자유주의 무역질서가 부여하는 경제적 동기가 정치행위자의 합리성을 결정짓는 것이 아니라 각 정치행위자가 체득한 역사적 경험, 문화적 특성, 공유된 정체성 등이 합리적 행동의 근원으로 작용한다는 주장을 근거로 하고 있다.

이 글은 개별 국가의 정치행위에 정당성을 부여하기 위해 탄생한 서구 국제정치이론과 달리 보편적 이익의 추구를 목표로 하는 국제정치이론의 구성이 가능하다고 주창하는 중국 특색 국제정치이론 사이에 실질적인 차이점이 존재하는지 살펴보는 것을 목표로 하고 있다. 이를 위해 아래에서 중국 특색 국제정치이론이 제기된 배경과 전개과정, 중국 특색 국제정치이론의 구체적인 사례, 이들 이론이 지니고 있는 한계를 비판적으로 분석하고 중국 특색 국제정치이론을 설립하려는 중국의 의도가 한국 국제정치학계와 중국학 연구자들에게 부여하는 함의에 대해 간략히 논의하고자 한다.

2. 중국 특색 국제정치이론의 등장 배경, 전개과정, 특징

가. 중국 특색 국제정치이론의 등장 배경

서구 사회과학에서 인간의 행위를 평가하고 분석하기 위해 사용되는 객관적인 지표는 합리성(rationality)이다. 합리성은 모든 행위자가 다양한 환경에서 수많은 정치적, 경제적, 사회적 행동을 결정해야 하는 순간 행위자의 이익 추구 여부가 판단의 가장 중요한 기준으로 작용한다는 가정이다.[6] 경제학에서 널리 사용되는 합리적 선택의 가설은 국제정치학을 포함해 서구 정치학의 이론 발전

6) Donald Green, Ian Shapiro, *Pathologies of Rational Choice Theory: A Critique of Applications in Political Science* (New Heaven: Yale University Press, 1996), pp.1-31; Douglass North, *Institutions, Institutional Change and Economic Performance* (New York: Cambridge University Press, 1990), pp.3-15.

과정에서 가장 중요한 준거점으로 작용해왔다. 즉, 모든 정치 행위자는 국제적인 세력균형이나 세계 자본주의 체제와 같은 국제체제 또는 국제적, 국내적으로 형성된 다양한 형태의 제도 하에서 어떤 행동이나 정책을 결정할 때 주어진 환경이 허락하는 범위 안에서 스스로의 이익을 극대화시키는 경향을 보인다는 것이다. 서구 국제정치이론의 주류를 형성하는 현실주의와 자유주의 패러다임에 속하는 모든 이론도 인간, 조직, 국가의 전략적 행동 원리를 이와 같은 합리성에 근거해 설명하고 있다.

예를 들어, 현실주의의 핵심 가정인 국제정치 행위자로서의 국가, 국가 행위의 목적인 국익 추구, 국익의 최상위 목표인 국가의 안전보장을 위한 세력균형 형성 그리고 이 모든 행위를 규정하는 국제체제의 중요성을 설명하는 논리가 모두 합리성의 가설에 근거하고 있다. 또한 자유주의 이론의 근간인 상호의존, 제도의 역할, 민주주의와 평화의 관계 등도 합리적 선택에 따른 이익 추구 현상에 그 기원을 두고 있다. 문제는 서구의 합리성에 뿌리를 둔 국제정치 이론을 통해 현재 부상하고 있는 중국의 역할을 분석하고 이에 따른 미래 국제정치 지형을 예측할 때 대부분의 서구 국제정치이론이 중국의 부상에 대해 부정적인 함의를 전달하고 있다는 점이다.

예를 들어, 현실주의 시각에서 일극체제(unipolarity)의 유용성을 강조하는 윌리암 월포스나 강대국 정치의 비극을 설파하는 존 미어샤이머는 부상하는 중국이 미국에 순응하기보다 미국의 이익에 도전할 가능성이 높다고 전망하면서 미국이 중국의 성장에 도움을 주는 연루정책보다 봉쇄정책을 시행하는 것이 장기적인 관점에서 미국의 국익과 세계 평화를 보장하는 방법이라고 주장한다.[7] 이처럼 강력한 단일 패권 국가의 존재가 국가의 이익과 세계 평화를 위해 더 안정적인 역할을 수행할 것이라든지 강대국 간 전쟁은 피할 수 없다는 현실주의의 전제는 부상하는 중국을 미국의 이익을 침해하는 명백한 위협으로 지목하고 있다.

---

7) John Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton & Company, 2014), pp.360-400; William Wohlforth, "The Stability of a Unipolar World," *International Security*, Vol. 24, No. 1 (July 1999), pp.5-41.

국제정치에서 현실주의와 결을 달리하는 자유주의 이론도 중국의 미래가 국제정치에 미치는 영향에 대한 함의를 밝히는데 있어 현실주의와 크게 다르지 않다. 브루스 러셋이 주창한 민주평화론(Democratic Peace)은 비록 민주주의 국가 사이에 갈등이 존재할 수는 있으나 전쟁은 발생하지 않았다는 역사적 사실에 근거해 자유주의 전통을 옹호하고 있다.[8] 에드워드 맨스필드와 헬렌 밀너도 민주주의 국가 간 무역의존도가 높은 사실을 민주주의 정치체제가 지니고 있는 선거 제도의 특성에서 찾으며 권위주의에 대한 자유주의의 장점을 강조하고 있다.[9]

현재 진행 중인 미중 무역 분쟁으로 인해 초미의 관심사로 대두된 미중 패권 경쟁에 대한 논의는 국가의 파워를 중시하는 현실주의 시각과 국제 제도의 역할을 강조하는 신제도주의 입장이 복합적으로 연관된 패권안정론을 기반으로 전개되고 있다. 이 중 신흥도전국의 정치적, 군사적 파워에 초점을 맞춰 미국에 도전하는 중국이라는 입장을 견지하는 현실주의자에게 중국은 명백한 수정주의 국가로 간주된다. 다른 한편 미국이 주도하는 자유주의 무역질서의 역할을 강조하는 시각에서 중국의 부상을 분석하면 다음과 같은 함의가 도출된다. 로버트 키오헨은 패권 이후(After Hegemony)라는 저서에서 비록 미국의 패권적 지위가 사라진다 할지라도 미국이 설립을 주도했던 자유주의 국제 제도가 제공하는 경제적 효과를 경험한 국가들은 미국 이후에도 자유주의 국제질서를 지지하는 합리적 선택을 할 것이라고 주장한다.[10] 같은 맥락에서 던컨 스나이달은 세계가 경제 위기에 처한 1970년대 후반과 1980년대 초반 미국의 패권적 지위가 약화되는 시점에서 왜 서독과 일본이 미국의 패권에 도전하지 않고 미국 주도의 경제 질서를 뒷받침했는지에 대한 분석을 통해 자유주의 국제경제 질서의 과실을 공유했던 경쟁국들이 미국에 도전하는 대신 미국과 협력하는 길을 선택했다고 주장하고 있다.[11] 존 아이켄베리와 찰스 쿠푸찬도 패권 국가의 몰락은 피할

8) Bruce Russet, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press, 1993), pp.3-42.

9) Edward Mansfield, Helen Milner, "Why Democracies Cooperate More," *International Organization*, Vol. 56, No. 3 (Summer 2002), pp.477-513.

10) Robert Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton: Princeton University Press, 1984), pp.85-109.

수 없는 길이지만 새로운 부상국이 자유주의 원칙, 규범, 가치를 공유한다면 패권 전쟁이 아닌 평화로운 세력전이가 가능하다고 주장하고 있다.[12]

위에서 간략히 살펴본 것처럼 전통적인 현실주의와 자유주의에 입각한 대부분의 서구 국제정치이론은 부상하는 비자유주의 국가인 중국이 세계 질서에 위협을 가할 것이며 불안정성을 높이는 역할을 수행할 것으로 예측하고 있다. 이는 서방 세계의 견제를 극복하고 지속적인 성장을 이뤄야 할 중국이 서구의 시각을 극복하고 자신의 부상을 정당화시킬 수 있는 국제정치 담론을 창출하고 이를 확산할 필요성의 강력한 배경이 된다.

나. 중국 특색 국제정치이론의 전개 과정

중국 국제정치학계에서 중국 특색 국제정치이론의 창출 가능성은 개혁 개방이 실시된 지 약 10여년이 경과한 1987년에 논의되기 시작했다.[13] 하지만 국제정치학계에서 중국 전문가들을 중심으로 중국 특색 국제정치이론의 도출 가능성이 본격적으로 논의되기 시작한 것은 2000년대 들어서이다. 중국학자 송신닝과 영국 학자 윌리엄 칼라한이 2001년 중국 특색 국제정치이론의 성립 가능성에 대해 논쟁을 벌인 이후 유사한 논의가 중국과 서구학자들에 의해 연속적으로 발표되었다.[14] 하지만 중국 국내정치와 외교정책을 분석하는데 있어 중국이 지니고 있는 특수성이 중요한 분석 기제로 고려되어야 한다는 주장은 냉전시대 서

---

11) Duncan Snidal, "The Limits of Hegemonic Stability Theory," *International Organization*, Vol. 39, No. 4 (Autumn 1985), pp.579-614.

12) John Ikenberry, Charles Kupchan, "Socialization and Hegemonic Power,"*International Organization*, Vol. 44, No. 3 (Summer 1990), pp.283-316.

13) Xuetong Yan, *Ancient Chinese Thought, Modern Chinese Power* (Princeton: Princeton University Press, 2011). p.200.

14) William Callahan, "China and the Globalisation of IR Theory: Discussion of 'Building International Relations Theory with Chinese Characteristics'," *Journal of Contemporary China*, Vol. 10, No. 26 (August 2001), pp.75-88; William Callahan, "Sino-speak: Chinese Exceptionalism and the Politics of History," *Journal of Asian Studies*, Vol. 71, No. 1 (February 2012), pp.1-23; Xinning Song, "Building International Relations Theory with Chinese Characteristics," *Journal of Contemporary China*, Vol. 10, No. 26 (August 2001), pp.61-74.

구 학자들에 의해 먼저 제기된바 있다. 당시 주장의 핵심은 중국에 내재하는 특수성을 통해 중국을 바라볼 때 중국의 정치와 외교정책을 올바로 이해할 수 있다는 논점으로 요약될 수 있다. 이런 논쟁의 핵심은 중국이 과거 아시아의 제국으로 존재했던 역사적 사실에 주목하며 중국에 내재하고 있는 고유한 세계관이 현대 국제정치에 반응하는 중국 외교정책에 일정한 영향을 행사할 것이라는 추론에 기반하고 있다. 이런 주장에 핵심적인 기반을 제공한 미국 역사학자 존 킹 페어뱅크는 중국이 아시아에서 유지했던 조공제도가 주권을 기반으로 형성된 근대 유럽의 국제정치와 상이한 형태의 질서를 구축했다는 점을 강조하고 있다.[15] 중국 고유의 특수한 성격이 외교정책에 반영되고 있다는 주장은 냉전 시기 중국의 외교정책을 연구했던 마크 맨컬[16]이나 존 크레이머-빙[17]에 의해 계승되었다.

하지만 위에서 간략히 언급한 것처럼 부상하는 중국이 현존하는 국제질서에 새로운 대안을 제시할 수 있을지에 대한 논의는 중국이 경제 대국으로 발을 내디디면서 본격화되었다. 구체적으로 데이비드 강은 2003년 중국과 아시아의 역사적 경험에 근거해 국제정치를 새롭게 해석하기 위한 분석 틀이 필요함을 제기했다. 그는 근대 이전 중국이 강력한 제국을 유지할 때 동아시아가 평화로울 수 있었던 것은 강력한 중국의 존재가 아시아 국가들로 하여금 중국의 가치와 규범을 적극적으로 받아들이게 만들었기 때문이라고 주장했다.[18] 그는 이후에도 중

---

15) John K. Fairbank, ed., *The Chinese World Order: Traditional China's Foreign Relations* (Cambridge: Harvard University Press, 1968).

16) Mark Mancall, "The Persistency of Tradition in Chinese Foreign Policy," *Annals of the American Academy of Political and Social Science*, Vol. 349 (September 1963), pp.14-26.

17) John Crammer-Byng, "The Chinese View of Their Place in the World: An Historical Perspective," *China Quarterly*, No. 53 (January/March 1973), pp.67-79.

18) 데이비드 강은 중국에서 명나라와 청나라가 지배하던 500년의 기간 동안 아시아에 형성된 지역질서와 동일한 시간대의 유럽 국제정치를 비교해 아시아가 공식적으로는 계서질서를 지니고 있었지만 비공식적으로는 평등한 관계를 형성하고 있었던 반면 유럽은 공식적으로는 주권 관계를 형성하고 있었어도 비공식적으로는 불평등한 관계를 유지했었다는 견해를 제시했다. David Kang, "Getting Asia Wrong: The Need for New Analytical Frameworks," *International Security*, Vol. 27, No. 4 (Spring 2003), pp.57-85; 동양과 서양에서 규범이 수행한 모순적인 역할을 분석하며 위와 상반된 주장을 펼친 연구로는 Stephen Krasner의 "Organized Hypocrisy in Nineteenth-Century East Asia,"

국의 조공체제가 유교문명권에서 수행했던 긍정적인 역할에 대한 평가를 연이어 발표했는데 이는 현재적 의미에서 중국이 강력해질수록 주변국이 과거처럼 중국을 중심으로 한 국제질서를 형성할 것이라는 주장으로 해석되며 논란을 불러일으켰다.[19]

비슷한 시기 미국 정치학자 브랜트리 워맥은 탈냉전 시기 국제정치를 해석할 수 있는 새로운 분석틀로 비대칭(asymmetry)이라는 개념을 제시했는데 그는 비대칭 개념에 사용된 아이디어의 골간을 중국의 도가와 유가에서 강조하는 음양과 조화의 원칙에서 차입했다. 워맥은 동아시아 역사에서 핵심적으로 작용하는 질서의 원리가 강대국인 중국과 주변 약소국 사이에 실행됐던 존중과 자율성의 맞교환이었음을 주장하며 주변국이 중국에게 강대국에 대한 존중을 표현했을 때 중국이 약소국의 자율성을 보장했다는 주장을 전개했다.[20] 강과 워맥의 접근법이 일치하지는 않으나 중국과 주변국 사이에 시행됐던 조공제도를 동아시아 질서를 유지했던 기제로 파악한다는 점에서 유사성을 보이고 있다.[21]

중국이 부상하는 시기 서구학자들이 과거 동아시아에 존재했던 질서의 원리를 재해석하고 이를 통해 현대 국제정치를 분석하는 작업을 시도하는 동안 중국의 학자들은 중국 특색의 국제정치이론을 창조하는 작업을 본격적으로 진행했

International Relations of the Asia-Pacific, Vol. 1, No. 2 (August 2001), pp.173-197을 참고할 수 있다.

19) David Kang, *East Asia before the West: Five Centuries of Trade and Tribute* (New York: Columbia University Press, 2010).

20) Brantly Womack, *China and Vietnam: The Politics of Asymmetry* (New York: Cambridge University Press, 2006).

21) 과거와 달리 조공제도를 역사적, 서술적으로 설명하지 않고 체계적, 이론적 수준에서 분석하는 연구들이 꾸준히 증가하고 있다. 대표적으로 다음의 연구들을 참고할 수 있다. Brantly Womack, "Asymmetry and China's Tributary System," *Chinese Journal of International Politics*, Vol. 5, No. 1 (Spring 2012), pp.37-54; Fangyin Zhou, "Equilibrium Analysis of the Tributary System," *Chinese Journal of International Politics*, Vol. 4, No. 2 (Summer 2011), pp.147-178; Feng Zhang, *Chinese Hegemony: Grand Strategy and International Institutions in East Asian History* (Stanford: Stanford University Press, 2015); Nianshen Song, "'Tributary' from a Multilateral and Multilayered Perspective," *Chinese Journal of International Politics*, Vol. 5, No. 2 (Summer 2012), pp.155-182; Yongjin Zhang, Barry Buzan, "The Tributary System as International Society in Theory and Practice," *Chinese Journal of International Politics*, Vol. 5, No. 1 (Spring 2012), pp.3-36.

다. 대표적인 인물로 현 중국 외교학원 원장인 친야칭과 칭화대학 국제관계학원 원장인 옌쉐통을 들 수 있다. 친야칭은 2007년 중국 국제정치이론이 존재하지 않았던 세 가지 이유를 설명하면서 중국의 영향력이 증가하고 중국 학계의 역량이 확보되면서 중국의 경험을 바탕으로 한 국제정치이론을 창조하는 작업이 가능해졌다고 주장했다.[22] 이와는 결을 달리하지만 중국 최초의 통일 왕조인 진나라 설립 이전 전국시대의 철학적 사조를 연구한 옌쉐통은 서구에 현실주의 전통이 존재하듯 중국에도 현실주의 사조가 존재했음을 주장하며 중국 전통 사상과 서구 국제정치이론의 결합을 통해 국제정치이론을 더욱 심화 발전시킬 수 있음을 내세우고 있다.[23]

중국 학계가 중국특색의 국제정치이론을 확립하고 이를 전파하는 방식을 보면 중국 특색 국제정치를 이론화하는 과정이 고도의 전략적 사고 하에 추진되고 있음을 알 수 있다. 그 근거로 우선 중국 국제정치학계가 중국 특색의 국제정치이론을 하나의 주요 화두로 제시하며 이를 범학계적인 차원에서 적극 추진하고 있는 점을 들 수 있다. 중국 국제정치학회 부회장을 역임하고 있는 한 인사는 "세계 질서를 설명하는 미국 중심의 서구 국제정치이론은 비서구 사회에서 발생하는 다양한 국제정치 현상을 제대로 설명하고 있지 못하며 설사 이런 연구를 수행한다 해도 서구만의 가치관과 세계관을 적용함으로 인해 비서구 세계에서 발생하는 현상을 올바르게 해석하지 못하는 한계가 있다"며 새로운 대안을 제시하는 과정에서 중국 국제정치 연구자들의 집중적인 노력과 협력이 필요함을 강조하고 있다.[24]

---

22) 친야칭은 신중국 출범 이후에도 중국 고유의 국제정치이론에 대한 고민이 부재했던 이유로 중국 사회가 전통적으로 국제성에 대한 인식이 부족했고, 중국 내부에서도 서구 국제정치이론의 영향력이 컸으며, 중국 학계 내부에 이론을 담보할 수 있는 연구능력이 부족했음을 들고 있다. Yaqing Qin, "Why Is There No Chinese International Relations Theory?" *International Relations of the Asia-Pacific*, Vol. 7, No. 3 (September 2007), pp.313-340; 같은 학술지에 실린 서론에서 아미타브 아차리아와 배리 뷰잔은 중국뿐만 아니라 비서구세계에서 국제정치이론이 존재하지 않는 이유에 대해 설명하고 있다. Amitav Acharya, Barry Buzan, "Why Is There No Non-western International Relations Theory? An Introduction," *International Relations of the Asia-Pacific*, Vol. 7, No. 3 (September 2007), pp.287-312.

23) Xuetong Yan, *Ancient Chinese Thought, Modern Chinese Power* (Princeton: Princeton University Press, 2011), pp.252-259.

다음으로 중국 특색 국제정치이론화 작업의 효율성을 제고하기 위해 중국 학계는 외국 학자들과의 협업을 중시하고 있다. 특히 기존 주류 국제정치학계와 입장을 달리하고 있는 영어권 학자들과의 적극적인 연대를 통해 이론적, 방법론적, 언어적 장벽에서 발생하는 불리함을 뛰어 넘고 있다. 특히 미국 주류 국제정치학계와 접근방식을 달리하는 영국학파(English School)와의 밀접한 학문적 유대를 통해 국제정치에서 역사, 문화, 철학이 지니는 중요성을 부각시키고 있다.[25] 이 중 현 영국학파를 대표하는 학자인 배리 뷰잔의 활약이 두드러지는데 그는 빈번한 중국 방문을 통해 미국에서 소외되고 있는 영국학파의 개념을 널리 홍보하는 동시에 영국학파와 중국 국제정치학계가 공유하는 논리를 이론으로 발전시키는 노력을 왕성하게 기울이고 있다.

끝으로 중국 국제정치학계는 중국 특색의 국제정치이론을 세계화시키고 중국에 우호적인 학술 논문 발표를 활성화시키는 방안으로 자체적으로 창간한 영문 학술지를 적극 활용하고 있다. 대표적인 사례로 옌쉐통 주도 하에 2006년 여름에 창간된 중국국제정치학술지(Chinese Journal of International Politics)를 들 수 있다. 이 학술지는 짧은 역사에도 불구하고 출발 단계부터 영국 옥스퍼드 대학교 출판사와 전략적 협력을 지속해 온 결과 현재 학계에서 널리 통용되는 학문영향력지수(Impact Factor)에서 매우 높은 평판을 유지하며 중국과 관련된 국제정치 분야의 유력한 학술지로 인정받고 있다. 이 학술지의 성공 사례로 미루어 볼 때 중국 국제정치학계는 자국의 학문 논리와 영향력을 확보할 수 있는 수단으로 보다 많은 영문 학술지를 발간하는 노력을 기울일 것으로 예상된다. 지금까지 살펴본 것처럼 중국 특색의 국제정치학은 중국의 부상을 계기로 주류 서구 국제정치이론의 접근 방법에 만족하지 못한 서구 정치학자와 중국의 부상을 정당화하고 새로운 대안을 제시하려는 중국 국제정치학자들 간 공통의

---

24) 2018년 6월 29일 장춘에서의 인터뷰. 인터뷰에 응한 인사가 익명으로 남아 있기를 요청해 이름을 생략했다.

25) Jiangli Wang, Barry Buzan, “The English and Chinese Schools of International Relations: Comparisons and Lessons,” *Chinese Journal of International Politics*, Vol. 7, No. 1 (Spring 2014), pp.1-46.

이해관계가 성립되면서 짧은 기간에 비약적인 성과를 축적해왔다.

다. 중국 특색 국제정치이론의 특징

중국 특색을 강조하는 국제정치이론은 성격상 서구 국제정치이론 패러다임 중 구성주의와 유사한 특성을 공유하고 있다. 구성주의적 접근 방식은 현실주의와 자유주의 전통을 계승하는 국제정치이론에 비해 뒤늦게 학자들의 주목을 받기 시작했지만 최근 이에 대한 관심이 크게 증가하며 다양한 연구 성과를 배출하고 있다. 구성주의가 국제정치학계에서 주목을 받게 된 결정적 사건은 냉전체제의 붕괴이다. 제2차 세계대전 이후 형성된 양극체제는 오늘 날 서구 국제정치학계의 지배적인 패러다임으로 군림하는 신현실주의 발전의 기틀이 되었다. 미국과 구소련이 세계를 양분하며 세력균형을 기반으로 한 국제질서를 형성하자 국제정치를 설명하는 요소로서 양극체제, 세력균형, 국제체제 등의 개념이 미국 외교정책을 뒷받침하는 핵심 논리로 자리 잡기 시작했다. 특히 신현실주의 패러다임은 근대 유럽의 역사적 경험을 기반으로 국력과 세력균형이 국가의 생존과 소멸에 미친 영향에 대한 연구를 통해 냉전 시기 동맹, 군비경쟁, 핵억지력 등 냉전질서를 정당화시키는 국제정치 이론의 체계적인 발전에 지대한 공헌을 했다.

하지만 영원히 지속될 것 같던 냉전질서의 붕괴는 이전까지 현실주의 이론에 크게 의지하던 국제정치학계에 커다란 충격을 불러일으켰다. 이는 경직된 사고와 협소한 세계관에 입각해 국제관계를 설명하던 학자들이 국가 간 행위를 이해하는 새로운 접근법의 필요성을 깨닫는 계기로 작용했다. 구성주의 발전에 큰 기여를 한 학자 중 한명인 알렉산더 웬트는 기존 국제정치학계에서 당연하게 받아들여지던 개념인 무정부(anarchy)에 대해 새로운 개념을 제시했다. 그는 국제정치에서 무정부는 주어진 것이며 어떠한 형태의 질서(archy)라도 무정부상태보다 이로울 것이라는 기존의 통념에 반대하며 무정부라는 개념 자체가 국가 스스로가 구성해낸 (anarchy is what states make of it) 정치적 결과에 불과

하다는 혁신적인 주장을 전개했다.[26] 그는 냉전시기 국제정치의 핵심 프레임으로 작용하던 신현실주의 국제체제(international system) 개념을 비판하면서 구조(structure)와 행위자(agent)간에는 상위에서 하위로 전달되는 일방적인 위계의 개념만이 존재하는 것이 아니라 구조와 행위자가 상호 작용을 통해 국제정치를 인식하며 이 과정에서 행위자는 구조와의 관계를 설정하는 개념과 원칙을 형성해낸다고 주장했다.[27]

중국 특색의 국제정치이론을 전개하는 학자들이 구성주의로부터 영향을 받고 있다는 점은 다음과 같은 사실을 통해 확인할 수 있다. 첫째, 중국이 가지고 있는 국제정치이론의 고유한 자원에 주목하는 학자들은 서구 국제정치이론의 핵심 패러다임인 현실주의와 자유주의 그리고 이들 이론의 중심 가설인 합리성에 대해 다양한 접근 양식이 필요함을 강조한다. 예를 들어, 데이비드 강의 경우 중국이 강성한 제국으로 존재할 때 주변 국가들이 중국 중심의 질서에 참여했던 이유를 당시 중국이 보유했던 파워도 중요했지만 중국이 지니고 있는 원칙, 가치, 규범, 문화 같은 비공식적(informal) 요소들에 대한 동화에서 찾고 있다. 브랜트리 워맥도 국가 간 역량의 비대칭 상황에서 평화가 유지될 수 있었던 근원을 강대국과 약소국의 관계를 규정하는 파워의 차이가 아닌 비대칭 구조에서 강대국과 약소국 각각이 상호 국가 역량의 차이를 인정하고 수용한 것에서 찾고 있다. 워맥의 논지를 요약하면 약소국이 강대국의 리더십을 수용하는 조건으로 강대국은 약소국의 안전과 자율성을 보장해주는 일종의 교환관계가 중국과 주변국에 형성되었고 양측이 이 규칙을 존중하면서 평화가 지속될 수 있었다는 것이다. 이에 더해 배리 뷰잔은 냉전과 탈냉전 시대 각 지역이 지니고 있는 안보이슈를 지역적, 세계적 차원에서 비교 검토한 결과 각 지역이 지니고 있는 고유한 정치적, 경제적, 군사적 복합성이 특정 지역에 근거한 독특한 안보질서를 형

---

26) Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization*, Vol. 46, No. 2 (Spring 1992), pp. 391-425.

