제3장

버추얼 창과 그물망 방패 : 사이버 안보의 세계정치와 북한

김상배

Ⅰ. 머리말

모순(矛盾)이라는 고사성어가 있다. 중국 전국시대의 초(楚)나라에 사는 어느 상인의 이야기이다. 창과 방패를 파는 상인이 “이 창은 예리해서 어떤 방패라도 꿰뚫을 수가 있다”고 자랑했다. 동시에 그는 “이 방패는 견고해서 어떤 창으로도 꿰뚫지 못한다”고 뽐냈다. 그러자 그 옆에 있던 사람이 “당신의 창으로 당신의 방패를 찌르면 어떻게 되는가?”라고 물었더니 상인은 대답하지 못했다고 한다. 이러한 아날로그 시대의 고사를 디지털 시대의 사이버 안보 문제로 옮겨서 개작해 보면 어떤 이야기가 될까? 해커들은 자신들이 뚫을 수 없는 방화벽이란 없다고 뽐낸다. 하루가 멀다 하고 새로운 컴퓨터 바이러스와 악성코드가 출현하고, 해커들의 창은 점점 더 보이지 않는 위력을 발휘한다. 이를 막기 위해서 정보보호 기술자들은 새로운 방화기술과 백신 프로그램의 개발에 열을 올린다. 아무리 교묘한 공격이라도 그 진원지를 추적해 색출할 수 있다고 장담 한다. 디지털 시대의 창과 방패가 서로 겨루고 있는 모습을 방불케 한다(김상배, 2011).

최근 북한의 소행으로 추정되는 사이버 공격의 사례가 늘어나고

있다. 이들 사이버 공격의 특징은 '버추얼(virtual) 창'이라고 비유할 정도로 그 실체를 파악하기 어렵다는 점이다. 잘 알려지지 않은 컴퓨터 바이러스나 악성코드를 사용할 뿐만 아니라 공격의 수법도 점점 더 교묘하게 바뀌고 있다. 아직은 사이버 공격의 대상이 공공기관이나 언론·방송사 또는 금융기관 등에 국한돼 있지만, 일단 유사시에는 재래식 공격이나 핵 공격과 연계될 가능성이 매우 크다는 점에서 큰 우려를 낳고 있다. 따라서 사이버 공격을 막아내고 그 범인을 색출하기 위한 대책 마련에 비상이 결릴 수밖에 없다. 다양한 행위자들이 나서서 다층적인 방어망을 만든다는 의미에서 '그물망 방패'의 구축을 방불케 한다. 기술적인 차원에서 방화벽을 구축하고 재난관리 시스템을 마련하려는 노력과 함께 효과적인 대책을 마련하기 위한 법제도적 방안의 모색이 한창이다. 아울러 국제적인 정보공유 네트워크를 구축하고 글로벌 및 지역 차원의 협력체계를 가동하기 위한 준비도 활발하다.

그런데 버추얼 창과 그물망 방패의 대결을 관전하는 국내외 국제정치학계의 논의를 보면 다소 우려스러운 부분이 있다. 현재 사이버 위협에 대처하자며 제기되는 주장들은 대체적으로 전통적인 국가안보론의 시각을 원용하고 있다. 그 중에서도 가장 눈에 띄는 주장은 나토(NATO)의 협력기구인 CCDCOE(Cooperative Cyber Defence Centre of Excellence)에 의해서 2013년 3월 발표된 사이버 전쟁의 교전수칙인, 소위 '탈린 매뉴얼(Tallinn Manual)'에 담겨 있다. 그 주장의 골자는 사이버 공격으로 인해 인명 피해가 발생했을 경우 해당 국가에 대한 군사적 보복이 가능하고, 핵티비스트 등과 같은 비국가 행위자에 대해서도 보복하겠다는 것이다. 더 나아가 사이버 공격의 배후지를 제공한 국가나 업체에 대해서도 국제법과 전쟁법을 적용하여 책임을 묻겠다는 것이다(Schimit, 2012).

국내외 학계 일각에서 제기되는 '사이버 억지'의 개념도 이와 유사한 맥락에 놓여 있다. 사이버 억지의 발상은 사이버 안보의 문제를 이해하고 해법을 모색함에 있어서 핵 안보 연구에서 비롯된 전략론의 시각을 적용하여 사이버 공간에서 발생하는 테러와 공격에 대처하겠다는 것이다(Morgan, 2010; Lupovici, 2011; Singer and Shachtman, 2011; 장노순·한인택, 2013). 이러한 주장들은 사이버 공격에 대해서는 그 진원지를 찾아 미사일을 발사해서라도 강력하게 보복하겠다는 미국 정부의 최근 입장과도 통한다. 2012년 5월 미국무부는 사이버 공격의 배후지를 제공한 국가의 주요시설에 대해서 사이버 보복을 가하거나 또는 그 가능성이 있는 국가에 대해서 사이버 선제공격을 가하겠다고 발표한 바 있다.

현재 국내외 일부 학계와 미국 정책 서클에서 제기되고 있는 이러한 주장들은, 사이버 공격의 범인을 찾아 보복하거나 책임을 묻겠다는 단호함을 표명하는 데에는 효과가 있을지 몰라도, 실제로 발생하는 사이버 위협에 대처하는 적절한 처방이 될 수는 없다. 무엇보다도 사이버 공간에서 발생하는 위협을 객관적으로 측정하고 이에 보복할 수 있다는 선형적(linear) 사고방식 자체가 논란거리이다. 복잡계 현상에 기반을 두고 있는 사이버 위협에 대한 대책을 단순계 발상에 기반을 둔 전통적인 안보와 억지 개념에서 구하는 잘못을 범할 우려가 있기 때문이다. 다시 말해, 인과관계를 밝힐 수 없거나, 혹은 밝힐 수 있더라도 매우 복잡한 인과관계에 기반을 두고 있어 공격의 주체와 보복의 대상을 명확히 판별할 수 없는 현상을 단순 마인드로 파악하는 오류를 범할 가능성이 크다(Beck, 1999; 2005; 민병원, 2007).

이러한 시각이 가장 크게 결여하고 있는 것은 사이버 테러와 공격이 발생하는 사이버 공간의 구조적 성격에 대한 이해이다. 사이버

안보는 기본적으로 복잡계의 양상을 보이는 '네트워크 구조'에서 비롯되는 문제이다. 그 구조와 작동방식의 성격상 누가 주범인지를 밝히기 어려운 복잡한 게임이다. '피해자는 있는데 가해자가 없다'는 말을 방불케 하는 게임이다. 만약에 범인을 찾는다고 하더라도 확증보다는 추정하는 경우가 많기 때문에 실제 범인을 색출하는 문제보다도 누가 범인인지에 대한 이야기를 구성하는 것이 더 중요한, 일종의 '범죄의 재구성 게임'이다. 방어하는 측의 입장에서 보더라도 사이버 공격을 막기 위해서 완벽한 방화벽을 치는 것은 쉽지 않다. 버추얼 창이 어디에서 날아올지 모르기 때문이다. 게다가 창을 막기 위해서 세운 사이버 방화벽은 대부분의 경우 '그물망'이지 '비닐막'이 아니다. 아무리 잘해도 빈틈이 생긴다. 사이버 안보와 관련된 문제의 많은 부분들이 인터넷이라는 독특한 시스템에서 비롯되기 때문이다. 이런 이유로 사이버 안보는 온전히 기술적 장치만으로는 보장될 수 없고 사회적 메커니즘을 빌어서 해결해야 하는 문제이다.

인터넷이라는 네트워크의 구조적 복합성에 대한 연구는 주로 컴퓨터 공학 분야에서 이루어져 왔다. 이들 연구는 사이버 안보의 문제 자체가 지닌 기술적 복합성이나 네트워크로서의 성격에 대한 이해를 바탕으로 논의를 펼치고 있다. 이들은 소프트웨어 엔지니어링이나 시스템 디자인 등의 분야에서 얻은 컴퓨터 안보, 네트워크 안보, 정보 보호 등의 개념을 원용하여 세계정치 현상으로서 사이버 안보 문제를 보는 시각을 도출한다. 그러나 이들 연구가 지니는 한계는 물리적 환경으로서 인터넷(또는 사이버 공간)이라는 기술체계가 구동되는 이면에 존재하는 세계정치 행위자들의 의도적 전략과 그 과정에서 작동하는 권력정치의 동학을 간과하고 있다는 점이다. 따라서 간혹 기술체계 자체에서 발생하는 가능성에만 주목하여 사이버 공격과 테러가 낳을 위험성을 과장하는 경향이 있다고 지적된

다(Matusitz, 2006; Galloway and Thacker 2007).

최근 사이버 안보의 문제는 더 이상 기술과 공학의 분야에만 국한되지 않고 21세기 세계정치 연구의 주요 주제로서 부상하였다.[1] 특히 국가 행위자가 사이버 공격의 주요 주체로서 부상한 현상은 사이버 안보의 세계정치라는 차원에서 중요한 주목거리임이 분명하다. 초창기의 사이버 테러와 공격은 국가 행위자들이 아니라 체계적으로 조직되지 않은 네트워크 형태의 비국가 행위자들이 벌이는 게임이었다.[2] 다시 말해, 공격이라는 면에서 사이버 테러는 비대칭 전쟁을 벌이는 초국적 핵티비스트나 테러리스트들의 게임이었으며, 또한 국내외 거버넌스 체계의 마련에서도 민간 전문가들의 역할이 중요했다. 그러나 2000년대 말엽 이후로 종전에는 비국가 행위자들의 배후에서 조연 배우의 역할을 담당하던 국가 행위자들이 사건의 전면에 나서고 있다. 또한 이러한 국가 행위자들이 국내외 차원에서 사이버 공간의 안보를 보장하는 방어자의 역할도 떠맡고 있다.[3]

이상의 논의를 종합해서 볼 때, 사이버 안보의 세계정치는 복잡계의 양상을 보이는 네트워크 구조 하에서 다양한 세계정치 행위자들이 서로 얽히면서 구성해 가는 게임이다. 다시 말해 전통적인 안

[1] 국제정치학의 시각에서 본 사이버 안보 연구로는 Eriksson and Giacomello, eds. (2007), Cavelty(2007), Manjikian(2010), Klimburg(2011) 등을 들 수 있다. 특히 네트워크 전쟁론의 시각에서 사이버 안보의 문제를 보는 이론적 단초를 제시한 연구로는 Arquilla and Ronfeldt(1996; 2001), Libicki(2009) 등을 들 수 있다. 국내의 국제정치학적 시도로는 이상현(2008), 최인호(2011), 조현석(2012) 등을 들 수 있다.

[2] 이런 점에서 초기의 사이버 안보의 주제는 비국가 행위자의 역할을 강조하는 자유주의 국제정치이론의 시각에서 조명되었다(Nye, 2010; Rattray and Healey, 2011).

[3] 사이버 안보 분야에서 구성주의 국제정치이론의 시각은 소위 코펜하겐 학파의 안보화(securitization) 개념의 적용이라는 맥락에서 발견된다(Buzan and Hensen, 2009; Hansen and Nissenbaum, 2009). 한편 국제정치이론에서 말하는 구성주의나 코펜하겐 학파와는 다소 다른 맥락이긴 하지만 예외적으로 Deibert, et al.(2002; 2008; 2010; 2011) 등에도 주목할 필요가 있다. 또한 공간 구성주의의 시각에서 사이버 안보의 국제정치적 이슈들을 다룬 Steinberg and McDowell(2003)도 있다.

