사이버안보 위협의 특징과 안보정책적 쟁점들

장노순 (한라대학교)

정부의 시스템, 국방 전력, 경제 활동 그리고 사회의 일상생활 등은 컴퓨터, 인터넷, 네트워크 시스템에 의존하는 정도가 더욱 심화되고 있다. 이런 사이버공간의 의존성은 비대칭 위협, 사이버전, 사이버테러 등의 용어로 설명되는 새로운 유형의 안보환경을 만들어내고 있다. 미국이나 남한은 정보통신 강국이나 사이버 강국으로 대외에 알려져 있지만, 한편으로 사이버 위협에 가장 취약한 국가처럼 논의되고 있다. 하지만 사이버안보의 위기가 심화되는 요인은 급격한 기술발달과 비교해서 안보정책과 전략의 부족, 정치지도자의 인식 부재, 제도적 미비, 정부 조직간의 관료정치적 장애, 민간기업의 비협조, 사회문화적 태도 등이 제대로 뒷받침되고 있지 못한데 기인한다. 여기에서 사이버안보에 대한 위협은 전통적인 안보위협과 어떤 차이점이 있는지를 안보수단 측면에서 설명하고, 사이버안보의 대내외 안보정책과 관련하여 논의되고 있는 중요한 쟁점들을 짚어 보았다.

1. 안보수단의 전략적 의미

(1) 전략폭격기

1차 세계대전을 치루면서 당시 주요 군사강대국들은 전략폭격기를 안보전략의 핵심으로 받아들였다. 현재에도 미국은 전략폭격기를 여전히 운용하면서 안보전략의 중요한 수단으로 활용하고 있다. 전략폭격기는 사활적인 생존이 걸린 국가간 분쟁에서 승리를 결정하는 수단이 되지 못한다. 그러나 국가 사이에 세력 불균형이 있는 분쟁에서 강대국이 단기적인 분쟁을 유리하게 이끌 수 있는 역할을 한다. 전략폭격기는 무력 공습의 특성이 무차별적인 폭격을 통해 상대방의 전쟁 의지와 역량을 약화시키는 것이다. 전략폭격기를 개발하고 보유하기 위해서는 엄청난 비용을 부담해야 하고, 전 세계 전략에 활용하기 위해서는 다른 국가들에 전략폭격기가 기착할 수 있는 공군기지가 있거나, 이를 탑재하는 항공모함이 기항할 수 있는 항구를 확보하고 있어야 한다. 현재 이런 조건을 만족시킬 수 있는 역량을 갖춘 국가는 거의 미국이 유일할 정도이다.

(2) 핵무기

2차 세계대전 중에 개발된 핵무기는 파괴력에 기초한 억지전략(deterrence)의 대표적인 수단이다. 냉전시기 미소 강대국의 장기적 평화를 유지할 수 있도록 하는 실질적인 영향을 미쳤다. 핵무기가 억지전략의 수단으로써 의미를 갖기 위해서는 미국과 소련은 20여 년간 핵전략의 개발과 논리 발전이 있었고, 미국과 소련의 핵

협상을 통해 상호 합의하는 긴 과정이 있었다. 그 동안 핵전략으로 상호확증파괴전략(MAD)이나 유연대응전략, 선제타격전략 등이 개발되었으나, 실제로 핵을 사용한 유일한 사례는 미국이 2차 세계대전 말 일본을 대상으로 항공 폭격이었다. 핵물질과 핵기술을 통제하려는 국제규범이 성공적으로 정착하여 예상보다는 훨씬 핵확산이 억제되었다. 아직 핵보유국은 한 자리수를 유지하고 있다. 하지만, 냉전체제가 와해되고 나서 핵무기 통제가 과거보다 느슨하고 테러조직의 수중으로 넘어갈 가능성이 매우 증대하였다. 그럼에도 불구하고 핵무기는 개발 비용이 높고 고도의 핵기술이 있어야 하며, 국제 제도와 규범은 핵사용과 확산을 막고 있다. 공격보다는 억지력을 보증하는데 효과적인 수단이다.

