사이버 공간의 평화적 이용을 위한 이론과 전략의 탐색

한 인 택

(제주평화연구원 연구위원)

사이버 공간의 평화적 이용을 위한 이론과 전략의 탐색

목차

I. 사이버 시대의 평화와 안보

새로운 기술의 등장은 새로운 안보적 위협과 과제, 기회를 낳고 심지어 국제관계의 성격도 변화시킬 수 있다. 과거 잠수함이나 인공위성 기술의 발전이 그랬듯이 정보통신기술의 발전도 여러 차원에서 안보적 위협과 기회를 낳고 있다. 따라서 정보통신기술의 발전이 주는 안보적 위협과 기회를 잘 이해하고 그에 대응할 필요가 있는데 이는 쉽지 않은 일이다. 기술은 계속해서 발전하며, 기술발전의 궤적은 종종 선형적이지 않기 때문이다. 새로운 기술은 전혀 예상치 못한 파급효과를 낳는가 하면, 때로는 기대에 못 미치는 결과를 낳기도 한다. 새로운 기술이 얼마나, 어떻게 발전할 것인지를 이해하고 예측하기란 지난한 일이다.

새로운 기술은 불가피하게 예측불가적인 특징이 있다. 뿐만 아니라 기존의 제도나 관념이 새로운 기술의 안보적 함의를 이해하고 대비하는 데에 장애가 될 수 있다. 새로운 기술의 등장은 기존의 제도와 조직, 그리고 기존의 관념이나 발상의 변화를 요구할 수 있는데, 기존 제도와 사고의 '관성'이 필요한 변화를 막는 장애요인이 될 수 있기 때문이다. 예를 들어 전통적인 의미의 안보와 평화를 담당해온 기존의 조직과 제도가 사이버 시대의 안보와 평화를 담당하기에 적당하지 않을 수 있으며, 전통적인 안보와 평화와 관련된 기존의 관념과 전략도 사이버 시대의 안보와 평화를 증진하는 데에는 적합하지 않을 수가 있다. 최근에 사이버 컨트롤 타워의 수립 필요성을 둘러싸고 진행되는 여러 가지 논의는 기존의 안보 체제와 제도가 사이버 시대 평화와 안보를 지켜나가는 데 미흡하다는 인식에서 비롯된 것이다.[1] 문제는, 변화가 자신의 역할이나 위상을 약화시킨다면 기존의 조직과 제도는 변화에 저항할 것이라는 점이다. 새로운 기술이 주는 위협과 기회를 이해하고 대응하는데 장애요인은 이러한 제도와 조직의 저항만이 아니다. 중요한, 어쩌면 보다 근본적인 장애요인은 눈에 보이지

1- 원유재, "사이버공격 대응하는 총괄 보안 컨트롤타워 필요하다," *과학과 기술*, 2013.5.

않는 사고의 관성으로서, 사이버 시대 평화와 안보를 지켜나가기 위해서는 그에 맞게 평화와 안보의 개념, 그리고 평화와 안보를 증진하는 전략 등에 관한 사고의 발전과 전환이 필요할 수 있다. 그러나 그러한 사고의 발전과 전환은 단기간 내, 특히 위기를 겪기 전에는 어려울 수 있다.

사이버 시대에 평화와 안보란 어떤 의미이고, 어떻게 지켜나갈 수 있는가? 먼저 사이버 공간이란, 물리적 세계와 달리 정보통신 기술과 기기를 통하여 구축되는 인공적인 영역이다. 사이버 공간 속에서는 거리나 시간의 의미가 물리적 세계에서와는 다르며, 현실세계에서는 중요한 국경이나 국적 등이 사이버 공간 속에서는 의미가 없거나 중요성이 크지 않다. 그렇다고 해서 사이버 공간이 현실세계와 완전히 별개로 존재하는 것도 아니다. 현실세계와 사이버 공간은 서로 밀접하게 결합되어 있어서, 사이버 공간과 현실세계가 존재하고 기능하기 위해서는 상호의 존재와 기능이 필수적이다.

문제는 평화와 안보에 대한 기존의 관념이나 전략이 이러한 사이버 공간의 특성이나 사이버 공간과 현실 세계의 상호의존성에 대한 이해를 바탕으로 하고 있지 않다는 데에 있다. 예컨대 기존의 안보 개념은 선형적이고 물리적이다. 국경선, 철책선, NLL 등의 경계선을 기준으로 '안'과 '밖'을 구분하고, 안보 전략은 '안'과 '밖' 사이의 경계선을 강화하거나 물리적으로 침범되지 않게 하는 데에 주력하였다. 최근의 변화들은, 특히 국제화와 정보화의 진전은 경계선의 의미를 많이 퇴색시켰고, 사이버 공격이 물리적 타격 못지않게 평화와 안보를 위협할 수 있음을 보여주었다. 사이버 시대의 평화와 안보 개념은 이러한 경계의 약화나 비물리적 위협의 등장을 반영하여야 한다. 특히 우리나라처럼 다른 나라에 비해서 정보통신기술의 이용이 활발하고, 사이버 공간에 대한 사회적, 경제적 의존도가 높은 경우에는 사이버 시대에 맞게 신속하게 제도와 사고의 진화가 필요하다.[2]

이러한 맥락에서 사이버 공간에서의 평화를 어떻게 정의하고, 어떤 사이버 평화를 추구하느냐는 중요한 문제이다. 현실 세계에서의 평화의 개념이 다양하

2– 한인택, "사이버 시대의 국가안보," *JPI PeaceNet*, 2013.1.

게 존재하는 것처럼 사이버 공간에서의 평화에 대해서도 다양한 시각이 존재할 수 있다. 현실 세계의 소극적 평화와 적극적 평화의 구분을 사이버 공간에도 적용하면, 소극적인 의미에서 사이버 평화는 사이버 공간 내에서 사이버 전쟁이나 사이버 테러, 사이버 범죄 등이 부재한 상태를 의미할 것이다. 한편 사이버 평화의 개념에 관하여 적극적으로 의견을 개진해온 세계과학자연맹(World Federation of Scientists)에 의하면 사이버 평화란 사이버 전쟁의 부재를 넘어서서 아래와 같은 요소/원칙으로 구성된다.[3]

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.

2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cybercriminals.

3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenceless, through violence or degradation.

4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and

---

3_ "Erice Declaration on Principles for Cyber Stability and Cyber Peace," World Federation of Scientists, Aug. 2009, http://www.aps.org/units/fip/newsletters/201109/barletta.cfm

utilizing privacy and security technologies.

5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.

6. Governments should actively participate in United Nations' efforts to promote global cybersecurity and cyber peace and to avoid the use of cyberspace for conflict.

이러한 사이버 평화의 정의에 의하면 사이버 평화는 사이버 분쟁의 부재 이상이다. 사이버 평화는 각국의 정부, 기업, 개인이 협력하여 자유롭고, 안전하고, 정의롭고, 안정적인 사이버 공간을 만들 때 달성된다. 한편 국제전기통신연합(ITU)에 의하면 사이버 평화는 "건강한 평온함과 무질서, 혼란, 폭력의 부재(wholesome state of tranquility, the absence of disorder or disturbance and violence)"에 바탕한 "사이버 공간의 보편적 질서(universal order of cyberspace)"로 정의되고 있다.[4] 이렇게 정의할 때 사이버 평화는 인권, 경제, 안보, 국제협력 등의 여러 측면을 지닌 복합적 현상으로, 단기간 내 한두 나라의 노력만으로 달성하기 어려운 목표이다.

소극적 의미에서 사이버 평화에서부터 적극적이고 포괄적인 의미의 사이버 평화까지 다양한 사이버 평화의 개념이 존재하는데 그 중 어느 개념을 목표로 지향하느냐는 국가적으로, 그리고 국제적으로 깊은 논의가 필요한 사항이다. 소극적인 의미의 사이버 평화를 지향할 때와 적극적인 의미의 사이버 평화를 지향할 때 필요한 국가적 전략과 국제적 협력이 다르기 때문이다.

평화뿐만 아니라 안보도 사이버 공간에서 다양하게 정의될 수 있다. 전통적 안보는 국가를 중심의 개념으로, 대외적 위협으로부터 국가의 핵심적 가치들--주권, 영토, 국민, 정치체제 등--을 보호하고 유지하는 것을 의미하였다. 냉전의 종식이후로는 안보의 개념이 확장되어서 안보는 인권, 에너지, 기후, 테러

4- ITU의 사이버 평화 정의는 다음의 웹페이지에서 재인용. http://ndias.nd.edu/publications/ndias-quarterly/the-meaning-of-cyber-peace/#.UvEo6_l_vt0

등까지 포괄하는 개념으로 발전되어 왔다. 사이버 공간의 발전은 안보의 개념을 또 다시 확장하는 계기를 제공하였다. 사이버 안보란 각종 위협으로부터 사이버 공간을 유지, 보호하는 것으로, 이는 정보통신망을 구성하는 하드웨어와 소프트웨어의 보호는 물론 정보와 데이터의 무결성(integrity), 정보와 데이터의 자유로운 흐름, 프라이버시와 기밀성의 보호 등을 포함한다. 이를 위해서는 정보통신망을 뒷받침하는 전력의 수급 안정성을 확보하는 것에서부터 악성코드의 예방과 치료는 물론 사이버 범죄나 테러까지도 예방하고 대응해야 한다. 사이버 공간이 확대되고 사이버 공간에 대한 의존도가 증가함에 따라 사이버 안보의 개념도 그에 맞춰 포괄적으로 정의될 것이다. 사이버 평화의 경우와 유사하게 사이버 안보의 개념을 어느 선까지 확장할 것인지는 국가적으로나 국제적으로 논의가 필요한 사항이다.

새로운 안보적 위협을 이해하기 위해서는 이러한 개념적인 검토와 더불어서 최근 발생하고 있는 사이버 공격을 경험적으로 살펴보는 것이 유용할 수 있다. 다음은 최근 들어 사이버 '피공격의 대상지'로서 그리고 사이버 '공격의 진원지'로서 급부상하고 있는 중동지역에서 발생한 사이버 공격의 주요사례들이다.[5]

- Stuxnet 공격: 2010년 상반기에 처음으로 확인된 이란 Natanz 소재 우라늄 농축시설에 대한 악성코드 공격. 이 공격으로 이란이 갖고 있는 원심분리기 5,000개중 약 1,000개 정도가 파괴되었고, 이란의 우라늄 농축 프로그램이 약 18개월에서 2년 정도 지연된 것으로 평가되고 있음. Stuxnet 공격은 미국과 이스라엘의 합동작전으로, 이로 인해 사이버 무기 사용에 대한 국제적 '금기'가 깨지게 되었다는 인식이 다수.
- Flame 공격: 2012년 5월 발견된 Flame은 소리, 화면, 키보드 동작, 네트워크 활동, 나아가 블루투스가 설치되어 있는 컴퓨터의 경우 그 주변에 있는 블루투스 기기의 활동과 데이터까지도 탐지하는 종합적인 첩보 프로그램으로, 이 프로그램의 개발과 투입은 이란에 대한 미국과 이스라엘의 합동작전으로 알

5_ 보다 자세한 내용은 한인택, "최근 중동지역 사이버 공격의 사례와 함의," *주요국제문제분석* (2012-42)을 참고..

려져 있음.

- Shamoon 공격: 2012년 8월에는 사우디아라비아의 국영석유회사 Aramco와 카타르의 RasGas에 대한 바이러스 공격이 발생하여 수만 대 컴퓨터의 데이터가 파기됨. 이란이나 이란의 비호를 받는 세력이 공격한 것으로 추정됨.
- 아울러 최근 들어서는 미국의 금융기관과 Google에 대한 중동발 사이버 공격도 증가하고 있음.

사이버 공격에 사용되는 코드나 수법은 그 대상이 특정 국가로 제한되지 않는다. 또 일반 무기와 달리 은밀하게 이전되고 쉽게 모방될 수도 있다. 따라서 공격자가 마음만 먹으면 중동지역에서 발생한 것과 같은 사이버 공격은 얼마든지 다른 나라와 지역에서도 발생할 수 있다. 예를 들어 3.20 해킹은, 작년 8월 15일 사우디아라비아의 석유회사 아람코의 전산망, 그리고 그로부터 2주 후에는 카타르의 가스회사 라스가스의 전산망에 대한 대규모 사이버 공격과 유사한 공격이다.

사이버 공간의 경제적, 사회적 중요성이 커지고, 사이버 공격의 위력과 가능성도 증가함에 따라서 이제는 사이버 안보도 국가안보의 중요한 부분으로 자리잡아야 할 때가 되었다. 하지만 우리는 그동안 남북대치, 특히 북핵의 위협 때문에 전통적인 평화와 안보가 최우선 순위가 되었고, 전통적 평화와 안보를 지키는 데 최대의 관심과 노력이 경주되어 왔다. 3.20 해킹 같은 사이버 공격이 발생한 배경에는 사이버 시대에 맞는 제도와 사고의 전환이 아직 미흡한 점을 들을 수 있다.