27) Alexander Wendt, "The Agent-Structure Problem in International Relations," *International Organization*, Vol. 41, No. 3 (Summer 1987), pp.335-370.

성했다는 논리를 전개하고 있다.[28] 중국학자들은 이와 같은 주장을 바탕으로 중국의 고유성, 유교문명의 독창성, 동아시아 지역에 존재하는 내재성 등이 아시아에서 서구와 다른 지역질서를 형성할 수 있었던 주요 변수로 작동했음을 강조하고 있다.

이는 중국 특색의 국제정치이론이 신현실주의자와 세계체제론자들이 주장하는 냉전과 자본주의 체제 같은 구조가 행위자의 합리성을 강제한다는 구조주의(structuralism) 시각에서 탈피해, 각 행위자가 구조에 대해 지니고 있는 개념과 인식은 오랜 기간 둘 사이의 관계를 통해 형성된 구조화(structuration)의 결과라고 주장하는 웬트의 접근법에 더욱 근접해 있음을 뜻한다. 다시 말하면, 중국 특색의 이론을 구성하려는 국제정치학자들은 구조가 부분을 제약한다는 서구 학계의 결정론(determinism)적 시각을 거부하고 각 부분과 전체가 상호 주고받는 관계에서 정형화되지 않은 고유한 관계를 형성한다는 전체론(holism)의 시각을 흡수하고 있다.

3. 중국 특색 국제정치이론의 사례

이 장에서는 중국의 외교정책이 미국이나 서구와 달리 전 세계 구성원의 보편적 이익을 추구하고 있음을 강조하면서 중국 특색 국제정치이론의 창출이 가능하다고 주장하는 학자들의 의견이 현실 국제정치에서 실제로 존립가능한지 구체적인 사례 분석을 통해 평가하고자 한다. 중국 특색 국제정치이론의 핵심이 중국 외교의 전통 사상과 현재 진행되는 중국 정부의 외교정책이 시공을 초월해 인류공동체의 보편적 이익을 추구하는 것에 초점이 맞추어져 있다는 점을 고려해 중국 특색이 강조하는 고유한 속성이 외교정책의 실천과정에서 어떻게 변질되어 가는지를 밝히는데 초점을 맞추고자 한다. 구체적으로 인식론적 측면에서

28) Barry Buzn, Ole Wæver, *Regions and Powers: The Structure of International Security* (Cambridge: Cambridge University Press, 2004), pp.40-82.

는 중국의 핵심 가치인 천하관(All under Heaven)에 대한 비판적 분석을 통해, 정책적인 측면에서는 '인류운명공동체'(人類命運共同體)론을 내세우며 지금까지 중국 정부가 추진하고 있는 일대일로 사업에서 드러난 실증적 결과에 대한 평가를 진행하고자 한다.

가. 사상적 기반으로서의 천하관

중국 정치와 역사에서 공통적으로 등장하는 것이 천하관이다. 천하관은 중국의 국내정치와 중국이 형성했던 전통적인 국제질서를 이해하기 위한 가장 핵심적인 개념이다. 중국은 전통적으로 천자를 하늘이 부여한 특권을 지닌 인물로 규정하며 천자에게 도덕적 권위를 부여했다. 즉, 하늘이 내린 명(Mandate of Heaven)을 받은 자만이 천자의 지위에 오를 수 있다는 논리를 통해 천자에게 절대적인 정치적, 도덕적 지위를 부여했다. 이는 중국인들이 하늘의 아들이자 절대적 권위를 지닌 천자를 중심으로 천자가 향유하는 문화와 예식이, 교화를 통해서든 무력을 통해서든, 야만적인 주변으로 확산되는 과정을 천하질서를 건립하는 과정으로 인식하게 만들었다. 따라서 무형의 문화, 도덕, 규범을 중시여기는 천하질서에는 서구 세계가 국제질서의 핵심으로 간주하는 주권, 민족국가, 평등, 조약, 국경의 개념이 생략되어 있다.

이로 인해 서구에서 개인주의, 평등, 정의, 민주주의 등이 핵심 가치로 대두되는 시기에도 중국에서는 왕도(Kingly Way)를 근거로 천자가 존재하는 중심과 그렇지 않은 주변 간의 관계를 설정하는 전통이 지속되었다. 즉, 특정한 인물이 내부의 중앙 권력을 차지하면 그는 하늘이 부여한 천명을 받은 자로 인식되어지고 외부에 위치한 주변은 그 권력을 받아들이는 것이 천하질서의 원칙으로 통용되었다. 야만적인 주변은 중앙에 대한 존중의 예로 조공을 바치는 것을 통해 천하질서에 포함될 수 있었다. 조공제도가 천하질서를 유지하는 제도로서의 당위성을 인정받을 수 있었던 것은 각각의 행위자가 자신에게 주어진 본분을 충실히 수행할 때 조화로운 질서가 구현된다는 유교사상이 동아시아에 광범위

하게 퍼져있었기 때문이다. 이와 같은 천하관은 서구가 중국을 침략했던 18세기 말부터 19세기 초까지 동아시아 유교 문명권의 국제질서를 유지하는 원천으로 작동했다.[29]

오늘 날 중국 국제정치학계는 과거의 천하 개념을 인용해 부상하는 중국에 정치적, 도덕적, 규범적 당위성을 부여하는 작업을 시도하고 있다. 이러한 시도는 천하질서를 하나의 '공유된 문화와 가치의 레짐'으로 정의하며 중국이 제공하는 가치체계를 지지하는 공동체의 건설을 통해 새로운 질서를 형성할 수 있다는 논리로 이어진다.[30] 또한 과거 중국의 천하관이 중국 사회가 올바르게 작동하는 도덕적, 윤리적 정당성을 제공했을 뿐만 아니라 대외적으로는 정의롭고 공정한 원칙을 국제적 규범으로 확산시키는 기능을 수행했다고 주장하며 천하관을 서구 철학 사조 중 공리의 추구를 목표로 했던 사해동포주의(Cosmopolitanism)와 같은 맥락에서 해석해야 한다는 주장도 제기하고 있다.[31] 더 나아가 다니엘 벨은 조공제도가 국가 간 경제교류를 촉진하고 영토분쟁과 갈등을 해결하는 순기능의 역할을 수행했다고 주장하며 이런 역사적 경험으로부터 오늘 날 분쟁 해결을 위한 실마리를 구할 수 있다는 주장으로까지 확대시키고 있다.[32]

천하질서를 해석하는 시각은 과거 위계적인 질서를 바탕으로 이루어진 조공제도와 천하관에만 국한되어 있지 않다. 린춘은 중화인민공화국의 건설을 통해 주권 국가로 거듭난 중국이 사회주의 정책을 통해 과거 천하관을 재현했다는 논지를 펼친다. 그는 사회주의 중국은 국내적으로는 모든 계급, 인종, 문화의 다양성을 포괄하는 정책을 실시했고 대외적으로는 사회주의국제주의(socialist internationalism) 정신에 입각해 제국주의와 자본주의에 맞서 식민지 국가의

29) 자오팅양 저, 노승현 역,『천하체계』(서울: 길, 2010).
30) Ban Wang, "The Moral Vision of Kang Youwei's Book of the Great Community," in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics* (Durham: Duke University Press, 2017).
31) Prasenjit Duara, "The Chinese World Order and Planetary Sustainability," in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics* (Durham: Duke University Press, 2017).
32) Daniel Bell, "Realizing Tianxia: Traditional Values and China's Foreign Policy," in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics* (Durham: Duke University Press, 2017).

해방을 지원하는 정책을 실천했음을 주장하며 이와 같은 중국의 외교정책이 과거 천하질서가 규범과 가치를 근간으로 국제주의를 실현했던 것과 같은 맥락에서 이해되어야 함을 강조하고 있다.[33] 서정경도 마오쩌둥 시기 구소련과 미국의 제국주의 침탈에 맞서 비서구 식민지 국가의 사회주의 혁명을 지원하며 스스로를 제3세계의 구심점으로 자임한 중국의 전략이 천하관과 일정한 관계가 있음을 지적한바 있다.[34]

중국 특색의 국제정치이론을 정립하기 위해 천하관과 천하질서를 적극 활용하는 학자들은 천하관을 과거 중국에 존재했던 '중국예외주의'(Chinese exceptionalism)로 규정하는 정도를 넘어 현 세계질서를 대체할 수 있는 하나의 대안으로 제시하고 있다. 그리고 이런 움직임은 천하관을 사해동포주의, 유교주의, 사회주의 국제주의, 초국가주의와 등치시키거나 이들 사조와의 유사성을 찾아 중국 외교정책을 재해석하려는 노력으로 구체화되고 있다. 하지만 천하관이 과거 유교문명권 영역에서 일정한 원칙과 규범으로 작동한 것이 사실이라 할지라도 현재 의미에서 천하질서의 부활 가능성을 강조하고 이를 현대 국제질서에 대입시키려는 시도는 국제권력 구조에 도전하는 중국의 행위에 정당성을 부여하려는 이데올로기적 의도가 숨어있는 것으로 보인다.[35] 또한 역설적으로 문화혁명 시기 유교사상을 구시대 악의 상징으로 간주하며 청산의 대상으로 강조했던 중국이 필요에 따라 유교사상을 국가 이데올로기로 조작하는 것은 역사적 유산을 이용해 자신의 이미지를 긍정적으로 포장하려는 의도가 반영된 것으로 볼 수 있다.

중국 특색 국제정치이론의 사상적 토대로 논의되는 천하관은 중국이 형성했던 동아시아 전통질서는 중국이 지니고 있던 독특한 세계관인 천하관을 기반으로 형성되었으며 이렇게 구축된 동아시아 질서가 유교문명권에 속해 있던 다양

33) Chun Lin, "China's Lost World of Internationalism," in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics* (Durham: Duke University Press, 2017).

34) 서정경, "미・중 민족주의의 특성과 양국 관계: 메시아니즘과 천자관의 조우,"『국가전략』, 제19권, 제3호 (2013 가을), p.15.

35) Chishen Chang, Kuan-Hsing Chen, "Tracking Tianxia: On Intellectual Self-Positioning," in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics* (Durham: Duke University Press, 2017).

한 정치 세력에 의해 하나의 보편적 규범으로 수용되었다고 주장한다. 이는 중국이 지니고 있는 천자와 천하질서에 대한 인식이 주변으로 확장되어 장구한 세월 동안 지속되면서 천하질서에 속한 정치 개체들이 주어진 질서를 변화시키기보다 질서에 순응하고 존재하는 방법을 통해 자신의 정치적 이익을 담보하고 국가의 생존을 모색했음을 뜻하는 것이다. 하지만 비록 특정한 공동체나 지역적 특성에 기초해 형성된 간주관성(intersubjectivity)이 탈보편적인 국제질서 출현에 영향을 미친다는 국제정치 학계 일각의 논의에 의미를 부여한다 해도 국제관계를 규정짓는 보편적 개념이 광범위하게 형성된 오늘 날 과거에 존재했던 지엽적 논리에 현대 국제정치의 일반적 행위를 꿰맞추는 작업이 타당한지에 대해서는 의문이 제기된다. 더욱이 천하질서의 부활을 논하며 중국 문명과 사고의 우월성에 지나치게 집착한 나머지 동아시아 전통질서를 형성하는 과정에서 중요한 역할을 수행했던 주변 국가나 정치 행위자의 역할에 대한 연구를 도외시하는 것이 오늘 날 동아시아 국가들에게서 환영 받을 수 있을지는 여전히 미지수로 남는다.

나. 외교 전략으로써의 일대일로

2013년 시진핑 주석은 카자흐스탄과 인도네시아에서 육상과 해상으로 유럽과 아시아를 하나로 연결하는 일대일로 구상을 발표했고 세계는 이를 중국이 유라시아 대륙을 기점으로 중국 중심의 새로운 국제질서를 구상하겠다는 의지를 드러낸 것으로 받아들였다. 일대일로가 발표된 이후 중국의 학계는 이 프로젝트를 뒷받침하는 논문을 홍수처럼 쏟아내고 있고 중국의 미디어도 하루가 멀다 하고 일대일로에 대한 기사로 지면을 장식하고 있다.[36] 또한 중국 공산당은 2017년 10월에 개최된 제19차 전국대표대회에서 '시진핑 신시대 중국 특색의 사회주의 사상'과 일대일로를 공산당 당헌에 삽입했는데 이는 시진핑 사상이 마오쩌둥

36) 중국 학술 전문사이트인 CNKI에서 일대일로를 검색한 결과 총 49,447개의 관련 연구 결과가 검색되었다. http://www.cnki.com.cn/index.htm(검색일: 2018. 7. 26)

사상, 덩샤오핑 이론과 함께 중국 공산당의 핵심 지도이념으로 격상됨과 동시에 시진핑의 퇴임 이후에도 일대일로가 중국 공산당의 핵심 전략으로 추진될 것임을 의미하는 것이기도 하다.

중국은 일대일로에 참가하는 연선 국가들이 이 프로젝트를 통해 공정한 혜택을 누릴 것이며 중국은 일대일로를 이용해 패권적 지위를 추구하지 않을 것이라는 메시지를 반복해서 발신했다. 하지만 중국이 이미 미국, 일본 등이 중심이 된 아시아개발은행과 세계은행이 존재하는 상황에서 아시아인프라투자은행(AIIB)을 설립하고 일대일로를 '중국의 꿈'(中國夢)을 실현하는 과정과 노골적으로 등치시킴에 따라 일대일로가 단순히 연선 국가들 간의 경제와 무역을 촉진하는 수단에만 머물지 않을 것이라는 반론이 꾸준히 제기되었다. 현재 일대일로는 총 6개의 경제회랑으로 구성되어 있는데 이 회랑에 포함된 국가들이 개발도상국 중에서도 경제적으로 매우 낙후된 그룹에 속한다는 점, 경제적으로 중국에 대한 의존도가 높은 국가라는 점, 그리고 이들 회랑이 지정학적으로 중국의 안전보장에 지대한 영향을 미치는 지역에 위치하고 있다는 점을 고려할 때 경제회랑 건설의 진정한 목표가 사실상 중국의 안전보장을 확보하려는 전략적 시도라는 지적이 일고 있다.

일대일로는 중국이 경제 대국으로 부상한 이후 시도하는 최초의 메가톤급 프로젝트이며 일대일로 계획이 현실화됐을 때 세계의 경제 지도를 바꿀 수 있을 것이라는 주장까지 제기되고 있다. 또한 중국 학계도 일대일로 프로젝트를 정당화시키는 학문 작업을 왕성하게 진행하고 있는 것이 현 상황이다. 이런 측면에서 일대일로가 세계의 평화와 공동번영에 기여할 것이라는 중국의 주장, 특히 미국 중심의 경제 질서에서 소외된 국가들이 공정하고 평등한 경제적 과실을 누리게 될 것[37]이라는 선전이 현실에서 실제로 체화되고 있는지 아니면 중국 정부의 수사학에 불과한지를 살펴보는 것은 중국 특색의 국제정치 담론이 주장하

37) 李向阳, "构建 '一带一路'需要优先处理的关系,"『国际经济评论』, 제1호 (2015), pp.54-64; 王义桅, 郑栋, "'替代一路'战略的道德风险与应对措施," 『东北亚论坛』, 제4호 (2015), pp.39-48; 杨思灵. "'一带一路'倡议下中国与沿线国家关系治理及桃战,"『南亚研究』, 제2호 (2015), pp.15-34.

는 내용을 실제 국제정치 무대에서 시험해 볼 수 있는 중요한 기제가 될 수 있다.

일대일로 사업을 위해 중국 정부와 기관이 공표한 투자금의 정확한 집계는 보고서마다 다르지만 지금까지 발표된 내용 중 가장 많은 금액을 표기한 곳에 따르면 미국 화폐 기준으로 약 8조 달러에 이른다.[38] 제2차 세계대전 이후 미국이 유럽부흥계획(European Recovery Program 혹은 Marshall Plan)에 따라 1947년부터 4년간 총 130억 미국 달러를 동맹국의 전후복구에 투자했다는 점을 고려할 때 일대일로를 통해 중국이 동원하고 있는 자본은 가히 천문학적이라고 할 수 있다.

당시 마샬 플랜에 따라 조성된 금액이 공산주의의 확장을 억제하고 전후 미국 동맹국의 경제적 재건을 돕기 위해 사용되었다면 현재 중국이 일대일로 프로젝트를 위해 투자하는 금액은 대부분이 유라시아와 아프리카 개발도상국의 인프라를 설치할 목적으로 이용되고 있다. 마샬 플랜의 결과 피폐화된 유럽 경제가 향후 20년간 괄목할만한 성장을 이룬 것과 달리 일대일로 프로젝트가 가동 된 지 5년이 지난 현 시점에서 일대일로 연선에 있는 국가들 중 아직 눈에 띄는 경제성과를 달성한 나라는 보이지 않는다. 비록 경제 체질에서 전후 유럽의 국가와 6개 경제회랑이 관통하는 개발도상국 사이에 커다란 격차가 있다는 것을 인정한다 해도 지금까지 일대일로 건설에 투자된 자본이 양산한 결과에 대한 분석을 통해 간접적이나마 일대일로의 경제적 효과를 측정해 볼 수 있을 것이다.

미국 수도 워싱턴에 위치한 글로벌개발센터(Center for Global Development)가 2018년 발표한 보고서에 따르면 중국으로부터 차관 형태로 자금을 도입한 일대일로 연선 국가의 재정 상태는 매우 암울해 보인다. 특히 몽고, 몬테네그로, 파키스탄, 몰디브, 지부티, 라오스, 키르기스스탄, 타지키스탄 8개국은 기존의 부채 외에 일대일로 프로젝트를 목표로 유입된 차관에 의해 심각한 재정난에 시달리고 있다. 예를 들어, 지부티는 인프라 사업을 목적으로 중국으로부터

38) Jonathan Hillman, “China’s Belt and Road Initiative: Five Years Later”, https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later-0(검색일: 2018. 7. 15)

약 14억 달러를 유입했는데 이는 지부티 국내총생산의 75%에 육박하는 금액이다. 지부티는 앞으로도 공항, 항구, 고속도로 건설을 목표로 중국과 협력을 계속할 전망인데 지부티의 경제력과 부채 비율을 감안할 때 중국에 대한 지부티의 종속 상황이 심화될 것으로 예견된다. 지부티가 중국에 해외 군사기지를 제공한 최초의 국가라는 점에서 향후 지부티에 대한 중국의 입김이 증가하거나 해군 기지가 위치한 지역에 대해 중국이 지배권을 강화할 가능성이 높아지고 있다. 실질적으로 중국은 스리랑카 정부가 2009년 함반토타에 항구를 건설할 목적으로 중국으로부터 들여온 차관 3억 7천만 달러를 제때 상환하지 못하자 2018년 이 항구에 대해 99년의 조차권을 설정했다.[39] 19세기 말 중국이 서구 제국주의 국가들에게 홍콩, 마카오를 비롯해 수많은 항구를 강탈당한 역사를 잊지 못해 '두 개의 100년'이란 국가 목표를 설정한 것을 고려할 때 중국이 함반토타 항구를 조차한 행위는 부상하는 중국이 역사로부터 배운 교훈을 어떤 식으로 적용할지에 대한 우려를 자아내기에 충분하다고 할 수 있다.

일대일로 사업의 동맥으로 간주되는 6개 경제회랑의 전략적 의도에 대한 의문도 증가하고 있다. 중국이 역점을 기울이는 중국-파키스탄 회랑의 경우 가장 주목받는 사업이 과다르 항만 건설이다. 중국이 40년 간 운영권을 확보한 과다르 항구는 현재 방파제 건설 작업이 마무리된 상태이다. 의혹의 핵심은 파키스탄에서 가장 낙후된 지역 중 한 곳에 신축되는 과다르 항만이 파키스탄에 가져올 실질적인 경제 효과가 얼마나 될 지에서 비롯된다. 과다르 항구는 세계 원유 수송의 20%가 통과하는 호르무즈 해협에 인접해 있어 중국이 중동 산 원유를 과다르 항에서 환적해 중국-파키스탄 경제 회랑을 통해 운송할 경우 원유 수송 거리가 1만 2천km에서 2천 395km까지 단축될 것으로 기대된다. 이는 과다르 항구 건설의 이면에 안전하고 경제적인 원유 수송로를 확보하는 것과 함께 아시아 경쟁국 인도를 서쪽에서 견제할 수 있는 물질적 자원을 파키스탄에 안착시키

39) John Hurley, et al., *Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective* (Washington D. C.: Center for Global Development, 2018), pp.10-18.

려는 중국의 전략적 의도가 숨어있다는 근거로 작용한다.[40]

인도의 동쪽에 건설 중인 방글라데시-중국-인도-미얀마 회랑에 대한 참여국의 전략적 우려도 증가하고 있다. 중국이 이 회랑을 동남아시아 시장에서 경제적 장악력을 높이는 기반으로 활용할 뿐만 아니라 인도를 견제할 수 있는 또 다른 전략적 요충지로 사용할 것이라는 우려 때문이다. 실제로 방글라데시와 미얀마를 비롯해 인접국인 동남아시아 국가들의 경제력을 감안할 때 중국이 건설 중인 방글라데시-중국-인도-미얀마 회랑은 이 지역의 경제 발전에 기여하는 것보다 중국의 글로벌 전략을 위해 이용될 가능성이 농후하다.[41] 마찬가지로 중국이 중앙아시아 국가들과 추진 중인 21세기 실크로드 경제벨트도 경제적으로 상호 이익을 추구하는 경제적 목표보다 테러리즘, 분리주의, 급진주의로부터 중국의 안보를 지키려는 지정학적 목표가 우선한다는 논의가 중론을 형성하고 있다.[42]

중국이 동북아시아 지역에서 추진 중인 중국-몽고-러시아 경제회랑은 일대일로 프로젝트 중 동북아시아 지역을 기반으로 추진되는 유일한 회랑이다. 중국-몽고-러시아 회랑은 다른 회랑들에 비해 국가 안보로 인한 제약이 상대적으로 적은 지역에 위치하고 있지만 역내 중국의 영향력 증가를 우려하는 러시아와 미국, 중국, 러시아 사이에서 균형외교를 전개하는 몽고의 외교 전략으로 인해 회랑 건설에 필요한 인프라 확충에 아직 뚜렷한 진전을 보이지 못하고 있다.[43]

---

40) Jeremy Garlick, "Deconstructing the China-Pakistan Economic Corridor: Pipe Dreams Versus Geopolitical Realities," *Journal of Contemporary China*, Vol. 27, No. 112 (February 2018), pp.519-533. 중국의 일대일로 정책이 스리랑카와 파키스탄에 가져오는 부정적인 경제 효과에 대한 구체적인 실례를 알기 위해서는 다음 논문을 참조할 것. Abdur Rehman Shah, "China's Belt and Road Initiative: The Way to the Modern Silk Road and the Perils of Overdependence," *Asian Survey*, Vol. 59, No. 3 (May/June 2019), pp.407-428.

41) Mohd Aminul Karim, Islam Faria, "Bangladesh-China-India-Myanmar(BCIM) Economic Corridor: Challenges and Prospects," *Korean Journal of Defense Analysis*, Vol. 30, No. 2 (June 2018), pp.283-302.

42) Jeffrey Reeves, "China's Silk Road Economic Belt Initiative: Network and Influence Formation in Central Asia," *Journal of Contemporary China*, Vol. 27, No. 112 (February 2018), pp.502-518.

43) 이문기, "중-몽-러 경제회랑과 한국의 북방 경제협력 방향," 『현대중국연구』, 제19권, 제2호 (2017), pp.307-336.

이는 연관된 국가들의 직접적인 충돌로 이어질 수 있는 당면한 안보 쟁점의 부재에도 불구하고 중국의 일대일로가 국가 안보에 가져올 수 있는 장기적인 결과에 대한 주변국의 우려를 반증하는 것이라고 볼 수 있다.

중국 공산당은 19차 당대회에서 인류운명공동체론을 내세워 일대일로 연선 국가들뿐만 아니라 세계의 모든 구성원이 중국의 운명과 분리될 수 없으며 중국이 지향하는 목표는 인류공동체가 함께 공존 공영하는 기틀을 마련하는 것이라고 주장했다.[44] 이는 현재 중국이 추진하는 글로벌 전략의 사상적 기원이 위에서 언급된 천하질서에서 연원하고 있음을 암시하는 대목이다. 하지만 중국이 구사하는 수사학과 달리 일대일로가 추진된 지난 5년 동안의 결과는 중국 특색의 국제정치 개념과 국익과 안보를 최우선시하는 서구 국제정치이론의 현실주의 사이에 두드러진 차이점을 제시하지 못하고 있다. 이는 중국 특색의 국제정치이론이 지향하는 '이상적' 방향과 국익 추구를 목표로 하는 외교정책 사이에 존재하는 현실의 갈등으로부터 중국이 자유로울 수 없음을 방증하는 것이다.