(3) 소총

개인 화기는 국가의 통제가 가장 느슨하게 관리되고 있다. 저렴하게 구입할 수 있고, 이를 통제할 수 있는 국제규범이나 제도도 엄격하게 집행되지 못하고 있다. 무기로써 가장 널리 광범위하게 확산되어 있고, 안보위협의 행위자도 다양하게 분포한다. 개인이 안보위협의 행위자로서 선택하기 쉬운 무기이지만, 파괴력과 심각성은 상대적으로 낮은 수준이다. 개인휴대용 무기는 사용과 보유가 용이하지만, 국제안보를 위협하는 요소가 되지 못한다. 더욱이 위협 행위자는 공격의 지리와 시간적 제약을 받기 때문에 공격의 대상이 제한적이고 안보전략적 영향은 높지 않다. 안보의영향력을 높이기 위해 테러 혹은 암살과 같은 수단으로 활용될 수 있지만, 불특정 다수를 살상하거나 국가와 사회를 혼란에 빠트리는 파급력은 낮다.

(4) 미사일

국제안보구조에서 공격력을 강화시키는 매우 효과적인 수단이다. 기술과 연구개발의 재원, 인적 자원 등의 진입비용이 높다. 공격을 높이기 위한 탄도의 거리 혹은 타격의 정밀성을 높이기 위해서는 진입비용이 높을 뿐만 아니라, 국제규범과 제도가 일정 수준에서 규제하고 있다. 1991년과 2003년 두 번의 이라크 전쟁에서 볼 수 있듯이, 미국의 정밀타격 무기는 군사작전의 효율성을 높이고 자국의 희생과 민간인의 희생을 줄이는 효과를 증명하였다. 크루즈 미사일 혹은 대륙간 탄도미사일을 보유하는 것은 적어도 군사력에서 상대 국가를 가격할 수 있는 수단을 확보한 것으로 간주되기 때문에 국제안보에 미치는 영향은 매우 높다. 그러나 비국가 행위자(nonstate actor)가 보유하고 사용하는데 극히 제약되어 있다. 첨단 기술을 보유하기도 어렵고, 미사일을 개발하고 보유하는 인적 및 재정적 지원이 불가능하다.

2. 사이버무기의 의미와 특징

사이버공간이 안보의 중요한 영역으로 평가되는 상황은 지속적으로 강화되고

있다. 사이버안보는 비대칭적 안보의 대표적인 사례로 인식되고 있듯이, 재래식 군사력과 핵군사력을 갖고 있는 강대국들은 사이버전략을 통해 자국의 안보우위를 유지할 뿐만 아니라 비대칭적 안보위협을 방어하기 위한 전략을 강구하고 있다. 그렇다면, 사이버무기가 기존의 무기 체계가와 어떤 차이점을 안고 있는지를 이해하는 것은 사이버안보의 전개 과정을 예측하는데 필요하다.

(1) 안보수단의 특성이 다르다. 사이버무기는 근본적으로 공격력이 방어력에 비해 우위에 있다. 사이버공간을 활용하기 위한 인터넷 시스템은 보안보다 자유로운 활용에 주안점을 두고 개발되었다. 사이버공간에서 새로운 안보수단의 등장은 안보딜레마를 심화시키는 결과를 가져올 것이다. 사이버무기는 동일 비용으로 안보수단으로 활용하는 경우에 공격이 방어보다 우위에 있다. 이런 특징은 공수균형의 변동이 공격 우위를 확보해 주기 때문에 국제안보구조의 안정성이 불안정해지고 사이버무기가 여러 유형의 목적을 위해 사용될 것임을 의미한다. 공격의 비용이 줄어들고 방어의 비용이 높아진다면 공격 의도와 계획을 갖고 있는 국가들은 상대적으로 저렴한 공격을 통해 원하는 목표를 얻을 수 있기 때문이다. 그러나 안보딜레마에 관한 기존의 연구는 안보딜레마를 야기하는 요소가 무엇인가 하는 문제와 공격력 무기(혹은 방어용 무기)가 발전하면 국제안보구조가 불안정해지는 이유를 설명하는데 집중되어 있다. 그러나 사이버무기는 기존의 무기체계와 달리 다양한 목적으로 사용되고 있고, 정교함이나 파괴력의 차이가 있을 수 있으나 사이버 공격의 수단을 국가와 비국가 행위자가 모두 보유하고 있으며, 기존의 안보전략이 효과적으로 적용되기 어려운 상황에서 안보딜레마의 변형된 모습을 만들어낼 수 있다.