만약 사이버 시대에 맞게 제도와 사고가 진화하였다면, 3.20 해킹 같은 사태를 막을 수 있었을까? 반드시 그렇지는 않다. 사이버 공간이란 그것이 개방되어 있고 그 속에서 개인의 자유와 프라이버시가 존중되는 한 근본적으로 방어가 힘든 영역이다. 비유하자면 사이버 공간은 '늑대와 양치기 소년' 우화 속 방목지와 같다. 양을 늑대로부터 확실하게 지키려면 양을 모두 축사에 가둬두거나, 양치기 소년만 아니라 마을 사람 모두가 방목지에서 망을 보아야 할 것이다. 전자의 경우에는 양이 크지 못할 것이고, 후자의 경우에는 마을 사람들이

다른 일을 못할 것이다. 극단적인 선택을 하지 않는 한 사이버 공격은 미리 예상했더라도 모두 예방하기는 힘들다.[6]

물론 완벽한 예방까지는 힘들더라도 사이버 공격의 피해를 줄이기 위한 대응조치들은 필요하다. 사이버 공격이 컴퓨터 하드웨어와 소프트웨어에 관련된 것이기 때문에 대응조치에 관한 논의들이 자연스럽게 기술적으로 흐르는데, 문제는 기술적 대비만으로는 불충분하다는 것이다. 먼저 공격자가 누구인지, 그리고 왜 공격하였는지부터 따져 보아야 한다. 만약 공격자가 사이버 범죄자나 반사회적인 해커라고 할 경우에는 컴퓨터 보안기술을 강화하는 것이 맞다. 그런 범죄자나 해커들에게는 해킹이 그 자체로 목적이거나 목적이 있어도 반사회적이기 때문에, 보안기술의 강화 외에는 뾰족한 대응방법이 없기 때문이다. 하지만 만약 공격자가 국가행위자일 경우에는 다르다. 그 경우 사이버 공격이란 국가의 목적을 달성하기 위한 수단에 불과하기 때문이다. 보안기술을 강화하는 것도 중요하지만, '당근과 채찍'을 사용하여 그 국가를 설득하고 사이버 공격을 단념하게 만드는 것이 우선되어야 한다. 통상적 군사공격에 비유하자면, 공격을 받을 때 방어를 잘할 수 있게 평소에 대비하는 것도 중요하지만 애초에 상대방이 공격을 시작하지 않게 억지하고 설득하는 것이 더 바람직하다. 사이버 시대에 오히려 외교의 중요성이 더 클 수 있다.

일부에서는 상대국가의 공격의사를 억지하는 방법으로 우리의 사이버 군사력을 강화하는 것을 주장하고 있다. 주권국가로서 강력한 사이버 군사력을 갖는 것은 당연하지만, 사이버 군사력이 과연 국가 간 사이버 공격을 억지하는지에 대해서는 의문의 여지가 있다. 뒤에서 더 구체적으로 설명하겠지만 사이버 공간에서는 효과적인 억지를 가능하게 하는 조건들이 부족 내지 부재하기 때문이다.

이제 사이버 공격은 통상적인 군사공격이나 테러공격과 함께 안정과 평화를 위협하는 새로운 변수로 부상하고 있다. 더욱이 사이버 무기는 그 특성상 사용

6_ 이러한 견해는 한인택, "사이버 공격, 어떻게 대응해야 하나?" *한겨레*, 2013.3.26을 통해 미리 발표한 바 있다.

이 특정 지역에 제한되지 않고, 이전도 은밀하게 진행될 수 있기 때문에 다른 지역으로 확산될 가능성이 존재한다. 중동이나 미국에서 발생한 사이버 공격이라 하더라도 한반도에서도 재연될 가능성을 배제할 수 없기 때문에 사이버 안보전략의 수립이 시급하다. 그리고 나아가 중장기적인 사이버 안보전략의 준비를 위해서 안보관련 제도와 조직을 개편할 필요가 있다. 제도와 조직의 편제 개편은 기존 제도와 조직의 '관성'을 극복하여야 가능할 것이며, 새로운 안보위협을 신속히 인식하고 선제적으로 대응하기 위해서는 사이버 안보를 담당하는 기구가 기존의 사고의 저항을 극복할 수 있도록 "학습하는 조직(learning organization)"일 필요가 있다.

사이버 시대의 안보 위협과 기회에 대처해야 하는 것은 단지 우리나라의 과제만은 아니다. 대개의 나라들이 최근에야 사이버 안보에 관심을 기울이기 시작했으며, 국제적으로도 사이버 공간의 평화적 사용이나 사이버 분쟁의 평화적 해결 등에 관한 규범이 아직 발달하지 못한 상태이다. 우리나라는 2013년 제3차 사이버스페이스 총회의 개최국으로서 사이버 공간에 관련된 국제적 규범을 창출하는 데 중요한 역할을 할 것으로 기대된다. 서울 사이버스페이스 총회에서 참가국들이 사이버 공간에서 허용되는 정당방위는 무엇인지, 사이버 무기의 군축을 위한 원칙과 절차는 어떻게 되어야 하는지에 대해 견해를 교환하고 의견을 수렴할 수 있다면 우리의 안보증진뿐만 아니라 국제적 위상도 높아질 것이다.

II. 사이버 위협을 보는 두 시각[7]

혁신적인 기술의 발전은 새로운 공간의 출현을 낳고, 새로운 공간의 출현은 그에 따른 국제안보적 파급효과를 낳는다. 정보통신기술의 발달로 지난 수십 년간 사이버 공간이 급격하게 팽창하여 왔고, 그에 따르는 새로운 안보적 위협과 기회를 발생시키고 있다. 그런데 사실은 이와 유사한 현상이 20세기 이후로 수차례 반복되어 왔었다. 20세기 초 비행기의 발명으로 그전에는 인간의 능력이 미치는 영역의 밖이었던 '공역(空域)'이 전략적 차원에서 '새로운' 공간으로 출현하였고, 잠수함 기술의 발달로 '해저'라는 '새로운' 공간이 생겨났다. 20세기 후반 로켓 기술의 발달은 '우주'라는 '새로운' 공간을 출현시켰고, 그에 따르는 새로운 안보적 위협과 기회도 낳았다. 이런 면에서는 사이버 공간이 과거에 출현한 공간들, 즉 공역이나 해저, 우주와 마찬가지이다.

새로운 공간이 출현하면 그 공간을 누가 지배하고, 어떻게 이용하느냐에 따라서 전략적 우열이 바뀔 수 있다. 과거 제해권, 제공권에 대한 논의나 현재 사이버 공간 내 주도권에 관한 논의는 그런 맥락에서 이해될 수 있다. 그런데 사이버 공간은 그 이전에 출현한 공간과 중요한 차이를 가지고 있다. 인간의 의지나 행동과는 무관하게 존재하는 물리적 공간과 달리 사이버 공간은 탄생이나 존재, 확대에 있어서 전적으로 인간의 의지와 노력의 산물이다. 정확히 말하면 사이버 공간은 행위자들에 의해 매일매일 '구성되는' 공간이라고 할 수 있다. 이에 따라 논리적으로 행위자들이 사이버 공간을 어떻게 '구성'하느냐에 따라서 발생하게 되는 안보적 위협이나 기회가 자연히 달라질 것이다. 예컨대 어떤 이유에서건 자국의 정보통신망을 외부로부터 분리시키거나 아예 정보통신망 구축 자체를 포기한다면, 그 나라에게는 사이버 공간 때문에 발생하는 안보적 위협도 안보적 기회도 존재하지 않을 것이다. 기존의 물리적 공간은 이와 다르

7_ 이 절의 초기본은 장노순·한인택 공저, "사이버안보의 쟁점과 연구경향," *국제정치논총* 제53집 3호 (2013)의 일부로 발표된 바 있다.

다. 예컨대 어느 나라가 공군을 만들지 않거나 활주로를 건설하지 않는다고 해서, 그 나라에게 외부로부터의 공습의 위협이 없어지는 것이 아니다. 기존의 물리적 공간과 그에 따르는 안보적 위협과 기회는 행위자에 의하여 '구성'되는 것이 아니고 행위자의 의사나 행동과 상관없이 존재하는 것이다.

이렇듯 사이버 공간을 행위자가 구성하는 공간이라고 한다면, 사이버 공간에 대해 행위자가 갖는 관념과 선택이 사이버 공간의 성격을 결정하는 중요한 변수가 될 수 있다. 우선 행위자들이 사이버 공간을 위험한 공간으로 보느냐 안전한 공간으로 보느냐에 따라 행위자들의 사이버 공간 관련 전략과 행동이 달라질 것이고, 행위자들의 전략과 행동에 따라서 궁극적으로는 사이버 공간의 질서나 성격이 달라질 수 있다. 따라서 사이버 공간의 안보적 함의를 보는 시각을 검토해 볼 필요가 있다. 이 절에서는 사이버 공간의 안보적 위협에 대한 행위자들의 견해를 '위협 실재론'과 '위협 과장론'으로 양분하고 그 내용을 소개하고자 한다.[8]

1. 위협 실재론 대 위협 과장론

미국에 대한 다음의 공격은 "사이버 진주만 공격"이 될 것이라는 미국 고위관료들의 연이은 발언에서 볼 수 있듯이 미국의 정책결정자들 사이에서는 사이버 공간을 위험한 공간으로 보는 시각이 지배적이다. 이러한 견해를 이 글에서는 편의상 '위협 실재론'이라고 부르고자 한다. '위협 실재론'은 물론 미국에서만 존재하는 것이 아니고 다른 국가 들에도 존재하고 있지만 미국에서 가장 강력히 표현되고 있는 것으로 보인다.

사이버 공격이 임박했고 사이버 공격의 위협이 심각하다고 주장하는 '위협 실재론'에 대조적으로, '위협 과장론'은 사이버 공간의 위협 요소를 낮게 평가한다. 위협 과장론은, 사이버 공간은 원래 위험스러운 것이 아니고 오히려 사이버 공간이 위험하다는 주장이 사이버 공간을 위험하게 만든다고 주장한다. 위

8_ 위협 실재론과 위협 과장론, 그리고 사이버 평화론은 이 연구에서 편의상 붙인 이름이다.

협 실재론이 지배적으로 되면 사이버 공간의 군사화를 부추겨서 사이버 공간을 자기실현적으로 위험하게 만들 수 있기 때문이다.

많은 전문가 사이에서는 위협 실재론이 지배적인 견해이다. 하지만 위협 과장론에도 또한 주의를 기울여야 하는 이유는, 인류최대의 위협이 되는 "사이버 게돈(Cybergeddon)"이 다가오고 있다는 반복되는 경고에도 불구하고 사이버 공격은 지금까지 상대적으로 희소하였고, 그 효과는 인류최대의 위협은커녕 일시적 불편함과 혼선만을 야기하는 정도였기 때문이다.[9] 이러한 사실이 주는 함의는 위협 실재론에서 주장하는 것보다 사이버 공격에 대한 방어가 효과가 있거나, 사이버 공격의 파괴력이 위협 실재론에서 생각하고 있는 것보다 제한적일 수 있다는 것이다. 나아가 만약 사이버 공격이 물리적 공격을 대체할 수 있다면, 사이버 공간의 등장은 물리적 공간에서의 충돌을 피해가 더 제한적인 사이버 공간으로 옮김으로서 역설적으로 국제안보와 평화에 기여할 가능성도 있다. 이 글에서는 이러한 견해를 편의상 '사이버 평화론'이라고 명명한다.

경험적으로는 위협 과장론이 더 타당하지만 우리나라나 미국에서 위협 실재론이 위협 과장론을 제치고 부상하게 된 것은 개방사회의 특수성으로 일부 설명할 수 있는 것으로 보인다. 우리나라나 미국은 정보화가 가장 먼저 진행된 개방사회로서 체질적으로 외부로부터의 위협에 취약할 수밖에 없는데다가 북한의 위협이나 9.11 테러 이후로 높아진 안보위기 의식이 한국과 미국에서 위협 실재론이 지지를 얻는데 기여하였다(The Economist, 2012). 중요한 것은 위협 실재론이 영향력을 갖게 되면 국가의 정책에 그러한 입장이 반영이 되고 나아가 사이버 공간 내 국제관계에까지도 영향을 미치게 된다.

예를 들어서 사이버 공간에서는 방어보다 공격이 유리하고, 선제공격이 특히 효과적이라는 생각이 지배적이라고 가정해 보자. 이러한 공격, 특히 선제공격의 우월성에 대한 믿음은 역사적으로 자주 발견된다. 대표적인 경우는 1차 세계대전이 발발하기 전의 기간으로서 기관포나 철조망, 철도 등의 발명으로 방

9– 물론 얼마큼 희소한 것이 희소한 것이고, 얼마큼 위협적인 것이 위협적인지는 명확하게 말할 수 없다.