보 행위자로서 국가 행위자 이외에 초국적으로 활동하는 비국가 행위자들의 존재감이 두드러진 분야일 뿐만 아니라 사이버 공간의 네트워크 구조, 즉 이 글에서 '비인간 행위자(non-human actor)'로 개념화한 변수가 독립변수로 작동하는 게임이다. 이러한 사이버 안보의 세계정치를 제대로 이해하기 위해서 필요한 것은 국가-비국가 행위자의 역할을 복합적으로 보는 동시에 사이버 공간의 물리적·관념적 구조와 그 안에서 작동하는 비인간 행위자들의 역할을 놓치지 않는 이론적 분석틀의 마련이다. 이 글이 전통적인 국가안보론의 시각으로 사이버 안보의 게임을 제대로 이해할 수 없다는 문제제기를 하는 이유는 바로 여기에 있다.

이러한 맥락에서 이 글은 사이버 안보에서 발견되는 국가-비국가-비인간 행위자의 삼각 구도를 보는 이론적 분석틀로서 네트워크 이론의 시각을 제시한다. 여기서 말하는 네트워크 이론의 시각이란 최근 자연과학과 사회과학 분야에서 주목받고 있는 네트워크 이론, 특히 소셜 네트워크 이론, 행위자-네트워크 이론, 네트워크 조직 이론 등의 성과를 국제정치 분야에 적용한 이론적 논의이다(하영선·김상배 편, 2010; 김상배 편, 2011). 이러한 세 가지 네트워크 이론에서 원용한 개념적 논의를 바탕으로 사이버 안보의 세계정치를 이해하는 분석틀을 마련할 수 있다. 특히 사이버 안보 분야에서 관찰되는 네트워크 구조와 전략, 그리고 변화하는 주체의 문제를 밝히는 데 도움을 얻을 수 있다. 이 글은 이러한 시각을 원용하여 북한의 사이버 공격을 보는 이론적 시각을 제시하고, 이를 바탕으로 사이버 안보 분야에서 한국이 모색할 국가전략의 방향을 짚어보고자 한다.

이 글은 크게 세 부분으로 구성되었다. 제2장은 소셜 네트워크 이론과 행위자-네트워크 이론 및 네트워크 조직 이론의 관점에서 사이버 공간의 구조적 특성을 살펴보고, 그러한 구조적 환경 하에서

활동하는 비인간 행위자 및 비국가 행위자들의 역할을 밝혀 보았다. 제2장에서 제시된 사이버 안보의 세계정치적 플랫폼 위에서 공격과 방어의 역할을 담당하는 국가 행위자, 소위 '네트워크 국가'의 두 얼굴을 다룬 것이 바로 제3장과 제4장이다. 제3장은 국가 행위자들이 개입한 사이버 공격의 글로벌 사례들을 살펴보고, 그 연속선상에서 북한의 사이버 공격과 그 수행 능력을 검토하였다. 제4장은 사이버 공격을 막기 위한 국내외 거버넌스의 구축 노력을 개괄하고, 한국이 구축할 그물망 방패의 내용과 방향을 짚어 보았다. 끝으로 맺음말에서는 이 글의 주장을 종합·요약하고 사이버 안보 분야에서 나타나는 세계정치의 특징을 다층적인 비대칭 망제정치(網際政治, inter-network politics)로 개념화하였다.

Ⅱ. 사이버 공간의 구조와 비인간 행위자

네트워크 이론은 사이버 공간의 구조와 그 안에서 벌어지는 사이버 안보 문제의 성격을 이해하는 데 유용한 이론적 자원을 제공한다. 현재 사회학이나 물리학, 그리고 역사학(주로 과학사) 등에서 논의되고 있는 네트워크 이론들은 매우 다양하다(Newman et al, 2006: p.1). 네트워크를 무엇으로 보느냐에 따라서 지난 10여 년 동안 이루어진 네트워크 이론의 시도들을 나누어 보면, 대략 세 가지 진영으로 구별할 수 있다(김상배 편, 2011). 첫째는 네트워크를 하나의 구조(structure)로 보는 이론 진영인데, 최근 사회학과 물리학 분야를 중심으로 많이 알려진 소셜 네트워크 이론(social network theory)이다. 둘째는 네트워크를 하나의 동태적 과정(process)으로 보는 이론 진영이데, 과학기술 사회학 분야에서 주로 원용되는 행위자-네트워크 이론(actor-network theory, ANT)이다. 마지막은 네트워크를 하나의 행위자(actor)로서 보는 이론 진영인데, 경제학과 사회학 분야의 조직 이론에서 원용하는 네트워크 조직 이론(network organization theory)이다. 네트워크의 시각에서 21세기 세계정치의 변화와 그 연속선상에서 본 사이버 안보 문제를 제대로 이해하기

위해서는 이러한 세 가지 이론 진영의 논의들을 복합적으로 원용해야 한다.

소설 네트워크 이론의 시각은 사이버 공격과 테러가 벌어지는 인터넷 또는 사이버 공간의 네트워크 구조의 의미를 이해하는 데 유용하다. 인터넷은 '네트워크들의 네트워크'이라는 속성을 지니는 까닭에, 소셜 네트워크 이론에서 말하는 소위 구조적 공백(structural hole) 또는 빈틈이 있을 수밖에 없다. 구조적 공백이란 어느 조직 또는 네트워크 내에서 정보의 흐름에서 나타나는 '단절'의 한 형태이다. 이러한 구조적 공백을 메우는 것은 전략적으로 매우 중요한 의미를 갖는다. 단절되어 있는 노드들 사이에 존재하는 구조적 공백을 공략함으로써 전략적으로 중요한 '위치'를 잡는 행위자는 그렇지 못한 행위자들에 대해서 우월한 경쟁력을 갖기 때문이다. 이러한 상황을 개념화하기 위해서 미국의 사회학자이자 경영학자인 로널드 버트(Ronald S. Burt)는 중개의 의미에 대한 이론을 개발했으며, 이를 네트워크 전체의 구조적 특성에 대한 논의로 일반화시킨 바 있다(Burt. 1992; 2005).

구조적 공백의 개념은 사이버 안보의 환경에서 프로그램상의 빈틈을 의미하는 착취혈(exploit)의 형태로 나타난다. 이러한 빈틈이 시스템 전체에 영향을 미치는 아킬레스건이 되는데, 그 이유는 바로 복합 네트워크라고 하는 구조적 특성에서 비롯된다. 몇 개의 빈틈이 있더라도 네트워크가 다운되지는 않지만, 그 빈틈이 치명적인 공격을 받게 된다면 그것이 전체 네트워크에 미치는 영향을 통제하기 어렵다. 특히 해커들의 공격은 어느 한 부분의 하드웨어의 파괴를 노리는 것이 아니라 소프트웨어 프로그램의 교란을 노리기 때문이다. 컴퓨터 바이러스나 각종 악성코드들은 이러한 빈틈으로 침투하여 시스템의 정상적인 기능을 착취하는 대표적 사례들이다(Galloway,

2004; Galloway and Thacker 2007).

이러한 점에서 사이버 안보의 문제는 국제정치의 전통적 안보 문제와는 다른 특성을 갖는다. 특히 네트워크의 시각에서 볼 때 가장 두드러진 점은 네트워크 자체가 사이버 테러와 사이버 공격의 힘이 먹혀 들어가는 빌미를 제공한다는 사실이다. 사이버 테러나 공격을 감행하는 행위자들은 개별적으로는 미미한 존재이지만 이들의 행위가 인터넷 세상에 큰 위협을 가할 수 있는 이유는 바로 이러한 구조적 속성에서 비롯된다(Koch and Greg, 2010). 실제로 아무리 잘 설계된 정보시스템이라도 기술적으로 복잡하다보면 그 부산물로서 버그(bug)를 완전히 없앨 수는 없다. 그런데 이러한 빈틈, 즉 착취혈은 해커들이 외부에서 침투하여 시스템의 변경이나 훼손을 시도하는 목표가 된다.

이렇게 착취혈을 공격하는 컴퓨터 바이러스에는 다양한 종류들이 있고 최근 미국과 이란의 사이버 공방에서 사용된 것들이 주목을 받고 있다. 그 중 논란의 중심이 된 것은 스틱스넷이다(Farwell and Rohozinski, 2011; Shakarian, 2011). 치밀한 정보수집과 실험을 걸쳐 탄생한 정교하고 정밀한 프로그램인, 스틱스넷은 원래 이란 나탄즈의 우라늄 농축시설에서 사용되는 독일 지멘스의 산업제어시스템(ICS)을 공격하기 위해 미국과 이스라엘이 사용한 웜 바이러스이다. 2102년 5월 플레임(Flame)이라는 악성코드도 이란에 대한 사이버 공격에서 새로이 발견되었다. 플레임은 컴퓨터 네트워크와 USB 메모리를 통해 전파되는데, 소리, 화면, 키보드 동작, 네트워크 활동 등을 엿보는 첩보 프로그램이다. 2012년 이란이 사우디의 아람코에 대해서 사용한 것으로 알려진 악성코드 샤문(Shamoon)도 있다. 샤문은 감염된 컴퓨터의 파일을 지우고 마스터 부팅 레코드를 파괴하여 컴퓨터가 부팅하지 못하게 만들었는데, 공격당한 컴퓨터에 있는

패스워드 등의 정보를 추출하여 인터넷에 올리는 기능도 한다.

이러한 컴퓨터 바이러스와 악성코드는 행위자-네트워크 이론에서 말하는 비인간 행위자(non-human actor)로서 작동한다. 행위자-네트워크 이론은 인간 및 비인간 행위자들이 동원되고 배열되며, 더 나아가 이들 요소들이 하나로 유지되면서 이종(異種) 네트워크를 구성해 가는 과정을 탐구한다. 어느 행위자-네트워크의 능력은 숱한 인간 및 비인간 행위자들과의 상호작용에서 비롯된 '관계적 효과'로서 이해된다. 다시 말해 인간 행위자들 간의 관계뿐만 아니라 인간들이 어떠한 도구와 기술을 활용하느냐, 즉 사물과 어떻게 '동맹(alliance)'을 맺느냐가 중요하다는 것이다. 이러한 시각에서 볼 때, 전쟁에서 사용되는 무기가 무엇이냐, 예를 들어 재래식 무기냐 핵무기냐에 따라서 전략전술은 다를 수밖에 없듯이 사이버 공격에서도 비인간 행위자의 성격은 사이버 안보의 게임 자체에 큰 영향을 미친다. 이러한 비인간 행위자는 단순한 도구가 아니라 인간 행위자들의 네트워크에 영향을 미치는 행위능력을 갖는다.

이런 시각에서 볼 때 최근에 국내 뉴스 미디어를 뜨겁게 달구었던 디도스(DDoS, Distributed Denial of Service, 분산서비스거부) 공격은 비인간 행위자의 역할을 엿보게 한다. 디도스 공격은 서버가 처리할 수 있는 용량을 초과하는 정보를 한꺼번에 보내 과부하로 서버를 다운시키는 공격 방식이다. 디도스 공격은 수많은 개인 컴퓨터에 악성 코드나 해킹 도구와 같은 것들을 유포하여, 이들 컴퓨터를 소위 '좀비 PC'로 만들고, 이렇게 좀비화된 PC를 통해 특정 서버를 목표로 하여 대량의 트래픽을 동시에 유발시킴으로써 그 기능을 마비시키는 수법을 쓴다. 이러한 좀비 PC들이 공격을 시작하는 시점은 일종의 프로그램화된 예약공격의 형태를 띨 뿐만 아니라 개별 좀비 PC들은 의도하지 않은, 또는 의식하지도 못하는 사이에 공격

에 가담하게 된다.