(2) 안보수단의 국가 통제에서 차이가 있다. 핵무기와 재래식 무기로 파괴력이 높고, 관리하고 개발하는 비용이 높을 경우에 국가의 통제력이 그 만큼 높다. 근대국가의 특징은 국가가 폭력을 합법적으로 독점함으로써 폭력과 물리적 공격을 제약할 수 있었다. 국가의 지배력이 확고한 사회에서 무기의 자유로운 유통이나 사용은 매우 제한된 상황에서 허용되고 있다. 물론 중앙정부의 통제가 약화되고, 내전이 일어나거나 부족이나 종족들간 분쟁이 발생한 지역에서 무력의 사유화가 광범위하게 나타난다. 따라서 국가는 국가안보 차원에서 강력한 무력을 확보하려는 꾸준히 시도하면서도 안보를 보호하기 위해 효율적인 안보수단을 관리한다. 사이버무기는 국가의 통제가 전통적인 방식으로 이루어지기에 근본적인 제약이 있다. 비국가 행위자들이 거의 제약 없이 사이버 공격 수단을 만들고 있을 정도로 국가의 통제가 현실적으로 거의 불가능하다. 우선 안보위협의 무기를 제조하고 관리하는 절차와 과정이 사이버공간에서 이루어지기 때문에 물리적 공간과 물질이 필요한 무기와는 다르다. 또한 비국가 행위자는 국가 정보기관과 연계를 통해 국가를 대신해서 사이버 공격을 주도하는 행위가 가능하다. 조지아 혹은 에스토니에 대한 러시아의 사이버 공격이나 중국의 미국 민간기업 공격 등은 국가의 지원을 받은 해커집단의 소행으

로 의심을 받는다. 안보수단에 대한 국가의 독점적 통제 영역에서 벗어나 사이버무기는 군사 목적과 경제 활동의 보안 사이에 경계가 분명하지 않다. 국내에서 범죄로 활용하거나 국외에서 안보 위협 수단으로 이용할 수 있다. 무력 수단이 국가통제를 벗어나 이용되는 안보위협의 대표적인 사례가 테러이다. 테러집단은 안보수단을 확보해서 중앙정부를 공격하려는 정치적 목적을 추구하는 비국가 행위자이다. 이런 점에서 테러집단이 사이버무기를 이용하여 사이버 공격을 시도할 수 있는 가능성이 매우 높다.

(3) 국제제도와 규범의 구축에서 차이가 있다. 재래식 전쟁은 엄청난 인명 살상을 동반한다. 무력 수단은 영토 정복이나 강압적 외교의 수단으로 확실한 효과를 제공하지만, 비인도적인 피해와 파괴 행위 때문에 무력 분쟁을 억제하려는 국제규범이 발전해왔다. 또한 근대국가가 국제사회의 주요 행위자로 자리 잡으면서 국가의 주권과 영토를 보호하려는 목적도 있었다. 결국 국제안보에 관한 규범들은 주권보호가 가장 중요했고, 인간의 보편적 권리를 보장하려는 목적에서 발전하였다. 핵무기에 대한 국제사회의 터부는 이를 반영한 좋은 사례이다. 핵무기가 억지수단으로 효용성을 인정받지만, 핵사용에 따른 인류의 재앙을 방지하기 위해 핵확산금지레짐이 형성되었다. 아직까지 어떤 사이버무기와 사이버 공격도 재래식 무기와 핵무기의 파괴력을 보여준 적이 없다. 사이버무기의 위협 심각성이나 파괴력이 현실화될 가능성이 있다고는 하지만, 사회의 혼란과 기밀 정보를 훔쳐가고, 금전적 목적의 범죄에 사이버무기가 이용되고 있다. 일반 무기처럼 확실한 파괴의 효과를 확보했다고 보기 어렵다. 이런 이유로 인해 사이버무기와 공격 행위를 통제하고 제재를 가하려는 국제규범은 크게 발전된 수준이 아니다. 그 이면에서는 미국과 러시아 혹은 중국 등 사이버 강대국 사이에 국제규제에 대한 큰 입장 차이가 작용하고 있다. 그리고 서구 국가들과 비서구 국가들 사이에도 사이버공간에 대한 규제를 둘러싸고 상당한 이견 차이를 보여주고 있다.