어가 공격보다 실제로는 더 유리하였음에도 불구하고 군인과 국가지도자들은 공격, 특히 선제공격이 유리하다는 믿음이 지배적이었다. 이러한 믿음 때문에 유럽 국가들은 외교를 통해 분쟁을 해결할 시간적 여유가 없다고 생각하고 경쟁적으로 선전포고를 하였다. 만약 당시 정책결정자들이 공격의 우위성에 대하여 다른 관념을 가졌다면--예컨대 공격보다 방어가 더 유리하다는 사실을 정확하게 인식했다면--성급하게 외교를 포기하고 전쟁을 시작하지 않았을 가능성이 크다.

사이버 공간의 안보적 위협을 둘러싼 견해의 차이는 해결이 될 수 없는 것일까? 이에 대한 대답은 지금으로서는 부정적이다. 역사적으로 볼 때 핵무기의 안보적 함의에 대한 논란은, 핵실험과 히로시마, 나가사키의 원폭 투하를 통해서 잠재워 졌다.[10] 하지만 사이버 공간에서는 위협론이 맞느냐 과장론이 맞느냐 하는 논쟁을 잠재울 만한 획기적인 사건이 아직 발생하지 않았고, 어쩌면 앞으로도 발생하지 않을 수 있다. 따라서 사이버 무기나 사이버 공격이 주는 안보적 위협에 대한 판단은, 사이버 무기의 효과나 사이버 공격의 결과를 보고 경험적으로 내린 것이 아니라, 주로 그들의 속성, 제한된 소수의 사례, 가상의 시나리오로부터 추상적으로 추론하여 내린 것이라고 볼 수 있다.

위협 실재론의 논리를 좀 더 자세히 살펴보면, 우선 사이버 무기가 국가뿐만 아니라 다양하고 다수인, 그리고 많은 경우 익명인 비국가 행위자들의 손에 들어갈 수 있다는 점을 강조하고 있다. 이것이 가능한 이유는 사이버 무기가 손쉽게 복제, 전파 가능할 뿐만 아니라 민간에서 이미 사용하고 있거나 개발가능한 프로그램이기 때문이다. 따라서 사이버 공간에서 잠재적 공격자와 공격수단이 증가하였을 뿐만 아니라, 공격자를 비공격자로부터 구별하거나 공격용 프로그램을 일반 프로그램과 구분하는 것이 어렵다. 어쩌면 공격용 프로그램과 일반 프로그램을 구분하는 기준은 궁극적으로 사용자의 의도밖에 없을 수도 있다. 한편 공격을 받을 수 있는 대상도 폭발적으로 증가하였다. 국가, 시장, 사회, 군

10_ 흥미로운 것은 논리적으로 일관성이 있는 핵전략은 1956-57년이 되어야 처음 등장한다는 사실이다(Trachtenberg, 1991). 신기술의 '등장'과 신기술의 주는 안보적 함의에 대한 체계적 '이해'는 상당한 시차가 있다.

사 등 모든 부문에서 정보와 통신의 사용과 의존도가 증가하였기 때문이다. 과거에는 안보적 위협이 증가하고 안보적 취약성이 늘어나더라도 국가가 개입하여 어느 정도의 위협관리가, 특히 국경 내에서는 가능하였다. 하지만 종래의 안보위협과 달리 사이버 공격은 초국경적이고 순식간에 발생하기 때문에 국가가 효과적으로 대처하기가 힘들다.

이러한 변화들--위협 요소의 증가, 취약성의 증가, 국가능력의 감소--로 인해 사이버 공간의 확장이 안보의 위협이 될 것이라고 기대하는 것은 놀라운 일이 아니다.[11] 앞에서 살펴본 최근 중동에서의 사이버 공격도 위협 실재론에 설득력을 더해 주고 있다. Stuxnet은 이란 핵농축시설에 타격을 가해 핵개발 개획을 2, 3년 지연시킨 것으로 평가되고 있으며, 사우디 아람코와 카타르 라스가스에 대한 공격은 자칫하면 세계에너지 시장을 교란시킬 뻔 했었다.

문제는 이러한 지적들이 사이버 공간의 특성과 사이버 무기의 추상적 속성에서 결론을 연역하고, 소수의 사례를 일반화시킨 것이라는 것이다. 과연 이러한 결론은 얼마나 유효한 것인가? 우선 위협 실재론을 주장하기에는 경험적으로 한계가 있다. 이미 언급하였지만 사이버 공격의 결과나 사이버 무기의 효과가 이견이 없을 정도로 확실하거나 심각하지 않다. 예컨대 사이버 공격으로 대량살상(mass destruction)이 발생한 적은 아직 없다. 뿐만 아니라 앞으로라도 사이버 공격으로 대량살상이 발생하는 경우는 잘 상상하기 힘들다. 또한 사이버 무기가 '직접적으로' 인명을 살상한 경우는 아직까지 없으며, 사이버 무기에 의한 물질적 피해도 지금까지는 경미하다(Rattray, 2001; Libicki, 2007).[12]

11_ 역사적으로 볼 때 국가가 효과적으로 대처할 수 없는 초국경적이고 순식간적인 안보위협의 등장은 이번이 처음이 아니다. 대륙간 탄도탄, 특히 핵탄두를 장착한 대륙간 탄도탄은 현재까지도 대처가 불가능한 초국경적이고 순식간에 막대한 피해를 주는 안보적 위협이다. 대륙간 핵탄도탄의 경우에는 핵물질의 희귀성, 대륙간 탄도탄 능력의 희귀성으로 인해서 사이버 공간의 안보위협과 차이가 있다. 사이버 공간에서는 잠재적 공격자와 공격수단이 무수히 많이 존재하고 있다.

12_ 이러한 평가는 전통적인 안보의 개념에 기반한 것이다. 만약 안보를 인명과 재산의 안전보다 더 넓게 정의한다면 대량살상이 없더라도 사이버 무기나 사이버 공격이 커다란 안보적 위협이 될 수 있다는 주장이 가능하다. 예컨대 안보를 폭넓게 금융의 안정성이나 통신의 안정성까지 포함하여 정의하면 금융망이나 통신망에 대한 사이버 공격은 심각한 안보적 위협으로 볼 수 있다.

역사를 돌이켜 보면 핵무기가 등장하고 난 직후에는 핵확산이 짧은 기간 내에 기하급수적으로 일어나고 조만간 핵전쟁도 터질 것이라는 우려가 지배적이었다. 하지만 그로부터 수십 년이 지난 오늘의 현실은, 핵확산이 더디게, 그리고 제한적으로 일어났으며, 히로시마와 나가사키에서 원자폭탄이 투하되고 난 이후 핵무기가 사용된 적은 없었다. 뿐만 아니라 핵무기는 억지력을 증가시키기 때문에 세계를 위험하게 만드는 것이 아니라 오히려 세계를 평화롭게 만든다는 주장까지 제기되었다. 소위 '핵평화론자' 들은 미국과 소련이 쿠바 미사일 같은 위기를 겪으면서도 충돌하지 않은 것은 바로 핵무기의 억지력 때문이라고 설명하고 있다(Waltz, 1981).

이러한 역사적 조망을 통해 얻는 메시지는 새로운 기술이 갖는 안보적 함의를 초기에 정확히 파악하고 예측하기 쉽지 않다는 것이다. 오늘날 우리는 사이버 공간의 확대가 의미하는 함의를 충분히 이해하지 못하고 성급하게 사이버 위협의 증가와 '사이버게돈'의 발발을 예측하고 있는지도 모른다. 신기술의 잠재성이 과대평가 되고 주식시장에서 거품현상이 주기적으로 일어나는 것처럼, 사이버 공간이 갖고 있는 안보적 함의를 정확히 알지 못하고 안보적 위협이나 기회를 과대평가 또는 과소평가할 가능성이 존재한다.

2. 사이버 안보 딜레마

사이버 공간의 등장, 특히 사이버 무기의 발달이 국제안보에 미치는 영향을 이해하는 또 다른 방법은 바로 사이버 공간에서 안보 딜레마의 성격에 대해 알아보는 것이다. 안보의 딜레마란 한 국가가 자신의 안보를 증진시키기 위해 취하는 조치들이 다른 국가들의 안보를 감소시키는 상충관계(trade-off)이다. 어떤 연유에서이건 상충 관계가 강해지면 국제관계는 제로섬 게임의 성격을 갖게 되며 국제평화와 국제협력이 어려워진다. 만약 상충관계가 약해지면 국제관계는 포지티브섬 게임의 성격을 갖게 되고 국제평화와 국제협력이 용이해진다.

사이버 공간에서 국가안보의 상충관계는 어떻게 변하는가? 안보 딜레마에 대한 논의는 지금까지 기존의 공간--공역, 해양, 육상--을 가정하고 이루어졌다.

이들 공간은 물리적 공간으로 국가가 자의적으로 벗어날 수 없다. 사이버 공간은 이와 달리 국가의 의지에 따라서 참여여부나 참여방식의 선택이 가능하다. 일부 국가의 경우 사이버 공간에 제한적으로 참여하고 있고, 사이버 공간에 대한 접근도 비대칭적이다. 예컨대 이란의 경우에는 독자적 인터넷망을 구축해서 외부로부터 접속을 차단하고 있는 한편, 외국의 인터넷망에는 필요에 따라 선택적으로 접속하고 있다. 북한의 경우도 상황은 비슷하다. 한편 한국이나 서구 국가들은 적극적으로 사이버 공간에 참여하고 있고, 사이버 공간에 대한 접근이 대칭적으로 이루어지고 있다. 이러한 사이버 공간의 특성 때문에 기존의 안보 딜레마 분석을 사이버 공간에 그대로 적용할 때 무리가 있다. 기존의 분석에 한차원을 더하여 사이버 공간에 적극 참여하는 경우(loyalty), 비판적으로 참여하는 경우(voice), 참여를 거부하는 경우(exit)를 각기 상정하고 그 안에서 안보 딜레마의 여하를 따져 볼 필요가 있다(Hirschman, 1970).

기존의 공간에서 안보의 딜레마의 강약은 공수균형(offense-defense balance)과 공수구분(offense-defense differentiation)에 의하여 일차적으로 결정되는 것으로 이해되고 있다. 방어가 공격에 비해 유리하다면 다른 나라에서 군비증강을 하더라도 상대적으로 큰 걱정을 하지 않게 될 것이다. 따라서 방어가 공격보다 유리할 때 안보의 딜레마는 경감된다. 한편 공격이 방어보다 유리하다면, 즉 방어가 공격에 비해 취약하다면 안보의 딜레마는 심화된다. 안보 딜레마에 영향을 주는 두 번째 요인은 공수구분으로, 무기이든 전략이든 그 목적이나 용도가 구분되면 구분될수록 투명성이 증가하여 안보의 딜레마는 경감된다. 특히 한 국가가 명백하게 수비가 목적인 무기를 증강하고, 명확하게 수비를 목적으로 하는 전략을 수립한다면 그런 조치에 대해서 다른 국가들이 걱정할 필요가 없다. 그 나라의 안보 증가가 다른 나라의 안보에 대한 위협을 증가시키지 않고, 다른 나라들이 그 사실은 잘 알고 있기 때문이다. 반면 공수구분이 힘들면 힘들수록 안보의 딜레마는 심각해진다.

사이버 공간에서 공수의 균형과 공수의 구분은 어떠한가? 이에 대한 대답은 앞에서 소개한 견해에 따라 다르다. 위협 실재론에 의하면 사이버 공간에서는 공격이 방어보다 유리하다. 공격자는 다수이고, 익명이며, 위치도 파악하기 힘

들며, 공격은 은밀하고 순식간에 다양한 방법으로 이루어질 수 있기 때문이다. 즉, 공격이 수비보다 유리하고 또 용이하다. 하지만 위협 과장론의 입장에서는 정말 공격이 유리하고, 수비가 불리한지에 대해 의문을 가져 볼 수 있다. 만약 사이버 공간에서 공격이 유리하고 용이했다면 이라크의 훗세인, 리비아의 가다피 등이 왜 체포되기 전까지 자신을 공격한 서방측에 대해 아무런 사이버 공격을 가하지 않았을까? 알카에다는 왜 아직까지도 미국에 대해 강력한 사이버 공격을 가하지 못하고 있는 것일까? 후세인이든 알카에다이든 결코 공격의 의지가 부족했던 것은 아니다. 그럼에도 불구하고 제대로 된 사이버 공격이 없었다는 것은 실은 공격이 감행하기 힘들거나 수비가 생각보다 강력하기 때문일 것이다. 달리 말하면 사이버 공격의 추상적 속성을 무비판적으로 받아들인다면 공격이 유리하다고 결론 내리겠지만, 경험적 현실은 그러한 결론과 합치하지 않는다.[13]

안보의 딜레마를 결정하는 다른 요인은 공수구분이다. 위협 실재론의 입장에서는 공격을 목적으로 소프트웨어나 하드웨어를 수비를 목적으로 한 소프트웨어나 하드웨어와 구분하기 힘들다고 지적한다. 예컨대 컴퓨터는 공격에 쓰일 수도 있고 수비에 쓰일 수도 있다. 공격용 컴퓨터가 따로 있고 수비용 컴퓨터가 따로 있는 것이 아니다. 뿐만 아니라 공격이 있었다고 하더라도 어느 컴퓨터가 공격에 사용되어 있는지 찾아내기란 쉽지 않다. 무기로 쓰인 컴퓨터하고 무기로 쓰이지 않은 컴퓨터하고 과연 현실적으로 구분이 되는가? 소프트웨어도 마찬가지이다. 수비를 목적으로 한 훌륭한 방화벽을 만들기 위해서는 다양한 공격 수법을 알고 방화벽 디자인에 반영을 하여야 한다. 그렇다면 좋은 방화벽을 만드는 기술과 지식은 마음만 먹으면 사이버 공격에 전용가능하다. 이러한 면에서는 위협 과장론도 하드웨어나 소프트웨어가 대개의 경우 공수겸용이라는 사실에 대해서 이론을 제기하기 힘들다.