주로 2000년대에 나타난 디도스 공격은 대량의 유해 트래픽을 특정 시스템에 전송하여 네트워크 과부하를 유발하는 일종의 융단 폭격과도 같은 대량공격 방식이다. 이에 비해 2010년대에 새로이 나타나서 차세대 사이버 공격으로 알려진 APT(Advanced Persistent Threat, 지능형지속위협) 공격은 좀 더 교묘한 방식으로 작동하는 비인간 행위자의 사례를 보여준다. APT 공격은 특정 표적을 겨냥해 명확한 목표를 두고 알려지지 않은 해킹 기법을 사용하여 지속적으로 은밀하게 기밀정보를 유출하거나 시스템 파괴하는 공격 방식이다. 이는 일종의 정밀타격 공격 또는 스마트 공격으로 이해할 수 있다. 비인간 행위자의 행위능력이 점차로 지능화되고 자동화되는 양상을 보여주는 사례라고 할 수 있다.

사이버 공간에서의 테러와 공격은 인간 행위자가 주체로 활동하지만 컴퓨터와 물리적 네트워크 자체가 단순한 객체가 아닌, 일종의 비인간 행위자로서의 행위능력을 발휘하는 복합 네트워크 환경을 배경으로 이루어진다. 국가나 비국 행위자와 같은 인간 행위자뿐만 아니라 비인간 행위자까지도 복합적으로 관여하여 비선형적인 방식으로 수행되기 때문에 누가 사이버 테러와 공격을 벌인 범인인지를 발견해내기란 쉽지가 않다. 다시 말해, 정체불명의 행위자들이 국가 등을 상대로 디도스 공격이나 APT 공격을 펼칠 수 있었던 것은 수많은 인간 및 비인간 행위자가 인터넷이라는 물적 네트워크를 토대로 손쉽게 연결되었기 때문이다. 그야말로 네트워크 그 자체가 범인이라고 할 수 있다.

그러나 사이버 테러와 공격의 문제를 단순히 컴퓨터나 인터넷의 물리적 속성과 관련된 기술적인 문제로만 보기는 어렵다. 사이버 테러와 공격은 위계조직의 모습을 따르지 않는, 다양한 행위자들이 네

트워크의 형태로 작동하는 면모를 보여준다. 네트워크 조직 이론은 사이버 공간에서 활동하는 비국가 행위자들의 부상을 설명한다. 지구화와 정보화의 진전은 수직적인 위계조직보다는 수평적인 네트워크 조직에 좀 더 친화적인 환경을 창출하였다. 예를 들어, 인터넷이라는 네트워크 환경은 전통적인 국가 행위자에 도전하는 비국가 행위자들에게 친화적이다. 사이버 안보 분야도 마찬가지이다. 이런 점에서 사이버 테러와 공격은 다양한 행위자들이 복합적인 네트워크 환경을 배경으로 하여 참여하는 소위 '비대칭 전쟁'의 대표적 사례이다. 비대칭 전쟁이란 힘과 규모의 면에서 비대칭적인 행위자들이 비대칭적인 수단을 동원하여 서로 다른 비대칭적 목적을 수행하기 위해서 이루어지는 전쟁을 의미한다.

기본적으로 사이버 테러와 공격은 국가 행위자들 간의 게임이 아니라 체계적으로 조직되지 않은 네트워크 형태의 행위자들이 벌이는 게임이었다. 사이버 공격을 벌이는 행위자들은 수직적 조직의 형태를 따르지 않고 수평적이고 분산적인 네트워크 형태로 존재하고 작동한다. 그러나 필요시에는 효과적인 타격을 가하는 세력으로 결집된다. 최근 인터넷의 확산으로 인해서 네트워킹에 드는 비용이 급속히 하락함에 따라 이러한 복합 네트워크의 메커니즘에 의지하는 비국가 행위자들이 역사의 전면에 그 모습을 드러내면서 예전에는 상상할 수도 없었던 독특한 종류의 '힘'을 발휘하고 있다.

이렇게 사이버 공격을 벌이는 이들은 악의 없는 해커일 수도 있지만 사회 시스템의 전복을 노리는 테러리스트들의 조직일 경우 문제는 심각하다. 사이버 테러와 공격에서는 행위자들이 수행하는 역할의 스펙트럼이 매우 넓다. 일반 사용자가 공격자가 될 수도 있고 악의적인 공격의 대상이 되기도 하며 디도스 공격에 이용되는 것처럼 자신도 알지 못하는 사이에 봇넷에 동원되는 소스가 되기도 한

다. 애국주의 해커집단은 국민국가와 암암리에 연대하여 다른 국가의 주요 정보인프라를 공격하기도 한다. 심지어 조직적인 범죄집단도 단독으로 산업스파이, 해적 행위, 금융자산의 절도 등을 행하지만 애국주의 해커집단과 함께 다른 국가의 정부 사이트를 공격하는데 가담하기도 한다. 게다가 이들은 국가기관에 의해 아무리 적발되어도 끊임없이 새로운 형태로 진화를 거듭해 나간다. 분산 네트워크로서의 특성 때문에 특정 대상을 선정하여 미리 억지하기도 또 대비해서 방어하기에도 매우 까다로운 안보 문제를 제기하고 있다.

2012년 8월 사우디 아람코에 대해 악성코드를 침투시킨 사이버 공격의 경우, '정의의 검(Cutting Sword of Justice)'이라는 해커집단의 소행으로 알려져 있다. 그들이 악성코드에 감염시켰다고 하는 컴퓨터의 대수(3만대)가 사우디 아람코에서 발표한 피해 컴퓨터 대수와 일치하는 것으로 보아서 그들의 주장이 나름대로의 신빙성을 얻고 있다. 최근 많이 알려진 사례는 어노니머스(Anonymous)이다. 어노니머스는 2010년 위키리크스 기부금을 막은 마스터카드, 비자카드, 페이팔 등에 대해 디도스 공격을 행한 바 있다. 2011년에는 튀니지, 이집트, 시리아, 리비아 등 아랍 독재국가 정부사이트들을 공격하여 유명해 졌다. 2013년에는 북한의 대남 선전용 웹사이트를 해킹하여 초기 화면을 변조하고 회원정보를 공개하기도 했다. 흥미로운 점은 이들 집단들의 행동의 이면에는 나름대로의 대항담론이 존재한다는 사실이다.

Ⅲ. 아날로그 북한의 버추얼 창

1. 사이버 공격에 나선 국가 행위자

사이버 공간의 복합 네트워크 환경을 바탕으로 벌어지는 핵티비즘이나 사이버 테러로 인식되던 사이버 안보의 문제가 최근 들어 국가 간에 벌어지는 사이버 공격의 문제로 그 성격이 바뀌는 양상을 보이고 있다. 사이버 공격의 배후에 숨어 있던 국가 행위자들이 나서면서 국가 간의 사이버 전쟁으로 비화될 가능성마저도 내보이고 있다. 사이버 공격은 정보 인프라와 전략적 데이터 자체를 공격함으로써 물리적 전쟁의 수행 능력이나 사회경제 시스템의 기능을 마비시키는 새로운 수단으로 거론된다. 실제로 물리적 전쟁의 개시를 전후하여 이와 병행하는 방법으로 국가 간의 사이버 공격이 감행될 가능성은 매우 크다. 2007년의 에스토니아에 대한 사이버 공격이나 2008년 그루지야에 대한 디도스 공격의 배후에 러시아 정부가 있었다는 의혹이 제기되었다. 이에 대해 러시아 정부는 개입사실을 부정했지만 러시아 정부가 이들 사이버 공격을 주도한 해커 집단들과

연루되었다는 의혹은 가시지 않았다(Evron, 2008; T. L. Thomas, 2009).

2010년 미국과 이스라엘의 대이란 사이버 공격은, 국가가 직접 나서서 사이버 공격을 주도한 것이 언론을 통해서 알려진 첫 사례이다. 이란의 우라늄 농축시설에 큰 피해를 입힌 것으로 알려진 스턱스넷에 의한 공격은 상당한 수준의 기술적 능력과 재정력이 없으면 불가능하다는 것이 일반적 평가이다. 스턱스넷처럼 정교하고 정밀한 사이버 무기를 개발하는 것은 국가가 아닌 다른 비국가 행위자들만의 능력으로는 감당하기에 벅차다. 막대한 시간과 자원 및 기술이 필요하기 때문이다. 따라서 스턱스넷 공격은 단순히 해커집단의 소행이 아니라고 추정되었는데, 스턱스넷이 미국과 이스라엘 정부의 공동작품이라는 사실이 최근 언론에 보도됨으로써 그러한 추정이 사실이었음이 확인되었다. 실제로 스턱스넷의 개발은 부시 행정부가 집권 중이던 2006년에 '올림픽 게임'이라는 이름의 작전으로 시작된 후 오바마 행정부에 의해서도 지속된 것으로 알려져 있다.

미국이 이란의 핵개발 프로그램을 지연 내지 좌절시킬 수 있는 방안으로서 스턱스넷 개발에 관심을 갖게 된 이유는, 사이버 공격이 이스라엘이 고려했던 이란 핵시설에 대한 공습보다 상대적으로 파장이 작을 것으로 예상되었기 때문이다. 사실 사이버 공격은 물리적 공격보다 효과적이고 은밀한 공격이라는 장점을 갖는다. 그러나 미국과 이스라엘이 감행한 사이버 공격의 경우 그 타격이 단순한 첩보나 컴퓨터 시스템에 피해를 주는 수준에 그치지 않고 원심분리기를 파괴시킴으로써 사이버 공간과 현실 공간의 벽을 뛰어넘는 피해를 주었다는 사실에 주목할 필요가 있다. 사이버 공간에서의 공격이 현실 공간의 피해로 이어진 사태는 사이버 공격의 위력을 증대시키는 직접적 효과는 물론, 그 동안 사이버 공격을 사이버 공간 내로 제한

해 온 암묵적 합의를 파기함으로써 향후 사이버 공격이 현실 공간의 전쟁에 동원될 될 가능성을 증대시켰다.

이러한 미국과 이스라엘의 공격에 대하여 이란도 여러 차례에 걸쳐서 사이버 공격으로 대응한 것으로 알려져 있다. 2012년 8월 사우디의 석유기업 아람코(Aramco)와 카타르의 가스기업인 라스가스(RasGas)에 대한 사이버 공격의 배후에 이란이 있다는 것이다. 미국 정보기관 관계자들에 의하면, 미국과 이란이 사이버 공간에서 공격과 반격을 주고받는 '그림자 전쟁'을 이미 진행 중이라고 했다(*New York Times,* 2012.10.13). 이와 관련하여 리언 패네타 미 국방장관은 2012년 10월 11일, 이란을 직접 거론하지는 않은 채, 적대적 국가나 집단이 미국의 핵심 전산망을 장악할 때 대규모 손실을 볼 수 있으며, 미국이 '사이버 진주만' 공격을 받을 위험에 처했다고 지적했다(연합뉴스, 2012.10.12).

