국제·지역연구 27권 4호 2018 겨울 pp. 1-35

트럼프 행정부의 사이버 안보 전략:
국가지원 해킹에 대한 복합지정학적 대응*

김상배 | 서울대학교 정치외교학부 교수

최근 발생하는 사이버 공격은 양적으로 늘어나고 있을 뿐만 아니라 그 공격 목적도 다변화되고 공격 수법이 다양화되는 질적 변화를 보이고 있다. 무엇보다도 큰 변화는 일견 일탈적 해커 집단의 소행으로 보이는 사이버 공격의 배후에 러시아, 중국, 이란, 북한 등과 같은 국가 행위자들이 개입하면서 지정학적 갈등과 연계될 가능성이 높다는 사실이다. 이러한 국가지원 해킹에 대해서 미국 트럼프 행정부는 부당한 해킹공격에 대해서는 맞공격도 불사하겠다는 강경한 모습을 보이고 있다. 군사적 옵션의 사용까지도 거론하며 공세적인 경향을 보여 온 트럼프 행정부의 사이버 안보 전략은 '신냉전 시대'의 도래라는 프레임까지 동원하며 과장되기도 했다. 그러나 최근 트럼프 행정부가 전개하고 있는 사이버 안보 전략을 단순히 물리적 공세의 강화라는 맥락에서만 이해하는 것은 사이버 안보 문제의 고유한 성격과 이에 대응하는 전략의 복합성을 간과할 우려가 있다. 최근 사이버 안보 문제는 단순한 해킹공격의 문제를 넘어서 통상마찰, 데이터 안보, 심리전 등과 같은 다양한 국제정치의 이슈들과 연계되고 있으며, 일국전략 또는 양자관계의 차원을 넘어서 다자적인 국제규범 모색의 문제로까지 진화하고 있기 때문이다. 이러한 인식을 바탕으로 이 글은 '복합지정학(complex geopolitics)'의 시각에서 최근 사이버 안보 분야의 변화 양상을 살펴보고, 이에 대응하는 트럼프 행정부의 사이버 안보 전략과 그 의미를 개념화하였다.

주제어: 사이버 안보, 트럼프 행정부, 복합지정학, 국가지원 해킹, 국가전략

* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924409).

I. 머리말

최근 들어 사이버 안보는 명실상부하게 국제정치 분야의 의제로 자리매김했다. 특히 2013년을 기점으로 사이버 안보는 국제정치학자들뿐만 아니라 정치지도자들의 주요 관심사가 되었다. 이러한 과정에 사이버 공격의 최대 피해국임을 자처하는 미국의 행보가 큰 영향을 미쳤다. 오바마 행정부는 국가기간시설에 대한 해킹을 국가안보 문제로 '안보화'하고 때로는 미사일을 발사해서라도 대응하겠다는 '군사화'의 논리를 내세우며 사이버 안보를 국가 안보 전략의 핵심 항목으로 격상시켰다. 무엇보다도 2010년대 초반 미국이 우려한 사이버 공간의 안보위협은 중국의 국가적 지원을 받는 해커 집단들이 미국의 공공기관과 민간시설에 대해 사이버 공격을 가해서 입히는 피해였다. 사이버 안보 문제는 미중 두 강대국의 주요 현안이 되었으며, 결국 2013년 6월에는 미중 정상회담의 공식의제로 채택되는 상황에까지 이르렀다.

2017년 트럼프 행정부 출범 이후에도 사이버 공격은 양적으로 늘어났을 뿐만 아니라 그 목적과 수법도 다양화되었다. 사이버 공간의 복합 네트워크 환경을 배경으로 발생하는 사이버 공격은 주로 다양한 비국가 행위자들에 의해 감행되었지만, 그 배후에 국가 행위자가 개입하는 경우가 늘어나서, 이른바 '국가지원 해킹'이 꾸준히 증가하는 추세를 보이고 있다. 급기야 미국의 정보기관을 총괄하는 국가정보국(DNI)이 의회에 제출한 보고서 '2017년 세계위협평가'에서 러시아, 중국, 이란, 북한 등을 미국에 위협적인 사이버 공격을 가하는 네 나라로 명시하기까지 했다(Coats, 2017). 이는 국가지원 해킹문제가 글로벌 차원뿐만 아니라 유럽과 동아시아 및 중동의 지역갈등을 유발할 가능성이 있는 사례임을 보여준다.

이러한 국가지원 해킹의 증가는 트럼프 행정부로 하여금 국가 안보전략 전반의 차원에서 사이버 안보 문제를 고민케 하였다(White House, 2017). 트럼프 행정부의 대응은 부당한 해킹공격에 대해서는 맞공격도 불사하겠다는 강경한 모습을 보이고 있다. 군사적 옵션의 사용까지도 거론하며 공세적

인 경향을 보여 온 트럼프 행정부의 사이버 안보 전략은 '신냉전 시대'의 도래라는 프레임까지 동원하며 과장되기도 했다. 그러나 최근 트럼프 행정부가 전개하고 있는 사이버 안보 전략을 단순히 물리적 공세의 강화라는 맥락에서만 이해하는 것은 사이버 안보 문제의 고유한 성격과 이에 대응하는 전략의 복합성을 간과할 우려가 있다. 최근 사이버 안보 문제는 단순한 해킹공격의 문제를 넘어서 통상마찰, 데이터 안보, 심리전 등과 같은 다양한 국제정치의 이슈들과 연계되고 있으며, 일국전략 또는 양자관계의 차원을 넘어서 다자적인 국제규범 모색의 문제로까지 진화하고 있기 때문이다.

이러한 인식을 바탕으로 이 글은 최근 양적·질적 변화를 보이고 있는 사이버 위협에 대한 트럼프 행정부의 대응전략을 살펴보고자 한다. 특히 최근 발생하고 있는 변화의 국제정치학적 의미를 해석하고, 대응전략의 일반모델을 모색하는 데 있어 미국의 사례가 주는 의미를 검토하고자 한다. 사실 최근 국가 행위자들이 적극적으로 개입하면서 사이버 공격은 본격적인 국제정치 현상이 되었다. 사이버 방어를 명분으로 내세우는 측에서도 공세적인 전략수립과 새로운 부대창설 등을 통해 사이버전에 대한 태세를 강화하고 있다. 그러나 이러한 변화를 전통적인 현실주의 시각에서만 이해하려는 것은 잘못이다. 공세적인 전략의 이면에서 작동하는 '안보화 담론'의 역할에 주목하는 구성주의 시각이나 국제협력과 규범형성을 강조하는 자유주의 시각이 그려내는 현실도 엄연히 존재하기 때문이다. 실제로 최근 트럼프 행정부의 대응은 단순 공세의 지평을 넘어서는 복합전략의 양상을 보이고 있다는 것이 이 글의 주장이다.