13_ 공수균형에 대한 판단과 실제 현실이 일치하기란 쉽지 않다. 1차 대전 시 공격이 우위라는 생각이 지배적이었지만 전쟁이 발발하고 난 후에는 수비가 우위라는 것이 경험적으로 확인되었다(Van Evera, 1984). 이와 대조적으로 2차 대전 시에는 수비가 우위라고 생각하였는데, 히틀러의 전격작전의 성공으로 실제로는 공격이 우위인 것으로 확인되었다.

다른 나라, 예컨대 중국이나 중동국가의 컴퓨터 숫자나 컴퓨터 전문가의 숫자가 증가하면 과연 우리나라에게 안보위협이 되는가? 컴퓨터 하드웨어나 소프트웨어가 공수겸용이기 때문에 논리적으로는 다른 나라의 컴퓨터나 컴퓨터 전문가의 숫자가 증가하면 우리나라에게 안보위협이 될 것이다. 하지만 다른 나라의 컴퓨터나 컴퓨터 전문가가 늘어난다고 해서 실제로 우리나라에 대한 안보위협이 객관적으로 증가되는지는 미지수이고, 주관적으로도 안보가 위협된다는 인식이 반드시 따르는 것 같지는 않다. 공수의 구분이 힘들다는 면에서 사이버 공간은 논리적으로 안보의 딜레마가 발생하기 쉬운 여건을 가지고 있지만 그러한 우려가 현실적으로나 인식 상으로 얼마나 실현되고 있는지는 분명치 않다. 공수균형과 공수구분이라는 두 기준으로 볼 경우 사이버 공간은 논리적으로 안보의 딜레마가 발생하기 좋은 여건을 가지고 있다. 공수의 구분이 쉽지 않은 데에다가 만약 위협 실재론의 입장이 옳다면 공격도 우위라서 국제관계는 제로섬 게임적의 성격을 가질 소지가 크다. 사이버 공간에서 주도권을 장악하려는 국가 간의 경쟁, 특히 미중 간의 치열한 경쟁은 이러한 결론을 뒷받침하는 것처럼 보인다. 하지만 언급하였듯이 이러한 논리적 결론이 현실적으로 반드시 타당한지는 명확하지 않다. 이웃 나라의 군함이나 항공기, 미사일 수가 증가하면 안보적 위협이 증가하는 경우가 일반적이지만, 이웃 나라의 컴퓨터나 컴퓨터 전문가가 늘어난다고 안보적 위협이 반드시 증가하지는 않는 것 같다.

아울러 물리적 공간과 사이버 공간이 중요한 차이점은 사이버 공간에 참여는 필요하기는 하지만 운명이 아니고 선택이라는 것이다. 만약 사이버 공간에 참여함으로써 오는 안보적 위협이 사이버 공간에 참여하여 얻는 혜택을 능가한다면, 극단적으로 사이버 공간에 참여하지 않거나 앞서 이란의 예에서 보았듯이 참여의 방식이나 조건을 바꿀 수 있다. 물론 지금보다 사이버 공간이 더 확대되고 사이버 공간에 대한 의존도가 더 증가한다면 그때는 사이버 공간에 참여가 더 이상 가역이 가능한 선택이 아니라 바꿀 수 없는 운명처럼 될 것이다. 하지만 상당수의 국가들은, 특히 후진국들은 사이버 공간의 발달이나 사이버 공간에 대한 의존이 불가역적일 정도로 진전되어 있지 않다. 사이버 공간의 발달과 이용은 아직까지는 선진국적인 특권이다.

사이버 공간의 특성과 사이버무기의 속성으로부터 사이버 공간의 안보위협을 연역하여 보면 사이버 공간은 위태롭고 갈등의 가능성이 높은 곳으로 보이지만, 사이버 공격의 횟수나 피해를 경험적으로 살펴보면 그와는 상당히 다른 평가가 가능하다. 공수균형이나 공수구분을 기준으로 사이버 안보 딜레마의 강약을 평가해 보면 국가 간의 안보관계가 마치 제로섬적 성격을 보일 것으로 생각이 들지만, 물리적 공간과 달리 사이버 공간은 선택적으로, 그리고 원하는 조건으로 참여할 수 있다는 점을 고려하면 사이버 안보 딜레마는 기대보다 경미할 수 있다.

사이버 공간을 어떻게 보고, 어떻게 분석하느냐에 따라서 사이버 공간의 안보적 위협이나 기회는 사뭇 다르게 보이게 된다. 사이버 공간의 안보적 함의에 대한 정확한 이해는 시간과 분석이 더 필요하다. "사이버 공간은 구성된 환경으로서 우리가 선택하여 만드는 대로이다(As a constructed environment, cyber-space(s) is very much what we choose to make it)."[14] 사이버 공간이 행위자들이 '구성'하는 공간이기 때문에, 행위자들의 시각과 관념을 이해하는 것이 중요하다. 행위자의 생각이 자기실현적으로, 경우에 따라서는 '자기부정적으로' 사이버 공간에서 현실로 실현될 수 있기 때문이다.[15] 이러한 복합적인 관계를 이해하고, 사이버 공간을 가장 안정적이고 평화적으로 만들 수 있는 시각과 관념이 무엇인지 찾아내고 주류화시키는 것이 필요하다. 그렇지 않으면 그릇된 군사교리(military doctrine)가 1차 대전을 촉발시켰던 것처럼 성급한 사이버

14– Dogulas C. Lovelace, Jr. (Director, Strategic Studies Institute and U.S. Army War College Press)의 코멘트 (Gray, 2013).

15– 자기실현적 예측이란 주식시장에 대한 부정적 전망이 투자자들을 주저하게 만들어서 실제로 주식시장의 침체를 낳는 경우처럼 예측이 그와 합치되는 결과를 초래하는 경향을 말한다. 자기실현적 예측은 Robert K. Merton에 의하여 잘 알려지게 되었다. '자기부정적' 예측이란 이와 반대로 예측이 그와 반대되는 결과를 발생시키는 경우를 말한다. 예컨대 주식시장에 대한 장밋빛 전망이 과도한 거품을 발생시켜서 궁극적으로 주식시장의 붕괴를 낳는다면 이는 예측이 그와 정반대의 결과를 낳는 경우이다. 이러한 경우를 필자는 자기부정적 예측이라고 부르고자 한다. 사이버 공간과 관련하여, 사이버 공간이 안전한 공간이라는 생각이 방심을 초래해서 사이버 공간의 방어가 취약하게 되면 사이버 테러나 사이버 공격이 발생하게 된다. 이런 경우를 자기부정적 예측이라고 볼 수 있을 것이다.

전략이 국제적 분쟁을 촉발시킬 우려가 있기 때문이다.

III. 사이버 공간에서의 동맹협력:
한미상호방위조약의 한계와 미-이스라엘 동맹의 함의[16]

사이버 공간도 과연 '공간'인지에 대해서는 의견이 분분하지만, 지난 수십 년간의 획기적인 정보통신기술의 발전으로 많은 국가와 지역에서 사이버 공간이 확대되고 사이버 공간에 대한 의존도가 급증하였다는 사실에 대해서는 이견이 없을 것이다. 특히 우리나라의 경우 정보통신기술이 발달하였고 정보통신망에 대한 의존도가 세계에서 가장 높은 수준이 되었다. 그에 따라 얻게 되는 우리가 얻는 사회적, 경제적 이익이 지대하다. 하지만 고도로 정보화된 개방사회로서 사이버 공간 내에서 우리나라의 취약성도 대단히 높다. 3.20 사태, 6.25 사태 등 연이은 사이버 공격 사례들은 사이버 공간 내에서 우리의 취약성을 여실히 보여주고 있다. 높은 수준으로 정보화된 개방사회로서 우리는 구조적으로 사이버 공격의 위협에 노출되어 있다.

사이버 공간을 보호하고 잘 활용하기 위해서는 개인 사용자가 조심하는 것만으로 불충분하고 민관군의 협력과 노력이 필요하며 국제적 협력도 매우 중요하다. 특히, 계속되는 사이버 공격은 북한의 소행으로 추정되는 바, 그간 북한의 도발을 억제하는 데에 중요한 역할을 해 온 한미동맹의 역할을 이해하고 동맹 협력을 강화할 필요가 있다.

이 글에서는 사이버 공간이 출현하기 훨씬 이전에 맺어진 한미동맹이 사이버 공간 내에서 어떻게 적용되는지, 그리고 한미동맹에서 대북 억지력의 골격을 이루고 있는 확장억지가 새로운 공간 내에서 어떻게 작동하는지 살펴보고자 한다. 앞에서 지적하였듯이 전통적 안보와 평화를 담당해온 기존의 조직과 제도가 사이버 시대의 안보와 평화를 담당하기에 적당하지 않을 수 있으며, 기존의 사고와 전략도 사이버 시대의 안보와 평화를 증진하는 데에는 적합하지 않을 수가 있기 때문이다. 따라서 전통적 안보와 평화를 위해 가장 핵심적인 역할을

16_ 이 절의 초기본은 2013년 10월 18-19일 공군사관학교에서 열린 *한미동맹 60년의 주요 현안과 발전과제 : KAIS 2013 안보국방학술회의*에서 발표되었다.

해온 한미동맹을 검토하고 필요시 개선방안을 찾아보는 것이 필수적이다.

1. 사이버 공격과 한미상호방위조약

6.25 전쟁의 종전 이후 반세기 이상 북한이 남한에 대해 대규모 공격을 감행하지 않은 데에는 미국의 확장억지 공약에 기반한 한미동맹의 역할이 크다. 여기서 확장억지란 북한이 남한을 공격할 때 미국이 자국이 보유한 우월한 군사력을 사용하여 북한에 대해 보복하는 것이다. 과거에는 확장억지와 '핵우산'이 거의 동의적으로 쓰였으나 최근 들어 미국이 '핵무기 없는 세상' 등을 이유로 핵무기에 대한 의존을 줄이면서 핵무기를 사용하지 않는 방식으로 확장억지를 제공할 가능성이 높아졌다.[17] 핵무기를 사용하지 않고 보복하는 경우를 포함하기 위해서는 핵우산보다는 확장억지가 더 정확한 개념이다. 만약 확장억지가 사이버 무기를 중심으로 이루어진다면 아직 사용된 적이 없는 표현이지만 '사이버 우산'이라는 표현이 가능할 것이다.

확장억지가 효과적이기 위해서는 뒷받침할 수 있는 '능력'과 필요시에는 실제로 능력을 사용하겠다는 '의지'가 확고해야 하는데, 능력이나 의지 중 하나라도 부족하게 보이면 억지력이 약화되어 상대방이 도발할 가능성이 생긴다. 확장억지의 효과는 이렇듯 조건부이다. 확장억지의 효과가 약화되는 경우는 단지 이론적 가능성이 아니라서, 지난 수십 년 간 북한이 행한 소규모 도발들은 소규모 도발에 대해서는 미국이 보복, 특히 핵무기를 사용한 보복을 할 '의지'가 없을 것이라고 믿고 소규모 도발을 시도하여 온 것이다. 달리 말하면 도발에 대해 보복을 할 능력이나 의지 중 어느 하나라도 부족하다는 인식이 발생하면--억지의 '신뢰성'에 대한 의심이 발생하면--도발의 가능성이 높아지고 실제로도 도발이 행해졌다.[18] 이처럼 확장억지가 그동안 중요한 역할을 해 왔지만, 확장억지의 성격 상 확장억지를 통해 막기 힘든 도발도 있는 것이다. 여기서 당연히

17_ 한인택, "'핵무기 없는 세상'과 핵우산," *JPI PeaceNet*, 2010.

18_ 한인택, "동맹과 확장억지: 유럽의 경험과 한반도에의 함의," 제주평화연구원, 2009.9.

생기는 질문은 사이버 시대에는 확장억지의 신뢰성이 어떻게 변화할 것이냐 하는 것이다.