이렇듯 미국-이스라엘과 이란 사이에서 오고간 사이버 공격은 사이버 안보를 국가 간의 안보 문제라는 새로운 지평에 올려놓았다. 국가 행위자가 직접 사이버 공격에 개입함에 따라 그 피해가 더욱 커질 수 있게 되었을 뿐만 아니라 국가와 국가 간 직접적 분쟁의 소지가 될 가능성이 커졌다고 볼 수 있다. 게다가 종전에는 방어자의 입장을 대변하던 미국이 나서서 국가 주도의 사이버 공격을 벌임으로써 다른 나라에서도 주저하지 않고 국가가 나서서 사이버 공격에 개입하게 되는 물꼬를 텄다는 우려와 비판도 제기된다. 그런데 아이러니컬하게도 모든 나라들이 국가 주도의 사이버 공격에 나설 경우 가장 취약할 수 있는 국가는 세계적으로 앞선 정보 인프라를 갖추고 있는 미국이다.

이렇듯 사이버 공간의 안보 문제는 새로운 국가 분쟁의 이슈가 되었으며 국가안보의 핵심적인 문제로 부상하였다. 만약에 사이버

공격으로 인해서 전신, 전화, 전기, 원자력 시설 등과 같은 국가 기간 시설에 대한 교란과 파괴가 이루어질 경우 이는 국가안보 자체에 큰 침해가 될 수밖에 없는 상황이 발생할 것이다. 이러한 상황은 강대국들 간의 관계뿐만 아니라 강대국과 약소국의 관계에 새로운 변화를 가져올 가능성이 크다. 다시 말해 통상적으로 재래식 무기로는 강대국과 경쟁할 수 없는 약소국들이 자국의 이익을 위해 사이버 전쟁을 국방전략으로 채택할 가능성이 크고, 이러한 전쟁양상은 소위 '비대칭 전쟁' 전략의 일환으로서 상대방에 대한 위협이 될 수 있을 것이기 때문이다. 이러한 상황에서 사이버 전쟁을 수행할 능력을 갖추는 것이 국가 차원의 주요 안건으로서 부각되고 있다.

2. 대남 사이버 공격과 북한

이상에서 살펴본 바와 같이 국가 행위자가 좀 더 적극적으로 사이버 공격에 개입하는 변화의 맥락에서 최근의 대남 사이버 공격을 이해할 필요가 있다. 실제로 최근 북한의 소행으로 추정되는 대남 사이버 공격의 횟수가 늘어나고 있다. 그 중에서 널리 알려진 주요 사건은 <표-1>와 <그림-1∽6>에 요약한 바와 같이, '7.7 디도스 공격,' '3.4 디도스 공격,' '농협 전산망 해킹 사건,' '중앙일보 해킹 사건,' '3.20 방송·금융사 침입 사건,' 그리고 '6.25 디도스 공격' 등의 여섯 가지를 들 수 있다. 이들 사이버 공격은 한국의 공공기관이나 금융사 및 언론방송사 등의 전산망의 빈틈을 노리고 수십만 대의 좀비 PC를 동원하여 디도스 공격을 벌이거나 좀 더 교묘하게 이루어지는 APT 공격을 가하는 방식으로 이루어진 것으로 알려졌다. 이러한 북한의 사이버 공격으로 인한 국내 피해액은 상당한 것으로 보도되었다. 2009년부터 2013년까지 디도스 공격이나 해킹 등으로 8,600

억 원의 피해가 발생한 것으로 나타났다. 이는 사이버 사령부가 주요 공격 중 집계 가능한 피해 금액만 추산한 것으로 국가기반시설 정보 등 기타 자료 유출을 포함하면 실제 피해액은 이를 웃돌 것으로 보인다(연합뉴스, 2013-10-15).

표 1. 북한의 소행으로 추정되는 주요 사이버 공격, 2007-2013년

	피해 내용	추정 근거	공격 방법
7.7 디도스 공격 (2009.7.7)	청와대와 국회, 네이버, 미국 재무부와 국토안보부 등 23개 사이트 마비	"테러에 동원된 IP 추적 결과, 북 체신성이 사용해 온 것으로 확인" (국정원 국정감사, 2009.10.29)	디도스 공격, 61개국 435개 서버 활용 좀비 PC 27만여대 동원
3.4. 디도스 공격 (2011.3.4)	청와대, 국가정보원 등 국가기관과 국민은행 등 금융기관 등 주요 웹사이트 마비	"사건 분석 결과 공격 방식이 2009년 7월 발생한 디도스 공격과 일치" (경찰청 발표, 2011.4.6)	디도스 공격, 70개국 746대 서버 활용 좀비 PC 10만여대 동원
농협전산망 해킹 (2011.4.12)	농협 전산망 악성코드 감영으로 장애 발생, 인터넷 뱅킹 등 서비스 중단	"공격 진원지인 노트북에서 발견된 IP가 과거 정찰총국에서 사용된 것" (검찰청 발표, 2011.5.3)	디도스 공격, 13개국 27개의 서버 동원
중앙일보 해킹 (2012.6.9)	내부관리자 PC를 경유하여 중앙일보 전산망 침입으로 홈페이지 변조 및 일부 데이터 삭제	"조선체신회사(체신청 산하)가 중국회사로부터 임대한 IP대역을 통해 접속" (경찰청 발표, 2013.1.16)	APT 공격, 국내 서버(2대) 해외 10개국 서버(17대) 동원
3.20 방송·금융사침입 (2013.3.20.)	KBS, MBC, YTN 등 언론사와 신한은행, 농협 등 금융기관 전산망 마비 내부망 백신업데이트 서버 및 업무 PC 감염	"공격에 사용된 IP주소 및 해킹 수법 분석 결과 7.7 디도스와 같이 북한 소행으로 추정되는 증거 상당량 확보" (민관군 합동대응팀, 2013.4.10)	APT 공격, 국내외 경유지 49개 동원 악성 코드 76종 사용
6.25 디도스 공격 (2013.6.25)	청와대, 국무조정실 홈페이지 해킹, 11개 언론사, 5개 정부기관 및 정당 등 16개 기관 해킹	"북한이 사용한 IP 발견, 공격방법이 3.20 사이버 테러와 동일" (민관군 합동대응팀, 2013.7.16)	변종 디도스 공격, 악성코드 82종 좀비 PC 활용

인터넷이나 휴대폰, 그리고 기타 정보기기의 보급률이 매우 낮은 것으로 알려진 북한의 상황을 고려할 때 북한은 여전히 '아날로그 국가'로 분류할 수 있겠지만, 최근 감행되고 있는 사이버 공격의 수준만 놓고 보면 정보화 선진국인 미국에 버금가는 능력을 갖추고 있는 것으로 추정된다. '아날로그 북한의 버추얼 창'이라고 비유해 볼 수 있겠다. 여기서 '버추얼'이라는 비유를 사용한 이유는 최근의 대남 사이버 공격이 북한의 소행이라는 것을 실증적으로 입증할 수 있는 문제라기보다는 여러 가지 정황 증거에 의해서 추정하는 문제이기 때문이다. 실제로 이들 사이버 공격을 북한의 소행으로 추정하는 이유는, <표 1>에서 정리한 바와 같이, 사이버 공격에 동원된 IP주소가 종전에 북한 체신성 또는 정찰총국이 사용하던 것이라든지 아니면 사이버 공격의 흔적으로 남은 해킹의 수법이나 악성코드들이 주로 북한이 사용하던 것이라는 정황 증거에 근거하고 있다. 사이버 공격을 받아 피해를 본 것은 실재(real)한데 그 공격의 진원지와 경로를 객관적으로 밝히는 것은 쉽지 않은 버추얼(virtual) 현상이 벌어지고 있다.

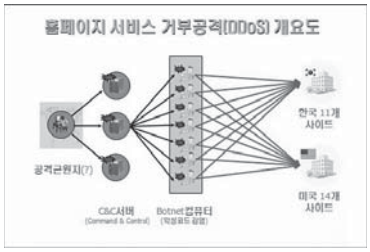


그림 1. 2009년 7.7 디도스 공격
출처: http://blog.daum.net/skyslove82/6991253

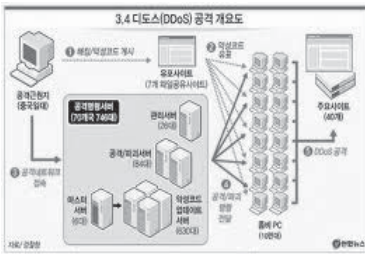
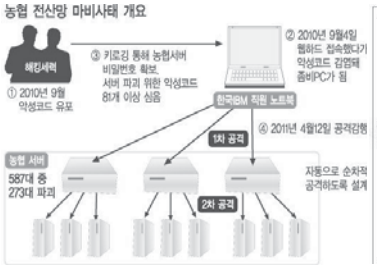


그림 2. 2011년 3.4 디도스 공격
출처: 연합뉴스



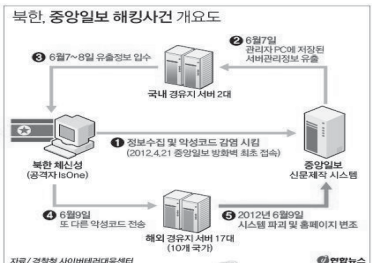


그림 3. 2011년 농협 전산망 해킹 사건
출처: 경향신문

그림 4. 2012년 중앙일보 해킹 사건
출처: 연합뉴스

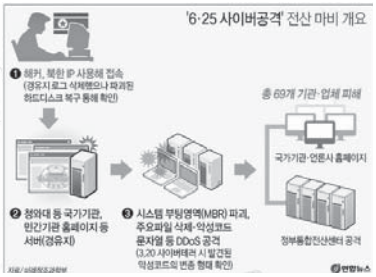


그림 5. 2013년 3.20 방송·금융사 침입 사건
출처: 임종인(2013)

그림 6. 2013년 6.25 디도스 공격
출처: <연합뉴스>

최근의 증언들에 의하면, 북한도 사이버 공격의 이러한 특성을 잘 이해하고 이를 적극적으로 활용하려는 시도를 별이고 있다. 예를 들어, 탈북 이전 북한의 컴퓨터공학과 교수이기도 했던 <NK지식인연대>의 김흥광 대표에 의하면, 북한은 첨단 IT의 급속한 발전을 따라잡지 못하고서는 나라의 발전은커녕 체제유지도 사실상 어려움을 깨닫고 1990년 초부터 북한 지도부가 직접 나서서 IT발전의 필요성을 역설하기도 하고 중국과 인도의 IT기술을 벤치마킹하기 시작하였다고 한다. 북한은 1995년경부터 사이버 전력 확보를 위한 전략수립과 부대창설, 사이버 공격 기술연마, 지휘체계 구축에 집중하기

시작하였다. 매년 해커요원을 양성해 왔으며 그들의 사이버전 능력은 미국의 중앙정보국(CIA)에 필적한다고 전해진다(김흥광, 2011).