4. 중국 특색 국제정치이론의 한계

중국 특색의 국제정치이론을 창출하기 위한 학자들의 노력에도 불구하고 현재까지 진전된 상황을 종합해 볼 때 중국 국제정치학계가 자국의 부상을 대변하는 한계를 넘어 국제정치 전반을 분석하고 예측할 수 있는 보편적 이론을 만들어내기까지는 아직 많은 시간이 걸릴 것으로 보인다. 중국 특색의 국제정치이론에 내재하고 있는 가장 큰 문제점은 인식론적 차원에서 중국 특색의 강조 자체가 이미 일반적이고 보편적인 이론의 창출을 가로막는 장애물로 작용하고 있다는 것이다. 어떤 특정한 시기에 출현했던 특수한 형태의 국제질서는 동일한 시기에 존재했던 국가 간 상호협력과 갈등 속에서 형성되기 마련인데 중국 특색의

44) 서정경, "시진핑 2기 정부의 외교 전망: 중국 공산당 19차 전국대표대회 정치 보고를 중심으로," 『국가전략』, 제24권, 제1호 (2018 봄), p.12.

국제정치이론은 중국 문화와 규범의 역할을 지나치게 강조한 결과 대부분의 연구들이 중국만을 독립변수로 상정하는 오류를 범하고 있다. 이는 사회과학이 지향해야 할 보편성과 일반성의 원칙에 충실하기보다 특정 지역이 지니고 있는 고유성과 특수성을 강조하는 '지역연구'에서 주로 나타나는 경향이다.[45]

또 다른 문제점은, 첫 번째 제기된 것과 연관된 것으로, 중국 특색의 국제정치이론이 중국 중심의 규범, 가치, 원칙을 강조한 결과 '환원론적 경향'을 보인다는 점이다. 국제정치이론이 성립되기 위해서는 다양한 행위자들의 의사결정에 영향을 미친 원인과 그 결과에 대한 분석이 체계적으로 수행되어야 하는데 중국 특색 국제정치이론과 관련된 대부분의 연구는 논의가 중국에서 시작해 중국으로 종결되는 경향을 나타내고 있다. 즉, 어떤 행위의 인과관계를 설명하기 위해서는 행위가 발생한 이전의 시점에서 내부적, 외부적 요인이 어떻게 상호작용을 했는지 또는 어떤 변인이 더 중요한 역할을 담당했는지에 대한 분석이 이루어져야 한다. 하지만 중국 특색을 강조하는 국제정치 연구들은 중국 특색이 국제정치 행위자 사이에서 잘 작동하면 긍정적인 결과가 발생하고 중국 특색이 제대로 작동하지 않으면 부정적인 결과가 나타난다는 식의 '이분법적' 주장을 펼치고 있다. 이런 흐름은 국제정치 행위나 국제질서를 촉진하는 과정에서 다른 행위자들이 수행한 역할을 경시하고 중국만을 중심에 놓고 사고하는 결과 발생하는 오류라고 할 수 있다.

중국 특색의 국제정치이론이 일반화되기 어려운 또 다른 이유는 객관적 사실을 바탕으로 논리체계를 형성하는 것이 아니라 중국 외교가 발생시키는 긍정적인 결과를 홍보하기 위한 목적의식이 연구 과정에 반영되어 있기 때문이다. 이는 다원성이 보장되지 않는 중국 정치체제의 특성상 학자들이 관방의 의견을 전달하는 역할에 머무는 정치적 현실에서 기인하고 있다. 실제로 일대일로와 관련

45) Harry Harding, "The Study of Chinese Politics: Toward a Third Generation of Scholarship," *World Politics*, Vol. 36, No. 2 (January 1984), pp.284-307; Lucian Pye, "The Confrontation between Discipline and Area Studies," in Lucian Pye, ed., *Political Science and Area Studies: Rivals or Partners?* (Bloomington: Indiana University Press, 1975), pp.3-22.

된 중국 연구들은 중국 정부의 정책을 무비판적으로 수용하거나 추상적인 언어로 낙관적인 청사진을 제시하는 경향을 보이고 있다. 반면 서구의 연구들은, 긍정적인 측면이든 부정적인 측면이든, 일대일로가 발생시킨 결과에 대한 원인을 분석하고 경험적 증거에 근거해 미래를 예측한다는 점에서 중국학자들과 차이점을 보이고 있다.

끝으로, 중국 국제정치학계가 중국 특색의 외교정책이나 국제정치행위를 입증시킬 만큼의 풍부한 논거와 실례들을 제시하는데 어려움을 겪고 있다는 점이다. 그 결과 전통적인 천하질서, 이를 뒷받침하는 사상으로서의 천하관, 현 중국 정부가 이미 국제정치 규범으로 안착된 레짐, 제도, 국제법을 준수하는지의 여부, 중국이 대외정책의 핵심으로 강조하는 불간섭원칙, 그리고 시진핑 정부가 주도하는 일대일로만이 중국 특색을 뒷받침하는 경험적 증거의 대부분으로 활용되고 있다는 점이다. 하지만 위의 사례들은 중국 고유의 사상, 현 국제 규범이 중국에 가하는 구속력, 국익을 우선시하는 당대 중국의 외교정책을 모자이크처럼 하나로 혼합한 모형물을 주조하는 작업에 불과하며 정작 중국적 가치와 특색이 어떻게 국제정치 동학의 원인으로 작동하는지를 밝히는 이론화 작업과는 거리가 있어 보인다.

위와 같은 결과가 발생하는 주된 원인은 중국 특색 국제정치이론의 필요성이 서구의 중국 때리기로부터 중국의 이익을 옹호해야한다는 정치적 요구와 깊이 관련됐기 때문이다. 달리 말하면, 서구 국제정치이론이 결과적으로 제2차 세계대전 이후 패권국으로 부상한 미국의 지배력을 정당화시키는 기능을 수행했던 것처럼 현 시기 중국 특색의 국제정치이론 개발 시도도 미국과 경쟁하는 중국의 현실적 고민에서 비롯됐음을 보여주는 것이다. 이는 중국의 부상이 국제질서에 가져올 도전과 이에 대한 응전이 현 시기 국제정치학계의 주요 쟁점임을 감안할 때, 중국위협론을 상쇄시킬 목적으로 특수한 역사적 경험만을 강조하는 중국 국제정치학계의 시도가 '이론'이 의미하는 진정한 학문적 결과를 달성할 수 있을지 의문을 자아내게 하는 대목이다.

5. 결 론

본 논문은 지금까지 중국 특색의 국제정치이론을 생성하기 위한 학계의 노력에 대한 비판적 고찰을 통해 새로운 시각의 국제정치이론의 출현 가능성과 제약 요소를 살펴봤다. 그 결과 중국 특색 국제정치이론의 필요성이 제기된 배경 자체가 중국의 부상과 국익 추구의 정당화라는 현실적 요구와 관련되어 있음을 발견했다. 이는 중국 특색의 국제정치이론을 창출하려는 노력이 서구의 지배적인 패러다임을 극복하기 위한 하나의 대안을 제시한다는 점에서는 신선하고 긍정적인 측면을 내포하고 있지만, 미국 중심의 국제정치이론이 서구적 가치와 서구식 방법론을 강조했던 것처럼, 중국 특색의 국제정치이론 또한 중국만의 가치와 사고를 강조하고 있다는 점에서 기존 학계의 동의와 지지를 확보하기까지 적지 않은 난관에 부딪힐 것임을 암시하는 부분이다.

최근 중국은 정치학이나 국제관계학뿐만 아니라 다른 사회과학 분야에서도 중국 특색을 강조하며 이런 연구를 지향하는 학자들에게 인센티브를 제공하는 모습을 보이고 있다.[46] 이는 중국이 국제사회의 주요 행위자로 등장하면서 쌓인 중국적 경험에 대한 자신감의 표출임과 동시에 중국 정부 차원에서 자국의 부상을 정당화하기 위한 학문적 작업을 동시다발적으로 진행하고 있음을 알게 하는 대목이다. 그럼에도 불구하고 중국의 이런 노력은 국제정치학계에서 절대적 우위를 점하고 있는 서구 주류학자들에게 환영받기 어려운 제약을 지니고 있다. 주된 이유는 서로 상이한 문화, 역사, 철학을 계승하고 있는 국가들에게 중국적 특색과 가치가 보편적으로 수용될 수 있을지에 대한 의문과 관련되어 있다. 이는 중국 특색을 강조하는 국제정치 학자들이 세계 정치 현상을 일관되게 설명할 수 있는 핵심 가설과 개념을 창출하지 못한다면 숲은 도외시한 채 나무만 강조하는 역설에 빠질 수 있음을 보여주는 것이다.

---

46) 2018년 8월 10일 연변에서 수행된 인터뷰. 인터뷰에 응한 복수의 연구자들이 익명으로 머무르길 선호해 실명을 밝히지 않았다.

결국 중국식 국제정치이론을 만드는 학자들이 해결해야 할 가장 큰 과제는 미국이 자국의 이익을 내세우고 미국이 주도하는 세계 질서를 정당화하기 위해 고안한 국제정치이론과 중국의 설명 방식이 실질적으로 어떤 점에서 차이를 보이는지를 입증하는 것이라고 할 수 있다.[47] 중국이 전개하고자 하는 논리가 이 함정을 극복하지 못해 학문적으로 가장 중요한 지지 세력이 되어야 할 주변국 학자들의 공감을 얻지 못한다면 결국 국제정치 학문이 강대국의 입장을 대변하는 역할을 수행한다는 비판을 넘어서지 못할 것이다.[48] 또한 로버트 콕스(Robert Cox)가 생전에 남긴 유명한 격언인 "이론은 항상 누군가의 목적을 위해 존재한다"는 것을 입증하는 또 하나의 사례로만 머물게 될 것이다.

한편 중국 특색의 국제정치이론을 창출하기 위한 시도는 한국 국제정치학계와 중국 연구자들에게 중요하고 임박한 두 가지 과제를 제시하고 있다. 첫째, 전근대시기 중국 특색 국제정치질서의 주요 사례로 가장 빈번하게 언급되는 것이 과거 한국과 중국이 오랜 기간 형성했던 조공체제라는 점이다. 중국 특색의 국제정치이론이 강조하는 중국의 전통적 세계관, 가치, 규범, 문화, 제도가 현실에서 가장 많이 구현된 곳이 과거 한국, 특히 조선시대의 정치 사회 구조였음은 주지의 사실이다. 문제는 동일한 문명권에 속한 두 나라 사이에 형성된 복잡다단한 외교사가 중국 특색 국제정치이론을 논의하는 과정에서 중국의 필요에 따라 일방적으로 해석되고 있다는 점이다. 이는 비록 과거 한국의 역사가 중국의 영향력으로부터 완전히 자유로울 수 없었다 할지라도 한국의 역사에서 조공체제와 한중관계를 둘러싸고 진행된 다양한 학문적 논의는 덮여진 채 중국의 규범과 제도에 일방적으로 편승했다는 역사적 왜곡이 국제정치학문 분야에서 고

47) 최근 발표된 카이 흐와 스티브 첸의 논문은 미중 간 패권경쟁을 바라보는 서구 이론과 중국 시각의 차이를 독특한 입장에서 설명하고 있다. 이들에 따르면 현 국제정치이론은 세력전이와 장주기이론을 통해 패권경쟁을 바라보지만 중국은 외부 환경에 반응하는 정치지도자의 생각이 미국과의 관계 설정에서 더 중요한 역할을 수행한다. Kai He, Steve Chan, "Thinking about Change: American Theorizing and Chinese Reasoning on World Politics," *International Studies Review*, Vol. 20, No. 2 (June 2018), pp.326-333.

48) Steven Smith, "The United States and the Discipline of International Relations: Hegemonic Country, Hegemonic Discipline," *International Studies Review*, Vol. 4, No. 2 (Summer 2002), pp.67-85.

착화 될 위험을 내포하고 있음을 의미한다. 국제정치학계에서 중국 편향 논의의 일방적 독주를 견제하기 위해서는 한국의 국제정치학자와 중국 연구자들이 중국 특색의 국제정치이론을 주장하는 무대에 적극적으로 뛰어들어 역사적 왜곡을 바로잡고 조공체제 등 과거 한중관계를 규정짓던 핵심 기제에 대해 한국의 다양한 입장을 전달할 필요성이 있다.[49]

둘째, 국제정치학계에서 이론이 지니고 있는 영향력과 관련된 부분이다. 현재 국제정치를 해석하고 예측하는 학문적 근거는 대부분 미국에서 고안된 이론적 프레임에 기초하고 있다. 이는 현 시기 주류 국제정치이론이 미국 정부가 추진하는 외교정책에 대한 정당성과 당위성을 뒷받침하는 근거로 작용하고 있음을 의미한다. 학문적 엄밀성에서 아직 중국 특색 국제정치이론이 서구의 학계를 따라잡는 것이 요원해 보인다 할지라도, 국제정치이론 자체가 강대국의 이익을 반영하고 있다는 점을 고려할 때, 중국 특색의 국제정치이론이 출현하게 된 배경을 간과하는 우를 범하지 말아야 할 것이다. 일단 중국 정부와 학계가 전략적 목표를 지니고 조직적으로 추진해온 중국 특색 국제정치이론이 국제정치학계에서 수용된다면 이 과정에서 홀대되고, 스스로를 소외시켜 온 한국의 학계가 뒤늦게 새로운 목소리를 첨가하는 데는 근본적인 한계가 있을 것이다.

비록 중국 중심의 국제정치이론을 창설하는 과정이 녹록하지 않더라도 이런 과정에 도전하는 자체가 적지 않은 서구 학자들에게 새로운 학문적 동기를 부여하고 있는 것이 현실이다. 그리고 중국의 영향력이 정치, 경제, 외교, 군사에만 국한되지 않고 학문 분야에서도 지속적으로 증가하는 것을 감안할 때 앞으로 중국 학계와 서구 학계의 협업은 더욱 강화될 것으로 예상된다. 이는 중국 특색의 국제정치이론이 현재 당면하고 있는 한계와 제약을 극복하고 더욱 탄력 있게 발전할 가능성을 예고하는 부분이기도 하다. 이 과정에서 한국 학계가 적극적인

49) 한중 관계에서 중국이 자국의 이익을 위해 역사를 왜곡한 대표적인 사례로 동북공정을 들 수 있다. 하지만 동북공정이 한중 두 나라 간의 역사적 사실을 곡해함으로써 한국인의 정치적, 역사적, 민족적 감정을 자극했다 할지라도 국제 사회에서 한국의 이익에 직접적인 침해를 가져오지는 않았다. 이와 달리 중국의 전략적 의도가 반영된 중국 특색 국제정치이론이 공고화되면 이는 국제정치무대와 학계에서 한국의 위상과 이익에 직접적이고 장기적인 피해를 불러일으킬 것이다.

참여를 통해 한국의 입장과 논리를 명확히 제시하지 않는다면 중국 학문의 영향력에서 자유롭지 못했던 선대의 경험과 미국 학문에 얽매여 있는 당대의 경험을 멀지 않은 미래에 재부상한 중국을 통해 다시 경험할지도 모른다.

참고문헌

1. 단행본

이정남. “민주주의에 대한 중국의 인식: 비교 역사적 관점을 중심으로.” 이정남 편.『민주주의와 중국』. 서울: 고려대 아연출판부, 2012.

자오팅양 저. 노승현 역.『천하체계』. 서울: 길, 2010.

판웨이 저. 김갑수 역.『중국이라는 새로운 국가모델론』. 서울: 에버리치홀딩스, 2010.

Bell, Daniel. “Realizing Tianxia: Traditional Values and China’s Foreign Policy.” in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics*. Durham: Duke University Press, 2017.

Buzan, Barry and Ole Wæver. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2004.

Chang, Chishen and Kuan-Hsing Chen. “Tracking Tianxia: On Intellectual Self-Positioning.” in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics*. Durham: Duke University Press, 2017.

Duara, Prasenjit. “The Chinese World Order and Planetary Sustainability.” in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics*. Durham: Duke University Press, 2017.

Fairbank, John K., ed. *The Chinese World Order: Traditional China’s Foreign Relations*. Cambridge: Harvard University Press, 1968.

Green, Donald and Ian Shapiro. *Pathologies of Rational Choice Theory:*

A Critique of Applications in Political Science. New Heaven: Yale University Press, 1996.

Hurley, John. et al. *Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective.* Washington D. C.: Center for Global Development, 2018.

Kang, David. *East Asia before the West: Five Centuries of Trade and Tribute.* New York: Columbia University Press, 2010.

Keohane, Robert. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton: Princeton University Press, 1984.

Lin, Chun. "China's Lost World of Internationalism." in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics.* Durham: Duke University Press, 2017.

Mearsheimer, John. *The Tragedy of Great Power Politics.* New York: Norton & Company, 2014.

North, Douglass. *Institutions, Institutional Change and Economic Performance.* New York: Cambridge University Press, 1990.

Pye, Lucian. "The Confrontation between Discipline and Area Studies." in Pye Lucian. ed., *Political Science and Area Studies: Rivals or Partners?* Bloomington: Indiana University Press, 1975.

Russett, Bruce. *Grasping the Democratic Peace: Principles for a Post-Cold War World.* Princeton: Princeton University Press, 1993.

Wang, Ban. "The Moral Vision of Kang Youwei's Book of the Great Community." in Ban Wang, ed., *Chinese Visions of World Order: Tianxia, Culture and World Politics.* Durham: Duke University Press, 2017.

Womack, Brantly. *China and Vietnam: The Politics of Asymmetry.* New York: Cambridge University Press, 2006.

Yan, Xuetong. *Ancient Chinese Thought, Modern Chinese Power.* Princeton: Princeton University Press, 2011.

Zhang, Feng. *Chinese Hegemony: Grand Strategies and International Institutions in East Asian History.* Stanford: Stanford University Press, 2015.

2. 논문

서정경. "미·중 민족주의의 특성과 양국 관계: 메시아니즘과 천자관의 조우." 『국가전략』, 제19권, 제3호 (2013 가을).

서정경. "시진핑 2기 정부의 외교 전망: 중국 공산당 19차 전국대표대회 정치보고를 중심으로." 『국가전략』, 제24권, 제1호 (2018 봄), pp.5-33.

이문기. "중-몽-러 경제회랑과 한국의 북방 경제협력 방향." 『현대중국연구』, 제19권, 제2호 (2017), pp.307-336.

李向阳. "构建 '一带一路'需要优先处理的关系." 『国际经济评论』, 제1호 (2015), pp.54-64.

王义桅. 郑栋. "'替代一路'战略的道德风险与应对措施." 『东北亚论坛』, 제4호 (2015), pp.39-48.

杨思灵. "'一带一路'倡议下中国与沿线国家关系治理及桃战." 『南亚研究』, 제2호 (2015), pp.15-34.

Acharya, Amitav and Barry Buzan. "Why Is There No Non-western International Relations Theory? An Introduction." *International Relations of the Asia-Pacific*, Vol. 7, No. 3 (September 2007), pp.287-312.

Callahan, William. "China and the Globalisation of IR Theory:

Discussion of 'Building International Relations Theory with Chinese Characteristics'." *Journal of Contemporary China*, Vol. 10, No. 26 (August 2001), pp.75-88.

Callahan, William. "Sino-speak: Chinese Exceptionalism and the Politics of History." *Journal of Asian Studies*, Vol. 71, No. 1 (February 2012), pp.1-23.

Crammer-Byng, John. "The Chinese View of Their Place in the World: An Historical Perspective." *China Quarterly*, No. 53 (January/March 1973), pp.67-79.

Garlick, Jeremy. "Deconstructing the China-Pakistan Economic Corridor: Pipe Dreams Versus Geopolitical Realities." *Journal of Contemporary China*, Vol. 27, No. 112 (February 2018), pp.519-533.

Ham, Myungsik and Elaine Tolentino. "Socialisation of China's Soft Power: Building Friendship through Potential Leaders." *China: An International Journal*, Vol. 16, No. 1 (February 2018), pp.45-68.

Harding, Harry. "The Study of Chinese Politics: Toward a Third Generation of Scholarship." *World Politics*, Vol. 36, No. 2 (January 1984), pp.284-307.

Ikenberry, John and Charles Kupchan. "Socialization and Hegemonic Power." *International Organization*, Vol. 44, No. 3 (Summer 1990), pp.283-316.

Kai, He and Steve Chan. "Thinking about Change: American Theorizing and Chinese Reasoning on World Politics." *International Studies Review*, Vol. 20, No. 2 (June 2018), pp.326-333.

Kang, David. "Getting Asia Wrong: The Need for New Analytical Frameworks." *International Security*, Vol. 27, No. 4 (Spring 2003), pp.57-85.

Karim, Mohd Aminul and Faria Islam. “Bangladesh–China–India–Myanmar(BCIM) Economic Corridor: Challenges and Prospects.” *Korean Journal of Defense Analysis*, Vol. 30, No. 2 (June 2018), pp.283–302.

Kennedy, Scott. “The Myth of the Beijing Consensus.” *Journal of Contemporary China*, Vol. 19, No. 65 (April 2010), pp.461–477.

Kivimaki, Timo. “Soft Power and Global Governance with Chinese Characteristics.” *Chinese Journal of International Politics*, Vol. 7, No. 4, (Winter 2014), pp.421–447.

Krasner, Stephen. “Organized Hypocrisy in Nineteenth–Century East Asia.” *International Relations of the Asia–Pacific*, Vol. 1, No. 2 (August 2001), pp.173–197.

Mancall, Mark. “The Persistency of Tradition in Chinese Foreign Policy.” *Annals of the American Academy of Political and Social Science*, Vol. 349 (September 1963), pp.14–26.

Mansfield, Edward and Helen Milner. “Why Democracies Cooperate More.” *International Organization*, Vol. 56, No. 3 (Summer 2002), pp.477–513.

Qin, Yaqing. “Why Is There No Chinese International Relations Theory?” *International Relations of the Asia–Pacific*, Vol. 7, No. 3 (September 2007), pp.313–340.

Reeves, Jeffrey. “China’s Silk Road Economic Belt Initiative: Network and Influence Formation in Central Asia.” *Journal of Contemporary China*, Vol. 27, No. 112 (February 2018), pp.502–518.

Shah, Rehman Abdur. “China’s Belt and Road Initiative: The Way to the Modern Silk Road and the Perils of Overdependence.” *Asian Survey*, Vol. 59, No. 3 (May/June 2019), pp.407–428.

Smith, Steven. “The United States and the Discipline of International

Relations: Hegemonic Country, Hegemonic Discipline." *International Studies Review*, Vol. 4, No. 2 (Summer 2002), pp.67-85.

Snidal, Duncan. "The Limits of Hegemonic Stability Theory." *International Organization*, Vol. 39, No. 4 (Autumn 1985), pp.579-614.

Song, Nianshen. "'Tributary' from a Multilateral and Multilayered Perspective." *Chinese Journal of International Politics*, Vol. 5, No. 2 (Summer 2012), pp.155-182.

Song, Xinning. "Building International Relations Theory with Chinese Characteristics."*Journal of Contemporary China*, Vol. 10, No. 26 (August 2001), pp.61-74.

Wang, Jiangli and Barry Buzan. "The English and Chinese Schools of International Relations: Comparisons and Lessons." *Chinese Journal of International Politics*, Vol. 7, No. 1 (Spring 2014), pp.1-46.

Wendt, Alexander. "The Agent-Structure Problem in International Relations." *International Organization*, Vol. 41, No. 3 (Summer 1987), pp.335-370.

Wendt, Alexander. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization*, Vol. 46, No. 2 (Spring 1992), pp.391-425.

Wohlforth, William. "The Stability of a Unipolar World." *International Security*, Vol. 24, No. 1 (July 1999), pp.5-41.

Womack, Brantly. "Asymmetry and China's Tributary System." *Chinese Journal of International Politics*, Vol. 5, No. 1 (Spring 2012), pp.37-54.

Zhang, Yongjin and Barry Buzan. "The Tributary System as International Society in Theory and Practice." *Chinese Journal of International Politics*, Vol. 5, No. 1 (Spring 2012), pp.3-36.

Zhao, Suisheng. “The China Model: Can It Replace the Western Model of Modernization?” *Journal of Contemporary China*, Vol. 19, No. 65 (April 2010), pp.419-436.

Zhou, Fangyin. “Equilibrium Analysis of the Tributary System.” *Chinese Journal of International Politics*, Vol. 4, No. 2 (Summer 2011), pp.147-178.

3. 인터넷자료

光明日报. “构建中国特色话语体系 增强国际影响力话语权: 深入学习习近平总书记系列重要讲话精神笔谈,” http://theory.people.com.cn/n/2015/1114/c40531-27815447.html (검색일: 2018. 9. 7)

Hillman, Jonathan. “China’s Belt and Road Initiative: Five Years Later,” https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later-0(검색일: 2018. 7. 15)

Qiushi, http://english.qstheory.cn/politics/201109/t20110924_112513.htm (검색일: 2019. 3. 2)

Xinhua News. “Hu Jintao Calls for Enhancing ‘Soft Power’ of Chinese Culture,” http://news.xinhuanet.com/english/2007-10/15/content_6883748.htm(검색일: 2018. 9. 1)

https://news.joins.com/article/22953849(검색일: 2018. 9. 1)

http://www.cnki.com.cn/index.htm(검색일: 2018. 7. 26)

Abstract

The Rise and Future Prospect of 'International Relations Theories with Chinese Characteristics'

Ham, Myungsik (Jilin University)

Contemporary dominant international relations theories consider the rise of China a threat to current international order. As a response, China has struggled to create new "international relations theories with Chinese characteristics". The primary goal of the project is to reduce the China threat concern and to provide legitimacy to its emergence. This article attempts to explore why China needs China-centered international relations theories, how it has developed the theories, and what features they include. In addition, the paper investigates the feasibility of the theory by finding out a linkage between Chinese foreign policy in practice and its substantial implications for Chinese efforts to construct new theories. Findings are as follows: first, Chinese foreign policy has been more aggressive, showing that the prediction of realism is more likely; and second, Chinese theory-building process and foreign policy in practice are conflicting and it provides a hard task for Chinese academia to construct international relations theories with Chinese characteristics.