(4) 공격수단 획득의 저렴함과 행위자의 다양화이다. 전통적인 안보는 강력한 안보수단을 개발하고 보유하기 위한 많은 재원과 기술력을 확보했을 때에 가능했다. 일반적으로 그 시대에 국력과 기술력이 가장 앞선 국가들이 새로운 무기를 도입하는 경향이 있다. 군비경쟁, 군사전략 개발, 동맹구축은 안보위협에 대처하는 가장 보편적인 방식이다. 오랜 역사에서 발전해 왔지만, 탈냉전 이후에 비대칭적인 관계에서 효과적인 위협 수단으로 테러가 각광을 받고 있다. 테러는 정치적 목적을 위해 저렴한 비용으로 상대국의 사회에 혼란을 야기하고 정치 및 경제적 비용을 부담하도록 한다. 테러와 달리 안보수단으로써 사이버무기는 진입비용이 매우 저렴하고 약간의 지식을 갖고 있는 사람은 정치적 목적이 아니더라도 누구나 사이버무기를 만들어 사용할 수 있다. 정교한 파괴력을 갖는 수준의 무기는 최고의 전문성, 재정적 지원 그리고 체계적인 환경이라면 훨씬 용이해 진다. 테러와 사이버안보 위협

의 또 다른 차이는 전자가 살상과 파괴를 공격의 주목표로 삼고 있지만, 사이버 공격은 사이버전, 사이버 범죄, 사이버 스파이 등 다양한 목적을 위해 이루어진다. 사이버무기는 반격이나 대응 수단으로써 재래식 무기에 비해 좀 더 유연하게 사용될 수 있다. 재래식 무기는 강대국의 공격력에 상응한 보복이나 대응을 약소국이 마련하기 어렵다. 파괴와 살상의 결과는 상대적인 우위를 평가하는 기준으로 본다면, 약소국은 강대국과 동일한 수준으로 반격하기 어렵다. 하지만 사이버무기는 파괴 목적으로 사용될 수 있지만 정보수집이나 사회혼란 목적에서 이용된다면 비대칭적 관계의 열세에도 대응이 가능하다.

3. 사이버안보관련 정책의 쟁점들

(1) 정부의 국가안보 활동과 민간영역의 사적 활동이 협력하는 문제이다. 안보의 개념과 의미가 국제안보환경의 변화에 따라 확대되고 있다. 인간안보, 사회적 안보, 경제 안보 등에서 볼 수 있듯이 국가안보 수준의 개념적 영역은 애매해졌다. 사이버공간은 특히 국가와 비국가 행위자들의 구분이 없어지고, 국가안보의 대상으로 보호받아야 하는 요소도 다양해 졌다. 그러나 국가안보와 민간영역 혹은 사기업의 목적이 항상 일치하지 않는다. 미국에서 볼 수 있듯이, 국가는 민간영역에 강제로 개입할 수 있는 부분이나 권한을 설정하는 미묘한 문제를 해결해야 한다. 특히 국가기간시설을 보호하려는 법률 정비, 정부의 조직, 비상조치계획 등에 관한 업무를 담당할 기관으로 정보기관, 법집행기관 혹은 독립적인 조직 등에 관한 논의가 필요하다. 이는 사생활 보호라는 헌법적 가치와 기업의 사적 이윤 추구라는 경제적 이념들이 내재해 있기 때문에 이를 해소하기 위한 방안이 필요하다.