이렇듯 북한군이 정보전과 사이버 전력 증강에 매달리고 있는 중요한 이유는 미군이나 한국군에 대한 전력의 열세를 보강하고 평상시에도 한국군에 대한 정보적 우위를 선점하려는 것이라고 한다. 특히 북한은 주변국인 중국과 러시아가 일찍이 사이버 부대를 창설해 대규모 사이버 군사 활동을 전개하고 있는 것에서 큰 영향을 받았다고 한다. 북한은 사이버 부대의 조직을 정비하고 사이버전 병력을 기존 5백 명에서 3천명 수준으로 늘렸다. 이렇게 북한이 사이버 전력을 증강한 이유는 구축 및 유지비용이 여타 전력에 비해 적게 들고, 평상시에도 효과적으로 활용할 수 있고, 공격행위를 쉽게 은닉할 수 있기 때문이라고 한다. 따라서 사이버 전력은 북한의 대남 전략 실현에 있어서 더없이 안성맞춤의 전력이자 강력한 비대칭성을 구사할 수 있다는 것이다. 북한의 인식에는 한국의 사이버 공간이 보안에 취약하며 공권력이 덜 미치는 '해방 공간'으로 비치고 있다(김흥광, 2011).

이러한 북한의 사이버 전력의 구축 과정에서 중점을 두는 요소는 두뇌풀, 장비, 시스템 등 세 가지라고 한다. 첫째, 두뇌풀은 "전산과 네트워크 이론을 마스터하고 사이버 테러나 공격기술로 무장한 정보 전사들"을 의미한다. 김 대표에 의하면, 세 가지 요소 중에서 북한이 가장 공을 들인 것은 사이버 인간병기인 정보전사(즉 해커) 양성이라고 한다. "정보전사 양성을 위해 북한은 1995년 경 중앙과 도소재지들에만 설치되어 있던 1중학교(영재학교)를 시, 군, 구역마다 하나씩 세우고 중앙에는 평양 1중학교외에 금성 1중학교와 2중학교에 컴퓨터 영재반을 새로 조직했다"고 한다. 또한 "북한은 이들을 김일성종합대학, 김책공업종합대학, 평양컴퓨터대학과 이과대학,

미림대학에 우선 입학시켜 전문기술을 배워주고 대학 졸업 후 전원 외국유학을 보내며, 귀국 후 대부분 해킹 전문부대들에 배치되기 때문에 전투원들의 평균 나이는 20대"라고 한다. 뿐만 아니라 북한은 "수시로 리더급 컴퓨터 영재들을 장교로 선발해 해킹공격에 대한 작전조직 지휘능력을 향상시켜 오고 있다"는 것이다(김흥광, 2011).

둘째, 장비는 "최고 사양의 각종 컴퓨터와 메인프레임과 주변설비, 인터넷 훈련망" 등을 의미한다. 북한은 정보전사들에게 첨단 장비시설들을 구비해 주는 데 돈을 아끼지 않았다고 한다. 바세나르 협약이나 미국 상무성 규제에 의하면 북한에 반입될 수 있는 컴퓨터는 IBM PC XT급 정도이다. 그러나 이러한 급의 컴퓨터로는 효과적인 해킹을 할 수 없다는 판단 하에 북한은 "정보전사들이 사용할 고성능 컴퓨터를 비롯한 첨단장비들을 중국과 해외에서 대량 입하하고 있다"고 한다. 특히 "중앙당 9국은 김정일과 일가족, 중앙당 특수부서들에서 필요되는 첨단전자제품들을 수입해오는 업무를 전담하는 부서"인데, 1995년 이후 사이버 부대가 해킹공격능력 함양에 필요되는 일체 설비들을 구입해 주고 있다고 한다. 중앙당 9국이 바세나르 협약에 가입하지 않은 국가에서 활동하는 해외공관과 무역회사들을 활용하여 사이버 전력 증강을 위한 모든 장비와 설비들을 가장 최신 것으로 구입한다는 것이다(김흥광, 2011).

끝으로, 시스템은 "정보전사들을 사이버 공격에로 조직하고 동원하기 위한 명령지휘 및 관리체계"를 의미한다. 김 대표에 의하면, 북한은 사이버전 작전과 전투실행, 명령지휘체계를 일체화하기 위한 사이버공격 시스템 완성에 주력하고 있다. 2007년부터는 독립적인 해킹공격 능력을 갖춘 복수개의 공격조를 운영해오던 종전의 시스템을 효율성 제고를 위해 대폭 개편하였다고 한다. 구체적으로 "시스템 분석팀, 공격작전팀, 코드처리팀, 개발팀, 검사팀, 네트워크

분석팀, 전투기획팀 등 다수의 직능팀들이 일사불란하게 명령체계에 따라 작동한다"고 한다. 특히 "사이버전에 대한 성과가 속출함에 따라 사이버 전력증강과 공격에 대한 일체화된 지휘를 위해 2010년에 인민무력성 정찰국 예하로 있던 사이버부대 121소를 정찰총국에 직속시키고 별도의 사이버전국(121국)을 만들어 남한의 전략적 기관들에 대한 사이버 테러와 공격, 민간기관과 단체들에 대한 해킹 및 인터넷대란을 일으키는 작전들을 총괄하는 총본산으로 기능하게 되었다"고 한다(김흥광, 2011).

Ⅳ. 디지털 한국의 그물망 방패

1. 사이버 안보의 국내외 거버넌스

국가 행위자는 사이버 공격의 주체가 될 수도 있겠지만, '창'을 막는 '방패'의 역할도 자임하고 있다. 이런 면에서 사이버 안보 분야에서 나타나는 국가 행위자는 두 얼굴을 가지고 있다. 그 하나가 공격자의 얼굴이라면 다른 하나는 방어자의 얼굴이다. 새로이 등장한 인터넷 환경에서 초국적으로 활동하는 비국가 행위자들을 교묘히 네트워킹하여 사이버 공격을 벌이는 국가의 모습이 있는가 하면, 비국가 행위자들뿐만 아니라 여타 국가 행위자들의 네트워킹을 통해서 사이버 안보를 지키려는 국가의 모습도 있다. 초창기의 사이버 안보 이슈가 초국적 비국가 행위자들의 위협과 이에 대응하는 전통적인 국가 행위자의 망제정치로 그려졌다면, 최근의 양상은 국가 행위자들 스스로가 사이버 공격과 방어의 문제에 본격적으로 관여하는 모습으로 나타나고 있다.

이렇게 두 얼굴을 한 국가의 몸체는 전통적인 위계조직이라기보다는, 비국가 행위자들과 좀 더 밀접한 관계를 맺으면서 변화하는

네트워크 조직이다. 소위 네트워크 국가(network state)라고 할 수 있다(하영선·김상배 편, 2006). 사이버 테러와 공격 그리고 사이버 안보의 분야는 네트워크 국가들이 벌이는 세계정치의 대표적인 사례이다. 특히 그물망 방패를 치는 일은 네트워크 국가의 역할이 요구되는 분야이다. 사실 앞서 언급한 사이버 공간의 구조적 속성상 사이버 방어는 종전의 위계조직의 형태를 갖는 국가 행위자가 홀로 나서서 맡기에는 벅찬 문제이다. 수평적 네트워크의 형태를 추구하는 비국가 행위자들과 적극적인 관계를 설정하면서도 다차원적인 목표를 유연하게 추구하는 네트워크 국가의 역할이 요구되는 분야이기도 하다. 이러한 네트워크 국가의 개념은 국내외 차원에서 추구되는 거버넌스(governance)의 개념과 통한다.

네트워크 국가의 거버넌스라는 시각에서 보았을 때, 사이버 안보 분야에서 앞장서서 그물망 방패의 역할을 수행하는 대표적인 나라는 단연코 미국이다. 대 이란 공격에서 보았듯이 미국은 사이버 공격을 감행할 수 있는 가장 우수한 자원과 기술을 보유하고 있는 나라이지만, 만약에 사이버 공격을 받을 경우 가장 많은 피해를 볼 수밖에 없는 나라이다. 다시 말해, 미국은 세계 어느 나라보다도 발달된 정보 인프라를 구비하고 있고, 국가 발전과 운영에 있어 이러한 인프라에 대한 의존도가 어느 나라보다도 높다. 게다가 사이버 공간의 거버넌스에 있어서도 미국은 개방적이고 민간 주도적인 접근법을 취하기 때문에 만약에 있을 사이버 공격으로부터 취약할 수밖에 없다. 따라서 전통적 군사력에서 열세인 국가들이 미국을 상대로 하여 사이버 공간에서 비대칭적 공격을 감행할 유인과 여건이 높은 것이 사실이다.

미국이 사이버 테러나 공격에 대한 대응을 고민한 역사는 1990년대에서부터 시작되었지만, 본격화된 것은 9.11 테러 이후이다. 2003년

부시 행정부는 본격적인 사이버 안보 전략 문서인 <National Strategy to Secure Cyberspace>를 발표했다. 국가안보회의(NSC), 국방부, 정보기관 등 전통적인 안보기구가 정책형성에 주로 참여하였고, 국토안보부가 사이버 안보 집행 기구로 참여하여 CERT (Computer Emergency Response Team)를 운영하였다. 부시 행정부 2기로 옮겨가면서 체계적인 노력들이 이루어졌다. 예를 들어, 2005년 미 국방부는 사이버 작전의 개념을 담은 보고서를 펴내기도 했으며, 부시 행정부는 2008년에 좀 더 체계적인 전략문서인 <Comprehensive National Cybersecurity Initiative, CNCI>를 발표했다. 2008년에는 국토안전부 장관 직속으로 국가사이버안전센터(National Cybersecurity Center)를 설치하기도 했다.

오바마 행정부는 부시 정부의 기본 정책인 CNCI를 기본적으로 계승하였다. 오바마 정부는 2011년 5월 <International Strategy for Cyberspace>를 발표하여 사이버 안보에 있어서 국제협력의 필요성을 강조하였다. 군사적인 차원에서도 오바마 정부는 2009년 전략사령부 하에 사이버 사령부(Cybercommand)를 창설하였다. 2011년 7월에는 미 국방부의 사이버 공간 작전수행을 위한 전략(Department of Defense Strategy for Operating in Cyberspace)이 발표되었다. 2012년 5월에는 미 국방부가 <Plan X> 프로젝트를 발표했는데, 이 프로젝트는 미 국방부의 사이버 전략 증강계획의 일환으로 2017년까지 1조 8,000억 원의 예산을 투입하여 사이버전 실전에 활용할 수 있는 사이버 무기 개발을 추진하고, 전세계 컴퓨터 도메인과 서버를 표시할 수 있는 디지털 전장지도를 개발하는 목표를 제시하였다.

이러한 일련의 전개과정에서 특히 주목할 것은 2010년에 접어들면서 사이버 안보에 대한 미국의 태도가 방어의 개념으로부터 공격

의 개념으로 변화했다는 사실이다. 방어를 위해서라면 선제공격의 개념을 도입할 수 있다는 미국 정부의 결연한 의지를 보여주는 사례는, 앞서 머리말에서 언급한 바와 같이, 사이버 공격에 대해서는 미사일을 발사해서라도 강력히 대응하겠다는 2012년 5월 미 국방부의 발표에서 발견된다. 그런데 이 발표가 다소 역설적으로 들린 이유는 도대체 '누구'를 향해서 미사일 공격을 가하겠다는 것인지 의문이 들기 때문이다. 앞서 제2장에서 살펴본 바와 같이, 사이버 안보라는 분야의 속성상 사이버 공격을 가할 위험이 있는 특정 대상을 선정하여 미리 억지하거나 대비한다는 것이 이 발표문의 내용처럼 쉬운 일은 아니라는 데 깊은 고민이 있다.