이러한 맥락에서 이 글은 사이버 안보의 국제정치와 대응전략을 이해하는 분석틀로서 '복합지정학(complex geopolitics)'의 시각을 제안한다(김상배, 2015). 최근 (고전)지정학적 성격을 드러내고 있는 사이버 안보의 변화에 주목하는 이 글의 의도가 사이버 공간의 탈(脫)지정학적 성격을 무시하는 데 있지는 않다. 오히려 디지털 시대의 온라인 탈지정학에 아날로그 시대의 오프라인 (고전)지정학 시각을 21세기 국제정치학의 관점에서 엮어 보려는 데 있다. 복합지정학의 시각은 사이버 공간의 탈(脫)지정학적 특성, 사이버 공격과 방어에 임하는 국가 및 비국가 행위자의 (고전)지정학 및 비판지정학적

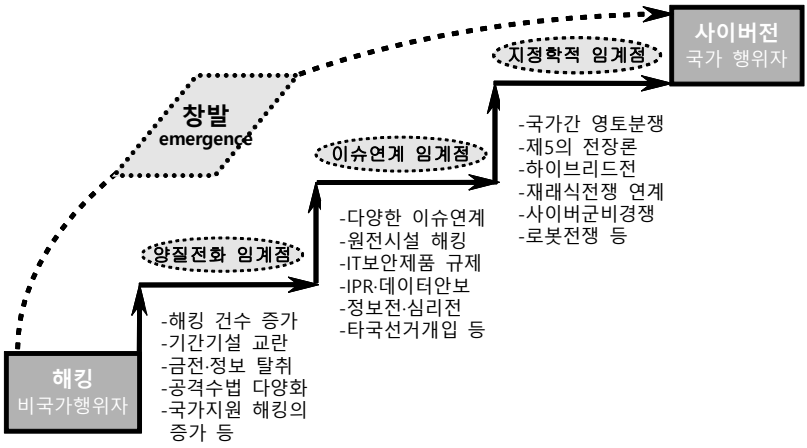
성격, 그리고 사이버 안보 문제를 풀어가는 세계정치의 비(非)지정학적 측면들을 복합적으로 고려할 것을 주장한다. 이런 점에서 복합지정학의 시각은 현실주의, 자유주의 및 구성주의 국제정치이론의 시각을 복합적으로 엮어내려는 새로운 국제정치이론의 시각과도 맥이 닿는다(김상배, 2018).

이 글은 크게 세 부분으로 구성되었다. 제2장은 최근 국가지원 해킹이 양적으로 증가하면서 질적으로 새로운 변화를 낳고 있는 사이버 공격의 (고전) 지정학적 메커니즘을 살펴보고, 이에 대한 대응전략의 모델을 이해하는 분석틀로서 복합지정학의 시각을 제시하였다. 제3장은 최근 러시아와 중국, 이란, 북한 등이 감행하고 있는 국가지원 해킹의 최근 양상을 이에 대한 미국의 인식과 탐지 및 대응에 초점을 맞추어 검토하였다. 제4장은 복합지정학적인 양상을 보이며 진행되고 있는 트럼프 행정부의 사이버 안보 전략을 사이버 안보 컨트롤타워의 변화, 행정명령과 '국가사이버전략'의 발표, 실무부처 차원의 대응, 상하원의 사이버 억지 및 대응 법안 통과 등의 사례를 통해서 살펴보았다. 끝으로, 맺음말에서는 이 글의 주장을 종합·요약하고 트럼프 행정부가 추진하는 사이버 안보 전략의 전개가 한국의 사이버 안보 전략에 던지는 의미를 간략히 살펴보았다.

II. 사이버 공격과 방어의 복합지정학

1. 국가지원 해킹의 지정학적 창발

초창기에는 해커들의 장난거리나 테러리스트들의 도발로 여겨지던 사이버 공격이 최근 들어 국가 행위자들이 직간접적으로 개입하면서 새로운 양상을 드러내고 있다. 물론 사이버 공격의 문제를 너무 전통적인 국가안보의 시각으로만 봐서는 곤란하다. 기본적으로 사이버 공격은 국가 행위자들이 주도하기보다는 비국가 행위자들이 중요한 역할을 하는 게임이기 때문이다. 그럼에도 최근의 양상을 보면 러시아, 중국, 이란, 북한 등과 같은 국가 행위자들이



〈그림 1〉 사이버 공격의 지정학적 창발

점차로 사이버 공격의 전면에 나서고 있다. 다시 말해, 사이버 공격이 양적·질적 변화를 겪는 과정에서 국제정치적 성격이 점차로 더 많이 가미되고 있다. 사실 사이버 안보는 미시적 안전(安全, safety)의 문제가 거시적 안보(安保, security) 문제가 되는 '신흥안보(新興安保, emerging security)'의 대표적 사례이다. 〈그림 1〉에서 보는 바와 같이, 비국가 행위자들의 해킹에서 시작된 사이버 위협이 창발(創發, emergence)의 메커니즘을 따라서 국가 행위자들 간의 사이버전을 우려케 하는 지정학적 이슈가 되고 있다(김상배, 2018: 39-42).

첫째, 사이버 안보 문제는 양적증대가 질적 변화를 야기하는 '양질전화(量質轉化)'의 성격을 갖는다. 최근 사이버 공격의 건수는 매년 가파르게 증가하고 있으며, 그 목적도 국가 기간시설의 교란에서부터 금전취득을 위한 해킹, 개인·기업 정보의 탈취, 심리적 선동과 교란 등에 이르기까지 다변화되고 있다. 공격 수법이라는 측면에서도 봇넷 공격, 악성코드 침투, 랜섬웨어 유포, 인공지능 활용 등으로 다양화되고 있다. 무엇보다도 큰 변화는 겉으로 보기에 이러한 사이버 공격은 비국가 행위자인 해커 집단의 소행으로 보이지만, 그 이면에는 러시아, 중국, 이란, 북한 등과 같은 국가 행위자의 그림자가 점점 더 짙게 드리워지고 있다는 사실이다. 악성코드 탐지 전문 업체 옵

스왓은 2017년 '글로벌 사이버 보안 위협 트렌드 6선'을 발표했는데, 그 중에서 1순위 위협으로 '국가 지원을 받는 해킹의 증가'를 꼽은 바 있다(디지털타임스, 2017/12/13).

둘째, 사이버 안보 문제는 미시적인 안전의 문제로 시작하지만 다양한 '이슈연계'의 과정을 거쳐서 거시적 안보의 문제로 비화될 가능성이 매우 큰 사례이다. 최근 사이버 공격이 원자력 시설을 포함한 주요 국가시설을 겨냥하여 민감한 국가안보의 사안으로 비화되거나, 또는 경제적 가치가 높은 산업기밀과 지적재산의 도용과 연관되어 국가적 차원의 경제안보를 위협하는 문제가 되었다. 최근 미국과 중국, 그리고 러시아 등 강대국들이 사이버 안보와 관련된 IT 보안 제품의 수출입과 이 분야의 다국적 기업들에 대한 규제를 강화하는 시도를 벌이면서 사이버 안보와 통상 이슈가 연계되는 현상도 발생하고 있다. 게다가 이러한 사이버 안보 관련 통상문제는 데이터 안보의 연계되기도 하며, 더 나아가 사이버 안보 문제는 타국의 선거개입 등과 관련된 정보전 또는 심리전 문제와도 연계되면서 이슈연계의 위험성이 증폭되고 있다.