(2) 사이버안보의 대비책은 방어적 전략과 공격적 전략을 동시에 발전시키는 문제이다. 재래식 무기 혹은 핵무기에 의한 군사력은 사이버무기와 관련해서 그대로 적용하기 어렵다. 사이버무기의 확산이 이루어진다면, 비국가 행위자들 혹은 경쟁관계에 있는 국가는 사이버무기를 동원해서 사이버공격을 가할 수 있다. 사이버공격의 방식이나 목표는 다양하기 때문에 재래식 무력공격처럼 단선적 확전 과정을 염두에 두고 안보전략을 마련할 수 없다. 지난 수년간 남한의 정부기관, 금융기관, 언론사가 공격받은 사이버위협은 비교적 저강도의 공격 행위이다. 최근 Stuxnet, Flame 등의 사례에서 볼 수 있는 것처럼, 사이버공격의 목표와 방식이 파괴적일 수 있음을 경험하였다. 그러나 미국과 같은 초강대국은 강압적인 방식으로 국제안보의 영역에서 자국의 의지대로 이끌어가는 안보수단을 사이버공간에서 마련할 수 있을지 관심사이다. 당장에는 사이버무기의 공격력, 방법(수단)에 관한 명확한 지식이 부재한 상태에서 강대국은 사이버안보 방어체제를 재래식 무기처럼 구축하는 목표를 달성하기 어렵다. 중요한 한 가지 이유는 첨단 사이버무기를 개발하는데 필요

한 기술의 대부분이 상업적으로 구매하여 이용할 수 있고, 완벽하게 통제되지 않기 때문이다. 또한 전통적 기술이나 군비통제레짐은 적용되기 어렵다. 그렇다고 공격적 사이버전략을 공개적으로 추진하는 경우 사이버공간의 군사화를 촉발시킬 수 비난을 감수해야 한다.

(3) 사이버안보를 총괄하는 조직과 대응체계를 마련하는 문제이다. 한국은 사이버안보와 치안을 담당하는 기관 그리고 민간분야를 담당하는 기관들이 사이버공격에 대응하는 체계이다. 청와대, 국방부, 국정원, 경찰, 한국인터넷진흥원 등이 영역별로 담당하고 있다. 이들 조직은 유사시에 유기적 협력과 공조를 위해 합동대응체계를 마련해 대처하고 있지만, 최근 논의되고 있는 사이버테러방지법 (혹은 사이버위기관리법)을 둘러싸고 논란이 일고 있다. 사이버 컨트롤타워에 대한 논의가 중심이 되고 있지만, 이는 국가안보와 사회치안의 경계가 제도와 문화적 합의가 없는 상태에서 정부의 한 부처가 총괄하는 것에 따른 문제점이 내재해 있다. 부처간 합의를 통합한 협력절차를 마련하는 작업이 필요하다. 또한 신속한 피해 복구와 사후 재발 방지를 위한 가외성을 확보하는 조직체계가 중요하지만, 안보전략은 완벽한 방어대책으로 가능할 것이라는 믿음이 역사적으로 현실화된 적이 없다. 사이버안보 정책을 담당하는 정부 부서는 결코 일원화되기에는 전략의 목표와 활동 방식에 따라 다양하게 논의되어야 한다.

(4) 유럽 국가들은 사이버위협에 공동 대처하려는 다자간 노력을 꾸준히 추진해오고 있고, 미국은 사이버안보를 확보하려는 국제 여론과 환경을 조성하려고 시도하고 있다. 사이버안보에 관한 국제규범을 구축하는 과정에서 한국은 대내외 전략과 방침을 마련하고 있어야 한다. 사이버 국력을 기준으로 본다면, 미국이 가장 우위에 서 있는 국가이다. 그 뒤를 이어 러시아, 중국, 이스라엘, 북한, 이란 등이 사이버 공격력을 두드러지게 강화하려는 국가이다. 하지만 사이버위협을 제어하기 위해 국제제도를 마련하려는 국제사회의 시도는 각국의 입장에 따라 다양하게 나타나고 있다. 사이버공간 통제에 대한 미국과 중국의 인식 차이, 미국과 러시아의 전략적 입장 차이, 서유럽국가와 비서구국가들 사이의 다른 시각에서는 국제정치의 현실주의적 특성이 잘 드러나 있다. 최근 일어나고 있는 사건들은 국제사회의 분위기를 반영하고 있다. 중국의 해킹에 대한 미국의 비판, 에드워드 스노든의 미국 정보활동 폭로, 미국과 러시아의 대립과 협상, 이스라엘과 이란의 갈등, 북한의 전략과 사이버 공격력 강화 그리고 남한의 사이버안보 취약성 등은 사이버안보에 관한 국제레짐을 구축하는 초기 단계에서 향후 발전을 이해하는 선명한 지표들이다.