초국적으로 발생하는 특성상 사이버 안보에 대한 대책은 일국 차원의 대응만으로는 부족하고 포괄적인 국제협력이 필요할 수밖에 없다(Hathaway, 2010; Hughes, 2010). 그런데 여기서 유의해야 할 점은, 그물망 방패를 마련하려는 국제협력의 모색도 버추얼 창의 시도와 마찬가지로 인터넷의 복합 네트워크 환경을 바탕으로 한다는 사실이다. 사이버 안보 분야에서 국가 및 민간 행위자들은 서로가 가진 지식과 기술을 손쉽게 공유하기 위해서 다양한 제도와 기구의 설립을 모색하고 있다. 기존의 정치군사 동맹이 국가 행위자들 간의 연대를 의미하는 것이었다면, 디지털 시대의 국제협력은 국가 행위자이외에도 민간 기업이나 시민사회 등과 같은 비국가 네트워크 행위자가 참여하는 것이 특징이다. 앞서 언급한 미 백악관의 2011년 5월 보고서도 사이버 안보의 국제협력을 강조하고 있다.

돌이켜보면, 지난 10여 년 동안 사이버 범죄나 테러에 대한 국제협력이 꾸준히 진행되어 왔다. 2001년 유럽사이버범죄협약(European Convention on Cybercrime), 소위 부다페스트 협약은 사이버 범죄에 대응해서 국가들이 나서 상호 간의 법제도를 조율하는

정부 간 네트워크를 구성한 초기 사례이다. 그 연속선상에서 선진국 정부들을 중심으로 사이버 안보를 논의하는 국제적 틀이 모색되고 있다. 예를 들어, 최근 영국의 주도로 2011년 런던에서 1차 회의가 열린 사이버공간총회를 들 수 있다. 런던 회의에서는 60개국 70여명의 정부 관계자, 비정부기구 대표 등이 모여 글로벌 인터넷 거버넌스의 쟁점들이 다루어졌는데, 특히 '사이버 공간에서 수용할만한 행태를 위한 규범'을 주제로 하여 경제성장과 개발, 사회적 혜택, 사이버 범죄, 안전하고 신뢰할 수 있는 접속, 국제안보 등의 5개 세부 의제를 논의하였다. 이후 2012년 부다페스트에서 제2차 사이버공간총회가 열렸으며, 2013년 10월에는 서울에서 제3차 사이버공간총회가 열린 바 있다.

사이버공간총회와는 별도로 진행되고 있는 사이버 안보에 대한 국제적 논의들에도 주목할 필요가 있다. 그 중의 일례가 바로 앞서 머리말에서 언급한 탈린 매뉴얼이다. 2013년 3월 나토의 CCDCOE는 총 95개 조항의 교전수칙을 담아 발표한 탈린 매뉴얼에서 사이버 공격을 '무력 분쟁'의 하나로 규정했다. 사이버 테러로 인해 인명과 재산 피해가 발생하면 군사력을 사용하는 일도 가능하도록 했다. 그 주요 내용은 사이버 공격을 받았을 경우 주변 피해를 최소화할 것을 요구하고 있으며, 해킹을 당했을 때 디지털 공격으로 보복이 가능하나 실제 공격은 사이버 공격으로 인해 사망자나 부상자가 있을 경우에만 허용하고 있다. 이 매뉴얼은 구속력이 없는 지침서의 형식을 취하고 있다. 탈린 매뉴얼은 전쟁 때 민간인과 포로에 대한 보호를 규정한 '제네바 협약'처럼 사이버 전쟁에도 국제법적인 교전 수칙을 만들려는 의도에서 추진되었다. 그러나 나토 회원국의 전문가들이 참여하여 만듦으로써 중국이나 러시아 등이 배제된 채 미국 중심의 시각에 반영된 결과라는 비판을 받고 있다(Schimit, 2012).

아시아지역에서도 아세안+3이나 APEC의 틀을 빌어 사이버 안보 분야의 국제협력을 논의한 경험이 축적되어 있다. 사이버 공격에 대한 대응으로서 아세안+3 국가들은 IT장관회의를 통해서 2005년까지 CERT를 모든 국가에 세우는 목표를 상정하였고 현재 대부분의 아시아 국가에서 CERT가 활동하고 있다. APEC도 아세안이나 OECD 등과의 협력을 통해서 아태지역 사이버 안보 문제의 해결을 위해 노력하고 있다. APEC은 9.11 이후 사이버 안보에 대한 대응을 본격적으로 논의해 왔는데 이는 2003년에 사이버 안보전략의 채택으로 구체화 되었다. 한편 동북아시아에서도 한·중·일 3국은 IT장관회의를 통해 이 분야의 협력을 모색하고 있다. IT장관회의는 2002년 모로코에서 1차 회의가 개최된 이후 정례적으로 모임을 갖고 있다. 그러나 전반적으로 동북아시아에서 사이버 안보를 위한 정부 차원의 국제협력은 아직 미흡한 상태이다. 사이버 안보 분야의 민간 협력을 모두 포함하더라도 아직 본격적인 사이버 안보의 국제협력 또는 지역협력 체계는 갖춰지지 않았다(Ortis, 2007; N. Thomas, 2009).

2. 한국의 사이버 안보 대응체계: 현황과 방향

이러한 맥락에서 한국이 벌이고 있는 사이버 안보의 거버넌스 구축을 위한 다각적인 노력에 주목할 필요가 있다. 한국의 사이버 안보 대책은 크게 세 가지 차원으로 나누어 진행되고 있다. 첫째, 국가정보원이 주도하고 있는 공공 부문의 사이버 안보 대책이다. 2005년 2월 발표된 <국가사이버안전관리규정>을 기초로 하여 국가정보원장 소속 하에 국가사이버안전전략회의를 설치하였으며, 실무기관은 국가사이버안전센터(NCSC: National Cyber Security Center)가

담당하였다. 2005년 3월에는 <국가위기관리기본지침>에 의거, NSC (National Security Council)에서 발간한 <사이버안전 분야 위기관리 표준 매뉴얼>과 국가정보원에서 제정한 <국가사이버안전관리규정>에 의거하여 사이버위기경보체계를 재정비하였다. 변경 전에는 예보-주의-경고-위험 등 4단계였던 것을 변경 후에는 정상-관심-주의-경계-심각 등 5단계로 조정하였다. 그러나 이러한 <국가사이버안전관리규정>은 국가 및 공공기관만 관장한다는 한계를 안고 있다.

둘째, 민간 부문의 사이버 안보의 실무를 담당하는 기관으로는 한국인터넷진흥원(Korea Internet and Security Agency, KISA)을 들 수 있다. 1996년 4월 정보화촉진기본법에 의거하여 설립된 한국정보보호센터가 2001년 7월 한국정보보호진흥원(Korea Information Security Agency)으로 승격되었다. 한국정보보호진흥원 주도로 한국정보통신망침해사고대응팀협의회(CONCERT)가 발족되었고, 1998년 1월 국제침해사고대응팀협의회에 가입했다. 한국정보보호진흥원의 주요 임무는 정보보호를 위한 정책 및 제도의 조사·연구, 정보보호 기술 개발, 정보보호 시스템의 연구·개발 및 시험·평가, 정보보호에 관련된 표준 및 기준 연구, 정보화 역기능 분석 및 대책연구 등 정보보호에 관한 다양한 활동 등이다. 이러한 업무는 2009년 7월에 한국정보보호진흥원, 한국인터넷진흥원, 정보통신국제협력진흥원 등이 통합되어 출범한 한국인터넷진흥원의 업무로 이어져 내려오고 있다.

끝으로, 군, 경찰, 검찰 차원의 사이버 안보 대응 체계이다. 2009년 7월 7일 디도스 공격을 계기로 군 차원의 사이버 안보의 필요성이 대두됨으로써 국군사이버사령부가 창설되었는데, 이는 사이버전의 기획, 계획, 시행, 연구·개발 및 부대 훈련에 관한 사항을 관장한다.

경찰 차원에서는 2000년 7월 창설된 경찰청 사이버테러대응센터 또는 사이버 수사대, 일명 네탄(NETAN = Network + 安·眼)이 해킹, 바이러스 제작 및 유포 등 각종 컴퓨터 범죄의 포착과 수사를 담당하고 있다. 검찰 차원에서는 2009년 7월 대검찰청에 인터넷범죄수사센터가 설치되어 해킹과 바이러스 유포, 전자상거래 사기, 개인 명예 및 신용훼손, 음란·폭력·자살 조장 등 컴퓨터 범죄 전반에 대한 동향과 수사를 펼치고 있다.

이러한 분산적 노력을 종합하려는 사이버 안보 대책으로는 2011년 8월 <국가사이버안보마스터플랜>을 사례로 들 수 있다. 이 계획은 국가정보원, 방송통신위원회, 금융위원회를 비롯해 15개 정부 관계부처가 합동으로 마련한 사이버 안보의 종합 계획이다. 2011년 상반기 디도스 공격에 이어 현대캐피탈 고객정보 유출 사고와 사상 초유의 농협 전산망 마비 사태를 겪으면서 국가 차원에서 총체적인 사이버위협 대응체계를 재정립하고, 세부 시행계획을 마련하기 위해 2011년 5월 범부처 차원에서 종합 계획을 마련하였다. 그러나 이렇게 발표된 사이버 안보 종합 계획은 사이버 공간을 영토·영공·영해에 이어 국가가 수호해야 할 중요한 영역으로 규정하였지만, '사이버 위협에 총력 대응하자'는 구호를 제시하는 상징적 수준에 그친 것으로 평가되었다.

이후 2013년 3.20 사이버 테러를 거치면서 국내 사이버 안보 대응체계의 정비 문제가 제기되었다. 이러한 맥락에서 논의된 것이 청와대에서 국내 사이버 안보 업무를 총괄하는 CSO(Cybersecurity Officer)의 설치 문제이다. 아울러 사이버 안보 대응체계의 체계화를 위한 법률정비의 필요성도 지속적으로 제기되고 있는데, 소위 '국가사이버위기관리법'의 제정 문제가 그것이다. 또한 외부로부터의 사이버 테러나 사이버 공격에 대응하여 사고를 분석하고 해결할

고급인력으로서 화이트 해커의 양성 문제나, 이 분야의 예산 확충 문제도 거론되었다. 이밖에도 유사시에 대비한 위기대응매뉴얼이나 사이버 방어를 위한 모의훈련, 민간 차원의 사이버 민방위 훈련 등의 구상이 등장하기도 했다.

이러한 공공 부문의 대책 마련과 더불어 효과적인 사이버 안보의 대응체계를 마련하기 위한, 정부와 민간 부문의 협력이 과제로 제기되고 있다. 다양한 경로를 통해 침투해 들어오는 사이버 공격을 정부 혼자서 대응할 수는 없기 때문이다. 비근한 사례로 2011년 농협 해킹 사건도 민간 금융기관인 농협의 부주의한 관리가 사건을 초래한 원인 중의 하나로 지적되었다. 미 국방부도 미군의 정보자원을 보호하기 위해 민간 영역과의 협력이 절대적으로 중요함을 인정한 바 있다. 이미 세계의 주요 25개국이 사이버 안보 관련 법안의 마련과 정부기구의 정비에 힘 쏟고 있으며 민간영역을 포함한 다양한 차원에서 CERT를 운영하고 있는 것으로 나타났다. 또한 정부와 기업체를 연결하는 회의체를 만들어 사이버 방어를 위한 민관의 동반 관계를 강화하고 있는 것으로 드러났다.