끝으로, 양질전화나 이슈연계의 임계점을 넘어선 사이버 안보 문제는 전통안보와 관련된 국가 간 갈등을 야기하는 지정학적 이슈가 된다. 실제로 최근 사이버 공격이 지정학적 이슈와 연계되는 사례가 부쩍 많이 발생하고 있는데, 2007년 에스토니아, 2008년 조지아, 2014년 우크라이나 등에 대한 러시아의 사이버 공격, 그리고 2010~12년 미국/이스라엘과 이란의 사이버 공방을 대표적인 사례로 들 수 있다. 최근에는 각국이 사이버 공간을 새로운 전쟁공간으로서 육·해·공·우주를 넘어서는 '제5의 전장'으로 인식하면서 사이버 안보의 지정학적 연계 가능성이 더욱 커지고 있다. 게다가 사이버 안보는 재래식 또는 핵전쟁뿐만 아니라 미래전쟁 문제와 연계되고 있는데, 최근에는 4차 산업혁명의 진전과 더불어 인공지능, 로봇, 드론, 우주무기 등과 연계될 가능성이 높아지고 있다. 이렇게 지정학적으로 연계되는 사이버 공격에 대응하기 위해서 주요국들은 사이버 군대를 신설하거나 확대 및 격상하는 조치를 취하고 있다.

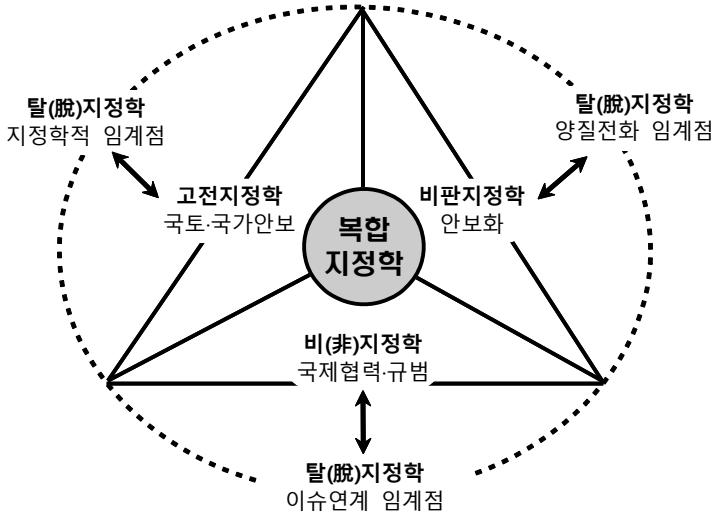
이러한 관점에서 보면 신흥안보로서 사이버 안보 문제는 전통안보와 구별되는 새로운 안보 이슈라기보다는, 오히려 그 개념적 경계 안에 전통안보의

문제도 포함하는 이슈라고 할 수 있다. 그러나 사이버 공격을 단순히 전통안보론에서 상정하는 바와 같은 '지정학적 전쟁'이라고 규정하기는 어렵다. 사이버 전쟁 자체를 별도의 전쟁 유형으로 다룰 것인가의 문제에서부터 논란의 여지가 많다. 사실 전통적인 의미의 국가 간 전쟁의 연속선상에서 규정하기에는 최근 발생하고 있는 사이버 공격의 형태가 매우 다양한데다가 관여하는 주체의 성격도 복잡하다. 사이버 전쟁이라고 부르기에는 다소 애매하고, 경우에 따라서는 사이버 테러나 사이버 간첩, 사이버 교란, 사이버 범죄 등으로 부르는 것이 더 적합한 경우도 있다. 요컨대, 최근 사이버 공격의 게임이 지정학적 성격을 띠면서 창발하는 것은 맞지만, 이를 제대로 이해하기 위해서는 좀 더 복합적인 인식의 틀이 필요한 것이 사실이다.

2. 사이버 안보의 복합지정학적 대응

기본적으로 사이버 안보는 전통적인 국가안보의 지정학 시각을 넘어서 이해해야 하는 문제이다. 최근 양질전화의 양상을 보이고 있는 사이버 안보 게임은 인터넷과 컴퓨터 바이러스, 악성코드 등과 같은 기술 변수와 해커나 테러리스트 등과 같은 비국가 행위자들의 활동을 기본적인 특징으로 한다. 이러한 게임은 정보통신의 물리적 인프라와 기술, 정보, 지식, 문화 등의 변수가 복합되어 만들어내는 사이버 공간을 배경으로 벌어진다. 이러한 사이버 공간은 정보통신의 복합 네트워크가 만들어내는 '흐름으로서의 공간(space as flows)' 또는 탈지정학적 공간이다(Castells, 2000). 이러한 탈지정학적 사이버 공간을 배경으로 발생하는 국제정치 현상으로서의 사이버 안보 게임을 이해하기 위해서는, 현실주의 시각에서 본 고전지정학, 자유주의 시각에서 본 비(非)지정학, 구성주의 시각에서 본 비판지정학을 원용한 복합지정학의 시각이 필요하다는 것이 이 글의 인식이다(〈그림 2〉 참조).

첫째, 앞서 설명한 바와 같이 '지정학적 임계점'의 문턱에까지 다다른 사이버 공격의 양상은 영토적 발상을 기반으로 하는 고전지정학의 시각으로 이해해야 하는 특징을 보인다. 고전지정학은 권력의 원천을 자원의 분포와 접근



〈그림 2〉 사이버 안보의 복합지정학

성이라는 물질적 또는 지리적 요소로 이해하고 이를 확보하기 위한 경쟁이라는 차원에서 국가전략에 접근한다(지상현 · 플린트, 2009; Mead, 2014). 이는 물질적 권력의 지표를 활용하여 국가 행위자 간의 패권경쟁과 세력전이를 설명하는 현실주의 국제정치이론의 인식과 통한다(Gilpin, 1981; Organski and Kugler, 1980). 고전지정학의 시각에서 본 사이버 안보 전략의 핵심은 기술과 인력의 역량개발을 통해서 영토와 자원 확보의 경쟁에서 우위를 점하는 것이다. 이를 위해 국가 행위자가 나서 사이버 공격을 감행하는 기술적 · 군사적 능력을 개발하고, 역으로 국가지원 사이버 공격을 방어 또는 억지하기 위한 능력배양과 이를 수행할 부대와 사령부 등을 설치한다. 최근 주요국들이 공세적인 사이버전 태세를 갖추는 추세는 이러한 시각을 바탕으로 한다.

둘째, 사이버 공격이 지정학적 임계점을 넘기 전에는 국가안보로 이해되기 어렵지만 그 이전에라도 '양질전화 임계점'의 문턱에 접근하는 과정에서 안보화(securitization) 담론 생성의 비판지정학이 작동한다. 비판지정학은 특정한 발언이나 재현이 영향력을 갖게 되는 담론적 실천으로 지정학을 이해한다. 지정학적 지식이 어떤 특정 정치집단에 의해 이용되고 생산되고 왜곡되는지와 관련된 권력과정의 분석이 주관심사이다(Ó Tuathail and Agnew, 1992;

Ó Tuathail, 1996; Dodds, 2001; Kelly, 2006). 이런 점에서 비판지정학은 구성주의 국제정치이론과 맥이 닿는다. 사이버 안보는 객관적으로 '실재하는 위험' 만큼이나 위험을 주관적으로 '구성하는 과정', 즉 국제안보 연구의 코펜하겐 학파에서 말하는 '안보화'가 중요한 게임이다(Hansen and Nissenbaum, 2009). 최근 사이버 안보 분야에서는 미국과 중국의 안보담론 경쟁이 벌어지고 있다. 사이버 위협의 성격이 무엇이고, 안보의 대상과 주체가 무엇인지, 그리고 사이버 안보 관련 양국의 국내체제와 세계질서의 미래에 대한 담론경쟁이 진행되고 있다.