미국이 확장억지를 제공하는 조약적 근거는 1953년 체결할 한미상호방위조약이다. 이 조약에 의하면 양국은 "행정관리 하에 있는 영토(territories under their respective administrative control)"에 대해 "외부로부터 무력공격(external armed attack)"이 있을 경우 협의를 통해서 필요한 조치들을 취하기로 약속하였다. 이는 실질적으로 남한의 영토에 대해 북한의 무력공격이 있을 때 미국이 개입하여 응징하는 것을 의미하였다. 당시로서는 그리고 지금도 미국의 영토에 대해 외부로부터 무력공격이 발생하고 한국이 그에 대해 응징할 경우가 발생할 확률은 높지 않다. "행정관리 하에 있는 영토"나 "외부로부터 무력공격" 등 조약에 사용된 표현들은 조약이 체결된 당시에는 적합하고 문제가 없었지만 사이버 시대가 도래하면서 과거에 예상하지 못했던 문제점들이 발생한다.

1) 사이버 공간이 국가가 행정적으로 관리하는 영토인가?

한미상호방위조약의 적용 지역은 한미양국이 행정적으로 지배하고 있는 영토이다. 그 외의 지역에서는 한미상호방위조약이 적용될 법적인 근거가 없다. 그럼에도 불구하고 그 외 지역에서 한미가 상호 방위를 돕기로 한다면 그것은 정치적 결정이지 조약상의 의무사항은 아니다.

사이버 시대가 도래하며 발생하는 한미상호방위조약의 문제는 사이버 공간이 한국이든 미국이든 특정국가가 행정적으로 지배하는 영토로 보기 힘들다는 점이다. 사이버 공간은 현재까지 초국가적이고, 초국경적인 공간으로 존재하고 있다. 이러한 인식은 미국의 정부문서에서도 발견되는데 미군의 한 출판물에 의하면 사이버 공간은 "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" 로 정의되고 있다.[19] 즉, 사이버 공간은 "전지구적 영역 (global domain)"으로서, 영토나

영공, 영해 등과 같이 법적으로 한 국가의 주권이 적용되는 물리적 공간과는 다르다. 이렇듯 미국의 정부 간행물에서조차 사이버 공간이 초국가적이고, 초국경적인 공간이라고 정의한다면, 사이버 공간은 법적으로 한미상호방위조약의 적용 지역이 아니다. 따라서 사이버 공간에서의 도발이나 충돌에 대해 한국이 미국의 원조를 기대할 수 있는 조약적인 근거는 없다.

한편 사이버 공간를 만들어내는 하드웨어--예컨대 인터넷 서버--는 영토 내에 존재한다. 만약 북한이 우리나라 영토에 소재한 정보통신 네트워크를 '무력으로' 파괴한다면 이 경우는 한미상호방위조약에 의거 미국이 개입할 근거가 된다. 하지만 북한이 우리나라 소재의 정보통신 네트워크를 '무력으로' 파괴하지 않고, 사이버 공간 내에서 혼란이나 마비만을 일으켰다면 이는 한미상호방위조약에 의거해서 미국이 개입할 근거가 될 수 없다. 영토 내에서 도발과 달리 사이버 공간 내에서의 도발은 조약의 적용대상이 아니기 때문이다.

2) 사이버 공격이 외부적 무력공격일 수 있는가?

한미상호방위조약은 외부로부터의 무력공격이 있을 경우에 대비한 것이다. 특히 외부로부터의 무력공격이 있을 시에만 조약상의 의무를 수행하겠다는 것이 미국의 분명한 입장이다. 즉, 내란이라든가 시위 등에 대해서는 한미상호방위조약이 발동할 가능성이 법적으로나 현실적으로나 없다.

사이버 시대가 도래한 후 발생하는 문제는 초국경적이고 초국가적인 공간 내에서 내부와 외부를 구분하는 것이 논리적으로 힘들고 기술적으로도 용이하지 않다는 것이다. 내부와 외부의 경계는 일반적으로 국경선인데, 사이버 공간에서는 국경선의 개념이 명확하지 않고, 설사 국경선이 있다고 하더라도 공격이 어디에서 누구에 의하여 이루어졌는가를 확인하는 데에는 기술적으로 어려움이 있다. 탄도를 계산해 도발의 원점을 찾아낼 수 있는 총포탄에 의한 공격과 달리 논리적 코드(사이버 무기)를 사용한 사이버 공격에 대해서는 도발의 원점

19_ Joint Chiefs of Staff, Joint Pub. 1-02, *Dept. of Defense Dictionary of Military and Associated Terms*, at 41 (12 April 2001).

을 파악하는 것은 쉽지 않다.

보다 더 큰 문제는 무력공격 규정이다. 총포가 사용되지 않고 인명의 살상도 없는데 사이버 공격을 무력공격의 경우라고 볼 수 있는가? 예컨대 3.20 사태나 6.25 사태가 무력공격에 해당하는가? 인명의 피해가 있을 경우에도 문제는 간단하지 않다. 만약 북한이 만든 악성코드 때문에 원자력발전소가 폭발되어 인명의 살상이 있었다면, 그것은 결과적인 의미에서 무력공격에 해당하는가? (만약 무력공격의 판단에 있어서 사용된 '수단'이 아니라 인명피해라는 '결과'가 중요하다면, 북한이 원자력발전소에 쏜 미사일이 불발이어서 원자력발전소가 온전하게 남았다면 이는 결과적으로 무력공격에 해당하지 않는가?) 이러한 질문에서 볼 수 있듯이 사이버 공격은, 非영토적 공간에서 非물리적 수단(사이버 무기)을 사용하여 대개의 경우는 물리적 피해 없이, 그리고 적어도 아직까지는 인명의 살상 없이 이루어지기 때문에 과연 무력공격으로 간주될 수 있는지에 대해서 커다란 이론의 여지가 있다. 이러한 이유로 북한에 의한 사이버 공격은 한미상호방위조약이 발동하는 조건을 구성하기 힘들다.

요약하자면, 사이버 공간은 영토도 아니고, 사이버 공격은 무력 공격으로 보기 힘들며, 사이버 공격이 내부에서 발생한 것인지 외부에서 발생한 것인지 파악도 힘들기 때문에 사이버 공격에 대응하여 한미상호방위조약이 발동되기는 힘들다.

3) 사이버 공간에서 확장억지는 가능한가?

만약에 법리적 판단이 아니라 정치적 결정으로 사이버 공간도 영토라고 간주하고, 사이버 공격도 무력공격으로 간주하여 북한의 사이버 공격이 있을 경우 한미상호조약을 발동시키기로 했다면--이는 현실적으로 가능성이 낮은 가정이다--미국에 의한 확장억지는 가능할까?

확장억지에 대해 관심을 갖는 이유는 확장억지가 한미동맹의 골간을 이루고 있어서이기도 하지만, 많은 전문가들과 정책결정자들이 사이버 공간에서는 방어가 힘들다고 생각하고 있기 때문에 대안으로 억지에 기대를 걸고 있기 때문

이다. 사이버 공간에서 방어가 힘들다고 생각하는 이유로 이들은 우선 사이버 공간에서 잠재적 공격자와 공격수단이 증가한 점을 지적한다. 앞에서 언급한 바 있듯이, 사이버 무기(악성코드)는 손쉽게 복제, 전파 가능할 뿐만 아니라, 민간에서 이미 사용하고 있거나 개발가능한 프로그램인 경우가 많다. 뿐만 아니라, 사이버 공간에서는 공격자를 비공격자로부터 구별하거나 공격용 프로그램을 일반 프로그램과 구분하는 것도 어렵다. 공격용 프로그램과 일반 프로그램을 구분하는 기준은 궁극적으로 사용자의 의도밖에 없을 수 있다. 한편으로 사이버 공간에서 공격을 받을 수 있는 대상은 폭발적으로 증가하였다. 국가, 시장, 사회, 군사 등 모든 부문에서 정보와 통신의 사용과 의존도가 증가하였기 때문이다. 따라서 사이버 공간에서는 위협이 증가하였을 뿐만 아니라 취약성도 증가하였기 때문에 방어는 용이하지 않다.

불을 물로 막을 수 없으면 불로 막듯이 사이버 공격에 대한 방어가 힘들 경우 '조건부' 공격의 위협을 통해서 사이버 공격을 저지하는 전략을 생각해 볼 수 있다. 이를 억지(deterrence)라고 하는데, 억지는 과거 미국과 소련, 그리고 오늘날 미국과 러시아의 핵심적 핵전략으로 채택되어 왔다. 사이버 공격에 대한 방어가 힘든 것처럼 핵공격에 대한 방어도 힘들다. 하지만 핵공격을 받으면 그에 대해 반드시 보복공격을 할 것을 위협함으로서, 미국은 자국에 대한 핵공격을 방지할 뿐만 아니라 우방국에 대한 핵공격도 방지할 수 있었다. 즉, 미국은 방어의 어려움과 공격의 용이함을 이용하여 자국뿐만 아니라 우방국에 대한 선제공격을 억지할 수 있었다.

핵공격에 대한 보복으로 핵공격을 실시하는 것처럼 사이버 공격에 대한 보복으로 상대방에 대해 사이버 보복공격을 실시할 경우 잔존 공격능력(핵전략에서는 제2차 공격능력에 해당)을 갖고 있는 것이 필수적이다. 물론 사이버 공격에 대한 보복이 반드시 사이버 보복공격의 형태로 이루어질 필연적 이유는 없다. 하지만 사이버 공격에 대해 물리적 공격으로 보복하는 데에 따르는 확전의 위험성과 그에 따르는 비난을 생각하면 사이버 공격에 대해서는 일단 사이버 공격으로 보복하는 것이 매력적일 수 있다.

그런데 상대방의 선제 사이버 공격으로 우리의 정보통신망이 마비되었을 경

우에는 보복에 필요한 우리의 잔존 공격능력도 같이 사라져버릴 수가 있기 때문에 설사 보복하려는 의사는 충분하다고 하더라도 보복할 수 있는 능력이 결여되어 억지의 신뢰성에 문제가 발생한다. 이런 경우 미국이 대신 보복을 해준다면 북한의 공격의도가 저하될 가능성이 증가한다. 특히 미국은 세계 최강의 사이버 공격 능력을 가진 것으로 알려져 있기 때문에 보복능력에 대한 신뢰성의 문제는 적다고 볼 수 있다.

그럼에도 불구하고 사이버 공간에서 확장억지를 비롯한 억지전략을 실제로 집행하는 데에 있어서는 여러 가지 어려움이 있다. 첫째는 식별(identification)의 문제로, 사이버 공간에서 발생한 문제가 단순히 사고(accident)나 버그(bug)인지, 아니면 범죄(crime)나 공격(attack)인지 신속하고 정확하게 구분해내기가 쉽지 않다. 문제의 원인을 파악하는 데에는 보통 많은 시간이 소요되며, 정확한 원인은 밝혀내지 못하는 경우도 배제하기 힘들다. 다음은 귀속(attribution)의 문제로, 발생한 문제가 사고나 버그가 아니라 사이버 공격이라고 결론이 나더라도 그 공격이 누구에게 '귀속'되는지, 즉 누가 공격자인지를 찾아내는 것이 쉽지 않다. 사이버 공격 시 공격자는 자신의 정체를 교묘한 방법으로 숨기며, 사이버 공간 내에는 개인에서부터 테러집단, 국가에 이르기까지 다양하고 다수의 행위자가 세계 도처에서 활동하고 있어서 공격자를 색출해내는 것이 쉽지 않다. 공격의 진원지가 북한이라고 확인이 되더라도 북한정부는 자신의 소행이 아니고 다른 집단의 소행이라고 부인할 소지가 크다. 최근 시리아에서 발생한 가스 공격의 경우에서도 알 수 있듯이 진정한 공격자가 누구인지를 확인하는 것은 현실 공간에서 화학무기가 사용된 경우에도 어려우며 사이버 공간에서 사이버 공격이 있었던 경우는 더 더욱 어렵다.

만약 공격을 식별하고, 공격자를 색출하였다고 하더라도 보복이 용이하지 않다. 보복은 보복의 대상을 전제로 하는데, 북한과 같이 폐쇄적이고 정보화가 진행되지 않은 사회의 경우 보복할 대상 자체가 희귀하다. 북한에는 현재 국제적으로 접속이 가능한 인터넷의 사용은 제한되어 있고, 대신 외부로부터 접속이 힘든 내부 전산망(인트라넷)이 발달되어 있다. 국제 해커그룹 '어나니머스'의 주장처럼 인터넷과 인트라넷을 연결시키는 '닌자 게이트웨이'를 만들면 외부망

과 내부망이 연결되겠지만, 이는 통상적으로 가능하지 않은 일이다. 또 북한은 자국 내에서 인터넷 사이트를 운영하는 대신 해외에서 인터넷 사이트롤 많이 운영하고 있으며, 남한에 대한 사이버 공격 시에 중국 등 해외에 있는 컴퓨터와 네트워크를 사용하고 있다. 그렇다고 해서 중국 내부에서 북한이 사용하고 있는 컴퓨터와 네트워크에 대해 보복을 하기는 힘들고, 북한 내부에는 응징의 대상이 될 수 있는 목표물이 많지 않기 때문에 억지전략이 효과적이기 힘들다.