Key Words: China, International Relations Theories with Chinese Characteristics, Western International Relations Theories, All under Heaven, Belt and Road Initiative

투고일: 2019.05.09 심사일: 2019.05.31 게재확정일: 2019.06.05.

Ⅳ

트럼프 정부의 2017 대북 선제공격 위협의 실효성 평가

: 미국의 과거 선제공격 사례 시사점을 중심으로

박창권 (한국국방연구원)

1. 머리말
2. 미국의 선제공격 고려시 주요 고려요소 및 조치사항
3. 미국의 선제공격 사례
4. 미국의 선제공격 사례의 주요 특성과 시사점
5. 트럼프 정부의 대북 선제공격 위협의 실효성 평가
6. 결 론

Summary

트럼프 대통령은 2017년 북한의 핵 개발을 포기시키기 위해 선제공격을 실제 이행할 가능성이 매우 높아 보였다. 트럼프 대통령은 북한에 대해 최대의 압박정책과 병행하여 가시적인 선제공격 위협을 고조시켰다. 트럼프 대통령과 김정은 위원장 간의 '말의 전쟁'과 한반도 주변에 대한 군사력 증강, 코피작전에 대한 보도 등이 연이어졌다. 최근 브룩스 전임 주한미군사령관은 미국이 2017년 실제로 군사옵션을 고려하였다고 밝혔다. 그럼에도 불구하고 이러한 미국의 선제공격 위협은 실제로 가능성이 높았는지, 그리고 북한이 이를 위협으로 인식하였는지는 불분명하다. 사실 북한은 미국의 군사공격이 실제 이행될 수 있다는 두려움을 보이지 않았고 트럼프 대통령의 위협에 호전적으로 대응하였다. 미국의 대북 군사공격에 가장 심각한 악영향을 받을 수 있는 한국 역시 비록 불안한 사회적 분위기는 있었으나 경제 등 제반 분야에서 위기의식은 높게 나타나지 않았었다. 본 연구는 트럼프 대통령의 선제공격 위협이 실제적으로 효과가 있었던 위협이었는가를 정성적으로 평가하고자 한다. 미국이 군사공격을 결정하고 이행할 때 고려하는 정치적, 군사적 요소들과 미국이 베트남전 이후 이행하였던 군사공격 사례의 시사점들을 기반으로 평가하였다. 본 논문은 트럼프 대통령의 선제공격 위협이 비록 목소리는 높았으나 실제로 이행될 가능성은 높지 않았으며, 결과적으로 북한에 대한 위협으로도 크게 작용하지 않았다고 주장한다.

| **주제어** | 트럼프, 선제공격, 미국의 군사공격, 북한

1. 머리말

트럼프 대통령은 2016-2017년 기간 중 북한의 핵 포기를 강요하기 위해 최대의 압박정책을 이행함과 동시에 선제공격 위협을 노골적으로 강화하여 한반도에 위기를 조성하였다. 미 주요 언론은 트럼프 정부가 북한에 몽둥이질을 하고 치욕을 주기 위한 '코피작전'을 계획하고 있음을 보도하였다.[1] 트럼프 대통령-김정은 위원장 간 벌어진 과격하고 호전적인 '말의 전쟁'은 이러한 군사작전 가능성을 보다 높여 주었었다. 2018년 1월 CIA 폼페이오 국장은 트럼프 대통령에게 북한에 대한 제한적 공격의 위험과 기회들을 브리핑하고 옵션을 제시하고 있다고 언급하였다.[2] 한반도 군사적 긴장은 한국이 2018 평창 동계 올림픽-평화올림픽을 성공적으로 개최하고 남북 및 북미 정상회담이 연이어 개최되면서 사라졌다. 그럼에도 불구하고 미국은 수시로 북한의 핵개발과 핵위협에 대해 항상 군사적 옵션이 책상위에 놓여있다는 사실을 분명히 하고 있다.

군사력은 정치적 목적을 달성하기 위한 폭력적 수단으로 외교적 수단이 작동하지 않을 때 최종적으로 이를 사용할 것을 위협한다. 통상 외교적 수단으로 군사력 시위는 다양한 방법이 있다. 간접적인 방식으로 수사적 위협이 없이 군사연습과 훈련, 군사력의 이동배치 등을 할 수 있으며, 군사력 시위와 함께 직접적인 군사공격 위협을 할 수 있다. 또한 군사공격은 직접적인 수사적 위협이나 군사력 시위 없이 기습적으로 이행될 수도 있다. 2016-2017 미국의 행동은 군사위협의 관점에서 볼 경우, 가장 높은 수준의 위협적인 행동이었다. 트럼프 대통령이 북한에 대해 '화염과 분노'를 언급하는 등 위협 메시지도 강력하였다, 그

1) '코피작전'은 북한의 특정시설에 대한 일회적성 타격작전으로 김정은의 관심과 두려움을 이끌어 협상장으로 이끌기 위한 작전으로, 그리고 The Telegraph는 코피작전으로 사이버 공격을 계획하였다고 보도하였다. Washington Examiner, "The 'bloody nose' option is a direct path to war with North Korea," 15 Jan. 2018. The Telegraph, "US preparing 'bloody nose' cyber attacks on North Korea, 20 Feb. 2018. Business Insider, "The US is reportedly considering a 'bloody nose' attack to humiliate North Korea-here's how it could go down," 9 Jan. 2018.

2) Daily Beast, "CIA Boss Gives Latest Indication Trump May Consider Preemptive Strike on North Korea," 23 Jan. 2019.

럼에도 불구하고 한반도에서 느끼는 실질적인 체감온도는 차이가 있었다. 미국의 선제공격 위협은 북한이 2018년 비핵화 협상에 나서는데 영향을 미쳤을 것으로 판단되지만 그 영향의 정도는 불분명하였다.

본고는 2017년 트럼프 정부의 대북 선제공격 위협이 실제로 실효성이 있었는가하는 질문에 대한 평가를 실시한다.[3] 미국의 군사력 사용은 이에 대한 정치·군사적인 명분과 정당성, 목표의 달성 가능성, 군사적인 준비능력 등을 중시하여 정책적 결정을 한다. 미국의 일반적인 정책결정은 이러한 제반 요소들을 검토하고 일련의 사전 행동들을 통해 이러한 상황을 만족할 수준으로 유리하게 상황을 조성한 이후에 군사공격을 결정한다. 따라서 본고는 미국이 군사력의 직접적인 사용을 위해 고려하는 주요 요소들을 분석하여 미국의 군사공격 가능성이 높았는지를 평가한다. 이는 트럼프 대통령의 북한에 대한 선제공격 위협이 실제적인 강압을 위해 효과를 가졌는지를 알 수 있도록 할 것이다. 또한 미국이 월남전 이후 실시하였던 주요 선제공격 사례를 분석하여 북한 상황과 비교하여 평가해 보고자 한다.

2. 미국의 선제공격 계획 시 주요 고려요소 및 조치사항

가. 선제공격에 대한 정당성과 명분 확보를 위한 주요 고려요소

미국의 대외정책은 미국 예외주의와 기독교 이념에 기반을 둔 도덕적 정당성을 중시한다. 부시 대통령의 이라크 전쟁이 대내외적으로 많은 비판을 받았던

3) 트럼프 정부의 선제공격 위협은 국제법적 개념으로는 선제공격이기보다는 예방공격에 속한다는 많은 주장이 있지만 여기서는 미국에서 실제로 직접 언급되었던 용어를 사용하고자 한다. 선제공격은 적이 공격을 할 것이라는 믿음 속에서 적의 공격을 허용하기보다는 먼저 타격을 하는 것이다. 예방공격은 적의 공격이 임박하여 공격하는 것이 아니라 나중에 전쟁을 하는 것보다는 빨리 전쟁을 하는 것이 좋다는 욕구에서 전쟁을 시작하는 것이다. 국제법적으로 선제공격은 자위를 위한 군사력 사용을 허용하고 있지만 예방공격은 허용되지 않고 있다. Muller, Karl P. and others, *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*(RAND, 2006), pp.xi-xii, 6-15.

주요한 이유도 정의의 전쟁 개념에 부합하지 않았다는데 있었다. 부틀러는 1945-1994년 간 미국의 해외 군사개입 사례를 개량적으로 분석해 본 결과 정의의 전쟁 원칙이 항시 미국의 대외 군사개입 결정에 중요한 영향을 미쳤음을 확인하고 있다. 미국은 냉전기 공산주의 세력의 팽창을 봉쇄하기 위해 다양한 형태의 군사개입과 전쟁을 실시하였으며, 이는 정의의 전쟁개념에는 미흡한 측면이 있었다. 그렇지만 이러한 군사 개입과 전쟁의 경우에도 정의의 전쟁이라는 믿음과 설명 하에서 행동을 결정하였다.[4] 미국은 21세기 들어 국제법, 규범에 기반을 둔 국제질서의 유지를 대외전략의 핵심기조로 설정하였다. 트럼프 정부는 '힘을 통한 평화보존'을 국가안보전략의 핵심기조로 설정하고 있다.[5] 또한 트럼프 대통령은 자신의 저서 '협상의 기술'에서 협상을 위한 원칙으로 자신의 선택방안을 최대화하고 레버리지를 적극 사용할 것을 주장하고 있다.[6] 트럼프 정부의 이러한 정책기조와 협상전략도 국제적 규범에 기반을 둔 정당성과 명분을 중시하지 않을 수 없으며, 이는 군사공격을 선택시 핵심적인 정치적 고려사항이 될 수밖에 없다,

주권국가는 자국의 영토방위를 위해 외부의 침략에 대응하기 위해 전쟁과 군사행동을 취할 당연한 권리를 갖고 있다. 주권국가 체제를 출범시키고 주권국가의 국내문제에 대한 외부세력의 개입을 금지하였던 웨스트팔리아 체제는 현대 국제법과 국제관계의 핵심적인 근간을 이루고 있다. 이러한 국제질서 체계 하에서 자국을 침공하지 않은 다른 주권국가를 선제공격하기 위해서는 이에 대한 정당성을 보편타당하게 인정받기 위한 합리적인 이유가 필요하다. 미국은 대외 군사개입, 특히 선제공격을 이행할 경우에는 이에 대한 도덕적 정당성과 명분, 국제

---

4) Buttler, Michael J. "U.S. Military Intervention in Crisis, 1945-1994: An Empirical Inquiry of Just War Theory," *The Journal of Conflict Resolution*, Vol. 47, No.2(Apr. 2003), pp.226-248.

5) The President of the United States, National Security Strategy of the United States of America, December 2017, pp.25-26. http://www.whitehouse.gov/…/NSS-Final-12-18-2017-0905.pdf(검색일: 2019. 3. 2). KIDA, 「NSS 2017: KIDA의 분석과 NSS 요약」(서울: KIDA, 2017), pp.39-40.

6) Trump, Donald J. and Tony Schwartz, *Trump: The Art of The Deal*(New York: Ballantine Books, 1987), pp.50-54.

법적 합법성을 주요한 가치로 중시하고 이를 위한 노력을 적극 기울이고 있다.

일반적으로 군사공격의 합법성(*Jus ad bellum*)과 관련한 정당성을 확보하기 위해서는 다음과 같은 여섯 가지 조건들을 갖추어 설득력을 보여주어야 한다.[7] 첫째, 합법적(정당한) 권위(legitimate authority)를 갖고 있는 주체가 선제공격 또는 전쟁을 결정하고 이행해야 한다. 미국은 1973년 베트남 전쟁 이후 대통령의 일방적인 대외 군사개입을 방지하기 위한 '전쟁권한법'(War Powers Acts of 1973)을 제정하여 대통령이 의회의 승인이 없이 해외에서 전쟁을 수행할 수 있는 기간을 60일로 정했으며, 이를 최대 30일 연장할 수 있도록 한정하였다. 또한 9.11테러 이후 '대테러 무력사용권(AUMF: Authorization for Use of Military Force)'을 제정하여 대통령이 국제테러리즘과 관련된 집단에게 무력을 사용할 수 있는 권한을 사전에 부여하였다.[8]

둘째, 국가나 국제기구의 최고 책임자가 전쟁을 선택하겠다는 공개적인 최후통첩을 선언하고, 이와 동시에 분쟁을 피하거나 종식시키기 위한 조건들을 제시하여 전쟁을 방지하기 위한 노력을 보여주는 것이다. 군사력 사용에 대한 의도를 공개적으로 선언하여 상대가 이를 명확하게 인식토록 하여 군사행동 이전에 상대에게 이를 회피할 수 있는 최종적인 선택방안을 제안하는 것을 중시한다.

셋째, 군사공격을 정당화할 수 있는 정당한 의도(just intent)이다. 전쟁으로 가기위한 정의로운 의도와 이유에 대한 일반적인 원칙은 현상 복구, 그리고 전쟁이 발생하지 않았을 당시의 국제관계 상황으로 되돌리기 위한 행동이다. 또 다른 정의로운 이유로는 어떤 잘못된 행동을 바로잡는 것, 사악한 행동을 처벌하는 것, 잘못된 공격에 대응하여 방어하는 행동이다. 냉전기 미국은 공산주의 정권의 확산 및 출현을 봉쇄하기 위해 군사개입을 실시하였다. 탈냉전기 들어 미국은 군사개입과 선제공격의 정당성을 인권유린과 같은 인도적 위기상황에

---

7) Wester, Franklin Eric, "Preemption and Just War: Considering the Case of Iraq," *Parameters*(Winter 2004-05), pp.20-33.

8) One Hundred Eventh Congress of the United States of America, "Text of S.J.Res. 23. (107th): Authorization for Use of Military Force, http://www.govtrack.us/congress/bills/107/sjres23/text(검색일: 2019. 3. 4)

대한 대응, 테러리즘 지원에 대한 처벌, 대량살상무기 개발・사용・확산 방지를 이유로 들고 있다..[9] 그러나 인권문제는 해석에 따라 차이를 갖는 국내 정치적 요인이 많이 작용하는 이슈이다. 따라서 이는 WMD와 테러지원 이슈보다는 선제공격의 명분으로는 정당성이 낮다.

넷째, 군사력 사용에 대한 자제와 정밀성을 요구하는 비례성(proportionality) 원칙이다. 전쟁은 인적, 경제적 비용을 사전에 예측하기가 매우 어렵다. 따라서 군사력의 사용은 군사력의 효과와 결과가 이해될 수 있는 수준이어야만 정당성을 인정받을 수 있다. 그러나 상대가 대량살상무기 사용을 위협할 경우, 이는 자신의 국민과 문명의 파멸과 같은 최악의 피해를 초래할 수 있는 상황이다. 따라서 WMD 위협에 대해서는 비례성의 범위와 수준을 임의로 확장하여 자신의 행동을 정당화하는 문제를 안고 있다.

다섯째, 선제공격은 원인제거를 위한 다른 수단이 모두 소진되었을 경우에 선택할 수 있는 최종 수단(last resort)이어야 한다. 즉, 전쟁이외의 다른 방법이 사전에 취해져야 한다는 것을 의미한다. 이는 분쟁을 피하고 해결하기 위한 다른 좋은 방법들이 실패한 이후 슬픈 일이지만 어쩔 수 없이 군사력 사용을 선택할 수밖에 없었다는 필요성을 명확히 하는 것이다. 그러나 모든 합리적인 옵션을 군사공격을 개시하기 이전에 사용해 보았는지에 대한 평가는 매우 주관적인 것이기 때문에 관련국들을 설득하고 이해시키는데 문제가 될 수 있다.

여섯째, 승리 가능성에 대한 합리적 근거가 뒷받침되어야 한다. 이는 승리의 기회가 없는 상황에서 무모하게 군사력을 사용하는 것을 방지하고자 한다. 군사행동은 지도자들이 전쟁 원인을 해결할 수 있다는 희망을 갖고 수많은 군인과 무고한 시민들을 죽음으로 내모는 도덕적으로 중대한 결정이다. 비례성 원칙은 국가 지도부가 무모하게 한 국가를 전쟁으로 이끌고 갈 수 있는 상황에서 군인과 국가를 보호하는 장치이다. 이는 문제해결 또는 현상복구가 가능하다는 기대를 할 수 있는 군사력 사용만이 윤리적일 수 있으며, 성공의 희망이 없는 복수나

9) Himes, Kenneth R.. “Intervention, Just War, and U.S. National Security,” *Theological Studies*, Vol. 65, Iss. 1(February 2004), pp.141-157.

자살적 행동과 같은 군사행동은 도덕적인 선택이 될 수 없다는 것을 의미한다.

선제공격의 국제법적 합법성은 선제공격을 국제법적 용어로 설명하는 선제적 자위(anticipatory self-defense)에서 찾고 있다. 선제적 자위는 국제법과 정의의 전쟁에서 정당한 이유로서 인정되고 있다. 그러나 선제적 자위를 위한 군사행동은 이를 정당화하기 위한 구체적인 기준에 부합하는 가의 문제에 대한 답을 요구하고 있다. 선제적 자위 행동을 정당화하는 구체적 기준은 위협의 심각성(the severity of the threat), 위협이 실제화 될 가능성(the degree of probability of the threat), 위협의 임박성(the imminence of the threat), 그리고 행동지연에 따른 비용(the cost of delay)이다.[10] 예를 들면, 북한의 경우, 북한이 핵무기를 짧은 기간 내에 확보하여 미국을 직접 위협할 가능성이 높으며, 이러한 위협이 발생할 가능성이 확실하고 임박하다는 사실을 설명할 수 있어야 한다. 나아가 지금 당장 군사행동을 취하지 않을 경우 향후 북한의 핵위협이 관리하기 어려울 정도로 커진다는 사실을 설득할 수 있어야 한다.

군사공격에 대한 정당성 및 명분과 관련된 요구 조건은 트럼프 정부가 북한에 대한 군사적 옵션을 선택하기가 어렵다는 사실을 말해준다. 위에서 명시된 정당성 및 명분과 관련된 조건들은 자신에 유리하게 주관적인 해석을 할 수 있는 내용들을 많은 부분 포함하고 있다. 그럼에도 불구하고 유엔이나 미 의회, 그리고 우방국 등의 지원을 확보하고, 군사공격을 통해서 원하는 목적을 달성할 수 있으며, 비용과 피해를 최소화 할 수 있어야 하며, 군사공격 이후의 후속적인 결과나 영향을 관리할 수 있어야 한다. 미국이 아프간전 및 이라크전을 시작으로 수행하였던 대테러전은 초기의 군사작전 성공에도 불구하고 현재까지 전쟁이 지속되고 있는 상황이며, 예상하지 못하였던 천문학적인 비용과 희생을 초래하는 결과를 야기하였다. 이는 미국 사회가 결과를 예단하기 어려운 군사작전에 소극적이거나 반대할 가능성이 높을 것임을 말해준다.

---

10) Wester, 앞의 글, pp.33-36.

나. 군사공격작전 계획을 위한 기본적인 준비 및 조치사항

군사공격은 정치적 목적을 달성하기 위한 확실하고 충분한 군사적 능력이 준비되었을 때 이행될 수 있다. 따라서 군사공격을 이행하기 위해서는 사전에 군사작전을 계획하고 준비하여, 이행하기 위한 일련의 행동들을 요구한다. 이러한 군사적 움직임은 보안을 유지하기 위해 폐쇄적인 방식으로 추진된다. 그렇지만 군사공격을 준비하는 참모와 부대들은 군사작전을 계획하고 수행하기 위해 군사교리 등에서 요구하는 일련의 정해진 일반화된 군사적 절차에 따라 준비조치를 철저이 이행하여 군사작전의 성공을 담보할 수 있도록 해야 한다. 이는 다양한 형태의 군사적 행동을 포함하기 때문에 대내외적으로 드러날 수밖에 없다.

또한 대북 선제공격 위협이 북한의 핵개발 중단 등을 요구하기 위한 정치적 강압을 목적으로 한 행동이라면 이에 대한 신뢰성을 증대하고 북한에게 미국의 의도를 정확히 커뮤니케이션하기 위한 가시적인 군사조치들이 요구된다. 즉, 미국의 의도와 능력을 북한이 사전에 인지하고 이에 정치적으로 대응할 수 있도록 요구하는 가시적 군사행동이 이루어진다는 것을 의미한다. 물론 군사적 기습작전은 이를 비밀리에 준비하여 사전 경보가 없이 이루어지기 때문에 정치적 강압을 목적으로 한 선제공격의 위협과는 차이가 있다.

미국은 군사작전을 계획하는 경우에는 다음과 같은 요인과 절차들을 중시한다.[11] 첫째, 군사공격의 목표 및 상대와 관련된 문제와 상황을 식별하며, 이와 관련된 환경을 이해하고 파악한다. 이를 위해서는 안보에 대한 위협의 심각성, 대통령 및 지휘관의 의도와 전략적 목표, 표적의 물리적・기후적・인구적/사회・문화적/정치・경제・사회적 요소, 기반시설, 교전규칙 등 작전의 제한점, 작전과 관련된 심리적 요소 등 다양한 이슈들을 검토하고 준비한다.

둘째, 군사공격의 목표(ends)-방법(ways)-수단(means)-위험(risk)을 반영하여 작전계획을 수립한다. 작전계획은 군사작전에 의해 달성 가능한 목표와 민

11) The U.S. Joint Chief of Staff, *Joint Planning: Joint Publication 5-0*. Washington. DC. 16 June 2017.

간차원의 행동 조치들과 연계한 군사작전의 행동 순서, 그리고 목표의 달성을 어떻게 평가하고 측정할 것인가를 명확히 설정한다. 임무를 완수하기 위해 요구되는 자원과 동원 가능한 자원을 평가하며, 군사작전의 실패 가능성 및 실패를 용인할 수 있는 수준과 수용할 수 없는 결과를 야기할 가능성 등을 평가한다. 그리고 목표 달성을 위한 가용한 군사작전 옵션을 설정한다.

셋째, 선제공격을 통해서 달성하고자 하는 최종 상태를 구체적으로 설정한다. 정치적 차원에서 허용되는 가용한 시간 속에 목표를 달성할 수 있도록 최종상태를 군사적으로 설정한다. 또한 군사작전의 종결을 선언하는데 요구되는 일련의 조건들에 대해서는 군사작전의 결과로 발생되는 상황이 설정된 목표에 충족하는지 여부를 판단하는 기준 등을 정한다.

넷째, 군사작전의 위험을 식별(군사작전의 부정적 효과 등)하고 이러한 위험을 완화하기 위한 방안을 강구한다. 군사작전의 목표가 아닌 경제적 기반시설에 대한 파괴를 회피하고, 민간인 등 표적과 관련되지 않은 대상에 대한 부수적 피해를 최소화할 수 있도록 군사작전 방안을 마련한다.

선제공격 군사작전을 이행하기 위한 구체적인 군사적 준비조치를 이행하는 과정은 미국이 과거에 수행한 선제공격 사례들 속에서 잘 보여지며,[12] 작전기획 절차 측면에서는 다음과 같은 절차와 요소들을 중시한다.[13] 무엇보다 대통령의 군사작전 계획 준비에 대한 공식적인 지시가 있어야 한다. 통상 대통령이 공식적으로 군사작전 계획에 대한 준비를 지시하기 이전에 다양한 경로를 통해서 군사작전에 대한 의지가 피력되고 강조되며, 대통령의 지시는 전반적인 여건이 조성되었을 때 이루어지는 공식적인 절차이다.

둘째, 대통령의 지시를 기반으로 군사작전 계획을 준비하고 집행하기 위한 지휘관을 임명하고 참모조직을 편성하는 등 군사작전 지휘통제 구조를 설정한다. 통상적으로 지역 전투사령관에게 지휘책임을 부여하나 임무특성에 따라 지휘관

12) Bush, George W., Decision Points(New York: Crown Publishers, 2010), pp.224-254. Fontenot, Gregory, Degen, E. J. and Tohn, David. *On Point*(Washington, DC.: Office of the Chief of Staff: U.S. Army, 2003), pp.29-84.
13) The U.S. Joint Chief of Staff, 앞의 책, pp.I-11~III-16.

을 별도로 지정할 수도 있다. 통상적으로 미국은 지휘통일의 원칙을 중시(unity of command)하여 단일 지휘관이 전체 작전을 준비하고 지휘할 수 있도록 하며, 필요한 부분을 합참 등 관련 부처에서 지원한다.

셋째, 군사작전을 계획하고 준비하기 위한 감시・정찰 작전, 특수작전 등을 조기에 실시하여 필요한 정보를 수집하고 여건을 조성한다. 정보자산을 목표지역 인근에 배치하여 정찰활동을 실시하고, 인적 정보를 최대한 활용하는 등의 활동을 강화한다. 관련국과의 정보협력도 적극 추진한다.

넷째, 군사공격작전에 대한 옵션을 검토하고 작전계획을 수립한다. 군사작전 계획은 목표의 달성가능성, 정치적 영향 및 효과, 부수적 피해, 작전에 요구되는 필요한 통합군 전력 및 예비전력, 군사능력 및 기술적 능력 검토, 필요시 예비전력의 동원 등과 관련된 사항들을 구체적으로 함께 평가한다. 기획된 선제공격 군사작전 계획은 1년 이상에 걸쳐 수립하나, 위기시 계획은 필요에 따라 단기간에 준비한다.