셋째, 사이버 안보는 영토국가의 공간에 기반을 둔 갈등의 발상을 넘어서 글로벌 공간에서의 협력의 발상으로 풀어야 하는 문제이다. 이러한 시각은 영토의 발상을 넘어선다는 의미에서 '비(非)지정학'이라고 할 수 있으며, 국가영토의 경계를 넘어서는 흐름의 증대에 주목하는 '상호의존'과 글로벌 거버넌스의 논의와 일맥상통하며, 국제협력과 규범형성을 강조하는 자유주의 국제정치이론의 시각과 맥이 닿는다(Ikenberry, 2014). 사이버 안보는 지정학적 공간에 고착된 일국적 시각을 넘어서 글로벌 차원에서 이해당사자들의 긴밀한 협력을 통해서 초국적 해법을 모색해야 하는 문제이다(Mueller, 2002, 2010). 최근 사이버 안보 문제가 다양한 차원에서 '이슈연계 임계점'을 넘나들고 있는 상황은 이러한 비지정학적 인식을 강화한다. 사이버 안보 문제에 대한 대응방안을 모색하는 데 있어서 양자 간의 합의와 협력이라는 지정학 구도를 넘어서는 글로벌 차원의 다자구도 형성이 필요하다. 실제로 최근 사이버 안보의 국제규범 형성과정에서 서방 진영과 비서방 진영의 경쟁과 협력의 구도가 형성되고 있다.

요컨대, 사이버 안보 문제는 전통적인 의미의 국민국가들이 벌이는 (고전)지정학적 게임이라는 관점만으로는 이해할 수 없다. 탈지정학적 공간으로서 사이버 공간의 부상은 테러 네트워크나 범죄자 집단들에 의해 도발될 '비대칭 전쟁'의 효과성을 크게 높여 놓았다. 그러나 탈지정학의 공간으로서 사이버 공간을 강조하려는 것이 기존에 영토의 발상으로 보는 (고전)지정학의 시각을 폐기하는 데 있지는 않다. 사이버 안보의 세계정치는 국가 및 비국가 행위자 그리고 경우에 따라서는 네트워크 환경과 기술 시스템이라는 변수들

까지도 적극적으로 관여하는 복합지정학의 게임으로서 이해해야 할 것이다. 이러한 과정에서 국가 행위자는 사이버 공격이라는 위협 요인을 제공하는 주체인 동시에 초국적으로, 또는 국가 간에 발생하는 사이버 위협을 방지하는 방어의 메커니즘을 만드는 주체로서 그 입지를 세워가고 있다. 최근 트럼프 행정부가 추진하고 있는 사이버 안보 전략은 이러한 복합지정학의 양상을 보여준다.

III. 국가지원 해킹의 최근 양상과 대응

1. 러시아발 사이버 공격의 양상과 대응

최근 국가지원 해킹의 주범으로 큰 주목을 끌고 있는 나라는 러시아이다. 최근의 사례로 러시아는 2014년 3월 크림 반도를 점령하는 과정에서 우크라이나에 대한 사이버 공격을 감행했다. 당시 러시아는 사이버 전력을 재래식 전력과 효과적으로 배합하는 하이브리드전(hybrid warfare)을 수행했는데, 2007년 에스토니아 사태나 2008년 조지아 사태와는 달리 국제사회의 비난을 피하려는 속내가 작용했다고 알려졌다. 2015년 12월과 2016년 초 우크라이나는 대규모 정전 사태를 겪었는데, 이는 샌드웜(Sandworm)이라는 러시아 지원 해커 그룹이 감행한 것으로 알려졌다. 2017년 6월에도 우크라이나는 러시아로 의심되는 세력의 낫페트야(NotPetya) 사이버 공격을 받았는데, 정부기관을 비롯해 금융·전력·통신·교통 등 수많은 기반시설이 운용에 차질을 빚거나 가동이 중단됐다(보안뉴스, 2018/01/03).

이외에도 러시아는 국경 인접 지역에 대해 사이버 공격을 가해 인접국의 의지를 시험하는 한편, 가짜뉴스 공작을 통해 이들 국가들의 내부 분란을 유도해왔다. 실제로 미국과 프랑스, 독일 등은 러시아가 선거에 개입했다고 비난하고 있다. 특히 러시아는 2016년 미국 대선에서 나토와 유럽연합 해체를 옹호한 트럼프 후보를 지원하기 위해 해킹을 감행한 의혹을 샀다. 실제로 당

시 미 민주당 진영을 상대로 가해진 사이버 공격이 러시아 해커 집단인 팬시 베어(Fancy Bear)에 의해 감행된 것으로 알려졌다. 민주당 경선이 한창이던 2016년 6월 경선을 관리하는 민주당 전국위원회와 민주당 지도부, 힐러리 대선캠프 측 인사 100여 명의 이메일이 팬시 베어에 의해 유출되어 공개되었다(매일경제, 2017/04/12).

시리아 내전을 둘러싼 미국과 러시아의 갈등이 고조되면서 사이버전의 가능성이 우려되기도 했다. 이러한 와중에 2017년 4월 미국을 포함한 핀란드, 스웨덴, 프랑스, 독일, 영국, 폴란드, 라트비아, 리투아니아 등 9개국은 러시아의 사이버 공작에 대응하는 차원에서 '유럽 하이브리드 위협 대응센터'를 발족하기로 합의했으며, 실제로 이 센터는 2017년 10월 핀란드 헬싱키에 설립되었다. 한편 2018년 들어 시리아 내전 사태가 미국을 중심으로 한 서방 진영과 러시아·중국·이란 간의 대리전 양상을 보이는 가운데 사이버 공간에서도 대결의 기운이 고조되었다. 2018년 4월 미국은 영국·프랑스와 함께 시리아의 화학무기 관련 시설에 대한 공습을 단행했는데, 이에 러시아가 미국과 영국을 겨냥해 사이버전을 개시했다는 분석과 경고가 이례적으로 미국과 영국 당국에 의해서 동시에 발표되기도 했다(디지털타임스, 2018/04/17).

러시아의 사이버 공격은 최근에는 동북아 지역에서도 논란거리가 되었다. 예를 들어, 2018년 2월 평창 동계올림픽 개막 즈음에 러시아의 지원을 받는 것으로 추정되는 정체불명의 해커 집단이 올림픽조직위원회 및 국제올림픽위원회(IOC) 소속 서버를 대상으로 해킹 공격을 감행했다. 이들 러시아 해커들의 공격은 국제올림픽위원회가 러시아 선수들이 금지 약물을 복용한 사건에 대해 이를 징계하여 평창올림픽에서 국가 참가자격을 박탈한 데 대한 보복으로 추정되었다. 미 정보기관들에 따르면, 평창 올림픽 개막식을 공격한 해커들은 러시아군 총정보국(GRU) 내 중앙특수기술센터(GTsST) 소속으로 추정되었는데, 이들은 2017년 6월 우크라이나에서 발생한 낫페트야 사이버 공격의 배후로도 지목되는 사이버 부대라는 것이었다(중앙일보, 2018/02/25).