이상의 분석을 통해 볼 때 북한의 사이버 공격은 지금 현재로의 한미상호방위조약을 통해서 대응하기에는 어려움이 많다. 따라서 한미상호방위조약에 의존할 필요가 없도록 사이버 공격에 대한 독자적인 대응능력을 갖춰야 하며, 다른 한편으로는 한미상호방위조약을 사이버 시대에 맞게 업데이트하는 노력이 필요하다.

2. 사이버 시대의 동맹협력: 미국과 이스라엘의 사이버 협력

사이버 시대에 맞게 한미동맹을 업데이트하고 강화하는 데에 있어서 유용한 시사점을 주는 사례는 이란의 핵개발에 대응한 미-이스라엘의 협력경험이다. 중동지역 국가들은 한국이나 미국 등과 같이 정보화가 앞선 국가들이 아니지만, '아랍의 봄'의 경우에서 볼 수 있듯이 SNS 등 정보통신 기술의 발달이 그 지역의 사회와 정치에 급격한 변화를 일으키고 있다. 사이버 공격에 있어서 중동지역은 근래에 들어 '피공격의 대상지'로서 그리고 '공격의 진원지'로서 부상하고 있다.[20]

20_ 중동지역 사이버 공격에 대한 보다 구체적 내용은 한인택, "최근 중동지역 사이버 공격의 사례와 함의," *주요국제문제분석* (2012-42)을 참고하라.

1) Stuxnet 공격

2010년 상반기에 이란의 Natanz 소재 우라늄 농축시설에서 Stuxnet이라고 불리는 악성 코드의 공격이 처음으로 확인되었다. Stuxnet은 원래 이란의 핵시설 컴퓨터만을 감염시켰는데 밝혀지지 않은 경로를 통해서 이란 밖으로 전파되어 그 존재가 확인되었다. Stuxnet은 한 때 155개국 약 100,000개의 컴퓨터를 감염시켰다.

Stuxnet 공격으로 이란이 갖고 있는 원심분리기 5,000개 중 약 1,000개 정도가 파괴되었고, 이란의 우라늄 농축 프로그램이 약 18개월에서 2년까지 지연된 것으로 평가되고 있다. 그럼에도 불구하고 이란은 Stuxnet이 외국으로 유출되어 그 존재가 확인되기 전까지 자신의 컴퓨터 시스템이 악성 코드에 감염되어 있다는 사실을 모르고 있었다. 이는 바로 앞서 언급한 '식별'의 문제를 잘 보여주고 있다. Stuxnet에 감염된 컴퓨터들이 다른 컴퓨터들과 철저히 분리된 시스템이었기 때문에 이란으로서는 악성코드가 원심분리기가 파괴된 원인이라고 인식하기 힘들었던 것으로 추정된다. 이처럼 철저히 분리된 컴퓨터 시스템에 악성 코드를 심은 점으로 보아 Stuxnet 공격은 단순히 해커집단의 소행이라고 보기 힘들다는 것이 지배적 의견이었는데, 미국과 이스라엘 정부 인사들이 Stuxnet이 미국과 이스라엘 정부의 공동작품이라는 사실을 밝힘으로서 그 탄생의 비밀이 밝혀지게 되었다. Stuxnet을 철저히 분리된 컴퓨터 시스템에 심는 것도 힘든 작업이지만 Stuxnet의 개발자체도 국가나 국가의 후원을 받는 집단이 아니면 생각하기 힘든 작업이었다.

이란의 핵개발을 저지하겠다는 일반적 동기 외에 미국이 Stuxnet 개발에 관심을 갖게 된 구체적인 이유는 이스라엘이 고려하고 있는 이란 농축우라늄 시설에 대한 공습이 그 효과는 불확실하지만 그에 대한 반발과 여파는 상당할 것으로 예상되었기 때문이다. 공습대신 이란의 핵개발 프로그램을 지연 내지 좌절 시킬 수 있는 방안으로 전에는 시도해 본 적이 없는 사이버 공격을 시도한 것이다. 아울러 경제제재의 효과가 나타나기를 기다리는 동안 이란의 핵프로그램의 진전을 막으려는 의도도 존재하였다. 이란에 대한 공습을 고려 중이던 이

스라엘이 Stuxnet의 개발에 참여하게 된 이유는 이스라엘이 Stuxnet 개발과 공격에 필요한 정보와 기술을 가지고 있었다는 점 외에도 Stuxnet을 투입해 본 결과 그 효과가 상당하다는 것을 알았기 때문이다. 앞서 언급했듯이 Stuxnet의 존재가 발각되기 전까지 Stuxnet은 이란의 우라늄 농축기의 1/5을 파괴하였다. 만약 Stuxnet의 존재가 발각되지 않았다면 Stuxnet의 효과는 더 컸을 것이다. 이런 면에서 Stuxnet 사례는, 사이버 공격이 공습의 대안으로 선택되었고 경제제재의 효과가 나타날 수 있는 시간을 벌었다는 점에서 앞서 언급한 '사이버 평화론'과 부합하는 측면이 많다.

Stuxnet 사례가 특별히 관심을 끄는 이유는 사이버 공격이 사이버 공간에서만 이루어지는 것이 아니라 현실 공간으로 확대되었기 때문이다. Stuxnet은 그 효과가 단순한 첩보나 다른 컴퓨터에 대한 피해에 그치지 않고 원심분리기를 파괴시켜 사이버 공간과 현실 공간 사이의 벽을 뛰어넘었다고 평가되고 있다. 이를 보고 일부에서는 비유적으로 사이버 전쟁의 '루비콘 강'을 건넌 것으로 표현하였다. 이렇듯 사이버 공간에서 현실 공간으로 도약은 사이버 공격의 위력을 증대시키는 직접적 효과는 물론, 그 동안 사이버 공간 내의 공격은 사이버 공간 내로 제한해온 암묵적 합의를 파기한 것으로 인식되어 향후 사이버 공격이 물리적 피해를 동반하게 될 가능성이 증대하였다.

2) Flame 공격

이란의 핵개발을 막으려는 미-이스라엘의 공동노력은 Stuxnet만에 국한되지 않는다. 지금까지 알려진 추가적인 사례로 Flame 공격을 들 수 있다. 2012년 5월 이란의 국립 CERT(Computer Emergency Response Team) 및 Kaspersky Lab 등 컴퓨터 보안기관들이 Flame이라고 불리는 첩보용 프로그램의 존재를 확인하였다. 컴퓨터 네트워크와 USB 메모리를 통해 전파되는 Flame은 소리, 화면, 키보드 동작, 네트워크 활동, 나아가 블루투스 설치되어 있는 컴퓨터의 경우 그 주변에 있는 블루투스 기기의 활동과 데이터까지도 탐지하는 종합적인 첩보 프로그램이다. 예컨대 블루투스를 통해서 컴퓨터 주변에 있는 스마트폰의

전화번호부에 접근할 수 있었다. Flame은 이란의 국립 CERT에 의해서 확인되었을 뿐만 아니라 감염된 컴퓨터의 다수가 이란에 위치하여 Stuxnet과 마찬가지로 이란을 대상으로 한 사이버 공격으로 생각되고 있다.

앞서 살펴본 Stuxnet과 Flame의 차이는 전자는 sabotage를 목적으로 한 것이라면 후자는 espionage를 목적으로 한 것인데, 전세계적으로 감염된 것으로 추산되는 약 1,000 대 컴퓨터 중 약 65%가 이란, 이스라엘, 수단, 시리아, 레바논, 사우디아라비아, 이집트 등 중동지역에 위치하고 그 중 많은 수가 이란에 소재하고 있다. 또한 Flame은 Stuxnet 보다도 약 20배 정도 더 크고 더 복잡한 프로그램으로 주로 정부기관과 교육기관 등을 목표로 하였다. Flame의 코드 분석에는 약 10년은 걸릴 것이라는 것이 전문가들의 평가이며, 발각되는 것을 피하기 위해 프로그램의 흔적을 스스로 지워버리는 기능도 탑재하였다.

이러한 프로그램의 복합성, 공격 대상의 특성 등을 고려할 때 Flame 역시 Stuxnet처럼 국가나 국가의 지원을 받는 개발자에 의해서 만들어졌을 가능성이 대단히 높은데, 워싱턴 포스트 지는 Flame도 Stuxnet과 마찬가지로 “올림픽 게임” 작전의 일환으로 미국의 National Security Agency와 이스라엘의 군대에 의하여 공동 개발되었다고 보도하였다. 이러한 주장은 이란의 CERT가 Flame에서 이스라엘에서만 발견되는 특별한 암호화 패턴을 발견했다고 주장으로 또한 뒷받침된다.

3. 소결

사이버 공격은 통상적인 군사공격이나 핵공격과 함께 한반도 평화와 안보를 위협하는 새로운 변수로 부상하고 있으나 그 정확한 함의에 대한 이해나 효과적 대응방안에 대한 논의가 부족한 상태이다. 그리고 한미동맹처럼 과거 평화와 안전을 보장했던 제도와 장치들은 사이버 공격에 대응하는 데에 한계를 보이고 있다. 따라서 사이버 공격을 받았을 경우에 대비하여 효과적이고 안정적인 대응책을 미리 수립해 놓을 필요가 있다. 이는 과거와 마찬가지로 한미 간의 협력이 중요한 요소가 될 것이고, 미국과 이스라엘 간 사이버 협력은 좋은 준거

사례가 된다. 만약 우리도 비핵확산 노력의 일환으로 북한에 대해 Stuxnet과 같은 사이버 무기를 한미가 공동으로 개발하여 사용했었다면, 북한의 핵개발을 방지하거나 미사일 개발 계획을 지연시킬 수도 있었을 것이다. 만약 한미 사이버 협력의 부족으로 사이버 무기가 개발, 투입되지 못하였다면--이는 공개적으로 확인하기 힘든 사항이다--북한의 핵무기 개발과 미사일 개발을 막을 수 있던 '기회의 창'을 놓친 것으로 볼 수 있다.

사이버 공간의 평화적 사용과 사이버 분쟁의 평화적 해결 등에 관한 국제적 규범이 아직 미발달한 영역이다. 우리나라는 2013년 제3차 사이버스페이스 총회의 개최국으로서 사이버 공간에 관련된 국제적 규범을 창출하는 데 중요한 역할을 할 것으로 기대되고 있다. 예컨대 사이버 공간에서 허용되는 정당방위는 무엇인지, 사이버 무기의 군축을 위한 원칙과 절차는 어떻게 되어야 하는지에 대해 서울 사이버스페이스 총회를 기회로 각국이 견해를 교환하고 의견을 수렴할 수 있게 하는 것이 바람직하다.

Ⅳ. 결론을 대신하여

1. 사이버 시대의 평화와 안보

새로운 기술의 등장은 새로운 안보적 위협과 기회를 낳는다. 평화와 안보를 증진하는 기존의 사고나 제도는 새로운 기술의 등장에 따르는 안보적 위협과 기회에 대응하는데 적합하지 않을 수 있다. 예컨대 기존의 안보 개념은 단선적이고 물리적이다. 국경선, 철책선, NLL 등의 경계선을 기준으로 '안'과 '밖'을 구분하고, 안보 전략은 '안'과 '밖' 사이의 경계선을 강화하거나 물리적으로 침범되지 않게 하는 데에 주력하였다. 최근의 변화들은, 특히 국제화와 정보화의 진전은 경계선의 의미를 많이 퇴색시켰고, 사이버 공격이 물리적 타격 못지않게 평화와 안보를 위협할 수 있음을 보여주었다. 사이버 시대의 평화와 안보 개념은 이러한 경계의 약화나 비물리적 위협의 등장을 반영하여야 한다. 변화가 필요한 것은 개념과 전략만이 아니다. 6.25 전쟁의 종전 이후 반세기 이상 북한이 남한에 대해 대규모 공격을 감행하지 않은 데에는 미국의 확장억지 공약에 기반한 한미동맹의 역할이 크지만, 사이버 시대에는 한미상호방위조약을 통해 제공되는 확장억지의 신뢰성이 크게 위협받고 있다. 따라서 기존의 제도와 사고를 점검하고, 새로운 안보 위협과 기회에 잘 대응할 수 있도록 정비할 필요가 있다. 특히 우리나라처럼 다른 나라에 비해서 정보통신기술의 이용이 활발하고, 사이버 공간에 대한 사회적, 경제적 의존도가 높은 경우에는 사이버 시대에 맞게 신속하게 제도와 사고의 진화가 필요하다. 그러기 위해서는 발생하고 있는 사이버 공격을 경험적으로 살펴보는 것이 유용할 수 있다. 중동지역에서는 이제 사이버 공격이 통상적인 군사공격이나 테러공격과 함께 안정과 평화를 위협하는 새로운 변수로 부상하고 있다. 더욱이 사이버 무기는 그 특성상 사용이 특정 지역에 제한되지 않고, 이전도 은밀하게 진행될 수 있기 때문에 다른 지역으로 확산될 가능성이 존재한다. 중동이나 미국에서 발생한 사이버 공격이 언제라도 한반도에서도 재연될 가능성을 배제할 수 없기 때문에 사이버

안보전략의 수립이 시급하다. 물론 사이버 시대의 안보 위협과 기회에 대처해야 하는 것은 단지 우리나라의 과제만은 아니다. 대개의 나라들이 최근에야 사이버 안보에 관심을 기울이기 시작했으며, 국제적으로도 사이버 공간의 평화적 사용이나 사이버 분쟁의 평화적 해결 등에 관한 규범이 아직 발달하지 못한 상태이다. 우리나라는 2013년 제3차 사이버스페이스 총회의 개최국으로서 사이버 공간에 관련된 국제적 규범을 창출하는 데 중요한 역할을 할 것으로 기대된다.