다섯째, 군사공격작전에 대한 옵션과 계획을 대통령에게 사전 보고하고 대통령의 지시에 따라 선정된 군사작전 계획을 연습한다. 군사공격의 연습은 보안을 필요로 하기 때문에 기계획된 연습을 활용하여 요구되는 연습을 가급적 실시하고, 필요시에는 다양한 이유를 근거로 한 새로운 연습을 계획하여 실시한다.

여섯째, 군사력을 사전 이동하여 배치하고 군사작전을 준비토록 한다. 군사력의 이동은 인근 우방국의 미군기지에 사전에 배치하여 군사작전을 준비하거나 작전지역에 인접한 미 영토로부터 수송수단에 의해 직접 이동하여 작전을 실시할 수 있는 방안들을 동시에 검토하고 이행한다.

일곱째, 군사공격작전 개시에 대한 대통령의 최종승인을 재가 받은 후 군사공격을 이행한다. 군사공격작전은 통상적으로 몇 개의 군사옵션 가운데 이들 각각의 군사옵션이 갖고 있는 강약점 및 위험 등을 평가하여 최종적으로 가장 적절한 군사옵션을 선택하여 이행한다.

군사공격작전을 위한 사전 준비 조치 사항들은 군사작전의 강도와 규모, 방법 등에 따라 차이가 있다. 예를 들면, 미 이지스함 및 폭격기 등에 의한 일부 시설

에 대한 토마호크 미사일 공격이나 원거리 정밀타격 작전은 사실 군사적 준비가 매우 적은 수준에서 이루어질 수 있다. 반면에 대규모의 군사작전은 많은 전력을 동원해야 하기 때문에 보다 철저한 계획 및 군사적 사전 조치를 요구한다.

만약 미국이 북한에 대한 대대적인 군사공격 의지와 계획을 갖고 선제공격을 위협하고 강압작전을 이행하였다면 이를 사전에 파악할 수 있는 객관적 사실들은 많이 있다. 무엇보다 미국은 군사공격을 계획하는데 있어 북한의 방어능력, 공격 표적 등에 대한 정찰·감시 정보활동을 강화한다. 이는 미국의 정보자산 이동 배치나 정찰·감시활동 등의 변화사항 등을 파악하여 확인할 수 있다. 또한 군사공격을 위한 사전 연습훈련, 군사력의 사전 이동 배치 등 능력 강화, 비전투원 철수작전의 준비 등은 가시적으로 확인할 수 있는 주요한 군사적 요소들이다. 반면에 미 대통령 및 군의 내부적 정책결정 및 준비사항은 확인이 매우 어렵다. 즉, 대통령의 군사작전에 대한 준비지시, 군사작전을 위한 지휘통제 구조 설정, 참모조직과 능력의 강화, 군사작전 옵션과 계획의 준비 및 검토, 군사공격 옵션을 포함한 의사결정 과정, 군사공격 이후의 안보상황에 대한 군사적 평가 및 준비 등은 파악하기가 어렵다, 따라서 이러한 군사공격에 대한 준비들은 대통령을 포함한 주요한 정책결정자들의 발언과 행동들을 통해서 확인할 수 있을 것이다.

3. 미국의 선제공격 사례

미국은 베트남전 이후 많은 군사작전을 수행하였다. 그렇지만 1991년 걸프전은 유엔안보리 결의에 기반을 둔 미국 주도의 다국적군에 의한 군사적 개입이었으며, 걸프전 이후 1990년대 동안 지속되었던 비행금지구역 강요를 위한 대이라크 타격작전은 걸프전의 연장선상에서 후세인 정권이 이웃국가와 국내 소수민족에게 무력을 행사하는 것을 방지하기 위해 이행되었다. 걸프전 이후의 군사

작전은 1992-1995년 간 보스니아-헤르체고비나의 군사개입과 1999년 유엔안보리 결의를 기반으로 한 NATO의 코소보전 군사개입이 있다. 여기서는 북한 상황을 고려하건데 유엔의 결의와 지지가 없는 가운데 이루어진 미국 단독의 공격작전 사례만을 살펴보도록 한다. 주요 사례는 미국의 1983년 그레나다 침공작전, 1986년 리비아 공습작전, 1989년 파나마 침공작전, 2003년 이라크 전쟁, 2017년 시리아 화학시설 공격사례들이다.

가. 1983년 10월 그레나다 침공작전(Operation Urgent Fury)

레이건 대통령의 그레나다 침공작전은 카리브해와 그레나다에서 소련과 쿠바의 영향력 증대에 대한 미국의 우려가 고조되는 가운데 이행되었다. 1979년 3월 쿠데타와 국민혁명에 의해서 수립된 공산주의 정권인 인민혁명정부의 비숍(Maurice Bishop) 총리가 1983년 10월 살해되고 정치적 혼란이 가중되었다. 미국은 그레나다 공산주의 정권이 쿠바, 소련 등 공산주의 국가와 긴밀한 관계를 유지하고, 쿠바군 주둔 병력을 증강시키며, 수도에 건설 중인 비행장을 소련과 쿠바의 비행시설로 내줄 가능성을 크게 우려하였다. 이러한 상황에서 그레나다 내 혼란이 발생하자 미국은 미국이 운영하는 의과대학교 미국 학생의 안전을 우려하여 이들의 구출을 계획하였다. 그러나 그레나다가 미국 영사의 의대 방문 및 학생 철수를 위한 여객선의 정박을 거부하면서 미국인을 인질로 할 수 있다는 위기감이 급격히 높아졌다. 이러한 상황에서 동카리브해 국가연합국(OECS: Organization of Eastern Caribbean States) 의장인 도미니카 수상이 미국의 군사개입을 공식 요청하면서 미국은 미국인 철수작전을 군사개입작전으로 전환(10월 21-22일)하여 침공작전을 짧은 기간에 결정하고 작전을 실시하였다.[14]

14) Stewart, Richard W., *Operation Urgent Fury: The Invasion of Grenada, October 1983.* U.S. Army Center of History. CMH Pub 70-114-1(U.S. Army Center for Military History, 2008), pp.5-10. Cole, Ronald H., *Operation Urgent Fury: Grenada*(Washington, DC., Office of the Chairman of the Joint Chief of Staff, 1997), pp.3-19. Zunes, Stephen. "The US Invasion of Grenada" Global Policy Forum: Foreign Policy in Focus, Oct. 2003(https://www.globalpolicy.org/component/

그레나다 침공작전은 베트남전 철수 이후 최초의 미국 해외 군사개입 작전으로 이 작전 이틀 전에 레바논 베이루트 해병대 막사에 대한 폭탄테러가 발생하여 위기의식이 높아졌던 상황이었다. 레이건 대통령은 1980년대 초 니카라과 산디니스타 공산주의 정권 및 엘살바도르 반란을 소련이 지원하자 이를 미국의 영향권인 중남미 및 카리브해 지역에 대한 위협으로 인식하고 대응하고 있었다. 그레나다 침공작전의 불법성에 대한 대내외적인 비판이 높았으나 레이건 대통령은 이 작전의 성공에 힘입어 국내적 지지율이 상승하였으며, 힘을 기반으로 한 강력한 대외정책을 추진할 수 있었다. 특히, 미국의 뒷마당인 카리브해에서 미국이 이익에 반하는 위험한 환경이 조성되는 것을 간과하지 않겠다는 미국의 전통적인 정책을 재확인시켜 주었다.

미국의 최초 행동은 그레나다에 대한 군사적 개입작전이 아닌 비전투원 철수작전에 관심을 집중하고 '위기사전계획그룹'(Crisis Pre-planning Group)을 구성하였다. 미 합참의장은 미 대서양사령부에 비전투원 철수작전을 준비토록 사전 경보 명령을 실시하고(10월 18일) 위기사전계획그룹의 구성과 함께 항모전투단을 이 지역으로 항진토록 지시(10월 20일) 하였다. 군사작전이 미국민 철수작전에서 개입작전으로 전환하면서 작전의 규모와 계획을 변경하였다. 미국은 성공적인 기습공격 작전에 의해 미국 학생들을 안전하게 구출하고 전 지역을 신속히 점령하였으며, 정권교체를 실시(3일작전)하였다. 그러나 예상치 않은 저항과 미군의 사전 준비가 미흡하여 발생하였던 공격부대에 대한 군수지원 문제, 공격부대 간 통신 및 상호운용성 문제 등으로 원하지 않았던 피해를 입었다. 이는 이후 1986년 골드워터-니콜스 법을 제정하여 합동작전 능력을 강화하기 위한 조치를 단행토록 요구하는 결정적인 계기를 마련하였다.[15]

미국의 선제공격 작전은 1개 항모기동부대와 1개 상륙기동부대, 육군 레인저 2개 대대 및 공정사단 1개 연대, 해병대 상륙단, 육군 및 해군의 특수전 부대, 항모 탑재기 및 수송항공기 등으로 구성되어 작전을 개시하였다. 육군 레인저부

---

content/article/155/25966.html(검색일: 2019. 3. 6).

15) Stewart, Richard W., 앞의 책, pp.8-12, 29-33. Cole, Ronald H., 앞의 책, pp.19-23.

대는 남부를 책임지는 가운데 공중강습작전에 의해 비행장을 점령하여 후속부대의 착륙을 위한 준비를 실시하면서 침공작전을 개시하고, 미국 학생들과 감금되어 있던 그레나다 총독(Governor General)을 구출하였다. 해병대는 상륙함으로부터 헬기를 이용한 공중돌격작전과 상륙장갑차량 등을 활용하여 그레나다 동부해안 Pearls 비행장 남부에 상륙돌격작전을 감행하여 신속히 비행장을 장악하고 작전을 수행하였다. 해병대는 레바논 폭탄테러에 대응하기 위해 레바논 파병을 위해 이동하던 도중에 그레나다 침공작전에 참가하여 작전을 완수하고 레바논으로 파병되었다. 육군 레인저 부대와 해병대는 근접 공중지원과 해군 함포지원 하에서 작전을 실시하여 목표지역을 점령하였다.[16)]

그레나다는 대내적인 정치적 혼란과 미국의 기습적인 공격작전으로 미국의 군사적 침공에 대한 실질적인 정치적, 군사적 사전 대응조치는 할 수 없었다. 그러나 지역방위를 담당하는 그레나다 군과 쿠바군은 미군 침공에 대한 대응공격을 감행하였으며, 미군에게 예상치 않은 손실을 입혔으나 그레나다 방위병력의 규모와 대응은 매우 미약하였다. 카리브해 주변의 도서국가들은 미국의 군사개입에 우호적인 입장을 표명하였으며, 미국의 개입을 공식적으로 요구하는 등 미국의 군사개입에 대한 우호적인 정치적인 여건이 조성되었었다. 미국은 성공적인 군사개입 작전 이후 미군의 군사개입과 내정간섭에 대한 국제적 비판에도 불구하고 구출된 그레나다 총독이 이끄는 새로운 정권이 수립되는 것을 지원하였다. 그레나다 작전과 관련된 유엔의 공식적인 행동은 없었으며, 미국은 지역기구인 OECS의 지원을 얻었었다.

나. 1986년 4월, 리비아 공습작전(Operation Eldorado Canyon)

레이건 대통령은 1986년 4월 리비아에 대한 공습작전을 통해 리비아의 테러지원 활동을 군사적으로 응징하기 위한 작전을 성공적으로 수행하여 카다피의 테러지원 활동을 중지시키는 등 행동을 강압하는데 성공하였다. 1980년대 중반

16) Stewart, Richard W., 앞의 책, pp.14-29.

리비아는 국제테러리즘의 핵심 후원국의 하나로서 리비아 내에 설치되어 있는 테러분자 훈련소를 지원하고, 이들에게 자금・무기・성역을 제공하였다. 이는 리비아에 대한 응징 분위기를 고조시켰다. 미국은 리비아의 테러지원에 대한 정보수집을 강화하였으며, 1985년 12월 로마와 비엔나 테러, 1986년 4월 TWA 항공기 테러와 베를린 디스코텍 테러에 직간접적으로 리비아가 연계되었다는 증거를 확인하게 되었다. 이러한 상황에서 미국은 리비아의 테러지원 증거를 확인한 후 곧바로 이를 응징하기 위한 공격작전을 이행하였다.[17)]

레이건 대통령은 테러에 대한 미국인의 피해가 증대하자 1984년 테러집단에 대한 선제 및 응징 타격 정책을 국가안보결정의 원칙으로 정립하였다. 실제로 1981-1986년 동안 미국인 300명 이상이 테러범들에게 살해되었다. 카다피는 테러활동을 적극적으로 지원하였을 뿐만 아니라 국제해역인 시드라만(Gulf of Sidra) 전체를 자국의 북부 영토이며 '죽음의 선'이라고 선포하였다. 미국은 시드라만에서 '항행의 자유작전'을 실시하고 이에 대응하는 리비아 함정과 대공미사일 기지를 타격하였으며, 리비아는 비행 중이던 미군 F-14s에 SA-5 대공미사일을 발사하는 등 긴장관계가 고조되었다[18)]

카다피는 미국이 리비아에 대한 제재와 응징을 공언하는 상황에도 불구하고 TWA 테러분자들을 칭송하고 미국에 대한 테러를 증대할 것을 맹세하는 등 강경하게 대응하였다. 그러나 미국의 응징 가능성이 높아지자 테러와 관련하여 미국과의 협력을 위한 대화를 제의하였으나 미국은 응답하지 않았다. 이러한 기간 중에 리비아가 미국 외교관 및 레이건 대통령에 대한 암살시도를 지원한다는 정보 등이 제공되었으나 정보는 불확실한 상태였다.

미국은 1981년 중반 카다피 문제를 다루기 위한 임무부서를 설치하고, 리비아

---

17) Endicott, Judy G. "Operation Eldorado Canyon," in *Short of War USAF Contingency Operations 1947-1997.* https://media.defense.gov.(검색일: 2019. 3. 15), pp.145-148. The New York Times. "Target Qaddafi." 22 Feb. 1987. Carina, Piazza Della, "On April 14th 1986, Ronald Reagan ordered a series of bombings directed against Libya under "Operation El Dorado Canyon"." 15 April 2013, https://piazzadcarina.wordpress.com(검색일: 2019. 3. 15), pp.1-3.

18) Endicott, Judy G. 앞의 책, pp.145-146. Carina, Piazza Della, 앞의 글, pp.5-6.

를 응징하기 위한 준비를 시작하였다. 미국은 리비아의 테러지원과 관련한 유엔 안보리 제재의 강화를 주도하였으며, 관련국들과 리비아 공습에 대해 사전 협의하여 지원을 확보하는 외교적 조치를 강구하였다. 국무부는 1985년 백악관이 지원하였던 리비아에 대한 미-이집트 연합군의 지상 및 공중 공격 계획을 폐기토록 하였다. 반면에 CIA는 1980년대 초 이래 리비아 망명집단, 그리고 이집트 및 프랑스 등 외국 정부와 함께 리비아 내 쿠데타 또는 카다피 암살 계획을 추구하였다.[19]

미국은 1985년 로마와 비엔나 테러 발생 이후 선제공격을 위한 군사작전 준비를 시작하였으며, 영국, 프랑스, 스페인과는 리비아 공습작전에 대한 지원을 논의하였고, 리비아에 대한 이태리, 독일, 영국, 프랑스, 스페인의 제재 강화를 압박하였다. 영국 대처 수상은 영국기지를 사용한 미 공군기들의 발진을 허용하였으나 프랑스와 스페인은 미국 항공기의 자국 영공 통과를 거부하였다. 따라서 미 공군 항공기가 영국에서 출격하여 리비아 공습작전 수행을 위해 왕복 약 6,000 마일의 공중작전 준비를 시작하였다. 레이건 대통령은 미 유럽사령관에게 우발계획을 준비토록 지시하였으며, 베를린 디스코텍 공격에 대한 리비아 개입이 확실하다는 증거를 미국 국가안보국(NSA: National Security Agency)이 도청하여 확보함으로써 공습작전에 대한 정의로운 명분을 확보하였다. 당시 이집트 등 북아프리카 국가들은 미국의 카다피 응징에 대해 우호적인 입장이었고, 사우디는 중재적 입장을 갖고 있었다.[20]

미국은 공중공격 표적으로 테러활동과 직접 관련된 4개의 시설과 리비아 방어체계를 레이건 대통령이 승인하여 선택하였다. 구체적으로는 카다피의 테러분자 관련 기반시설로서 트리폴리의 테러분자 네트워크의 지휘통제시설 및 카다피 거주시설, 트리폴리 인근 해군 특수전 요원 및 테러분자 훈련소, 트리폴리 비행장과 이곳의 IL-76 수송기와 무기, 테러분자 집결지 및 무기 은닉장소인 뱅가지 군 막사, MiG-23 전투기 등을 배치하고 있는 뱅가지 전투기 기지로 선

19) Carina, Piazza Della, 앞의 글, pp.6-9.
20) Endicott, Judy G., 앞의 책, pp.148-149. The New York Times, Feb. 22, 1987.

정하였다. 특히, 민간인들에 대한 부수적 피해와 경제기반 시설을 파괴하지 않도록 신중하게 표적을 선택하여 공격을 실시토록 준비하였다.[21]

공중 공격작전에는 영국으로부터 발진한 F-111s 전폭기 18대를 포함하여, 전자전기 및 공중급유기, 그리고 지중해에 배치한 항모로부터 발진한 F/A-18s 및 전자전기, 근접지원기 A-7s가 참가하였으며, GBU-10s 폭탄이 사용되었다. 표적에 대한 오인으로 유도폭탄 하나가 프랑스 대사관 인근에 투하되어 피해를 야기하였으나 부수적 피해를 최소화한 가운데 공격작전을 성공적으로 수행하였다. 카다피는 미국의 공습작전 이후 테러지원 행위를 실질적으로 중단하였다.[22]

다. 1989년 12월, 파나마 침공(노리에가 체포) 작전(Operation Just Cause)

파나마 독재자 노리에가와 미국 사이의 긴장관계가 1987년부터 높아졌다. 1987년 6월 노리에가의 전임 측근이 1984년 선거에서 노리에가가 어떻게 선거를 조작하고 발레타(Nicolas Barletta) 대통령의 사임을 요구하였는지를 언론에 밝혔다. 이에 따라 미국은 노리에가의 사임을 요구하였다. 노리에가는 반노리에가파의 반대시위를 폭력적으로 진압하고 노리에가 지지세력은 미 대사관을 공격하였으며, 미 의회는 파나마에 대한 경제·군사 지원을 중단하였다. 1988년 2월 탐파와 마이애미 연방대배심은 노리에가를 마약밀수와 돈세탁 혐의로 기소하였다. 1989년 5월 선거에서 노리에가 반대정파 후보가 대통령에 당선되자 노리에가는 이 선거를 외부 개입결과로 공표하고 무효화시켰다. 레이건 대통령은 CIA에 노리에가를 퇴출시키기 위한 비밀전략을 준비할 것을 지시하였으며, 국방부는 심리작전을 강화하였다. 미국은 군사력 시위활동 등을 통해 경고를 보내기 시작하였으며, 반노리에가파가 주도하는 군부 쿠데타가 발생하였으

21) Endicott, Judy G., 앞의 책, pp.149-150.
22) Endicott, Judy G., 앞의 책, pp.150-155.

나 실패하였다. 노리에가는 미국에 맞서는 강력한 반미 정책을 추구하였으며, 파나마 주둔 미군들의 활동을 위협하였다. 부시대통령은 미국은 파나마 운하의 권리보호 및 노리에가 정권의 제거를 목적으로 대대적인 군사침공 작전을 결정하고 노리에가를 체포하여 미국으로 압송하였으며, 미국이 지원하는 정권의 수립을 지원하였다.[23)]

미국의 군사작전 준비와 이행은 점진적으로 이루어졌다. 먼저 노리에가에 대한 경고로 파나마 주둔 전투병력을 증강하고 군사연습과 활동을 증대하였으며, 파나마 군 가족을 철수시키는 등 경고 신호를 보냈으나 노리에가는 이를 무시하고 오히려 강력히 대응하였다. 1989년 11월 베를린 장벽이 무너지고 소련의 동유럽에 대한 영향력이 극도로 약화되자 미국의 행동공간이 확장되었다. 특히, 1989년 12월 15일 파나마 의회와 노리에가는 군부 쿠데타 시도와 관련하여 미국을 강하게 비판하고 미국과의 전쟁상태를 선포하였다. 이러한 상황에서 12월 16일 파나마 군 검문소 경비병이 미군에게 총격을 가하여 미군 병사가 사망하고 미군 및 미군가족에게 폭력을 행사하는 사건이 발생하였다. 미군은 이 사건을 계기로 군사적 침공을 개시하여 노리에가 정권을 전복하고 노리에가를 체포하여 미국으로 후송하여 재판에 회부하였다. 1988-1989년 기간 동안 노리에가는 쿠바, 니카라과, 리비아에 경제·군사적 지원을 의존하였고, 쿠바와 니카라과는 무기와 군사교관을 지원하였었다.[24)]

미국의 군사작전 준비는 1988년 연방정부가 노리에가를 기소하자 합참은 남부사령관에게 지시하여 파나마 주둔군을 증강하는 우발계획을 수립하면서 시작되었다. 1989년 5월 노리에게가 선거결과를 뒤집자 파나마 침공작전 책임 사령관을 교체하고 군사적 침공을 기본으로 하는 전략과 작전계획을 수립하였다. 파나마 침공계획은 3일 작전, 군사적 목표로서 노리에가 나포, 노리에가의 전위세

---

23) Cole, Ronald H. *Operation Just Cause: Panama*(Washington, DC.: Joint History Office: Office of the Chairman of the Joint Chiefs of Staff.1995), pp.5-16. Taw, Jennifer Morrison, *Operation Just Cause: Lessons for Operations Other Than War*(RAND Arroyo Center, 1996), pp.3-6. The Telegraph. "How Panama's military dictator Manuel Noriega was defeated by rock'n roll," 30 May 2017.

24) Cole, Ronald H., 앞의 책, pp.27-30.

력인 파나마 국방군의 무장해제 및 해체를 목표로 하였다. 레이건 대통령과의 회의에서 정치적 목표로 파나마 거주 미국 시민 3만 명의 보호, 파나마 운하와 142개의 미국 방어거점의 보호, 파나마 반대집단을 지원하여 진정한 민주정권의 수립, 파나마 국방군을 무력화하고 노리에가를 법정에 세우도록 설정하였다. 침공작전 직전인 1989년 10월 작전부대는 중대 및 대대급 수준에서 훈련을 실시하였고, 지휘부와 참모부서는 작전계획과 절차 등을 점검하고 확인하였다. 민간인 피해를 방지하기 위해 인구밀집 지역, 병원, 학교 등 시설에서 중화기를 사용하는 것을 엄격하게 규정하는 교전규칙을 설정하였다. 군사작전 이후의 혼란을 방지하고 민주정권 수립을 위한 민사작전과 안정화 작전을 중시하고 이를 위한 전문화된 부대를 배치하여 작전을 실시토록 준비하였다.[25]

군사작전의 이행은 특수작전 부대가 F-117의 근접 항공지원 하에 최초 작전을 개시하였다. 곧바로 기동부대가 작전을 개시하여 목표지점을 점령하였으며, 파나마군은 사령부 보호를 위해 강력한 저항을 하였으나 미군이 사령부 대부분을 파괴하고 저항세력을 분쇄시킴으로 파나마 군의 대대적인 저항은 종식되었다. 노리에가는 교황청 대사관으로 피신하였다가 항복하였다. 파나마 군사작전을 위해 약 27,000명 병력이 참가하였다. 주요 지상군 전력은 파나마 주둔 병력 이외에도 미 본토에서 공정여단, 레인저 부대 및 특수전 부대, 그리고 민사작전 부대 및 심리전 부대 등이 참가하였다. 항공전력은 스텔스 전폭기 F-117A를 포함하여 200대 이상의 전력들로 구성되었다. 부시 정부는 파나마 군사침공의 정당성에 대한 국내적 지원을 확보하기 위해 파나마 군사작전 개시 당일 오전 TV에서 전쟁의 정당성을 설명하였다. 군사작전에 대한 보도를 위해 주요 언론사 종군기자들을 초청하여 취재토록 조치하였으나 보안의 이유로 이를 사전에 공지하지 않아 종군기자들이 사전 준비를 제대로 하지 못하였고, 군이 이들을 지원할 수 있는 체제를 제대로 준비하지 못함으로 종군기자들의 활동은 제한되었다. 파나마 침공작전은 작전의 특수성으로 인해 지역국가들의 반응은 크게 중시

25) Cole, Ronald H., 앞의 책, pp.17-30. Taw, Jennifer Morrison. 앞의 책, pp.9-29.