이들 러시아 해커 집단은 팬시베어라는 이름 이외에도 소파시(Sofacy), APT28, 스트론티움(Strontium), 세드닛(Sednit), 차르팀(Tsar Team), 폰스

톰(Pawn Storm) 등으로도 불리며, 러시아 정부의 후원을 받고 있는 국가지원 해커라고 할 수 있다. 러시아 보안업체인 카스퍼스키(Kaspersky)에 의하면, 이들 러시아 해커 집단은 그 동안 나토 회원국들과 우크라이나를 집중적으로 공격했었는데 최근 그들의 활동영역을 중동 및 중앙아시아로부터 동아시아 국가들로 넓히고 있다고 한다. 카스퍼스키의 수석 보안 전문가인 커트 바움가트너(Kurt Baumgartner)에 의하면, "2017년 한 해 동안 이 고차원의 해커 집단(소파시)은 표적을 점진적으로 확장"시켰는데, "나토 국가 및 우크라이나에서 처음에는 중동 쪽도 건드리기 시작"했으며, "그리고는 중앙아시아를 지나 계속해서 동쪽으로 공격 범위를 확대"하고 있다고 분석했다(보안뉴스, 2018/02/21).

2. 중국발 사이버 공격의 양상과 대응

미국의 입장에서 더욱 논란거리가 된 것은 중국발 사이버 공격의 양적·질적 변화이다. 2015년 9월 미국과 중국은 민간시설과 지적재산에 대한 사이버 공격을 금지하는 데 합의한 바 있다. 카스퍼스키에 의하면, 이 시점부터 미국과 영국을 겨냥한 중국발 사이버 공격이 급격하게 줄어들었다고 한다. 그러나 중국발 해킹 공격 자체가 완전히 사라진 것은 아니었는데, 미국 보안업체인 파이어아이(FireEye)는, 중국을 기반으로 하는 해커 집단이 2015년 말부터 2016년까지 중국 주변 국가들의 정부기관과 군사조직들을 지속적으로 공격했으며 그 공격은 점점 더 조직화되었다고 분석했다. 특히 중국의 해커 집단은 한국과 러시아, 베트남 등을 공격하거나, 영유권 분쟁을 벌이는 남중국해 국가들을 공격 대상으로 삼았다고 분석했다(연합뉴스 2016/06/21).

2018년 들어서는 남중국해를 둘러싸고 미국과 중국의 갈등이 고조되면서 중국 해커들이 남중국해와 관련된 엔지니어링·방위산업 업체들을 공격하기 시작했다. 이러한 사이버 공격을 감행한 것으로 의심되는 해커 집단은 템프.페리스코프(TEMP.Periscope)로 알려졌다. 파이어아이의 선임 애널리스트인 프레드 플랜(Fred Plan)은 "해커들은 남중국해와 연관이 있는 미국 해상 기

업들이나 그들과 거래 관계를 맺고 있는 업체들을 타깃으로 삼고 있다"면서, "미국과 중국은 지난 2015년 상대방 민간 업체를 공격하지 않기로 합의했지만 최근 들어 중국의 공격이 다시 늘고 있다"고 말했다(뉴시스, 2018/03/16). 2018년 초 인도의 티베트인 공동체와 미국 알래스카 주 정부를 목표로 한 사이버 공격의 진원지로 중국 칭화대 소속 해커들이 지목되기도 했다(연합뉴스, 2018/10/04).

2018년 1~2월에는 중국의 국가지원 해커들이 해군 수중전센터와 계약한 업체의 컴퓨터를 해킹하여, 2020년까지 운용하는 초음속 대함 미사일과 수중전에 대한 세부 정보계획을 포함한 614GB가량의 매우 민감한 데이터를 훔쳤다. 도난당한 데이터에는 신호 및 센서 데이터와 관련된 씨드래곤(Sea Dragon)으로 알려진 프로젝트, 암호화 시스템과 관련된 잠수함 통신실 정보, 해군 잠수함 개발팀의 전자전 라이브러리와 관련된 자료가 포함되어 있었다. 미 정보기관과 해군 당국은 중국 국가안전부가 이 해킹 작전을 벌였다고 주장하였다(IT World, 2018/06/14; 한국일보, 2018/06/25). 이와 관련하여 미국 보안업체 시만텍도, 2018년 들어 쓰립(Thrip, 삽주벌레)으로 불리는 중국 해커 집단이 인공위성과 통신, 방위산업체에 대한 공격을 감행하고 있다고 발표하였다(연합뉴스, 2018/06/20).

중국의 사이버 공격은 미국 이외에도 일본, 한국, 대만, 캄보디아 등을 대상으로 다변화되었다. 2018년 4월 파이어아이는 중국의 해커 집단인 APT10이 북핵문제와 관련한 일본 정부의 정책 정보를 입수할 목적으로 일본 방위산업체들을 해킹했다고 발표했다(조선일보, 2018/04/23). 이러한 중국의 해킹 공격은 한국에도 가해졌는데, 2018년 5월초에는 아시아·태평양 지역 공기업과 민간 기업을 담당하는 중국의 사이버 첩보 조직인 템프.틱(TEMP.Tick)이 한국 조직을 공격 대상으로 삼은 바 있었다(노컷뉴스, 2018/06/07). 한편, 대만도 독립파인 차이잉원(蔡英文) 총통 집권 이후 중국의 사이버 공격에 시달리는 것으로 알려졌다(연합뉴스, 2018/06/25). 마찬가지로 중국 해커들은 2018년 7월 총선을 앞둔 캄보디아를 대상으로 해킹 공격을 가한 것으로도 알려졌다(연합뉴스, 2018/07/16). 이외 국가들에 대한 해킹과 관련하여, 파이어아이는 중국의 해커 그룹이 '일대일로(一帶一路)' 정책의 관련 국

가들을 대상으로 전방위적인 사이버 공격을 감행하고 있다고 밝혔다(KINEWS, 2018/09/01).

2018년 10월 블룸버그 비즈니스위크는 중국이 애플, 아마존 등 30개 미국 주요 기업과 정부기관 IT기기에 스파이 칩을 심어 감시했다고 보도하여 논란이 일었다. 중국 서버 제조업체인 '슈퍼마이크로(Supermicro)'는 쌀알 크기의 칩을 마더보드에 심어 애플 등 주요 기업에 납품했다는 것이었다. 슈퍼마이크로의 고객사 중 하나인 엘리멘탈의 서버는 미 국방부 데이터센터와 중앙정보국(CIA) 드론 작전, 해군 함선 간 네트워크에 사용된다. 블룸버그는 이같이 하드웨어를 통한 해킹은 소프트웨어를 통한 해킹보다 발견하기가 어렵고 더 큰 피해를 입힌다고 지적했다. 미 정부는 2015년부터 이와 관련 비밀리에 조사를 시작했다. 하지만 애플은 이와 같은 보도에 대해 부인했다(연합뉴스, 2018/10/05).

3. 이란발 사이버 공격의 양상과 대응

2010년 미국과 이스라엘은 스턱스넷을 사용해 이란 나탄즈 우라늄 농축시설에서 사용되는 독일 지멘스 산업제어시스템을 집중 공격하여 원심분리기의 가동을 방해함으로써 이란의 핵무기 개발을 지연시킨 것으로 알려져 있다. 그 무렵 미국은 이란 핵합의에 실패할 경우 이란의 핵시설과 전력공급체계, 통신망 등을 일제히 마비시키는 사이버 공격을 계획했던 것으로 드러났다. 오바마 대통령은 존 앨런 당시 미 중부사령관에게 외교적 노력이 실패할 경우를 상정한 군사계획을 마련하라고 지시했다. 이란의 핵시설과 주요 사회기반시설을 마비시키는 내용의 사이버 작전계획, '니트로 제우스'는 북한의 한국 공격 등에 대비한 위기대응계획보다 더 긴박하게 다뤄졌다고 보도되었다(국민일보, 2016/02/17).