이러한 맥락에서 볼 때 사이버 안보 분야의 대책은 정부 차원을 넘어서 군, 경찰, 검찰까지도 포함하는 공공 부문과 민간 부문의 유기적 네트워크 구축을 통해서 마련되어야 할 성질의 것임을 알 수 있다. 다시 말해, 최근 북한의 소행으로 추정되는 사이버 공격에 대한 효과적인 대응체계를 만들기 위해서는 국가 행위자 혼자서는 안 되고 여러 행위자들이 나서서 그물망을 짜서 방패를 구축하려는 노력이 필요하다. 앞서 언급한 네트워크 국가의 역할을 기대케 하는 대목이다. 그렇다면 한국의 네트워크 국가는 향후 사이버 안보 분야에서 효과적인 그물망 방패를 구축하기 위해서 무엇을 해야 할 것인가? 이 글에서는 앞서 제시한 이론적 시각의 연속선상에서 사이버

안보의 국가전략에 시사점을 주는 몇 가지 방향을 지적하고자 한다.

첫째, 사이버 위협에 대처하기 위한 보안 인프라의 구축과 보안 인력의 양성이 시급하게 필요하다. 예를 들어, 일견 완벽해 보이는 '방패'의 구축은 해커들로 하여금 섣불리 '창'을 들 수 없게 하는 효과를 낳을 수 있다. 아무리 예리한 창으로 공격해도 뚫을 수 없는 방패라는 인식을 심어 주어 사이버 공격 자체를 아예 단념시키는 억지의 효과를 노릴 수 있기 때문이다. 또한 사이버 안보 관련된 기술과 지식을 두루 갖춘 고급 전문가들을 양성하는 것도 사이버 테러와 공격에 대한 효과적인 사전 예방 및 사후 대응이라는 차원에서 매우 중요하다. 한편 사이버 안보 인프라의 구축과 관련하여 마이크로소프트의 컴퓨터 운영체계에 대한 지나친 의존에서 벗어나야 한다는 지적의 목소리에도 귀를 기울일 필요가 있다. 사실 현재 한국의 운영체계는 윈도우가 지배하고 있고 인터넷 브라우저는 익스플로러가 독점하고 있다. 상황이 이렇다 보니 윈도우와 익스플로러만 해킹되면 국가 전산망 전체가 위험에 처하게 되는 상황이 발생할지도 모른다는 우려가 생기는 것은 당연하다.

둘째, 사이버 테러와 공격에 대응하기 위한 국내외 정보공유 네트워크 구축이 필요하다. 해커들의 동향이나 악성코드에 대한 정보, 특히 빅데이터를 공유하는 환경을 구축하는 것이다. 이는 민간 부문과 정부가 나서 위키피디아 방식의 협업체계를 만드는 구상으로 통한다. 사전 대비가 쉽지 않은 사이버 위협의 특성상 체계적인 사후 대응을 통해 피해를 최소화하고 신속하게 공격의 원인을 분석하여 근원지를 역추적하는 대책이 거론되고 있다. 예를 들어 국가 사이버 안보 강화를 위한 포렌식 준비도(forensic readiness)의 도입이 그 일례이다. 포렌식 준비도란 사후 대응 시에 디지털 포렌식 증거 수집 및 분석의 역량을 극대화하고 비용을 최소화하기 위한 환경을

사전에 준비하는 것이다. 이러한 종류의 노력을 보여주는 대표적인 사례로서 전 지구적으로 형성된 CERT의 네트워크를 들 수 있다. 컴퓨터비상대응팀인 CERT들은 국가, 기업, 소규모 단체 등 다양한 수준에서 네트워크를 형성하고 침해사고의 이상 징후를 감지하고 이에 대한 효과적이고 신속한 대응체계를 구축하려는 노력을 벌여 왔다.

끝으로, 사이버 안보의 글로벌 거버넌스를 구축하는 과정에 적극 참여할 필요가 있다. 현재는 사이버 테러와 공격이 발생하고 그 공격 주체를 색출하더라도 국제적으로 호소하거나 공격행위에 대한 처벌이나 제재에 대해 논의할 수 있는 외교의 공간이 마련되어 있지 않다. 예를 들어 천안함 사건이나 연평도 포격 사건이 발생했을 때에는 유엔 안보리에 호소할 통로가 있었으나, 북한의 소행으로 추정되는 사이버 공격이 발생해도 마땅히 호소할 통로(예컨대, 사이버 안보리)는 없는 실정이다. 보이지 않는 공격이 이루어지는 사이버 안보는 기술의 논리로만 풀어갈 문제가 아니라 정치외교의 논리가 가세해야 하는 문제일 수 있다. 이런 맥락에서 다양한 경로를 통해서 진행되고 있는 사이버 안보 분야의 국제규범 형성이나 글로벌 거버넌스의 모색 과정에 한국은 적극 참여할 필요가 있다. 최근, 앞서 언급한 사이버공간총회를 서울에서 개최한 것은 큰 성과라고 볼 수 있다. 다만 우려스러운 점이 있다면 이들 국제적 논의의 장에 참여함에 있어서 한국은 아직도 사이버 안보 문제를 어떤 입장에서 다루어야 할지에 대해 명확히 입장 설정을 하지 못하고 있다는 사실이다.

요컨대, 최근 늘어나고 있는 북한발 사이버 공격에 대처하는 방책의 핵심은 국내외 차원에서 다층적인 그물망 방패를 짜려는 노력을 경주하는 데 있다. 물론 그물망을 아무리 촘촘하게 짜더라도 빈

틈이 없는 것은 아니다. 앞서 언급한 바와 같이 사이버 공간의 네트워크 구조는 디지털의 논리에 맞추어 0과 1을 모아서 씨줄과 날줄을 삼아 아무리 촘촘하게 짤 지라도 착취혈을 없앨 수 없기 때문이다. 그럼에도 불구하고 그물망 방패를 만들려는 노력을 멈출 수는 없다. 복합 네트워크 환경을 바탕으로 발생하고 있는 북한발 사이버 테러와 공격의 위협은 단순히 일국 차원에서 대응책을 마련하거나 법제도를 정비하는 문제를 넘어서 좀 더 포괄적인 차원에서 네트워크 국가들의 국제협력을 통해서 풀어나가야 하는 문제이다.

Ⅴ. 맺음말

최근 북한의 소행으로 추정되는 사건들이 늘어나면서 사이버 테러와 공격의 위협이 단순히 잠재적으로 존재하는 위협이 아니라 현실화될 가능성이 매우 큰 위협으로서 인식되기 시작했다. 무엇보다도 인터넷이 우리의 삶에서 차지하는 비중이 커지면서, 총알이나 포탄이 날아와 우리의 생명을 위협하지 않더라도, 인터넷이 다운되는 것 자체가 사회시스템 차원에 큰 위협이 된다는 점을 알기 시작했다. 만약에 한반도에서 재래식 전쟁이나 핵전쟁이라도 발발한다면, 사이버 공격이 뇌관의 역할을 할 것이고, 그 피해는 상상을 넘을 것은 뻔하다. 객관적으로 입증하는 것이 어렵다는 유보사항이 있지만, 북한이 이미 한국을 향해 여러 차례의 사이버 공격을 감행했다고 추정되는 근거가 많이 발견된다. 실제로 북한은 미국이 수행한 테러와의 전쟁으로 인해 정권의 안위를 걱정하게 되면서 재래식 전력의 약점을 보완하기 위한 수단으로서 핵무기와 함께 사이버 전력을 전략적으로 육성해 온 것으로 알려져 있다.

아무리 국가 행위자가 적극적인 주체로 나서더라도 사이버 공격은 전통적인 국가안보의 시각을 넘어서는 좀 더 복합적인 시각에서

이해해야 하는 문제이다. 사이버 안보 분야는 영토성을 기반으로 하여 국가가 독점해온 안보유지 능력의 토대가 잠식되는 현상을 보여주는 좋은 사례이다. 사이버 공간에서 등장한 새로운 위협은 국가에 의해 독점되어 온 군사력의 개념뿐만 아니라 군사전략과 안보의 개념 자체도 그 기저에서부터 뒤흔들어 놓고 있다. 인터넷 환경은 테러 네트워크나 범죄자 집단들에 의해 도발될 소위 비대칭 전쟁의 효과성을 크게 높여 놓았다. 이러한 비대칭 전쟁이 가장 첨예하게 드러나는 분야가 바로 사이버 테러와 공격이다. 이러한 상황에서 최근 미국-이스라엘과 이란 간에 벌어진 사이버 전쟁은 해커들의 장난이나 도발적인 비국가 행위자들의 테러 정도로만 인식되었던 사이버 안보의 영역에 국가 행위자가 명시적으로 개입하게 됨으로서 사태를 더욱 복잡하게 만들었다.

이러한 변화에 직면하여 기존의 국제정치이론은 시원스러운 해답을 제시하지 못하고 있다. 국가 단위에만 주목하는 안보 이론으로는 사이버 안보의 복합성을 제대로 이해할 수 없다. 특히 냉전 시대에 개발된 국가안보나 핵 안보의 개념과 이론을 섣불리 사이버 안보의 문제에 적용해서는 곤란하다. 기존의 국제정치 연구는 주요 행위자로서 국가 간의 양자 또는 다자 관계라는 맥락에서 세계정치의 안보 문제를 탐구해 왔다. 그러나 사이버 안보의 문제는 이러한 군사안보와 국가안보의 단순 시각으로는 제대로 파악되지 않는 고유한 성격을 갖는다. 이러한 맥락에서 이 글은 네트워크 이론을 원용하여 다양한 네트워크들 간에 벌어지는 정치, 즉 다층적인 망제정치를 보는 새로운 시각을 제시하였다.

창과 방패를 파는 두 상인의 이야기를 다룬 모순(矛盾)이라는 중국의 고사성어에서 창과 방패의 대결이 어떤 결과를 낳았는지 전하지 않듯이, 디지털 시대를 사는 우리가 관전하는 버추얼 창과 그

물망 방패의 결투도 쉽사리 결말을 논할 수는 없다. 다만 현재 우리에게 필요한 것은 문제를 너무 단순하게 보지 않는 신중함이다. 아날로그 시대의 '모순'이 한 개의 창으로 한 개의 방패를 찌르는 이야기였다면, 디지털 시대의 '모순'은 여러 개의 보이지 않는 창으로 찌르는 공격을 여럿이 힘을 합쳐서 얼기설기 만든, 그물망과도 같은 방패로 막아내는 야야기이기 때문이다. 이러한 시각을 원용하여 네트워크 국가를 주인공으로 하여 벌어지고 있는 사이버 안보의 세계정치를 이해해야 한다. 특히 이 글은 아래와 같은 다섯 가지 차원으로 구별되는 '비대칭 망제정치(asymmetric inter-network politics)'의 동학을 이해하는 것이 향후 한국의 사이버 국가전략을 수립하는데 있어서 중요하다는 점을 강조하고자 한다.