되지 않았으며, 파나마 내부의 혼란 방지를 위한 안정화 작전을 중시하였다.[26]

라. 2003년 3월, 이라크 전쟁(Operation Iraq Freedom)

부시정부의 이라크 전쟁은 9.11테러 이후 예견된 수순으로 진행되고 시작되었다. 9.11테러 이후 2002년 미국은 이라크를 시리아 및 북한과 함께 '악의 축'의 한 국가로 지정하였다. 1991년 걸프전 이후 미국은 시아파와 쿠르드 족을 보호하기 위해 비행금지 구역을 설정하고 이를 점진적으로 확대하여 바그다드를 제외한 이라크 거의 전 지역으로 확장하였다. 미국은 비행금지 구역을 강제하기 위한 작전을 강력히 이행하였으며, 미군 작전을 방해하는 레이더 기지 및 대공미사일 기지 등에 대한 공습작전과 미사일 공격작전을 지속적으로 실시하였다. 1998년 12월 실시한 '사막의 여우'작전은 대표적인 이러한 작전이다. 또한 미국은 이라크의 잔악한 인권유린 행위와 대량살상무기 제조 의혹을 명분으로 유엔안보리 제재를 지속적으로 강화하였다. 부시 대통령은 9.11테러 이후 이라크 전쟁을 적극적으로 준비하였으며, 후세인 정권이 유엔안보리 결의를 위반하고 WMD 개발을 추구한다는 명목으로 2003년 3월 이라크를 침공하여 후세인 정권을 성공적으로 제거하였다.[27]

후세인은 미국의 비행금지구역 강요 작전에 강력히 대응하는 등 미국에 대한 강경입장을 고수하였다. 시아파와 쿠르드족의 저항을 잔혹하게 진압하고 정적을 숙청하는 등 독재체제를 강화하였으며, 미국의 대량살상무기 제조와 관련한 의혹제기에 대해 모호한 입장을 유지하였다. 유엔안보리 결의에 따른 유엔사찰위원회와 국제원자력기구의 조사활동을 수용했으나 이에 대한 협력에 소극적이

---

26) Cole, Ronald H., 앞의 책, pp.32-69.

27) Bush, George W., 앞의 책, pp.223-271. Dale, Catherine. (2008). *Operational Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress*(Congressional Research Service, 28 March 2008), CRS Report for Congress, RL34387, pp.1-40. Flyn, Matthew J. *First Strike*, 임은성 역, 「선제전쟁: 시작과 종말, 그리고 제한된 보상(서울: 북코리아. 2011), pp.308-348. 이근욱. 「이라크 전쟁: 부시의 침공에서 오바마의 철군까지」(서울: 한울아카데미, 2011). pp.41-131, 박창권. 「최근 전쟁사례를 중심으로 한 해군력의 역할 분석」. KIDA 연구보고서 안04-2049. 2004, pp.66-150.

어서 미국의 이라크 공격에 대한 명분을 무력화하는데 실패하였다.

부시정부는 전쟁의 명분을 확보하기 위해 후세인의 인권유린 행위, 1987-1988년 쿠르드족에 대한 화학무기 사용, 핵개발 추진 의혹, 테러지원 활동을 적극 부각시키고 비판하였다. 이를 통해 이라크 군사작전에 대한 대내외적으로 우호적인 여론을 조성하고 유엔안보리 결의를 추구하였으며 동맹국 및 우방국의 지원을 얻고자 하였다. 영국은 미국의 이라크전을 지지하고 연합작전을 수행하였으나 유엔안보리 이사국인 중국, 러시아, 프랑스를 설득하지 못하였고, 독일은 이라크전을 반대하였으며, 사우디와 터키는 미국의 군사기지 사용을 거부하였다.[28)]

부시 대통령은 2011년과 2012년 발표된 부시독트린을 통해 테러지원 국가들을 군사적으로 패배시킬 것임을 명확히 하였다. 이는 테러집단의 공격을 기다려서는 안된다는 선제공격의 정당성을 주장하였으며, 우리 편에 서거나, 그렇지 않으면 테러집단의 편에 서는 것이라는 경고를 통해 국제사회가 미국 편에 설 것을 요구하였다. 2002년 10월 의회는 대통령에게 이라크에 대한 군사력 사용에 대한 권한을 부여하는 결의안을 통과시켰다. 부시대통령은 군사침공에 대한 유엔안보리 결의를 확보하려고 노력했으나 지원을 받는 데는 실패하였다. 유엔안보리는 이라크 정부에게 무장해제 의무를 이행할 마지막 기회를 주며, 이를 이행하기를 거부하면 심각한 결과에 직면할 것이라는 경고만을 결의하였다. 부시대통령은 2003년 3월 17일 후세인과 그의 아들이 72시간 이내에 이라크를 떠날 것을 요구하는 최후통첩을 실시하였으나 후세인은 이를 거부하였다. 미국은 이라크 작전의 개시와 함께 전쟁의 목표를 이라크의 대량살상무기를 폐기하고, 후세인에 의한 테러리즘을 종식시키며, 이라크 국민을 해방하는 것으로 발표하였다.[29)]

이라크전의 군사적 준비는 2001년 가을부터 소수의 폐쇄적 구조로 작전계획

---

28) Bush, George W., 앞의 책, pp.226-240. 이근욱, 앞의 책, pp.100-104.
29) Bush, George W., 앞의 책, pp.250-253. Flyn, Matthew J., 임은성 역, 앞의 책, pp.311-315.

준비를 시작하여, 여러 차례에 걸쳐 수정하였고 2003년 1월 최종 계획을 부시 대통령에게 보고하였다. 사실 중부사령부는 부시 대통령의 2002년 '악의 축' 발언 이후 이라크에 대한 전쟁을 기정사실화하자 사전에 군사적 준비를 실시하였으며, 감시활동 및 특수작전을 통해서 필요한 정보를 획득하고 조치토록 하였다. 군사작전은 럼스펠드 장관의 지시에 의해 압도적인 군사력 투입이 아닌 효율적 군사력을 운용토록 정하고, 군사작전에 대한 계획·준비·동원·전개와 관련된 사항들을 검토하고 단계적으로 이행토록 하였다. 미군의 작전계획은 걸프전 당시 건설하였던 사우디 기지를 사용할 수 없게 됨에 따라 걸프전 이후 쿠웨이트에 준비된 시설을 기반으로 전역 군사력 기반을 강화하였다. 전쟁준비와 관련하여 RSOI(Reception, Staging, Onward-movement, and integration) 기반, 항만 및 공수관련 시설, 사전배치 장비, 지휘통제 구조, 합동 연습 및 훈련, 예비군 동원, 이동 등과 관련된 사항들을 점검하고 조치하였다. 전쟁 이후의 작전계획은 전쟁계획과 별도로 국무부와 군은 각각 이라크 안정화 및 재건 계획 등을 2002년부터 검토하였으며, 2003년 1월 대통령 국가안보지시로 재건 및 인도적 지원 조직(ORHA: Office for Reconstuction Authority and Humanitarian Assistance)을 창설하여 주도적으로 준비토록 하였다.[30]

미국의 군사작전은 미군의 첨단 무기체계와 기동능력을 기반으로 한 '충격과 공포'(Shock and Awe)의 작전에 의한 새로운 방식으로 신속히 이행되었으며 단기간에 후세인 군사력을 붕괴시키고 승리를 달성하였다. 전쟁개시 이전부터 이메일 발송, 전단 및 라디오 살포 등을 통해 심리전을 적극 전개하였고, CIA 특수전 요원을 침투시켜 정보수집 활동을 실시하였으며, 쿠르드족과 연계한 민병대를 조직하는 등 활동을 전개하였다. 전쟁개시와 함께 후세인 거처 및 이라크 지휘통제 시설에 대해 잠수함 및 수상함으로부터의 토마호크 미사일 공격, F-117 전폭기 및 F-15E에 의한 타격을 실시하였다. 이는 이라크군의 지휘통제 체계와 방공체계를 초기부터 마비 및 무력화시켰다. 결정적 작전은 27일간 수

30) Dale, Catherine, 앞의 책, pp.10-18. Fontenot, Gregory, Degen, E. J. and Tohn, David, 앞의 책, pp.29-80.

행하였으며, 정밀타격작전에 의해 이라크군의 방어능력을 무력화시키고, 지상군에 의한 신속한 비선형적 기동작전을 실시하였다. 미국의 첨단무기인 정찰·감시체계와 정밀유도무기, 그리고 지상군의 신속한 기동작전이 결합된 정밀성과 속도에 기반을 둔 작전의 효율성을 전 세계에 과시하였다. 미국은 걸프전에 비해 정밀도가 획기적으로 증대한 정밀유도무기를 대폭적으로 많이 사용하였고, 무인기, JDAM, 대형폭탄(MOAB), 열기압 폭탄 등 등 새로운 무기를 투입하여 전쟁을 수행하였다.[31]

마. 2017년 4월 시리아 화학시설 타격작전(2017 Shayrat Missile Strike)[32]

시리아 화학시설에 대한 타격작전은 오바마 정부와 차별화된 트럼프 정부의 대외 군사개입 의지를 잘 보여주었다. 2017년 4월 4일 시리아 전투기가 북부 반군 점령지역에 화학폭탄을 투하하여 어린이를 포함한 많은 사상자가 발생하였다. 트럼프 대통령은 곧바로 책임 대상에 대한 군사적 옵션을 준비토록 지시하여 계획을 준비하였고, 4월 6일 화학탄 공격을 감행하였던 바그다드 인근 Shayrat 시리아 공군기지에 대한 토마호크 미사일 공격을 실시하였다. 트럼프 대통령은 중국 시진핑 주석의 공식적인 미국 방문 행사 중 저녁 만찬시간에 시리아 미사일 응징 공격을 발표하여 시리아뿐만 아니라 북한에게도 WMD 사용에 대해 미국이 과감히 행동할 것이라는 의지와 능력을 동시에 과시하였다.[33]

미국은 시리아가 화학무기 공격을 한 것이 분명하며, 이는 국제 화학무기금지협정을 위반한 것이고, 유엔안보리결의를 무시한 것으로 공격의 정당성을 주장하였다. 또한 이 공격은 아사드의 화학무기 사용을 용인하지 않겠다는 것을 보여주는 것이나 아사드를 제거하기 위한 전면적인 전쟁 개시를 위한 조치

---

31) 박창권, 앞의 책, pp.99-140. Fontenot, Gregory, Degen, E. J. and Tohn, David, 앞의 책, pp.85-141.

32) 미군은 2017년 시리아 화학시설 타격 작전에 대한 공식적인 명칭을 부여하고 있지 않으며, Shayrat 공군기지 타격작전으로 이해하는 것이 타작전과 구분하기가 용이하다.

33) The Telegraph. "Assad bears full responsibility': how the world reacted to Donald Trump's missile strike on Syria." 7 April 2017. CNN, "A dangerous choice looms for Trump on North Korea," 8 Dec. 2017.

가 아니며, 시리아의 화학무기 공격을 자행한 시설에 대한 공격으로 비례성에 입각한 공격이며, 트럼프 정부는 금진된 선을 넘는 상대에 대해서는 행동할 것임을 보여주는 조치라고 강조하였다. 미국은 러시아에게 1시간 전 미사일 공격 계획을 사전에 통보하여 러시아와의 분쟁을 피하기 위해 노력하였고 러시아와의 협력의지를 피력하였다. CBS 뉴스 여론조사는 미 국민들의 57%가 트럼프 대통령의 미사일 공격을 찬성하였으나 시리아에 대한 전면적 개입은 과반수가 반대하였고, 과반수는 시리아와의 전쟁은 의회 승인을 득해야 한다는 입장을 보여주었다.[34)]

시리아의 아사드 정권은 이 사건이 가공된 것이라고 주장하였다. 아사드 정권을 지원하는 러시아 푸틴대통령은 미국의 행동을 근거가 없는 구실을 갖고 국제법을 위반하는 주권국가에 대한 침략행위로서 국제적 대테러전 협력체제를 구축하는데 주요한 장애물이 될 것이라고 비판하였다. 그러나 유럽연합, 중국을 포함한 대부분의 국가들은 아사드의 화학무기 사용을 비판하고 미국의 행동을 지지하였다.[35)]

선제공격은 지중해에 배치하고 있던 미국 구축함 USS Ross가 36발, USS Porter가 23발의 토마호크 순항미사일을 발사하여 시리아 화학공격과 관련이 있던 시설들을 타격하여 상당한 수준의 피해를 가하였다. 주요 표적은 공군기지의 항공기, 항공기 격납고, 연료 및 군수물자 저장시설, 탄약보관 벙커, 공중방어체계 등 비행장 운용체계이다.[36)] 또한 미국은 2018년 4월 아사드 정권이 바그다드 반군 점령지역에 화학무기를 사용하여 또다시 살상을 자행하자 동맹국인 영국, 프랑스와 함께 시리아 화학시설 3곳에 대해 105발의 미사일 공격을 감행하여 응징을 실시하였다.[37)]

---

34) New York Daily News. “Majority of Americans support Trump’s Syria missile strike: poll.” 10 April 2017.
35) BBC, “Syria war: World reaction to US missile attack,” 7 April 2017.
36) CNN, “Trump launches military strike against Syria,” 7 April 2017.
37) The New York Times, “U.S., Britain and France Strike Syria Over Suspected Chemical Weapons Attack,” 13 April 2018.

4. 미국의 선제공격 사례의 주요 특성과 시사점

가. 정치적 특성과 시사점

미국의 선제공격은 공화당 정권인 레이건, 조지 부시(George W. Bush), 조지워커 부시(George H. W. bush), 트럼프 대통령에 의해 이행되었다. 즉, 1980년대 이후 모든 공화당 정권은 정치적 수단으로 군사공격을 실시하였으며, 민주당 정권은 이러한 공화당 정권의 군사력 사용과 관련된 상황을 해결하고 관리하는데 노력을 기울였다. 물론 클린턴 정부는 NATO의 일원으로서 유엔 안보리 결의를 기반으로 보스니아-헤르체고비나에 대한 군사작전을 실시하였지만 일방적인 선제공격의 사례라고 할 수는 없다. 미국은 군사공격을 실시하는데 있어 정당성과 명분을 내세움으로 국제적 지원과 협력을 얻고자 한다. 미국의 과거 대외적인 선제공격 사례는 다음과 같은 정치적 특성과 시사점을 준다.

첫째, 선제공격의 명분은 미국 국민의 보호, 테러, 민주정권 수립, WMD 개발, 화학무기 사용, 인권 유린 및 잔혹 행위를 들었다. 그러나 탈냉전기 이후 미국의 군사공격은 테러, WMD 개발 및 사용과 관련된 이유가 주를 이루고 있다. 인권문제를 이유로 한 군사공격의 선택은 보다 신중한 모습을 보인다. 중국 및 러시아 등 주요 관련국들이 인권문제와 관련한 미국의 군사작전을 반대하고 있는 상황이기 때문에 이와 관련한 군사개입은 보스니아-헤르체고비나, 코소보 전에서 보여준 바와 같이 미국의 일방적인 작전보다는 국제적인 지원과 협력을 기반으로 한 다국적군 작전의 형태를 보여준다.

둘째, 냉전기 미국의 선제공격은 대부분 대통령의 결정과 미국의 일방적 행동에 의해 수행되었으나 1991년 탈냉전기 이후의 군사작전은 유엔 및 의회의 지원과 협력 등 대내외적인 여론을 보다 중시하고 있다. 레이건 대통령의 그레나다 침공작전, 리비아 공습작전, 파나마 침공작전은 대내외적인 지원과 협력을 구하기 위한 노력을 크게 중시하지 않고 미국의 국익을 보호한다는 목적 하에 신속히 결정되고 이행되었다. 반면에 탈냉전기 이후의 선제공격인 이라크

전은 유엔에서의 지원을 확보하고 의회의 승인을 받기 위한 노력을 중시하였다. 트럼프 대통령의 시리아 화학시설 공격은 오바마 정부가 레드라인 선언에도 불구하고 아사드 정부의 화학무기 공격에 대해서 무기력하게 대응하여 비판을 받았던 사례를 반영하여 대내적인 지원과 대외적인 명분을 확보한 군사적 응징이었다.

셋째, 선제공격을 위해 이에 대한 관련국 및 우방국의 지원을 확보하여 정치적 정당성을 강화하고 군사작전에 필요한 지원을 얻고자 하였다. 예를 들면, 군사작전을 이행하기 위한 영공 또는 영해의 통과, 군사기지의 사용, 필요한 군사적 지원 또는 군수지원의 확보, 외교적 지원의 확보 등을 위해 노력하였다. 미국이 수행한 선제공격은 우방국 및 관련국, 지역 기구 등의 지원과 협력, 묵인하에 이루어졌다. 특히, 이라크전 및 시리아 화학시설 공격에서 보듯이 탈냉전기 군사작전은 동맹국 및 우방국과의 연합작전을 추구하였다.

넷째, 선제공격을 통해 정치, 군사적 목표를 달성할 수 있다는 자신을 갖고 군사작전을 실시하며, 미군의 예상되는 피해 및 부수적 피해 발생 가능성 등을 매우 중요하게 고려한다. 미국은 선제공격을 사전에 시간을 갖고 기획하거나 우발적 위기상황에서 단시간에 계획하는 상황이거나에 관계없이 군사작전의 성공 가능성을 확신하고 군사작전을 실시한다. 대통령이 선제공격을 최종적으로 결정하는 단계에서 군사기획자들은 군사작전의 성공을 최종결정권자인 대통령에게 확신시킨다. 선제공격 군사작전의 실패는 미국이라는 초강대국 위상뿐만 아니라 대통령 개인에게도 회복하기 어려운 정치·군사적 비용을 요구한다는 사실을 잘 반영한다.

또한 군사작전의 성공에도 불구하고 미군의 피해가 크거나 부수적 피해가 발생될 경우 정치적 실패를 야기할 수 있다는 사실을 중시한다. 따라서 미국은 선제공격시 군사표적 선정을 매우 신중하고 구체적으로 선택하여 이행한다. 예를 들면, 미국은 2017년 시리아 비행장 공격시 러시아에게 한 시간 전 이러한 공격계획을 사전에 알려서 러시아 군이 자신의 피해를 방지할 수 있는 조치를 하도록 하였다. 1986년 리비아 공습시 인근 프랑스 대사관의 피해 가능성을 심각하

게 검토하여 이를 최소화하기 위한 방안을 강구하였다.

다섯째, 대규모 군사작전은 군사작전 이후의 상황 및 정치·군사적 요구(예, 안정화 작전)를 동시에 준비한다. 부시정부는 이라크전의 군사적 승리에도 불구하고 전쟁 이후의 상황, 안정화 작전을 제대로 준비하지 않았다고 혹독한 비평을 받았다. 그러나 부시정부도 이라크전을 수행하면서 전쟁이후의 작전, 안정화 작전을 계획하고 준비하였다. 비록 이러한 계획이 현실을 제대로 파악하지 못한 잘못된 계획이었음이 후에 확인되었지만 선제공격 당시에는 이러한 작전계획을 수립하였다. 이라크전 교훈은 미국이 향후 선제공격에 있어 이후의 정치·군사적 요구사항을 보다 중시하고 체계적으로 준비할 것을 요구한다. 트럼프 정부가 시리아에 대한 제한적인 정밀타격 작전을 선택한 것도 시리아 상황의 복잡성을 고려하여 응징은 하되 직접적인 군사개입을 회피하고자 하는 전략적 계산을 보여준다.

여섯째, 위협 및 위험의 제거를 위한 군사작전의 시급성에 대한 공감대를 확보하고자 노력하며, 선제공격을 정당화하는 직접적인 촉발요인을 중시하고 이를 기회로 활용한다. 정의의 전쟁 개념에서 중시하고 있듯이 현 상황을 방치하거나 지연시킬 경우, 막대한 비용과 희생이 따를 수 있는 결과 또는 부정적 영향에 직면할 수 있음을 부각하고 인식시킨다. 미국은 2003년 이라크 및 2017년 시리아 공격시 WMD 문제, 잔악한 인권 유린 행위를 더 이상 방치할 수 없으며, 즉각적이고 시급한 응징이 필요하다고 강조하였다. 또한 군사작전의 필요성을 촉발시키는 상황을 활용함으로써 정치적 명분과 지원을 확보한다. 2003년 이라크전의 경우에도 이라크가 유엔안보리 결의에 근거한 유엔특별사찰단 활동에 비협조적인 태도를 보이자 이를 촉발요인으로 활용하였다.

일곱째, 미국은 군사력 사용 이전에 전쟁을 피할 수 있는 최후통첩이나 이와 유사한 조건과 행동방안을 상대에게 제시하여 군사적 수단보다는 외교적 노력을 우선한다는 행태를 직접적 또는 상징적으로 보여준다. 이라크전시 후세인에 대한 최후통첩이 대표적인 사례이다. 대내외적으로 군사적 폭력수단이 아닌 외교적, 경제적 수단 등을 통해서 문제를 해결하고자 하고 있다는 사실을 각인시

키기 위해 노력한다. 그러나 미국은 대체로 상대국 독재자들이 받아들이기 어려운 선택을 요구하고 있는 것도 사실이다. 미국의 선제공격 사례들을 보면 대부분의 상대국 독재자들은 이러한 미국의 요구에 타협하기보다는 강경하게 대응하는 입장을 선택하였다.

나. 군사적 특성과 시사점

미국의 선제공격과 관련된 교리, 작전계획 및 과정 등과 관련된 구체적인 내용에 대한 분석은 각각의 사례들에 대한 별도의 연구를 요구한다. 따라서 여기서는 일반적이고 공통적으로 보여주는 내용들을 중심으로 제한하여 평가를 하고자 한다. 미국의 선제공격 사례는 다음과 같은 특성과 시사점을 보여준다.

첫째, 미군의 선제공격 준비를 위한 과정은 작전기획 매뉴얼에서 제시하고 있는 제반 절차를 따라 철저히 추진된다. 즉, 상대의 군사능력 및 군사표적 등을 사전에 파악하여 분석하고, 대통령은 군사작전 준비를 지시하고 이를 위한 책임지휘관과 임무수행 부대 및 조직을 지정하며, 책임을 맡은 지휘관은 군사작전 옵션을 준비하여 대통령에게 보고하고, 대통령은 당시 여건을 고려하여 최상의 군사옵션을 선택하여 군사작전을 이행토록 한다. 또한 군은 대통령의 공식적인 군사작전 계획 준비 명령 이전에도 상황을 판단하여 준비차원에서 군사작전에 대한 사전 계획에 착수하여 대비한다. 군사작전 준비가 공식적으로 지시되어 이행되면 군사작전 계획뿐만 아니라 이에 필요한 연습훈련, 군사력의 사전 전개 및 배치, 비전투원 철수작전을 준비하고 이행한다. 특히, 상대를 기만하기 위해서 군사 연습훈련이나 군사력 전개를 정기적인 연습훈련 등을 활용하여 실시함으로서 기습의 목표를 달성하고자 한다. 물론 우발적인 긴급 군사작전은 이러한 과정이 단축되고 압축되어 진행될 것으로 판단된다.

둘째, 군사공격은 압도적인 군사력에 의해 신속하고 결정적인 작전에 의해 확실한 성공을 보장토록 준비되고 이행되었다. 미국의 선제공격은 이라크를 제외

하고는 대부분 매우 군사력이 미비한 약소국에 대한 작전이었다. 그럼에도 불구하고 예상이외의 피해 등이 발생할 수 있었지만 대부분 커다란 문제점 없이 성공적으로 작전을 수행하였다. 시리아 작전과 같이 군사적 개입을 제한하고자 하는 공격작전은 제한된 표적에 대한 제한된 정밀타격작전에 의해 정치적 강압을 위한 응징능력을 과시하였다. 또한 그레나다 작전에서 예상치 못하였던 일부 피해가 있었지만 미국은 이를 효과적으로 극복하였으며, 이라크전은 군사작전의 성공에도 불구하고 안정화 작전의 실패로 많은 비용을 지불하고 있다.

셋째, 선제공격은 정치적 강압행위로 사전에 이에 대한 정치적 메시지를 전달하고 군사력 시위활동을 전개하지만 군사작전 자체는 최고의 기습성을 유지할 수 있도록 준비하고 이행하였다. 모든 군사작전에서 상대는 미국의 군사공격을 사전에 준비하여 대비하지 못함으로 거의 무방비 상태에서 공격을 당하였다. 이러한 기습작전은 공격작전의 형태와 방식, 공격 수단과 무기체계의 선정 등을 통해서 달성하였다.

넷째, 군사작전의 목표와 수준, 표적선정을 정치적 목적에 부합하게 매우 신중하게 계산하여 선택함으로 군사작전의 성공을 보장하고 과시토록 하였다. 리비아 공습작전은 표적이 도시에 집중되어 있다는 사실을 반영하여 표적에 부합한 무기체계를 선정하고 경제기반 시설을 파괴하지 않도록 신중을 기하였다. 그레나다 및 파나마 침공작전, 시리아 화학시설 공격도 정치적 목적에 부합한 맞춤형 군사작전의 형태를 잘 보여준다.

다섯째, 우방국의 군사적 지원이 필요한 군사작전은 이에 대한 군사적 지원을 보장받을 수 있도록 노력하였다. 미국은 원정작전, 원거리 작전을 수행할 수 있는 능력을 갖추고 있기 때문에 우방국의 지원없이 독자적으로 군사작전을 수행할 수 있는 능력을 상당 수준 갖추고 있다. 그럼에도 불구하고 미국은 군수지원, 영공 또는 영해의 통과, 필요한 군사적 지원, 외교적 지원을 확보하기 위해 관련국들의 군사적 지원을 확보하는 것을 중시한다.