2. 사이버 위협을 보는 두 시각

혁신적인 기술의 발전은 새로운 공간의 출현을 낳고, 새로운 공간의 출현은 그에 따른 국제안보적 파급효과를 낳는다. 새로운 공간이 출현하면 그 공간을 누가 지배하고, 어떻게 이용하느냐에 따라서 전략적 우열이 바뀔 수 있다. 과거 제해권, 제공권에 대한 논의나 현재 사이버 공간 내 주도권에 관한 논의는 그런 맥락에서 이해될 수 있다. 그런데 사이버 공간은 그 이전에 출현한 공간과 중요한 차이를 가지고 있다. 인간의 의지나 행동과는 무관하게 존재하는 물리적 공간과 달리 사이버 공간은 탄생이나 존재, 확대에 있어서 전적으로 인간의 의지와 노력의 산물이다.

사이버 공간은 행위자들에 의해 매일매일 '구성되는' 공간이기 때문에, 사이버 공간에 대해 행위자가 갖는 관념과 선택이 사이버 공간의 성격을 결정하는 중요한 변수가 될 수 있다. 우선 행위자들이 사이버 공간을 위험한 공간으로 보느냐 안전한 공간으로 보느냐에 따라 행위자들의 사이버 공간 관련 전략과 행동이 달라질 것이고, 행위자들의 전략과 행동에 따라서 궁극적으로는 사이버 공간의 질서나 성격이 달라질 수 있다. 사이버 공간의 안보적 위협에 대한 견해를 크게 '위협 실재론'과 '위협 과장론'으로 양분할 수 있다.

사이버 공격이 임박했고 사이버 공격의 위협이 심각하다는 주장을 '위협 실재론'이라고 한다면, '위협 과장론'은 그와 반대로 사이버 공간의 위협 요소를 낮게 평가한다. '위협 과장론'에 의하면 사이버 공간은 원래 위험스러운 것이

아니고 오히려 사이버 공간이 위험하다는 주장이 사이버 공간을 위험하게 만든다고 주장한다. 위협 실재론이 지배적으로 되면 사이버 공간의 군사화를 부추겨서 사이버 공간을 자기실현적으로 위험하게 만들 수 있기 때문이다.

많은 전문가 사이에서는 위협 실재론이 지배적인 견해이다. 하지만 위협 과장론에도 주의를 기울여야 하는 이유는, 인류최대의 위협이 되는 "사이버게돈(Cybergeddon)"이 다가오고 있다는 반복되는 경고에도 불구하고 실제로 사이버 공격은 지금까지 상대적으로 희소하였고, 그 효과는 인류 최대의 위협은 커녕 일시적 불편함과 혼선만을 야기하는 정도였기 때문이다. 이러한 사실이 주는 함의는 위협 실재론에서 주장하는 것보다 사이버 공격에 대한 방어가 효과가 있거나, 사이버 공격의 파괴력이 위협 실재론에서 생각하고 있는 것보다 제한적일 수 있다는 것이다. 나아가 만약 사이버 공격이 물리적 공격을 대체할 수 있다면, 사이버 공간의 등장은 물리적 공간에서의 충돌을 피해가 더 제한적인 사이버 공간으로 옮김으로서 역설적으로 국제안보와 평화에 기여할 가능성도 있다.

위협 실재론의 논리를 좀 더 자세히 살펴보면, 우선 사이버 무기가 국가뿐만 아니라 다양하고 다수인, 그리고 많은 경우 익명인 비국가 행위자들의 손에 들어갈 수 있다는 점을 강조하고 있다. 이것이 가능한 이유는 사이버 무기가 손쉽게 복제, 전파 가능할 뿐만 아니라 민간에서 이미 사용하고 있거나 개발가능한 프로그램이기 때문이다. 따라서 사이버 공간에서 잠재적인 공격자와 공격수단이 증가하였을 뿐만 아니라, 공격자를 비공격자로부터 구별하거나 공격용 프로그램을 일반 프로그램과 구분하는 것이 어렵다. 어쩌면 공격용 프로그램과 일반 프로그램을 구분하는 기준은 궁극적으로 사용자의 의도밖에 없을 수도 있다. 한편 공격을 받을 수 있는 대상도 폭발적으로 증가하였다. 국가, 시장, 사회, 군사 등 모든 부문에서 정보와 통신의 사용과 의존도가 증가하였기 때문이다. 과거에는 안보적 위협이 증가하고 안보적 취약성이 늘어나더라도 국가가 개입하여 어느 정도의 위협관리가, 특히 국경 내에서는 가능하였다. 하지만 종래의 안보위협과 달리 사이버 공격은 초국경적이고 순식간에 발생하기 때문에 국가가 효과적으로 대처하기가 힘들다.

사이버 공간의 특성과 사이버 무기의 속성으로부터 사이버 공간의 안보위협을 연역하여 보면 사이버 공간은 위태롭고 갈등의 가능성이 높은 곳으로 보이지만, 사이버 공격의 횟수나 피해를 경험적으로 살펴보면 그와는 상당히 다른 평가가 가능하다. 공수균형이나 공수구분을 기준으로 사이버 안보 딜레마의 강약을 평가해 보면 국가 간의 안보관계가 마치 제로섬적 성격을 보일 것으로 생각이 들지만, 물리적 공간과 달리 사이버 공간은 선택적으로, 그리고 원하는 조건으로 참여할 수 있다는 점을 고려하면 사이버 안보 딜레마는 기대보다 경미할 수 있다.

"사이버 공간은 구성된 환경으로서 우리가 선택하여 만드는 대로이다(As a constructed environment, cyberspace(s) is very much what we choose to make it)." 사이버 공간이 행위자들이 '구성'하는 공간이기 때문에, 행위자들의 시각과 관념이 중요하다. 행위자의 생각이 자기실현적으로 경우에 따라서는, '자기부정적으로' 사이버 공간에서 현실로 실현될 수 있기 때문이다. 이러한 복합적인 관계를 이해하고, 사이버 공간을 가장 안정적이고 평화적으로 만들 수 있는 시각과 관념이 무엇인지 찾아내고 주류화시키는 것이 필요하다.

3. 사이버 공간에서의 동맹협력: 한미상호방위조약의 한계와 미-이스라엘 동맹의 함의

6.25 전쟁의 종전 이후 반세기 이상 북한이 남한에 대해 대규모 공격을 감행하지 않은 데에는 미국의 확장억지 공약에 기반한 한미동맹의 역할이 크다. 미국이 확장억지를 제공하는 조약적 근거는 1953년 체결할 한미상호방위조약이다. 이 조약에 의하면 양국은 "행정관리하에 있는 영토(territories under their respective administrative control)"에 대해 "외부로부터 무력공격(external armed attack)"이 있을 경우 협의를 통해서 필요한 조치들을 취하기로 약속하였다. 그런데 "행정관리 하에 있는 영토"나 "외부로부터 무력공격" 등 조약에 사용된 표현들은 조약이 체결된 당시에는 적합하고 문제가 없었지만, 사이버 시대가 도래하면서 과거에 예상하지 못했던 문제점들이 발생한다.

사이버 시대가 도래하며 발생하는 한미상호방위조약의 문제는 첫째, 사이버 공간이 한국이든 미국이든 특정국가가 행정적으로 지배하는 영토로 보기 힘들다는 점이다. 사이버 공간은 현재까지 초국가적이고, 초국경적인 공간으로 존재하고 있다. 사이버 공간은 법적으로 한미상호방위조약의 적용 지역이 아니다. 따라서 사이버 공간에서의 도발이나 충돌에 대해 한국이 미국의 원조를 기대할 수 있는 조약적인 근거는 없다. 둘째로, 한미상호방위조약은 외부로부터의 무력공격이 있을 경우에 대비한 것이다. 특히 외부로부터의 무력공격이 있을 시에만 조약상의 의무를 수행하겠다는 것이 미국의 분명한 입장이다. 사이버 시대가 도래한 후 발생하는 문제는 초국경적이고 초국가적인 공간 내에서 내부와 외부를 구분하는 것이 논리적으로 힘들고 기술적으로도 용이하지 않다는 것이다. 내부와 외부의 경계는 일반적으로 국경선인데, 사이버 공간에서는 국경선의 개념이 명확하지 않고, 설사 국경선이 있다고 하더라도 공격이 어디에서 누구에 의하여 이루어졌는데 확인하는 데에는 기술적으로 어려움이 있다. 보다 더 큰 문제는 무력공격 규정이다. 이 사이버 공격은 非영토적 공간에서 非물리적 수단(사이버 무기)을 사용하므로 대개의 경우는 물리적 피해 없이, 그리고 적어도 아직까지는 인명의 살상 없이 이루어지기 때문에 과연 무력공격으로 간주될 수 있는지에 대해서 커다란 이론의 여지가 있다. 이러한 이유들로 북한에 의한 사이버 공격은 한미상호방위조약이 발동하는 조건을 구성하기 힘들다.

하지만 만약에 법리적 판단이 아니라 정치적 결정으로 사이버 공간도 영토라고 간주하고, 사이버 공격도 무력공격으로 간주하여 북한의 사이버 공격이 있을 경우 한미상호조약을 발동시키기로 했다면 미국에 의한 확장억지는 가능할까?

사이버 공간에서 확장억지를 비롯한 억지전략을 실제로 집행하는 데에 있어서는 여러 가지 어려움이 있다. 첫째는 식별(identification)의 문제로, 사이버 공간에서 발생한 문제가 단순히 사고(accident)나 버그(bug)인지, 아니면 범죄(crime)나 공격(attack)인지 신속하고 정확하게 구분해 내기가 쉽지 않다. 문제의 원인을 파악하는 데에는 보통 많은 시간이 소요되며, 정확한 원인은 밝혀내지 못하는 경우도 배제하기 힘들다. 다음은 귀속(attribution)의 문제로, 발생

한 문제가 사고나 버그가 아니라 사이버 공격이라고 결론이 나더라도 그 공격이 누구에게 '귀속'되는지, 즉 누가 공격자인지를 찾아내는 것이 쉽지 않다. 사이버 공격 시 공격자는 자신의 정체를 교묘한 방법으로 숨기며, 사이버 공간 내에는 개인에서부터 테러집단, 국가에 이르기까지 다양하고 다수의 행위자가 세계 도처에서 활동하고 있어서 공격자를 색출해내는 것이 쉽지 않다. 셋째, 만약 공격을 식별하고, 공격자를 색출하였다고 하더라도 보복이 용이하지 않다. 보복은 보복의 대상을 전제로 하는데, 북한과 같이 폐쇄적이고 정보화가 진행되지 않은 사회의 경우 보복할 대상 자체가 희귀하다. 이상의 분석을 통해 볼 때 북한의 사이버 공격은 지금 현재로의 한미상호방위조약을 통해서 대응하기에는 어려움이 많다. 따라서 한미상호방위조약에 의존할 필요가 없도록 사이버 공격에 대한 독자적인 대응능력을 갖춰야 하며, 다른 한편으로는 한미상호방위조약을 사이버 시대에 맞게 업데이트하는 노력이 필요하다. 사이버 시대에 맞게 한미동맹을 업데이트하고 강화하는 데에 있어서 유용한 시사점을 주는 사례는 이란의 핵개발에 대응한 미-이스라엘의 협력경험이다. 만약 우리도 비핵확산 노력의 일환으로 북한에 대해 Stuxnet과 같은 사이버 무기를 한미가 공동으로 개발하여 사용했었다면, 북한의 핵개발을 방지하거나 미사일 개발 계획을 지연시킬 수도 있었을 것이다. 만약 한미 사이버 협력의 부족으로 사이버 무기가 개발, 투입되지 못하였다면 북한의 핵무기 개발과 미사일 개발을 막을 수 있던 '기회의 창'을 놓친 것으로 볼 수 있다.

V. 정책고려사항

○ 사이버 공간의 확장으로 경제가 효율적으로 되고 비즈니스가 글로벌해지는 등 장점이 많지만, 사이버 공간을 어떻게 평화롭고 안전하게 지킬 수 있는지 아직 모르는 상태에서 사이버 공간에 대한 의존이 심화되고 있음.