첫째, 비인간 행위자와 인간 행위자 간에 형성되는 망제정치이다. 이는 물리적 네트워크와 소셜 네트워크 사이에서 벌어지는 동학이다. 행위자-네트워크 이론의 틀에서 보면, 사이버 안보 문제는 '네트워크들의 네트워크'라는 별명을 가진 인터넷이라는 비인간 행위자와 해커와 국가라는 인간 행위자들이 형성하는 네트워크의 게임이다. 이러한 네트워크 게임은 소셜 네트워크 이론에서 말하는 네트워크상의 구조적 공백, 특히 착취혈이라고 불리는 취약점을 해커들이 공략하거나, 반대로 국가 행위자가 나서서 그 공백을 메우는 망제정치의 게임이다.

둘째, 초국적 테러 네트워크와 국가 행위자들이 벌이는 망제정치이다. 다시 말해, 버추얼 창을 들고 공격하는 비국가 행위자들의 네트워크와 이를 막으려고 그물망 방패를 든 국가 행위자들의 네트워크 사이에서 벌어지는 망제정치이다. 머리말에서 언급했듯이, 해킹 기술은 점점 더 교묘해지고 하루가 멀다 하고 새로운 컴퓨터 바이러스가 출현한다. 이에 대응하여 새로운 방화기술과 백신 프로그

램이 개발되고 해커들의 은신처를 찾아내는 기법도 점점 더 발달하고 있다. 이러한 기술 변화의 와중에 초국적 비국가 행위자와 국가 행위자가 펼치는 망제정치가 진행되고 있다.

셋째, 국가들 간에 벌어지는 버추얼 창과 그물망 방패의 망제정치이다. 최근에 사이버 안보에서 두드러지게 나타나는 현상은 비국가 행위자들이 시도하는 사이버 테러와 공격의 이면에 국가 행위자들이 깊숙이 관여하고 있다는 사실이다. 최근 러시아, 중국, 북한 등에서 보고되는 사이버 테러 부대의 존재는 이러한 국가의 그림자를 엿보게 하는 증거이다. 여기에 상황을 더욱 복잡하게 만드는 것은 사이버 공격과 관련하여 가장 많은 자원력과 기술력을 지닌 미국이 새로운 사이버 공격의 주체로 등장했다는 사실이다.

넷째, 일국 차원에서 벌어지는 사이버 안보의 대응책과 여러 나라가 협의하는 국제협력의 메커니즘을 취하는 사이버 안보의 대응책 사이에서 나타나는 망제정치의 모습이다. 복합 네트워크의 메커니즘을 빌어 발생하는 사이버 테러와 공격은 단순히 일국 차원의 대응책 마련과 법제도의 정비 등으로 해결될 문제가 아니다. 기본적으로 국민국가의 국경을 초월하여 발생하는 문제이니만큼 긴밀한 국제협력을 통해서 그 해법을 모색하는 것이 필요하다.

끝으로, 전통적인 정부 간 협력의 틀과 민간 행위자들도 참여하는 글로벌 거버넌스의 틀 사이에서 형성되는 망제정치이다. 최근의 양상은 초국적 위협으로 제기된 사이버 테러와 공격의 문제에 대해서 국제협력이나 국가 간 협약과 같은 메커니즘으로 해결하려는 움직임의 등장이다. 그러나 초국적으로 발생하는 사이버 안보 문제의 해결을 위해서는 '국가 행위자들 간의 정치'를 의미하는 '국제정치'의 발상을 넘어설 필요가 있다. 이러한 과정에서 국제레짐의 메커니즘과 경합하는 글로벌 거버넌스 모델이 부상하고 있다.

요컨대, 사이버 안보의 세계정치는 전통적인 의미의 국민국가들이 벌이는 게임은 아니다. 새로운 주인공으로서 네트워크 국가들이 벌이는 게임으로서 이해해야 할 것이다. 이러한 과정에서 네트워크 국가는 사이버 공격이라는 위협 요인을 제공하는 주체인 동시에 초국적으로 또는 국가 간에 발생하는 사이버 위협을 방지하기 위한 메커니즘을 만드는 주체이기도 하다. 다시 말해 사이버 안보의 문제를 둘러싸고 벌어지는 망제정치의 과정에서 중심성(centrality)을 제공하는 주체이다. 이러한 지적은 21세기 네트워크 세계정치의 급속한 진전의 와중에도 국가는 그 역할을 자기조정하면서 새로운 역할과 형태를 찾아가고 있다는 논의로 통한다. 최근 국내에서 일고 있는 사이버 안보에 대한 국가적 관심이나 북한의 사이버 공격에 대한 우려도 이러한 세계정치의 변환에 대한 이해를 바탕으로 방향을 잡아야 할 것이다.

참고문헌

김상배. 2011. “사이버 안보의 국제협력.” JPI PeaceNet, 11-08.

김상배. 편. 2011. 『거미줄 치기와 벌집 짓기: 네트워크이론으로 보는 세계정치의 변환』 한울.

김홍광. 2011. “북한의 사이버 테러능력.” 북한민주화네트워크 편, 『2011 북한의 사이버 테러 관련 긴급 세미나 자료집』.

민병원. 2007. “탈냉전기 안보개념의 확대와 네트워크 패러다임.” 『국방연구』 50(2), pp.23-55.

이상현. 2008. “정보보안 분야의 지식질서와 동아시아.” 김상배 외. 『지식질서와 동아시아: 정보화시대 세계정치의 변환』 한울, pp.295-330.

임종인. 2013. “사이버전과 Tallin Manual.” 국립외교원 사이버안보 세미나. 4월 25일.

장노순·한인택. 2013. “사이버안보의 쟁점과 연구 경향.” 『국제정치논총』 53(3), pp.579-618.

조현석. 2012. “사이버 안보의 복합세계정치.” 하영선·김상배 편. 『복합세계정치론: 전략과 원리, 그리고 새로운 질서』 한울, pp.147-189.

최인호. 2011. “사이버 안보의 망제정치: 사이버 창이냐? 디지털 방패냐?” 김상배 편. 『거미줄 치기와 벌집 짓기: 네트워크 이론으로 보는 세계정치의 변환』 한울, pp.285-325.

하영선·김상배 편. 2006. 『네트워크 지식국가: 21세기 세계정치의 변환』 을유문화사.

하영선·김상배 편. 2010. 『네트워크 세계정치: 은유에서 분석으로』 서울대학교 출판사.

Arquilla, John and David Ronfeldt. 1996. *The Advent of Netwar.* Santa Monica, CA: RAND Corporation.

Arquilla, John and David Ronfeldt. 2001. “The Advent of Netwar (Revisited).” in John Arquilla and David Ronfeldt, eds. 2001. *Networks and Netwars: The Future of Terror, Crime and the Militancy.* Santa Monica, CA: RAND Corporation.

Beck, Ulrich. 1999. *World Risk Society.* Cambridge, UK: Polity.

Beck, Ulrich. 2005. “World Risk Society and the Changing Foundations of Transnational Politics.” in Edgar Grande and Louis W. Pauly, eds. 2005. *Complex Sovereignty: Reconstituting Political Authority in the Twenty-first Century.* Toronto: University of Toronto Press.

Burt, Ronald S. 1992. *Structural Holes: The Social Structure of Competition.* Cambridge, MA: Harvard University Press.

Burt, Ronald S. 2005. *Brokerage and Closure: An Introduction to Social Capital.* New York: Oxford University Press.

Buzan, Barry and Lene Hensen. 2009. *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Cavelty, Myriam Dunn. 2007. *Cyber-security and Threat Politics: US efforts to Secure the Information Age.* New York: Routledge.

Deibert, Ronald J. 2002. “Circuits of Power: Security in the Internet Environment,” in James N. Rosenau and J.P. Singh. eds. *Information Technologies and Global Politics: The Changing Scope of Power and Gover-*

nance. Albany, NY: SUNY Press, pp.115-142.
Deibert, Ronald, et al. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: The MIT Press.
Deibert, Ronald, et al. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: The MIT Press.
Deibert, Ronald, et al. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics.* Cambridge, MA: The MIT Press.
Eriksson, Johan and Giampiero Giacomello eds. 2007. *International Relations and Security in the Digital Age.* London and New York: Routledge.
Evron, Gadi. 2008. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs.* 9(1) pp.121-126.
Farwell, James P. and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War," *Survival.* 53(1), pp.23-40.
Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization.* Cambridge, MA: MIT Press.
Galloway, Alexander R. and Eugene Thacker. 2007. *The Exploit: A Theory of Networks.* Minneapolis and London: University of Minnesota Press.
Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly,* 53(4), pp.1155-1175.
Hathaway, Melissa. 2010. "Toward a Closer Digital Alliance." *SAIS Review,* 30(2), pp.21-31.
Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs,* 86(2), pp.523-541.
Klimburg, Alexander. 2011. "Mobilizing Cyber Power." *Survival.* 53(1), pp.41-60.
Koch, Richard and Lockwood Greg. 2010. *Superconnect: Harnessing the Power of Networks and the Strength of Weak Links.* New York: W.W. Norton & Co.
Libicki, Martin C. 2009. *Cyber Deterrence and Cyber War.* Santa Monica, CA: RAND Corporation.
Lupovici, Amir. 2011. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Strategic Affairs.* 3(3), pp.49-62.
Manjikian, Mary McEvoy. 2010. "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly,* 54(2), pp.381-401.
Matusitz, Jonathan A. 2006. *Cyberterrorism: A Postmodern View of Networks of Terror and How Computer Security Experts and Law Enforcement Officials Fight Them.* Ph.D. Dissertation, University of Oklahoma.
Morgan, Patrick M. 2010. "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm." Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S.

Policy. National Research Council.
Newman, Mark, Albert-László Barabási, and Duncan J. Watts. eds. 2006. *The Structure and Dynamics of Networks*. Princeton and Oxford: Princeton University Press.
Nye, Joseph S. 2010. "Cyber Power." Belfer Center for Science and International Affairs, Harvard Kennedy School.
Ortis, Cameron J. 2007. *Bowing to Quirinus: Compromised Nodes and Cyber Security in East Asia*. Ph.D. Dissertation, University of British Columbia.
Rattray, Gregory J. and Jason Healey. 2011. "Non-State Actors and Cyber Conflict." Kristin M. Lord and Travis Sharp, eds. *America's Cyber Future: Security and Prosperity in the Information Age*. Vol.2. Washington, DC: Center for A New American Security.
Schmitt, Michael N. 2012. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal*. 54, pp.13-37.
Shakarian, Paulo. 2011. "Stuxnet: Cyberwar Revolution in Military Affairs." *Small Wars Journal,* April.
Singer, Peter W. and Noah Shachtman. 2011. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive." August, 15, The Brookings Institution.
Steinberg, Philip E., and Stephen D. McDowell. 2003. "Global Communication and the Post-Statism of Cyberspace: A Spatial Constructivist View." *Review of International Political Economy*. 10(2), pp.196-221.
Thomas, Nicholas. 2009. "Cyber Security in East Asia: Governing Anarchy." *Asian Security,* 5(1), pp.3-23.
Thomas, Timothy L. 2009. "Nation-state Cyber Strategies: Examples from China and Russia." in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. eds. *Cyberpower and National Security*. Washington DC: Center for Technology and National Security Policy, National Defense University. pp.465-488.