5. 트럼프 정부의 대북 선제공격 위협의 실효성 평가

트럼프 정부는 2016-2017년 기간 동안 북한에 대한 선제공격 위협의 강도를 고조시켜 한반도에 군사적 긴장을 조성하였다. 그럼에도 불구하고 트럼프 정부의 대북 선제공격 위협이 과거와 달리 실제 이행 가능성과 위협의 효과가 높았었는지는 객관적 평가가 필요하다. 미국은 1993-1994년 북핵 위기시 북한에 대한 선제공격 위협을 실제화 하였었다. 북한이 1993년 3월 NPT(Nonproliferation Treaty) 탈퇴를 선언하면서 위기가 고조되었다. 북한은 1994년 3월 남북회담에서 한국에 대해 '서울 불바다'를 위협하여 남북회담을 결렬시켰다. IAEA는 북한이 IAEA의 요구에 응하도록 압박하기 위한 유엔안보리의 강력한 제재조치를 요구하였다. 미국은 군사작전을 직접적으로 위협하고 IAEA의 특별사찰을 요구하였으며 미북은 뉴욕채널을 통해 협상을 진행하였지만 실패하였다. 국방부는 소위 오시라크(Osirak) 옵션으로 지칭되었던 군사옵션을 준비하여 클린턴 대통령에게 설명하였으며, 부분적인 군사력 증강 조치를 이행하였다. 그러나 한국과 중국은 미국의 군사작전 옵션을 반대하였으며, 북미협상을 지지하였다. 군사작전의 위험에 대한 우려가 증대되는 가운데 카터-김일성 회담의 결과로 위기는 완화되었다.[38)]

트럼프 정부의 2016-2017 대북 선제공격 위협은 1993-1994년에 비해 보다 실효성이 컸었는가? 과거 북한 핵위기 상황에 비해 군사작전을 이행할 수 있는 여건이 보다 좋아졌었는가? 트럼프 정부의 북한에 대한 선제공격을 이행하기 위한 정치적 정당성과 명분은 그렇게 높지 않은 상태였다. 미국은 핵 개발을 빌미로 이라크에 대한 군사공격을 실시하였지만 인도와 파키스탄에 대한 군사작전을 이행하지는 않았다. 미국은 핵 확산 저지를 국가대전략으로 유지하지만 핵 개발 저지를 위해 군사작전을 반드시 실시하지는 않았으며, 미국의 전략적 이익

38) Oberdorfer, Don, *The Two Koreas: Contemporary History*(Indianapolis: Basic Books. 1997), pp.287-345. Wit, Joel S., Danniel B. Poneman, and Robert Gallucci. Going Critical: The First North Korean Nuclear Crisis, 김태현 역, 「북핵위기의 전말: 벼랑끝의 북미협상」(서울: 모음북스. 2005) pp.143-300.

에 따라 행동을 결정하였다. 즉, 선제공격에 대한 정당한 의도 측면에서 미국은 일관성 있는 정책을 취하지 못하였다. 또한 제한적인 선제공격을 통해 북한의 핵개발을 저지하고 상황을 되돌릴 수 있는 가능성도 매우 낮았다. 1993-1994년 북핵 위기시에는 북한이 핵개발을 진척시키지 못한 상황이었기 때문에 군사공격을 통해 북한의 핵개발을 포기시킬 수 있는 가능성은 보다 높았다. 그러나 2017년 상황은 북한이 6차 핵실험을 성공적으로 실시하고 핵개발의 완성을 선언한 시기로 이를 역전시키기는 쉽지 않은 상황이었다. 북한은 핵개발을 위해 국제적 제재 하에서 많은 비용을 지불하고 정권의 운명을 걸었으며, 핵능력을 자신의 위상과 업적으로 내세우고 있기 때문에 상징적인 수준의 군사공격에 겁을 먹고 핵무기를 포기하고 무장해제할 가능성은 거의 없었다.

트럼프 정부는 선제공격에 대한 합법적 권위를 인정받기도 쉽지 않은 상황이었다. 물론 전면적인 군사작전이 아닌 정밀타격과 같은 제한적인 군사작전은 대통령의 권한과 결정에 의해 이행될 수 있다. 그러나 북한과 같은 위험한 상대에 대한 군사작전은 국제사회뿐만 아니라 대내적인 지원과 공감대를 어느 정도 확보할 수 있어야 한다. 미국은 2016년 10월 북한의 1차 핵실험 이후 총 10차례에 걸쳐 주요한 유엔안보리 제재조치를 결의하였다. 미국은 이러한 유엔의 대북제재를 주도하였으며, 이와 별도로 독자적인 제재를 강화하고 EU, 일본, 한국이 독자적인 제재를 강화토록 협력하였다.[39] 그럼에도 불구하고 유엔안보리에서 북한에 대한 군사작전에 대한 결의와 지원을 얻어내기는 어려웠다. 중국과 러시아는 미국의 북한에 대한 군사력 사용을 항상 공개적으로 반대하였다. 문재인 대통령은 "군사적 선제타격으로 전쟁이 나는 방식은 결코 용납할 수 없다." "우리의 동의 없이 한반도 군사행동은 있을 수 없다고 미국에 단호히 밝혔다."고 강조하고 있다.[40] 미일은 2017년 11월 미일 정상회담에서 미국의 군사옵션을 논의했고 아베수상은 미국의 군사적 옵션을 선택지로 두고 있는 대북 전략을

39) U.S. Department of the Treasury, "North Korea Sanctions," https://www.treasury.gov/resource-center/sanctions/programs/Pages/nkorea.aspx(검색일: 2018. 3. 16)
40) 연합뉴스, 문대통령 "선제타격으로 전쟁나는 방식 결단코 용납못해," 2017. 12. 6.

100% 지지한다고 표명하였다지만 일본이 미국의 선제공격을 실제로 지원할 수 있었는지는 불분명하였다.[41]

특히, 트럼프 정부는 대북 선제공격에 대해 의회의 승인이나 의원 다수의 지지를 확보할 가능성, 우호적인 국민여론의 지원을 받을 가능성은 매우 낮았다. 그러나 여론은 상황에 따라 변하고 위기시 대통령을 지원하는 미국의 정치적 특성을 감안할 수 있다. 당시 공화당 린지 그램(Lindsey Graham) 상원의원은 북한의 군사기술 발전이 선제공격 가능성을 높이고 있으며, 시간이 얼마 남지 않았다고 언급하였다.[42] 그러나 민주당 의원들은 군사옵션을 반대하였으며, 트럼프 대통령이 대북 선제공격을 위해서는 의회의 승인을 받아야 한다고 주장하였다.[43] 2017년 10월 퓨연구소(Pew Research Center) 여론조사에 따르면 공화당원 68%가 미국을 직접 공격하지 않은 상대에 대한 군사력 사용을 지지할 뜻을 보였다.[44] 반면에 11월 여론조사에서 미국 국민 86.4%는 군사적 옵션이 마지막 수단으로 사용되어야 하며, 약 71%는 미국의 해외 군사개입을 제한하는 새로운 법을 의회가 제정해야 한다고 응답하였다. 특히, 미 국민들은 군사공격에 따른 인적 피해가 증대한다고 상정할 경우 군사공격에 대한 반대가 높은 것으로 나타났다.[45] 트럼프 대통령의 북한에 대한 군사공격에 대한 대내적 지원은 매우 불확실하였으며, 전략적 위험도 높은 상태였다.

트럼프 정부는 선제공격에 대한 정치적 목표를 설정하고 이러한 정치적 목표 달성을 자신하기가 어려운 상황이었다. 선제공격의 목표가 북한의 추가 핵실험이나 ICBM 시험발사를 저지시키고 제한하면서 미국의 힘을 과시하기는 비교적 용이할 수 있다. 그러나 북한의 핵개발을 포기시키고 핵능력을 완전히 제거하기

41) The Japan Times, “Abe’s support for ‘all options’ on North Korea complicates efforts to bring abductees home.” 7 Nov. 2017.
42) CNN, “A dangerous choice looms for Trump on North Korea” 8 Dec. 2017.
43) The Guardian. “Democracies push bill to stop a Trump pre-emptive strike on North Korea.” 26 Oct. 2017.
44) Newsweek. “Do Americans Want War With North Korea? Republicans For More Likely to Support Preemptive Strike Than Democrats” 28 Nov. 2017.
45) Newsweek. “Do Americans Want War with North Korea? Majority of U.S. Public is Against Military Interventions, Poles Says.” 9 Jan. 2018.

위한 목표를 달성하기는 어려운 상황이었다. 미국이 북한의 비밀 핵시설이나 핵무기 은닉장소를 모두 파악하기도 거의 불가능하였다. 오히려 미국의 군사공격은 북한이 이를 정치적으로 이용할 수 있는 명분과 기회를 줄 수 있다. 북한의 호전적 행태를 고려하건데 자칫 북한의 대응 군사행동으로 인해 한반도에 통제하기 어려운 새로운 위기를 촉발시킬 수 있는 위험도 컸다. 또한 군사공격에 의해 제한적 성과를 달성하는 것이 미국에게 실질적인 이득이 될 수 있을 가능성도 매우 불확실하였다. 핵무기 개발을 성공시킨 북한에 대한 군사공격은 이에 뒤따르는 후속적인 결과와 영향을 예측하기 어렵고 비용도 높을 수 있었다.

그럼에도 불구하고 미국은 북한에 대한 군사적 공격의 명분을 상당 수준 축적해 나갔다. 북한을 WMD 보유・확산・사용 가능성이 가장 높은 매우 위험한 국가로 지정하고 이를 국제사회에 인식시키는데 성공하였다. 김정은 정권이 인권유린 국가임을 세계적으로 확인시켰으며, 이에 대한 제재를 실시하였다. 특히, 오토 웜비어 사건은 북한을 잔인한 인권유린 국가로 명명토록 하고 대북 강경정책에 대한 대내외적인 지원을 확보토록 하였다. 미국은 2008년 북한을 테러지원국 명단에서 해제했지만 김정남의 말레이시아 공항 테러사건을 전기로 2017년 11월 테러지원국으로 재지정하였다. 유엔안보리 대북제재 결의를 지속적으로 실시하고 강화시켜 북한에 대한 보다 확실한 새로운 강제조치의 필요성을 인식시켰다.

미국은 선제공격 직전의 마지막 경고라 할 수 있는 북한에 대한 최후통첩 또한 이와 유사한 요구조건을 명확히 통보하지는 않았다. 그럼에도 불구하고 미국은 북한의 ICBM 위협을 레드라인으로 명시하지는 않았지만 이에 강력히 대응할 것임을 시사하였다. 트럼프 대통령은 당선자 신분 당시부터 북한이 미국을 직접 위협하는 ICBM 개발을 용인하지 않을 것임을 공개적으로 천명하였으며, 2017년 들어 김정은 정권과 '말의 전쟁' 강도를 높여왔다. 트럼프 대통령은 2017년 9월 유엔연설에서 김정은을 '로켓맨'으로 언급하고, 북한이 도발한다면 북한을 완전히 파괴할 것이라고 공약하였다. 8월에는 미국의 북한에 대한 군사적 해결방안 완전히 준비되어 있으며, 북한은 세계가 아직까지 본적이 없는 '화

염과 분노', 힘에 직면에 할 것이라고 위협하였다.[46] 맥매스터 국가안보보좌관은 북한과의 전쟁위협이 매일 증대하고 있다고 언급하였다. 폼페이오 CIA 국장은 북한이 수개월 내에 미국을 공격할 핵미사일 능력을 갖게 될 수 있을 것을 우려한다고 공식 표명하였다.[47]

전반적으로 트럼프 대통령의 북한에 대한 선제공격 위협은 정치적 정당성과 명분의 측면에서 보면 실효성이 높지 않았다. 미국의 과거 선제공격 사례와 비교해서 살펴보면 다음과 같은 상황을 보여 주었다. 트럼프 정부는 유엔 및 의회, 우방국 등을 포함한 대내외적인 주요 행위자들과 여론의 지원을 확보하기 어려운 상황이었다. 트럼프 대통령은 유엔안보리 결의나 지원 및 의회의 지원을 얻기 위한 공식적, 비공식적인 협의나 움직임을 보이지 않았으며, 당시 상황은 이들로부터 이러한 지원을 얻기도 불가능한 상황이었다.

특히, 미국의 선제공격을 선택하기 어렵게 하였던 변수는 군사작전을 통해서 원하는 정치적 목표를 달성하기가 어려웠으며, 선제공격 이후의 후속적인 결과 및 영향을 관리할 수 있는지도 불확실하였다. 과거 클린턴 정부와 오바마 정부 모두가 군사공격을 선택하지 않았던 이유도 군사작전의 성공여부보다는 군사작전 이후에 발생할 수 있는 후속적인 정치, 군사적인 결과와 영향을 확신할 수 없었기 때문이다. 트럼프 정부의 선제공격도 이러한 문제를 극복할 수 없는 상황이었다. 북한을 강압하기 위해서는 보다 대대적인 작전이 필요하나 이는 미국이 감당하기 어려운 비용과 피해를 야기할 수 있었다. 그렇다고 효과가 불분명하고 역효과가 보다 클 수 있는 제한적인 정밀타격을 대내외적인 지지와 협력도 없는 상황에서 이행하기도 어려웠다. 북한의 핵능력은 이미 완성단계로 발전되었기 때문에 과거에 비해 정치적 목표를 달성할 가능성은 더욱 낮아졌으며, 군사작전에 따른 위험과 비용은 통제하기 어려울 정도로 훨씬 커진 상황이었다.

그럼에도 불구하고 트럼프 정부는 북한에 대한 군사공격의 명분을 상당 수준

46) Fox News, "Trump on North Korea, from 'Rocket Man' to 'Fire and Fury'." 15 Jan. 2018.
47) The Guardian. "CIA chief draws new 'red line on North Korea nuclear buildup." 23 Jan. 2018.

축적하였던 것도 사실이다. 비록 일관성 있는 정책은 아니었지만 핵개발을 빌미로 이라크 전쟁을 개시하였던 바와 같이 이를 시급한 군사공격의 명분으로 삼을 수 있었다. 트럼프 대통령은 북한에 대해 강력한 경고를 발하였으나 북한은 유엔안보리 결의를 위반하고 핵실험과 미사일 발사시험을 지속하였다. 특히, 미국은 북한의 ICBM 시험 발사를 용인하지 않겠다고 반복하여 강조하였기 때문에 북한의 장거리 미사일 발사를 군사공격의 촉발요인으로 활용할 수 있는 기제를 갖고 있었다. 특히, 트럼프 대통령의 예측하기 어려운 행동방식은 미국의 선택에 대한 불확실성을 높여주었다. 이는 트럼프 대통령의 선제공격 위협이 보다 높은 신뢰성을 갖도록 해주는 요인으로 작용하였으며, 북한이 미국의 군사공격 가능성을 실제로 인식하고 두려움을 갖도록 해주었다고 본다.

그렇다면 미국은 선제공격을 위한 군사적 준비를 효과적으로 이행하였는가? 브룩스 한미연합사령관은 당시 미국이 군사작전을 실제로 준비하였음을 언급하였다.[48] 그렇다고 이러한 준비가 실제로 군사작전 실행을 위한 준비였는지, 단순한 군사적 옵션에 대한 검토였는지는 불확실하다. 미국은 1차 핵 위기시인 1994년, 그리고 오바마 정부 초기에 군사공격 옵션을 검토하였으나 정치적 목적을 달성할 가능성이 불확실하고, 막대한 비용과 피해가 발생할 가능성 등을 고려하여 이를 선택하지 못하였다.[49] 북한이 2017년 핵무기 완성을 선언하였다는 사실을 감안하면 트럼프 정부의 정치적, 군사적 부담은 보다 컸으며, 신중할 수밖에 없었다고 판단할 수 있다.

군사작전의 준비와 관련한 실질적인 조치들은 거의 보도되지 않았으나 군사력 배치 및 증강 등과 관련된 움직임은 가시적으로 보여 주었다. 예를 들면, 북한에 대한 작전의 가장 중요한 책임자들인 주한미군사령관과 합참과 조직들의 선제공격과 관련된 특이한 군사적 움직임에 대한 보도는 없었다. 미국은 2017년 들어 비전투원 철수작전에 대한 연습을 실시하고 이를 개선하기 위해 노력하

48) 세계일보, “브룩스 전 한미연합사령관 ‘2017년은 전쟁에 가까워져… 대화 안하면 오산 위험,” 2019. 1. 24.
49) Woodward, Bob, Fear: Trump in the White House(New York: Simon & Schuster, 2018), pp.94-95.

고 있음을 밝혔으나,[50] 실제 선제공격을 대비한 군사적 조치의 준비는 확인되지 않았었다. 그러나 미국은 북한과 관련된 정찰・감시 활동을 상시 수행하고 있으며, 군사작전 계획을 항시 발전시키고 있고, 매년 다양한 형태의 군사 연습・훈련을 실시하고 있기 때문에 제한적 정밀타격 군사작전은 손쉽게 준비하고 이행할 수 있었다. 특히, 2017년 미국은 북한에 대한 무력시위를 강화하였다. 2017년 9월에는 B-1B 전력폭격기가 주일미군 F-15C와 함께 동해 공해상에서 NLL을 넘어 비행하는 무력시위를 실시하였다. 트럼프 대통령의 방한 기간인 11월에는 3개 항모강습단이 한반도 근해에 집결하여 한국군과 합동연습을 실시하였다. 핵무기 투발이 가능한 전략폭격기 B-2 3대와 B-52H를 2018년 1월 괌에 배치하여 훈련을 실시하였다. 또한 주한미군은 2018년 2월 최신형 무인공격기 '그레이 이글(MQ-1C) 12대로 구성된 중대를 군산에 창설하였으며, 이를 4월부터 정식 운용할 것이라고 밝혔다.[51] 미국은 북한의 도발시 수시로 전략폭격기를 한반도에 전개하여 무력시위를 실시하였다.

군사적 준비는 전반적으로 미국의 제한적인 군사작전에 대한 위협의 실효성은 높았으나 대규모적인 군사작전의 위협은 실효성이 상대적으로 낮았음을 말해준다. 미국은 주한미군과 주일미군, 전략자산 등을 활용하여 제한적인 표적에 대한 정밀타격과 같은 군사작전은 손쉽게 준비하여 선택하고 이행할 수 있는 능력을 갖추고 있다. 이러한 제한적인 군사작전은 미군의 능력을 고려하건데 자신감을 갖고 신속하고 결정적으로 이행하여 원하는 군사적 목표를 달성할 수 있도록 할 수 있다. 그러나 사전 철저한 준비와 계획이 요구되는 대규모의 대대적인 군사공격을 준비하고 이행하고자 하는 움직임은 보이지 않았으며, 이러한 작전을 전달하기 위한 정치・군사적 커뮤니케이션도 이루어지지 않았었다,

종합적으로 보면 트럼프 정부의 북한에 대한 선제공격 위협은 북한을 압박하여 공포를 조성하고 북한의 행동을 강압하는 효과는 있었으나 북한에 핵포기를 강압할 수 있는 수단으로서 실효성은 높지 않았다. 북한의 핵개발 상황과 당시

50) 뉴스타운, "미 국방부, 한반도 유사시 주한미군 가족 철수 작전 개선중," 2018. 2. 21.
51) 한국일보, "주한미군 무인 공격기 '그레이 이글' 부대 창설," 2018. 2. 21.

의 정치적 여건은 트럼프 정부가 선제공격에 대한 정당성과 명분을 얻기 어렵게 하였으며, 군사공격의 선택 옵션이 제한되었고, 이를 통해 정치적 목적을 달성할 가능성도 크지 않았다, 또한 군사공격 이후 발생할 수 있는 정치, 군사적인 후속적인 결과와 영향을 관리하기도 매우 어려운 상황이었다. 트럼프 정부의 선제공격 위협에도 불구하고 한국사회는 비교적 안정된 모습을 보였으며, 북한은 트럼프 대통령과 말의 전쟁을 지속하고 핵 실험과 미사일 발사 시험을 감행하였다. 이러한 상황은 역으로 관련 행위자들이 미국의 군사위협이 안고 있는 한계를 인식하고 반응하였다고 판단해야 할 것이다.

6. 결 론

트럼프 대통령의 2017년 북한에 대한 강력한 선제공격 위협은 이를 뒷받침하기 위한 빈번한 무력시위 등에도 불구하고 정치적 실효성이 높지 않았다. 물론 트럼프 대통령의 독단적 행동이라는 변수를 고려하면 위협의 강도가 전례 없이 높았다고 할 수 있다. 그러나 미국의 군사공격 시 주요 정치·군사적 고려요소와 과거 선제공격 사례들은 트럼프 대통령이 대북 선제공격에 대한 정치적 명분과 정당성을 확보하기 어려웠다는 사실을 말해준다. 비록 북한의 핵실험 및 미사일 시험발사가 군사공격의 명분과 촉발요인을 제공할 수 있었지만 이것만으로 선제공격을 정당화하기는 어려웠다. 무엇보다 군사공격을 통해서 원하는 정치적 목표를 달성하기 어려웠으며, 정치적 목표 달성을 위해서 대대적인 군사공격을 계획하기도 어려웠다. 비록 제한적인 정밀타격을 성공적으로 이행할 수 있었지만 이는 문제를 해결하기보다는 정치적 상황을 보다 어렵게 할 가능성이 높았다. 즉, 정치적 목표를 달성하기 위한 군사적 방법 및 수단이 사실상 매우 제한되었으며, 이는 트럼프 대통령의 구두위협에도 불구하고 한반도 안보상황이 안정적인 모습을 보여주었던 이유이기도 하다.

2017년 트럼프 대통령의 대북 선제공격 위협 사례는 향후 미국이 북한에 대한 군사적 옵션을 선택하기 어려울 것이라는 사실을 말해준다. 비록 트럼프 정부는 북한에 대한 군사옵션이 항상 책상 위에 놓여있다고 언급하지만 이러한 수사적 위협의 실효성은 보다 낮아지고 있다. 왜냐하면 북한의 핵능력이 실제로 강화되고 관련국들이 이를 반대하고 있는 상황에서 정치적 목적의 달성을 보장할 수 있는 군사적 방법과 수단을 찾기가 어렵기 때문이다. 또한 이는 미국이 북한 비핵화 협상에서 제재 레버리지를 중시하고 이를 양보하거나 포기하지 않고자 하는 정책적 이유를 설명한다, 미국의 강압전략은 군사적, 경제적 수단을 모두 활용하여 추진되었다. 군사적 수단은 가장 직접적이고 효과적인 수단이다. 그러나 북한에 대한 군사적 수단의 효용성이 떨어진 상황에서 미국은 북한 비핵화를 위해 경제적, 외교적 레버리지를 보다 효과적으로 사용하기 위한 방안을 지속 강구할 것으로 예상된다.

참고문헌

1. 단행본

이근욱.「이라크 전쟁: 부시의 침공에서 오바마의 철군까지」. 서울: 한울아카데미, 2011.

박창권.「최근 전쟁사례를 중심으로 한 해군력의 역할 분석」. KIDA 연구보고서 안 04-2049. 2004

KIDA,「NSS 2017: KIDA의 분석과 NSS 요약」. 서울: KIDA, 2017.

Bush, George W., Decision Points. New York: Crown Publishers, 2010.

Cole, Ronald H. *Operation Just Cause: Panama*. Washington, DC.: Joint History Office: Office of the Chairman of the Joint Chiefs of Staff, 1995.

Cole, Ronald H., *Operation Urgent Fury: Grenada.* Washington, DC., Office of the Chairman of the Joint Chief of Staff, 1997.

Dale, Catherine, *Operational Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress*(Congressional Research Service, 28 March 2008), CRS Report for Congress, RL34387.

Flyn, Matthew J. *First Strike*, 임은성 역,「선제전쟁: 시작과 종말, 그리고 제한된 보상」. 서울: 북코리아. 2011.

Muller, Karl P. and others, Striking First: Preemptive and Preventive Attack in U.S. National Security Policy. RAND, 2006.

Oberdorfer, Don, *The Two Koreas: Contemporary History*. Indianapolis: Basic Books. 1997.

Stewart, Richard W. *Operation Urgent Fury: The Invasion of Grenada, October 1983.* CMH Pub 70-114-1. U.S. Army Center for Military

History, 2008.

Taw, Jennifer Morrison, *Operation Just Cause: Lessons for Operations Other Than War*. RAND Arroyo Center, 1996.

The President of the United States, *National Security Strategy of the United States of America*, The White House, December 2017.

The U.S. Joint Chief of Staff, *Joint Planning: Joint Publication 5-0*. Washington. DC. 16 June 2017.

Trump, Donald J. and Tony Schwartz, *Trump: The Art of The Deal*. New York: Ballantine Books, 1987.

Wit, Joel S., Danniel B. Poneman, and Robert Gallucci. Going Critical: The First North Korean Nuclear Crisis, 김태현 역,「북핵위기의 전말: 벼랑끝의 북미협상』(서울: 모음북스). 2005.

Woodward, Bob, *Fear: Trump in the White House*. New York: Simon & Schuster, 2018.

2. 논문

Buttler, Michael J. "U.S. Military Intervention in Crisis, 1945-1994: An Empirical Inquiry of Just War Theory," *The Journal of Conflict Resolution*, Vol. 47, No.2(Apr. 2003). pp.226-248.

Himes, Kenneth R.. "Intervention, Just War, and U.S. National Security," *Theological Studies*, Vol. 65, Iss. 1(February 2004), pp.141-157

Wester, Franklin Eric, "Preemption and Just War: Considering the Case of Iraq," *Parameters*(Winter 2004-05), pp.20-33

3. 신문

뉴스타운, “미 국방부, 한반도 유사시 주한미군 가족 철수 작전 개선중,” 2018. 2. 21.

세계일보, “브룩스 전 한미연합사령관 ‘2017년은 전쟁에 가까워져… 대화 안하면 오산 위험,” 2019. 1. 24.

연합뉴스, “문대통령”선제타격으로 전쟁나는 방식 결단코 용납못해, 2017. 12. 6.

한국일보, “주한미군 무인 공격기 ‘그레이 이글’ 부대 창설,” 2018년 2. 2.

BBC, “Syria war: World reaction to US missile attack,” 7 April 2017.

Business Insider, “The US is reportedly considering a ‘bloody nose’ attack to humiliate North Korea–here’s how it could go down,” 9 Jan. 2018.

CNN, “A dangerous choice looms for Trump on North Korea” 8 Dec. 2017.

CNN, “Trump launches military strike against Syria,” 7 April 2017.

Daily Beast, “CIA Boss Gives Latest Indication Trump May Consider Preemptive Strike on North Korea,” 23 Jan. 2019.