이란도 미국과 걸프만 국가들에 대해 여러 차례에 걸쳐서 사이버 공격을 감행한 것으로 알려져 있다. 이란 정부와 연계된 해커들은 2012년 1월 미국 은행들을 상대로 대대적인 서비스 거부 공격을 가했다. 이들은 또 2012년 7

월 사우디아라비아 석유회사의 전산망에 '샤문' 바이러스를 퍼뜨려 컴퓨터 3만 대의 데이터를 파괴했고, 8월에는 카타르 천연가스 업체인 라스가스를 공격해 웹사이트와 이메일 시스템을 무력화했다. 2012년 9월에는 뱅크오브아메리카, JP모건체이스, PNC 파이낸셜 서비시스, 웰스파고 등 미국 주요 은행의 고객들이 온라인상으로 계좌 접근을 거부당하는 공격을 받았다. 이란이 사이버 공격을 감행한 것은 미국의 경제제재와 스턱스넷 공격에 대한 보복 차원으로 알려져 있다(보안뉴스, 2012/10/15).

미 당국자들은 이란 정부의 지원을 받은 해커들이 사이버 간첩, 선전 행위를 계속하고 있으며, 자국 안보를 지키고 특정 사건이나 대외인식에 영향을 주거나 역내 미국 동맹 등 자국에 대한 위협에 대응하기 위해 사이버 공격을 가했다고 주장했다. 예를 들어, 2013년에는 이란 해커가 미국 댐 산업제어시스템에 침입했고, 2014년 2월에는 미국에 기반을 둔 카지노 기업인 '라스베이거스 샌즈'의 컴퓨터 시스템을 마비시킨 사이버 공격을 가한 바 있다(MK뉴스, 2017/05/16). 뉴스캐스터(Newscaster), 뉴스비프(NewsBeef)라고도 알려져 있는 이란의 사이버전 단체인 차밍 키튼(Charming Kitten) 소속 해커들이 '왕좌의 게임'으로 유명한 미국의 방송사인 HBO를 해킹한 후 미(未)방영 에피소드를 유출하겠다고 협박한 사건이 발생하기도 했다(보안뉴스, 2017/12/07).

한편 파이어아이에 따르면, 2016년 중순부터 2017년 초까지 이란의 APT33은 미국의 항공업계를 공격했으며, 이 중에서 사우디아라비아의 항공기업과 연관된 업체를 집중적으로 공격했다. 이와 동시에 한국의 정유 및 석유화학기업도 목표로 삼아 공격했는데, 2017년 5월부터는 사우디아라비아의 석유화학기업과 연관된 한국의 기업들을 공격했다(월간조선, 2017/11). 이란 해커들이 미국 등 전 세계 300개 이상의 대학 전산망을 해킹해 대학교수는 물론 학생과 교직원들의 도서관 계정 등을 수집했다가 적발되기도 했다. 2018년 3월 미국 법무부는 사상 최대의 해킹 단속 캠페인 가운데 하나에 연루된 이란의 해킹 네트워크를 적발해 이슬람혁명수비대(IRGC) 관련 해커 9명을 기소하고 제재를 가했다. 이들은 이란에 본사를 둔 민간회사 마브나인스티튜트(Mabna Institute)와 연계됐다고 알려졌다(연합뉴스, 2018/03/27).

이란과 미국의 갈등이 2015년 핵 협상이후 잠잠해졌을 때 이란의 사이버 공격도 그 빈도가 낮아졌다. 그런데 2018년 5월 미국 트럼프 대통령이 이란 핵협정을 탈퇴하겠다고 발표한 이후 이란 해커들의 사이버 테러 위험이 눈에 띄는 변화가 있었다고 미국의 보안업체 크라우드스트라이크(CrowdStrike)가 밝혔다. 이란 해커들은 미국 동맹국, 외교관들에게 악성 코드가 포함된 이메일을 전송했다. 이란 해커들은 지난 몇 년 동안보다 정교한 디지털 무기를 보유하고 해킹에 나서고 있다고 알려졌다. 핵협정 체결 이래로 이란의 중동 주변 국가들이 해커들의 목표가 됐지만, 이제는 미국 비즈니스와 사회 생산 기반에 대해 전방위적으로 사이버 공격을 실행할 가능성이 있다는 것이었다(전자신문, 2018/05/14).

4. 북한발 사이버 공격의 양상과 대응

2010년대 초중반 북한은 한국의 국가 기간시설과 언론사 등을 상대로 여러 차례에 걸쳐서 사이버 공격을 가한 것으로 알려져 있다. 한반도 밖에서도 북한은 2014년 11월 소니 해킹을 감행하여 북미 간에 긴장이 감돌았다. 미국은 북한의 소니 해킹을 자국의 국가안보에 대한 중요한 도전으로 간주하고 강경한 반응을 보였다. 2016년 2월에는 북한의 소행일 것으로 추정되는 방글라데시 중앙은행의 SWIFT 시스템 해킹이 발생했다. 이후에도 국제사회의 대북제재가 한층 강화되면서 돈줄이 막힌 북한이 7천여 명으로 구성된 해커 부대를 앞세운 대대적인 외화벌이 작전에 나섰고, 북한 해커들은 2017년 12월 국내 비트코인 거래소 유빗을 해킹해 파산시키기도 했다. 또한 북한은 한국의 국방망과 국내 방위산업체 등을 해킹해 해군 이지스함과 잠수함, 공군 F-15 전투기의 취약점을 파악할 수 있는 설계도면과 관련 핵심 자료들을 훔쳐갔다고 알려졌다(중앙일보, 2018/04/06).

2017년 5월 들어 논란을 일으킨 해킹 사건은 라자루스로 알려진 해커 집단의 워너크라이(WannaCry) 랜섬웨어 공격인데, 이는 단숨에 전 세계 150여 개국 30만 대 이상의 컴퓨터를 감염시켜 큰 피해를 입혔다. 라자루스는

2014년 소니 해킹 사건과 2016년 방글라데시 중앙은행 SWIFT 시스템 해킹 사건의 배후로도 지목된 해커 집단이다(연합뉴스, 2017/06/16). 이러한 해킹 사건의 진전과 관련하여 2017년 12월에는 이례적으로 미국 정부의 당국자가 직접 나서서 워너크라이 사이버 공격의 배후로 북한을 공식 지목하기도 했다(연합뉴스, 2017/12/20). 이와 유사한 맥락에서 미국의 커스텐 닐슨(Kirstjen Nielsen) 국토안보부 장관도 2018년 7월 뉴욕에서 열린 전국사이버안보회의에서 워너크라이 랜섬웨어 공격이 북한의 소행이라고 밝혔다(Radio Free Asia, 2018/07/31).