- 광대역 인터넷(브로드밴드) 보급률은 전세계적으로 약 40퍼센트, 미국의 경우는 60퍼센트, 한국의 경우는 90퍼센트 이상임. 물론 인도, 중국, 필리핀처럼 아직까지 낮은 광대역 인터넷 보급률을 보이고 있는 경우도 아직 존재함.
- GDP 대비 '인터넷 경제'의 비율도 영국의 경우 8%, 한국의 경우 7% 수준이며, 선진국 평균이 4%, 후진국 평균도 3%를 상회하는 등 인터넷의 경제적 비중이 상당 수준에 도달.

○ 사이버 공간은 현실 세계에 비해 자유롭고 개방적. 하지만 사이버 공간 내 평화와 질서를 규율할 수 있는 상위 권위체가 존재하지 않는다는 면에서 무정부적임. 뿐만 아니라 사이버 공간은 차기의 전장(next operational domain)으로 간주되어 군사화가 급속하게 진행되고 있음.

- 이란이나 북한처럼 사이버 공간에 대한 접근이나 사이버 공간 내에서의 활동에 대해 제한을 가하고 있는 경우가 있기 때문에 사이버 공간을 일률적으로 자유롭고 개방적 공간이라고 볼 수는 없음.
- 사이버 공간의 군사화와 관련하여, 현재 100여 개국 이상에서 사이버 무기를 개발 중인 것으로 알려져 있음.

○ 사이버 공간 내에서 위협이 최근 기하급수적으로 증가하고 있으며, 교통시설(항공, 철도, 해운) 등 기간시설에 대한 공격도 계속되고 있음.

- 사이버 공격의 유형과 수법은 다양. 사이버 전쟁은 희귀하지만 사이버 테러, 사이버 사보타지, 사이버 첩보, 사이버 범죄, 해킹 등이 자주 발생하고

있으며, 공격방법도 악성코드 투입에서부터 DDoS 공격, 백도어 (back-door) 등으로 다양화.

- 가장 흔한 공격수단은 바이러스, 웜, 트로이잔이고, 가장 잘 안 쓰이는 그렇지만 사용 시 효과가 큰 공격방법은 Denial of Service(DOS) 임.

○ 사이버 공격이 가장 자주 발생하는 지역은 아태지역임. 2012년 현재 아태지역에서 관측된 사이버 공격의 42퍼센트가 발생하였음. 유럽에서는 관측된 사이버 공격의 35퍼센트가, 북미와 남미에서는 21퍼센트, 그리고 아프리카에서는 단지 1.5퍼센트가 발생.

- 지역 내에서도 국가별로 차이가 발생하여 미국과 한국의 컴퓨터에 대한 사이버 공격이 가장 많으며, 인도나 네덜란드, 독일 등의 컴퓨터에 대한 사이버 공격이 가장 낮음.

○ 사이버 공격은 일반적으로 아래와 같은 특징을 가지고 있는 것으로 생각되고 있음. 하지만 이러한 특징이 경험적으로 현실과 일치하는지에 대해서는 검토가 필요할 수 있음.

- 공격자가 무수하고, 익명이며, 국내나 해외에서 활동할 수 있고, 국가뿐만 아니라 비국가 행위자일 수도 있음.
- 공격에 비용이 크게 들지 않으며, 순간적이고, 비대칭적이며 초국경적인 특징을 가지고 있음.
- 사이버 공격은 보통 인명의 살상을 낳지 않음.

○ 이러한 특징 때문에 사이버 공격에 대응하는 데에 있어서 여러 가지 문제가 발생함. 첫째 '인식'의 문제로, 사이버 공간에서 발생한 문제가 사고나 오류의 결과인지 범죄의 결과인지 아니면 공격의 결과인지 알기 어려움. 둘째로 '귀속'의 문제로, 공격으로 확인되더라도 공격자가 누구인지 파악하기 쉽지 않음. 마지막으로 보복이 쉽지 않음. 이는 단순히 '인식'과 '귀속'의 문제 때문이 아니고 기술과 규범의 문제이기도 함. 효과적인 보복은 기술적으로 힘

들고, 보복에 관한 국제규범이 정립되어 있지 않아서 국제적으로 비판과 반대에 봉착할 위험성도 존재.

-이러한 문제들은 단지 한국에 대한 사이버 공격에서만 발생하는 것이 아니고 보편적인 문제임.

○ 평화와 안보를 유지, 증진하는 국가들의 전략들이 사이버 공간에서는 효과적이지 않음.

- 공격이 순간적이고, 공격자는 익명이며 위치도 파악이 안 되는 경우가 많기 때문에 '방어'는 쉽지 않으며, 비슷한 이유로 '억지'도 용이하지 않음. 더군다나 사이버 공격에는 대개의 경우 인명살상이 따르지 않아서 만약 보복이 심할 경우에는 국제적으로 지탄을 받을 우려도 있음. 결국 기술적 이유, 규범적 이유로 사이버 공간에서 억지전략은 신뢰성 및 정당성의 문제로부터 자유롭지 않음.

○ 기존의 국가전략들이 사이버 공간에서는 비효과적이기 때문에 집단적인 노력, 즉 국제협력이 중요할 수 있음. 문제는 사이버 공간에서도 안보의 딜레마가 존재하기 때문에 국제협력에 장애가 될 수 있음.

- 안보의 딜레마란 한 국가가 자신의 안보를 증진시키기 위해 취하는 조치들이 다른 국가들의 안보를 감소시키는 상충관계(trade-off)를 의미.
- 어떤 연유에서이건 상충 관계가 강해지면 국제관계는 제로섬 게임의 성격을 갖게 되며 국제평화와 국제협력이 어려워짐.
- 만약 상충관계가 약해지면 국제관계는 포지티브섬 게임의 성격을 갖게 되고 국제평화와 국제협력이 용이해짐.

○ 안보의 딜레마의 경중을 결정하는 요소로 '공수균형'과 '공수구분'이 대표적임.

- '공수균형'이란 공격과 수비 간 상대적 우위에 관한 것으로 방어가 공격보다 유리할 때 안보의 딜레마는 감소하고, 공격이 방어보다 유리할 경우

안보의 딜레마는 심화됨.

- '공수구분'이란 무기나 전략이 얼마나 명확히 공격용과 수비용으로 차별되는가에 관련된 것으로 공수의 구분이 명확할수록 안보의 딜레마가 감소.

○ 공수균형과 공수구분이라는 두 기준으로 볼 경우 사이버 공간은 논리적으로 안보의 딜레마가 발생하기 좋은 여건을 가지고 있음.

- 공수의 구분이 쉽지 않은 데에다가 공격도 우위라서 국제관계는 제로섬 게임적의 성격을 가질 소지가 큼.

○ 사이버 공간의 특성과 사이버무기의 속성으로부터 사이버 공간의 안보위협을 연역하여 보면 사이버 공간은 위태롭고 갈등의 가능성이 높은 곳으로 보임. 하지만 사이버 공격의 횟수나 피해를 경험적으로 살펴보면 그와는 상당히 다른 평가가 가능.

- 공수균형이나 공수구분을 기준으로 사이버 안보 딜레마의 강약을 평가해 보면 국가 간의 안보관계가 마치 제로섬적 성격을 보일 것으로 생각이 들지만, 물리적 공간과 달리 사이버 공간은 선택적으로, 그리고 원하는 조건으로 참여할 수 있다는 점을 고려하면 사이버 안보 딜레마는 기대보다 경미할 수 있음.

○ 사이버 공간에서는 평화와 안보를 지키는 전통적 전략--방어, 공격, 억지--이 갖는 한계 때문에 전통적 전략을 보완 또는 대체할 수 있는 국가적, 국제적 노력이 필요함.

- '역량구축(capacity building),' '신뢰구축(confidence building),' '규범구축(norm building)'은 국가들이 단독적으로 또는 협력을 통해서 사이버 공간에서 평화와 안보를 유지, 증진할 수 있는 조치임.

○ '역량구축'이란 사이버 공간을 방어하고 위기를 예방하고 대응하는 기술적, 기술 외적(外的) 능력을 육성하는 것으로 다른 나라의 호응이 없어도 단독

으로 시행할 수 있음.

○ ‘신뢰구축’이란 사이버 공간에서 국가 간 긴장과 갈등을 줄이는 조치들로 국가 간의 소통을 증진시키는 조치, 행동이나 선택에 제한을 가하는 조치, 정보의 공유나 투명성을 제고하는 조치 등을 포함.
- 쿠바 미사일 위기 이후 미국과 소련 간 설치된 핫라인(hotline) 같이 국가 간 소통을 돕는 조치는 위기 시 의도치 않은 갈등의 심화를 방지.
- ‘선제 불사용 정책(no first use policy),’ ‘민간 타깃 불공격 정책(no civilian target doctrine),’ ‘현실 공간-가상 공간 비확전 공약(no cross-domain escalation commitment)’ 등 사이버 공간 내에서 행동이나 선택을 제한하는 조치들은 의도하지 않게 분쟁이 확대되는 것을 방지.
- 투명성을 증대하는 조치와 검증(verification)은 전통적으로 신뢰구축에 도움이 되나 사이버 공간에서 실행이 어려울 수 있음.

○ 신뢰구축은 국가 간 불신과 위기 시 불확실성을 해소하는 데에 도움이 되기 때문에 안보 딜레마를 완화시키고 국제협력의 가능성을 제고할 수 있음.

○ 국가의 행동을 규율하는 규범이 아직 미비한 사이버 공간에서는 ‘규범구축(norm building)’도 평화와 안보를 위해서 중요한 과제임.
- 새로운 영역으로서 사이버 공간에서는 규범 발달이 미비. 잘 발달된 규범은 국가의 선호와 행태에도 영향을 줄 수 있기 때문에 사이버 공간에서도 규범의 구축이 바람직.
- 현실 공간에서 국가 간 무력충돌에 전쟁법이 일정한 역할을 하는 것처럼 사이버 공간에서의 분쟁에 적용될 수 있는 규범이 발달되면 분쟁이 평화적으로 해결되거나 불필요한 확전을 방지할 수 있음.

○ 사이버 공간은 새로운 공간으로 평화와 안보를 유지하고 증진하기 위한 국가전략이나 국제협력에 대한 연구와 논의가 지금 활발히 진행 중임. 한국은

중견국가로서 국제적 논의에서 목소리를 내고 있으며, 특히 IT 분야 강국으로서 인정받고 있기 때문에 사이버 공간에서의 평화와 안보에 관련된 연구와 논의에서 선도적 역할을 수행할 수 있음.

- 특히 스페이스 총회는 한국이 사이버 공간에서의 역량구축, 신뢰구축, 규범구축을 위한 논의와 행동에서 적극적으로 참여하고 리더십을 발휘하여 좋은 기회가 될 수 있기 때문에 적극적으로 활용할 필요가 있음.

참고문헌

원유재, “사이버공격 대응하는 총괄 보안 컨트롤타워 필요하다,” *과학과 기술*, 2013.5.

장노순·한인택, “사이버안보의 쟁점과 연구경향,” *국제정치논총* 제53집 3호(2013).

한인택, “동맹과 확장억지: 유럽의 경험과 한반도에의 함의,” 제주평화연구원, 2009.9.

한인택, “‘핵무기 없는 세상’과 핵우산,” *JPI PeaceNet*, 2010.

한인택, “최근 중동지역 사이버 공격의 사례와 함의,” *주요국제문제분석*(2012-42).

한인택, “사이버 시대의 국가안보,” *JPI PeaceNet*, 2013.1.

한인택, “사이버 공격, 어떻게 대응해야 하나?” *한겨레*, 2013.3.26

-----, “Cyber-warfare: Hype and fear" *The Economist*(Dec. 8th, 2012).

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*(Strategic Studies Institute, U.S. Army War College Press, 2013).

Joint Chiefs of Staff, *Joint Pub. 1-02, Dept. of Defense Dictionary of Military and Associated Terms, at 41*(12 April 2001).

Hirschman, Albert. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*(Harvard Univ. Press, 1970).

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge Univ. Press, 2007).

Rattray, Greg. *Strategic Warfare in Cyberspace*(MIT press, 2001).

Trachtenberg, Marc. “Strategic Thought in America 1952?1966.” in *History and Strategy*, (Princeton, NJ: Princeton University Press, 1991).

Van Evera, Stephen. “The Cult of the Offensive and the Origins of the First World War,” *International Security*, Vol. 9, No. 1(Summer, 1984).

Waltz, Kenneth. “The Spread of Nuclear Weapons: More May Better,” *Adelphi Papers*, Number 171(London: International Institute for Strategic Studies, 1981).

World Federation of Scientists, “Erice Declaration on Principles for Cyber Stability and Cyber Peace,” Aug. 2009, http://www.aps.org/units/fip/newsletters/201109/barletta.cfm