Fox News, “Trump on North Korea, from ‘Rocket Man’ to ‘Fire and Fury’.” 15 Jan. 2018.

Newsweek. “Do Americans Want War With North Korea? Republicans For More Likely to Support Preemptive Strike Than Democrats” 28 Nov. 2017.

Newsweek. “Do Americans Want War with North Korea? Majority of U.S. Public is Against Military Interventions, Poles Says.” 9 Jan. 2018.

New York Daily News. “Majority of Americans support Trump’s Syria

missile strike: poll." 10 April 2017.

The Guardian. "CIA chief draws new 'red line on North Korea nuclear buildup." 23 Jan. 2018.

The Guardian. "Democracies push bill to stop a Trump pre-emptive strike on North Korea." 26 Oct. 2017.

The Japan Times, "Abe's support for 'all options' on North Korea complicates efforts to bring abductees home."" 7 Nov. 2017.

The New York Times. "Target Qaddafi." 22 Feb. 1987.

The New York Times, "U.S., Britain and France Strike Syria Over Suspected Chemical Weapons Attack," 13 April 2018.

The Telegraph. "Assad bears full responsibility': how the world reacted to Donald Trump's missile strike on Syria." 7 April 2017. CNN, "A dangerous choice looms for Trump on North Korea," 8 Dec. 2017.

The Telegraph. "How Panama's military dictator Manuel Noriega was defeated by rock'n roll," 30 May 2017.

The Telegraph, "US preparing 'bloody nose' syber attacks on North Korea, 20 Feb. 2018.

Washington Examiner, "The 'bloody nos' option is a direct path to war with North Korea," 15 Jan. 2018.

4. 인터넷 자료

Carina, Piazza Della, "On April 14th 1986, Ronald Reagan ordered a series of bombings directed against Libya under "Operation El Dorado Canyon"." 15 April 2013, https:piazzadcarina.wordpress.com (검색일: 2019. 3. 15), pp.1-3.

Endicott, Judy G. "Operation Eldorado Canyon," in *Short of War USAF*

Contingency Operations 1947-1997. https://media.defense.gov. (검색일: 2019. 3. 15)

One Hundred Eventh Congress of the United States of America, "Text of S.J.Res. 23. (107th): Authorization for Use of Military Force, http://www.govtrack.us/congress/bills/107/sjres23/text(검색일: 2019. 3. 4)

U.S. Department of the Treasury. "North Korea Sanctions," https://www.treasury.gov/resource-center/sanctions/programs/Pages/nkorea.aspx(검색일: 2018. 3. 16)

Zunes, Stephen. "The US Invasion of Grenada" Global Policy Forum: Foreign Policy in Focus, Oct. 2003(https://www.globalpolicy.org/component/content/article/155/25966.html(검색일: 2019. 3. 6)

Abstract

A Study on the Actual Effect of 2017 Preemptive Attack Threat to North Korea by Trump Administration in Comparison to the Past Cases of US Military Attack

Park, Chang Kwoun (Korea Institute for Defense Analyses)

It was widely perceived that President Trump would choose preemptive attack option in 2017 to enforce North Korea give up its nuclear program. President Trump carried out maximum pressure strategy and at the same time escalated the overt threat of preemptive attack on North Korea. 'War of Words' between Trump and Kim practically enhanced such a possibility. General Brooks, the Commander of US Forces in Korea at the time, mentioned recently that the US actually considered military option on North Korea in 2017. Nevertheless, it was questionable that North Korea perceived US threat on preemptive attack as a real one. In fact, North Korea aggressively responded to the Trump's threat without showing much fear on the coming military attack. Also, South Korea which could get affected severly by the US military action remained relatively calm under the tense situation. This paper is to evaluate the actual effect of President Trump's preemptive attack threat to North Korea with major factors which the US considers most importantly in calculating military attack. In addition, it examined and draw implication from the previous cases of US military attack

overseas toward 2017 North Korea situation.

Key Words: U.S. preemptive attack, military options, North Korea nuclear program

투고일: 2019.05.17 심사일: 2019.06.03 게재확정일: 2019.06.05.

필진 소개

(가나다순)

박창권

한국국방연구원 연구위원, 미국 미주리 대학교 정치학 박사. 주요 관심은 전쟁 및 분쟁, 한미동맹, 핵전략, 해양안보, 남북관계 및 국방전략 등이며, 주요 저서는 미중관계 전망과 한국의 전략적 대응 방향(2010, 공저), 한국의 중장기 안보전략과 국방정책(2011, 공저) 등이 있음

장노순

한라대학교 경찰행정학과 교수. 플로리다주립대학교에서 정치학 박사를 취득했음, 주요 관심 분야는 사이버안보, 안보전략이론, 정보활동과 정책, 기술과 국제안보 등임. 주요 연구실적은 〈국제관계와 신뢰외교〉 (공저), "정보기관에 대한 민주적 통제와 미국의 경험," "사이버안보와 선도국 우위의 전략적 선택," "한반도에서 중층적 안보구조와 고비용의 신호," "사이버 안보위협과 사이버 방첩의 역할과 전략" 등 다수의 논문이 있음.

함명식

중국 지린대학 공공외교학원 부교수, 지린대학 국제관계사 박사, 주된 연구 주제는 중국외교정책, 한중관계, 북중관계, 동아시아 국제정치. 주요 연구 성과로는 Socialization of China's Soft Power: Building up Friendship through Potential Leaders (공저, 2018), From Autonomous Areas to Non-Autonomous Areas: The Politics of Korean Minority Migration in Contemporary China (공저, 2012), '중국 특색의 세계화 전략'에 대한 재중 아프리카 유학생들의 인식 조사 (2018), 중국의 대한국 공공외교 성과와 한계 분석: 시진핑 집권 시기를 중심으로 (공저, 2017), 북한-중국 동맹관계에 대한 이론적 재고찰: 약소국의 비대칭 전략과 자율성 증가 (2016) 등이 있음.

홍석훈

통일연구원 연구위원. 미국조지아대학 정치학박사. 주요 관심은 북한외교 · 정치, 북미관계 및 동북아국제관계, 남북관계, 한반도 평화체제. 주요 논문과 저서로 “North Korea’s Transition of its Economic Development Strategy: Its Significance and the Political Environment of the Korean Peninsula”, 『The Korean Journal of Defense Analysis』 Vol. 30 No.4,(2018), 『한반도 평화의 국제정치학』 공저(2018), 『12개 주제로 생각하는 통일과 평화, 그리고 북한』 공저(2019) 등.

최근 발간자료 안내

2012 국제문제연구

| 봄호 |

1. 핵비확산과 국제정치학과 정책대안 — 최아진
2. 오바마 행정부의 새 국방전략 평가 : 긴축재정하의 '선택과 집중' — 이동준
3. 신국제질서의 태동에 대한 미국의 인식과 전략 — 조성렬
4. 북한의 서해상 도발리스크에 대한 테계적 관리모델의 개발 : 인디케이터 분석모델의 적용을 중심으로 — 손효종 · 김재호 · 김용호
5. 지지율로 본 조지 W. 부시 대통령의 임기 — 가상준

| 여름호 |

1. 서울 핵안보 정상회의와 글로벌 거버넌스를 위한 한국의 역할 — 손기영
2. 미국 대외정책에서의 체제전환정책과 한국적 함의 — 박인휘
3. 중국의 부상과 일본 안보전략의 변화 — 신정화
4. EU FTA협상전략에 관한 삼차원 게임이론 분석 : 한-EU FTA 사례를 중심으로 — 김현정
5. 2011~2012 러시아 총 · 대선 결산 : 평가와 시사점을 중심으로 — 장세호
6. 푸틴 집권3기 대외정책 전망과 對 러 대응전략 — 서동주
7. 김정은 시대의 북한과 대북정책 아키텍처(Architecture) : 공진화 전략과 복합적 관여정책의 모색 — 김성배
8. 북한의 핵 · 미사일 위협에 대한 한국의 미사일 방어대채 — 박휘락

| 가을호 |

1. 한미 동맹과 한중 전략적 협력관계 ; G2시대 한국의 전략적 선택을 중심으로 — 차창훈
2. 한국의 해양안보위협의 변화와 전개양상에 관한 연구 : 미국의 新 국방전략지침 발표 이후 미·중 경쟁을 중심으로 — 백병선
3. 중국의 '대전략' 논쟁에 관한 연구 : 비판적 시각에서 — 차이동지애
4. 국방개혁 : 유럽 사례분석을 통한 한국적 함의 — 박민형
5. FTA 협상 분석의 이론적 틀 : 협상 구조와 과정을 중심으로 — 김기홍
6. 이익집단정치와 미국의 다원주의 : 유태계 미국인 사례를 중심으로 — 유성진

| 겨울호 |

1. 제2기 오바마 정부의 동북아시아 외교정책 추진방향 분석 — 김정현
2. 한탈냉전기 군사혁신론과 오바마 행정부 시기 미 공군의 군사혁신 — 엄정식 · 설인효
3. 중국공산당제 18차 당 대회와 중국의 대외정책 전망 — 신종호
4. 일본 FTA 정책의 변화 — 손준헌
5. 국제사회의 북한인권 개입과 남북한의 대응 — 정주신
6. '인간안보'의 북한적 함의 : 북한인권문제 개입을 중심으로 — 이승열
7. 민간외교 활성화를 위한 정부의 역할에 관한 일 연구 : 45개 민간외교단체 서베이 결과를 중심으로 — 송경재 · 김형호

2013 국제문제연구

| 봄호 |

1. 오바마 행정부의 핵비확산 정책과 미국의회 — 황지환 · 최아진
2. 개혁개방이후 시민사회논의의 중국적용에 대한 적실성 고찰 : 종교영역관련 비영리단체활동사례들을 중심으로 — 박만준
3. 아시아 금융감독 거버넌스의 구조와 함의 — 김치욱
4. 남북관계 세가지 제약요인과 대북정책 — 임재천

| 여름호 |

1. 한반도 정전 60년, 실패한 정전협정 혹은 성공한 정전체제? 김재한
2. 인터넷 규제와 소셜미디어 선거운동의 영향력
   : 종교영역관련 비영리단체활동사례들을 중심으로 차재권
3. 갈등적 동아시아 해양질서 : 국제조약, 국제레짐 그리고 패권 도전국 전기원
4. 중앙아시아 정치공간의 인문 지리학적 구조
   : 내재적 문화 복원과 외재적 문화 침투 현상을 중심으로 이영형

| 가을호 |

1. 독도 방어 능력의 발전 방향 : 포클랜드 전쟁의 교훈을 중심으로 김재엽
2. '투키디데스'가 바라 본 북중군사관계의 동인(動因)
   : 펠로폰네소스 전쟁사를 중심으로 강정일
3. 이명박 정부의 에너지 외교 정책 : 평가와 정책적 시사점 최원기

| 겨울호 |

1. 중국의 미중 신형대국관계 구축제의와 함의 유희복
2. 일본 '무기수출 3원칙' 완화 과정의 배경과 전망 정재욱
3. 미국의 유럽 미사일방어(MD) 추진과 러시아의 대응 고재남
4. 국제안보환경 변화와 한국의 전략적 항공수공능력 발전방향 남창희 · 김순태
5. '80년대 남북관계와 한국사회의 대북관 : 이상과 현실 남성욱

2014 국제문제연구

| 봄호 |

1. 중국의 민주화 : 2010년 선거법개정안을 중심으로 유현정 · 민태은
2. 냉전시대 그린데탕트의 경험과 남북한 환경협력에 대한 시사점 고상두
3. 비전통안보 부상과 아 · 태지역 미국 주도 동맹체제 강호 : 한미동맹의 함의 박재적 · 김동수
4. 남한의 '3단계 통일방안'과 북한의 '연방제'에 있어 정당역할 남광규

| 여름호 |

1. 이어도 분쟁의 가능성과 대응방안 : 중국의 민족주의적 접근을 중심으로 고경민
2. 중국의 대한국 외교관계 변화 연구 곽덕환
3. 네트워크 이론의 관점에서 본 북핵문제와 6자 회담 전재성
4. 프랑스 민족전선(FN) 지지기반 확대 : 이민문제와 정치화 김민정
5. 냉전기 한국의 지역협력 외교 : 박정희의 국가건설구상과 ASPAC 창설 이용철
6. 호주와 스웨덴의 성인지 예산제도의 비교를 통한 한국에의 함의 설진배 · 최성은
7. 세월호 참사와 위기관리체계 : 문제점과 개선방향 허태회

| 가을호 |

1. 지정학적 완충체계 이론과 한반도 김연지
2. 중국과 러시아의 북한 동북부 진출과 유라시아 동부지역 Pivot area의 성격 이영형
3. 중동 독재국가 군부의 분영양상과 민주주의 혁명 김인수
4. 핵무장국 사이의 제한전쟁 수행과 한반도에의 적용
   : 1999년 인도·파키스탄의 카르길 전쟁사례를 중심으로 김재엽
5. 그린데탕트의 개념과 추진전략 경제희 · 김재한
6. 북한핵문제의 다차원적인 접근 : 전통적-비전통적 안보의 동시병행 중심 이윤식
7. 소셜 빅데이터를 활용한 북한관련 위협인식 요인 예측 송주영 · 송태민

| 겨울호 |

1. 초연결사회의 사이버위협에 대비한 국가안보 강화방향 이상호
2. 글로벌 세력전이와 한국의 중견국 외교 : 대 브릭스(BRICS)전략을 중심으로 김치욱
3. 북한주민에 대한 효과적인 블렌디드 러닝 방안과 정책 방향 채정민
4. 사이버 안보위협의 문제와 전략적 의미, 그리고 대응방안에 대한 연구 윤민우
5. 생물안보와 안보전략의 이중구조: 생물무기의 방어수단과 공격대상으로서 함의 장노순
6. 식량안보를 위한 국가정책 : 역사적 평가(해방후~2012) 조성권
7. 한국형 통합위기관리체제 도입의 필요성과 대안모색 이홍기 · 박준석 · 권혁빈
8. Community Participation Process and Publric Administration Reforms in Vietnam
   : Obstacles and Challenges Ngo Viet Hung · So Jin Kwang

2015 국제문제연구

| 봄호 |

1. 러시아의 에너지 무기화 전략과 미국의 대응
   : 셰일혁명이 글로벌 에너지 질서 및 전략판도에 미치는 영향 — 김충남

2. 주한미군 감축과 한미동맹의 방향성에 대한 분석 — 이정우

3. 시진핑의 '발전자'대외정책경향과 중국의 대외정책 특징
   : 마가렛 허만의 최고지도자 '인격특징'이론을 중심으로 — 이민규

4. 크림반도의 러시아 귀속과 중·러관계 전망
   : 협력과 갈등 그리고 회피 — 김진용·연성흠

5. 대한민국 평화유지활동의 신패러다임
   : 스마트파워 강화를 위한 국방·외교 전략 — 최윤미

6. 국제사회의 대북한 공적개발원조에 대한 탐색적 분석 — 정헌주·박건우·이윤아

| 여름호 |

1. 2009-2015년 중국과 러시아의 중앙아시아에서의 협력과 경쟁 — 김연규

2. 2011년 정상회담 이후 러·북관계: 러시아의 대북 인식 분석 — 우평균

3. 북한의 권력승계는 왜 안정적인가?
   : 지배의 정당성과 북한 권력승계의 안정성 — 이지원

| 가을호 |

1. 한미동맹과 미일동맹의 실태 비교 : 동맹구성요소를 중심으로 — 박휘락

2. 김정은 시대 북한의 경제·핵무력 병진노선의 의미와 평가 — 권숙도

3. 북한문제를 둘러싼 한중간 안보 딜레마 — 정재홍

4. 북한 잠수함발사탄도미사일(SLBM)의 실증적 위협 분석과 한국안보에의 함의 — 이경행·임경한

5. 일대일로(一代一路)와 중국의 21세기 세계전략 형성 — 이지용

6. 안보수단의 비대칭화와 안보딜레마의 전이 — 장노순

7. 국제관계에서 '신뢰'의 세 가지 이미지 — 김상훈·윤용석

| 겨울호 |

1. 한국의 안보위협 변화에 대한 전망 — 윤종준 · 백병선
2. 현대테러리즘의 진화 추세에 따른 연구접근 방법론 고찰 — 조용만
3. 통일 25주년 동서독 사회통합에 대한 경제적 평가 — 고상두
4. 독일 통일 후 구동독지역 노동시장의 변화와 통일정책적 시사점 — 고명덕

2016 국가안보와 전략

| 봄호 |

1. 한국군 파병국가에 대한 공적개발원조 현황과 과제 — 김인수
2. 아태 재균형과 중미 신형대국관계 구축의 전개 현황 분석
   : 상호 경쟁과 협력의 이중성을 중심으로 — 유희복
3. 2008년 광우병 시위에 관한 국내연구의 성과와 한계 — 심양섭
4. 중국의 대북정책 변화 가능성에 대한 소고
   : 2000년 이후 미중관계 변화와 중국의 대북 딜레마를 중심으로 — 이기현
5. 시진평 시기 중국의 부패 통제 메커니즘
   : 공산당 권력 강화와 의법치국 사이의 딜레마 — 김진용
6. 투키디데스의 펠로폰네소스 전쟁 원인 고찰:
   신고전적 현실주의 접근을 중심으로 — 정재욱

| 여름호 |

1. 한미동맹의 동맹 딜레마와 향후 한국의 한미동맹 전력 — 전재성
2. 한반도 안보환경 변화에 따른 항공전략 정립방향 — 정표수
3. 국가안보에 따른 국가핵심기술 수출통제제도의 국제통상법적 허용성 — 이상미
4. 중국공군의 현대화 추세와 동아시아 안보 — 이성훈
5. 북한 민법의 의사표시제도 — 김영규

| 가을호 |

1. 김정은 체제 변동 가능성과 추동 전략 — 김열수 · 김경규
2. 남중국해 美 · 中간 해양갈등 분석 및 한국의 대응방향 — 백병선
3. 한 · 중간 이어도 분쟁과 유형별 대응방안 — 고경민
4. 한국전쟁 발발과 미국 트루먼 행정부의 정보실패 — 석재왕
5. 21세기 일본의 대외정보기구 창설 관련 논의동향과 그 함의 — 이상현
6. 호주와 일본의 대아세안 지원 협력 비교
   : 다자 효용성을 중심으로 — 배기현
7. 글로벌 대테러리즘 포럼(Global Counterterrorism Forum) 참여에 대한 한 · 일 비교 — 엄정식 · 조재원

| 겨울호 |

1. 미국의 사이버 전략에 관한 연구
   : 북한, 중국, IS에 대한 목표, 방법, 수단의 비교를 중심으로 — 표상호 · 정맹석 · 조관행
2. 분점정부에서 미(美) 연방의회 다수당 지도부에 대한 여론 — 민태은
3. 중국동포정책의 통일 및 경제 측면에서의 의의 — 심양섭

2017 국가안보와 전략

| 봄호 |

1. 트럼프 시대 미러관계의 개선전망과 동북아에 대한 함의 — 고상두
2. 푸틴-아베 재집권(2012)이후 러 · 일 관계변화 동인과 전략적 함의 — 김정기
3. 미국에서 북핵 문제 정세 재평가와 정책 논쟁 (2016-2017.2) — 박형중
4. 북핵 고도화와 대응방안 모색
   : 선제공격 제한성의 극복방안을 중심으로 — 이성훈 · 김한규
5. 중국 미사일방어망(Missile Defense)의 역사와 한반도에 대한 함의 — 이상호 · 안성규
6. 일본 사이버안보 전략의 변화 — 이승주
7. 미국의 아프가니스탄 전쟁 목표와 전략의 변화양상
   : 대테러전과 대반란전 논쟁을 중심으로 — 윤태영

| 여름호 |

1. 미국과 중국의 사이버안보 전략과 한국의 안보정책에 대한 함의 — 김소정 · 양정윤
2. 사이버안보와 선도국 우위의 전략적 선택 — 장노순
3. 한국 사이버안보 대응체제에 관한 민 · 관 인식의 격차 — 황기식 · 김현정
4. 2003년 이라크전 유지연합(Coalition of the Willing) 참여 동기에 대한 연구 — 양희용
5. 공세적 대북 안보전략의 실행 조건
   : 북한의 핵, 미사일 위협에 대한 대응을 중심으로 — 문순보

| 가을호 |

1. 신정부의 대미정책 및 한미관계 — 김현욱
2. 문재인 정부의 대일정책
   : 한국 외교의 '대전략'과 한일관계 — 남기정
3. 문재인 정부의 대러시아 중점협력과제와 극대화 전략 — 이영형
4. 북핵 고도화와 새로운 대북정책의 모색
   : 공세적 핵전략으로의 진화와 우리의 대응전략 — 홍석훈 · 나용우
5. 트럼프정부의 대북정책과 전개방향 전망 — 이영균 · 이범찬
6. 얽힘 이론과 동맹의 안보 딜레마
   : 한미동맹 사례 — 이수형
7. 플랫폼모델을 통한 공공외교 전략 분석 — 남석상

| 겨울호 |

1. 미국 의회의 북한 관련 입법 활동 분석
   : 법안 발의의원과 발의 네트워크를 중심으로 — 구본상 · 최준영 · 김준석
2. 일대일로(一帶一路) 구상의 지경학(地經學)
   : 중아합작(中俄合作) 대 연아타중(連俄打中) — 이왕휘
3. 경제제재의 비의도적 효과에 대한 고찰과 대북제재에의 함의 — 박지연
4. 포스트냉전 시대 동아시아공동체 담론의 이상과 현실
   : 동아시아시대 한국의 지정학적 운명 극복을 위한 길 — 고성빈
5. 사이버공간의 특성과 안보화 문제 — 문인철

2018 국가안보와 전략

| 봄호 |

1. 중국 특색의 '사이버 안보' 담론과 전략, 제도 분석 — 차정미

2. 미국의 안보정책과 한국군의 국방력 발전방향
: 군사적 역할을 중심으로 — 김순태

3. 김정은 정권의 핵개발 동기와 지속 요인
: Scott D. Sagan의 핵개발 동기 모델의 확장 — 부승찬 · 박경진

4. 트럼프 행정부 FTA 정책의 탈국제정치화와 국내정치화 — 박진수

5. 아베 정부의 글로벌 외교
: 국제공헌 확대 외교의 모순성 — 이기태

| 여름호 |

1. 해외 방첩법제 비교를 통한 정책적 시사점 연구 — 허태회

2. 북한의 대중 석탄수출에 대한 유엔 안보리 분야별 제재의 한계 — 김현경 · 김성진

3. 무력분쟁 재발 이론으로 보는 서해교전의 발발원인
: 북한의 도발방식 변화 — 송태은

4. 베트남에 대한 중국의 경제지원과 경제제재, 1960~1978 — 최규빈

| 가을호 |

1. 이스라엘의 핵전략과 군사력 건설이 북한에 주는 함의 — 김태현

2. 동북아플러스책임공동체
: 제도화된 협동을 위한 조건과 노력 — 박창건

3. 강성 권력과 연성 권력 측면에서 바라본
사우디아라비아와 이란의 주도권 경쟁 — 세이훈 마흐무들루 · 신상윤

4. 영미법계 국가의 대테러정책과 형사특례절차 연구 — 윤해성 · 임유석

| 겨울호 |

1. '인도-태평양' 구상
   : 배경과 현황, 그리고 함의 — 김재엽

2. 미국-적대국간 관계정상화를 통해 본 북·미 관계정상화 가능성에 관한 연구
   : 중국, 베트남, 리비아, 쿠바 사례와의 비교 — 박경진 · 김용호

3. 한국 언론의 중국 뉴스 보도 경향에 관한 연구 — 양갑용 · 장영태

4. 미중 패권 경쟁과 북미 관계
   : 부시 행정부에서 트럼프 행정부 시기를 중심으로 — 이원영

5. 북한의 헌법 개정과 권력구조 변화 — 최선 · 김재우

2019 국가안보와 전략

| 봄호 |

1. 비핵평화 프로세스와 대북 관여정책의 지속성
   : 이론과 정책 — 박인휘

2. 21세기 일본의 대중국 견제정책의 원인 — 김태중

3. 미국의 군사부문 혁신(1977-1991)에 대한 RMA적 사후해석의 극복
   : 카터 행정부의 '상쇄전략'에 대한 기술 기회론적 분석을 중심으로 — 박상연

4. 일본의 사이버안보 수행체계와 전략 — 이상현

『국가안보와 전략』 원고모집

국가안보전략연구원에서는 학술지『국가안보와 전략』을 연 4회(3・6・9・12월) 발간하고 있습니다. 이 학술지에는 국제정세, 안보, 북한・통일문제, 남북문제, 주요국가의 외교정책과 국가전략 등 외교・안보 전 부문에 관한 논문을 수록합니다.

저희 연구원에서는 이 분야의 학술 및 연구활동에 종사하시는 분들의 논문 기고를 환영합니다. 보내주시는 기고문은 소정의 심사를 거쳐 게재하고, 채택된 원고에 대하여는 소정의 원고료를 지급하며, 기고문은 반환하지 않습니다. 저희 연구원에서는 시사 또는 학술적인 내용으로 독창적이고 정책 대안이 담긴 논문을 선호함을 밝힙니다.

기고문은 200자 원고지 150매 내외를 기준으로『국가안보와 전략』출간물을 참고하여 작성하시되 600자 내외의 서술식 국・영문 요약문도 작성해 주셔야 합니다. 기고문은 최종원고와 요약문을 기고자의 연락처와 함께 편집위원회 E-mail 주소(publication@inss.re.kr)로 보내주시기 바랍니다.

『국가안보와 전략』 편집위원회



INSS
INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

92
9 772466 225006
ISSN 2466-2259