파이어아이는 2018년 2월 발표한 보고서에서 북한이 한반도 밖으로 사이버 공격을 확대하고 있는데 "핵·미사일 프로그램 개발로 제재에 묶인 북한 정권이 돈줄을 찾기 위해 해킹 작전을 강화했다"고 밝혔다. 파이어아이는 이들 집단이 "북한에 기반을 두고 있고 북한의 이익에 부합하는 타깃을 목표로 선택한다"고 설명했다. 파이어아이는, 리퍼(Reaper)라고 명명한 이 집단에 대해서 APT37이라는 식별표를 달기도 했다. 리퍼는 2012년부터 활동을 시작했는데, 초기에는 한국 정부, 군, 국방 시설, 미디어 부문 공격에 집중했으며, 이어 일본과 베트남, 중동을 포함해 활동 범위를 넓혔고, 화학 물질에서 통신에 이르기까지 분야도 확대했다는 게 파이어아이의 설명이었다(뉴스1, 2018/02/22).

2018년 4~5월에는 북한이 한미 및 북중 정상회담 등 파격적인 외교 행보를 보이는 가운데, 지나 해스펠(Gina Haspel) 미국 중앙정보국(CIA) 국장 내정자는 북한이 사이버 프로그램을 통해 국가기밀을 훔치고 불법적인 금전을 벌어들이고 있다고 밝혔다(뉴스핌, 2018/05/10). 2018년 6월초에는 북미 정상회담을 앞두고 중국 및 러시아와 연계된 해커 집단의 사이버 공격 시도가 증가하고 있다고 파이어아이가 밝히기도 했다(노컷뉴스, 2018/06/07). 2018년 6월 북미 정상회담 직후에도 북한의 악의적인 사이버 활동을 미 국토안보부는 경고했는데, 북한이 컴퓨터를 사용하지 못하게 만들거나 컴퓨터 시스템을 손상시키는 트로이 목마 변종 악성코드를 사용했다는 것이었다(VOA뉴스, 2018/06/07).

한편 2010년 초중반 북한에 대한 미국의 사이버 공격도 진행되었음에 주

목할 필요가 있다. 오바마 대통령이 재임 중이던 2014년 북한의 핵·미사일 발사에 사이버전으로 대응하는 방안을 세웠다고 알려져 있다. 오바마 행정부가 2013년 2월 북한의 3차 핵실험 후, 북한의 미사일 발사를 무력화시키는 목적으로 '발사의 왼편(Left of Launch)'이라는 이름의 사이버전 작전을 세웠다는 것이다(조선일보, 2017/03/05). 실제로 '발사의 왼편' 도입 이후 북한 미사일이 발사 직후 폭발하거나, 궤도를 이탈하는 등의 실패 확률이 이례적으로 높아졌다. 이에 대해 영국의 일간지 더타임스(The Times)는 "실패한 북한의 미사일 발사 가운데 일부는 성능 결함 때문이지만 다른 일부는 미 국방부가 첨단 컴퓨터 바이러스를 이용해 발사를 교란시킨 탓으로 보인다"고 보도했다(조선일보, 2017/04/18에서 재인용).

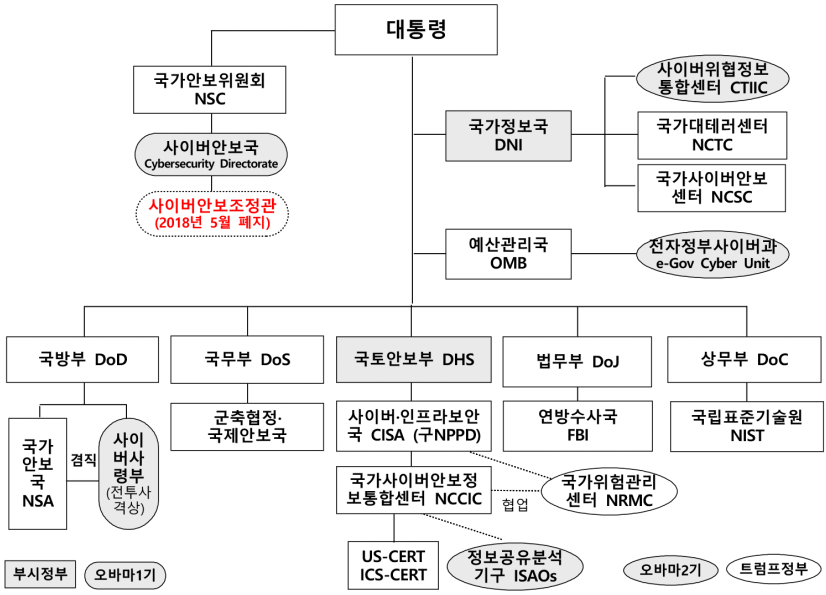
요컨대, 최근 사이버 공격은 그 숫자가 양적으로 증가하고 있을 뿐만 아니라 이를 바탕으로 그 질적인 성격도 변화하고 있다. 특히 사이버 공격의 목적과 수법이라는 점에서 시스템 교란, 금전 및 지적재산 탈취, 정책정보 수집, 군사적 목적 등에 이르기까지 다양해지고 있다. 이렇게 변화하는 사이버 공격의 배후에는, 해당 국가들이 부인하고 있음에도, 러시아, 중국, 이란, 북한 등과 같은 국가 행위자의 그림자가 드리워져 있다. 비국가 행위자들의 비체계적인 해킹이 국가의 지원을 받아 조직화되는 경향을 보이고 있다. 게다가 이러한 국가지원 해킹의 양적 증가는 여타 이슈와 연계되면서 사이버 안보 문제를 세계정치의 현안으로 인식케 하고 있다. 이러한 상황은 자칫 지정학적 임계점을 넘어서 미러 및 미중 등 강대국들의 군사적 충돌을 유발할 가능성을 예견하면서 군사적 긴장을 고조시킬 가능성도 안고 있다. 사이버 안보가 미국 트럼프 행정부의 공세적인 대응의 관심사로 부상하는 것은 바로 이러한 맥락이다.

IV. 트럼프 행정부의 사이버 안보 전략

1. 사이버 안보 컨트롤타워의 변화

미국의 사이버 안보 추진체계는 기본적으로 연방정부의 각 기관이 각기 역할과 책임을 다하는 분산 시스템을 운영하는 가운데, 정책의 통합성을 제고하고 각 기관들의 유기적 협력을 도모하기 위한 총괄·조정 기능을 갖추는 형태로 진화했다(〈그림 3〉 참조). 부시 행정부에서는 국토안보부(DHS)와 국가정보국(DNI)이 총괄 기능을 수행했다. 오바마 행정부 1기에 접어들어 국가안보위원회(NSC) 산하 사이버안보국 내의 사이버안보조정관이 국토안보부, 국가안보국, 연방수사국, 국무부, 상무부 등 실무부처들이 개별적으로 수행하는 사이버 안보 업무를 총괄하도록 하였다. 이후 오바마 행정부 2기에는 실무부처 업무의 통합성과 민관협력의 실현을 위해서 세 개의 기관이 추가로 설치되었다. DNI 산하에는 사이버위협정보통합센터(CTIIC)가 설치되어 사이버 위협과 사고를 종합적으로 분석하여 유관기관에 정보를 제공케 했다. 예산관리국 내에는 전자정부사이버과를 설치하여 연방기관의 업무를 감독·조율하게 했다. 민관협력 촉진을 위해 정보공유분석기구(ISAOs)를 설치하여, 국토안보부 산하에서 민관 정보공유를 담당하는 국가사이버안보정보통합센터(NCCIC)와 협력하도록 했다(김상배, 2018: pp.155-156).

이러한 추진체계는 트럼프 행정부에서 변화를 겪었는데, 가장 큰 변화는 2018년 5월 NSC 산하 사이버안보국 내의 사이버안보조정관 직을 폐지한 조치였다. 이에 앞서 2018년 4월 토머스 보서트(Tomas Bossert) 국토안보보좌관이 사임했는데, 그는 백악관에서 미국 국내안보, 테러리즘, 사이버 문제를 관장하는 중추적인 역할을 맡아왔었다. 그의 사임이 새로이 백악관 국가안보보좌관에 강경파인 존 볼턴(John Bolton) 전 유엔대사가 취임한지 하루 뒤에 이루어졌다는 점에서 구설수에 오르기도 했다(뉴시스, 2018/04/11). 보서트 보좌관 사임 며칠 후 롭 조이스(Rob Joyce) 사이버안보조정관은 사직하



출처: 김상배(2018), p.155를 보완·수정.

〈그림 3〉 미국의 사이버 안보 추진체계

고 국가안보국(NSA)으로 복귀했다(Nextgov, 2018/04/16). 2018년 5월에는 사이버 안보 업무의 컨트롤타워 역할을 담당했던 사이버안보조정관의 직책 자체가 폐지되었다(Helpnetsecurity, 2018/05/16).

이러한 추진체계의 변화는 미국의 사이버 안보 전략의 약화로 비춰질 수도 있지만, 그 내용은 오히려 공세적으로 나타나고 있는 것으로 해석 가능하다. 이러한 변화는 볼턴 보좌관이 주도한 것으로 보이는데, 이후 볼턴 보좌관의 행보를 보면 국가안보전략 전반의 맥락에서 사이버 안보 전략을 통괄하려는 의도로 해석할 수 있기 때문이다. 이러한 양상은 2018년 11월 중간선거를 앞두고 백악관이 자국 안보를 위협하는 사이버 공격에 대해 대응하는 과정에서 드러났다. 2018년 8월 19일 볼턴 보좌관은 러시아를 비롯해 중국·이란·북한 등 네 나라가 중간선거에 개입할 가능성이 있으며, 이들 국가들의 선거개입을 막기 위해 사이버 안보를 강화할 필요성을 강조했다. 그는 폴 나카소네 국가안보국(NSA) 국장이 외부로부터의 선거개입에 대응하여 공격적

인 사이버 작전을 진행한다고 밝힌 사실을 인용하며, “선거뿐만 아니라 모든 범위의 취약한 시스템을 보호하기 위해 총 역량을 동원하는 것이 최우선 과제”라고 강조했다. 아울러 그는 사이버 안보를 보장하기 위한 억지력 있는 조직을 만들어서 미국에 대해서 사이버 작전을 수행했거나 또는 고려하고 있는 국가들이 큰 대가를 치르도록 하겠다는 엄포를 놓기도 했다(조선일보, 2018/ 08/20).

2. 행정명령과 국가사이버전략 발표

2017년 출범 이후 트럼프 행정부의 사이버 안보 전략이 즉시 공세적으로 추진되어 러시아, 중국 등과의 관계가 악화될 가능성이 전망되었으나, 실제로 2017년에는 미러, 미중 등 강대국 관계는 다소 소강국면을 맞은 양상을 보였다. 2016년 미 대선에 대한 러시아의 개입으로 긴장되었던 미러 관계는, 오히려 2017년 7월 10일 G20에서 미러 정상의 사이버 안보 동맹 체결의 가능성 거론이 와전되는 등 혼란을 겪었다. 미중 간에도 다양한 채널을 통해서 사이버 안보 협의가 지속되었으나, 2017년 11월 10일 미중 정상회담에서도 사이버 안보에 대한 합의를 도출하지는 못했다. 그러한 와중에도 국내 차원에서는 사이버 안보 전략을 정비하였는데, 2017년 5월 11일 트럼프 대통령은 연방네트워크 및 주요 기반시설의 보안강화를 목적으로 사이버 안보의 책임이 각 정부기관의 수장들에게 있다는 내용을 골자로 하는 사이버 안보 관련 ‘행정명령 13800’을 공표했다. 이 행정명령은 장기적인 사이버 안보의 역량 강화 등을 포함한 3대 분야에 걸쳐서 15개의 실태평가 및 계획보고서의 제출을 지시하였다(Presidential Executive Order 13800, 2017/05/11).

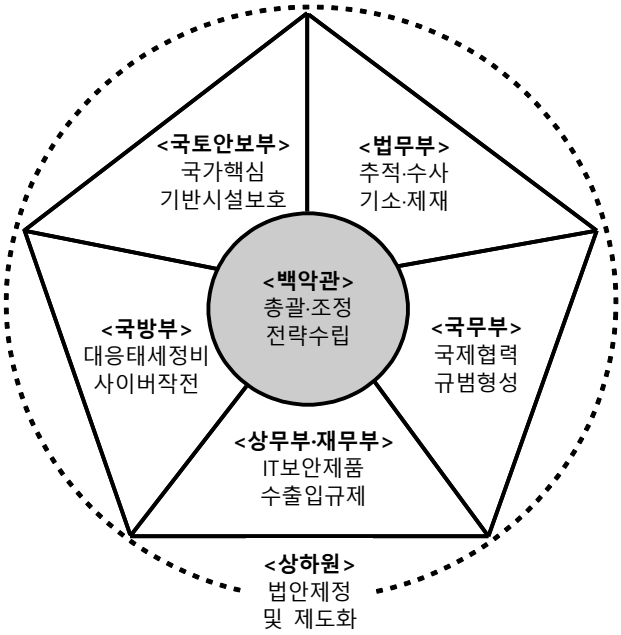
트럼프 행정부의 공세적 태도 변화는 2018년 9월 15일 트럼프 대통령이 지난 수년 동안 미국 사이버 안보정책의 가이드라인을 제시했던 오바마 대통령의 정책지침 PPD-20를 폐지하는 행정명령에 서명하면서 나타났다(Security Newspaper,2018/09/15). 오바마 행정부는 2012년 국방부 등에서 외국을 겨냥한 사이버 공격을 수행할 경우 정부 유관부처들의 사전 승인을

받도록 했었다. 그러나 트럼프 대통령은 이를 뒤집는 내용의 행정명령에 서명함으로써 "사이버 보안 관련 업무를 수행하는 정부기관들은 외국의 적들을 공격하는 데 더 많은 권한을 갖게 됐다"(뉴스1, 2018/09/21). 이 행정명령은 2018년 11월 6일 중간선거를 두 달여 앞둔 시점에서 나왔는데, 소셜 미디어를 이용한 각종 유언비어 살포나 해킹 등 악의적인 사이버 공격 시도에 대해 단호하게 맞대응하려는 트럼프 행정부의 의지를 엿볼 수 있는 것으로 해석되었다.

또한 2018년 9월 20일 트럼프 행정부는 2003년 이후 15년 만에 처음으로 연방 차원의 '국가사이버전략'을 발표했다. 이 '전략'은 사이버 공간에서도 '힘을 통한 평화 유지'를 기치로 내걸고, 국가지원 해커들의 악의적인 사이버 활동을 억지하고, 더 나아가 사이버 공간에서 책임 있는 국가행동을 보장하기 위한 규범 마련에 앞장서겠다고 천명했다. 이 '전략'은 연방네트워크 및 기반시설 보안강화를 규정했던 2017년 5월 11일의 '행정명령 13800'과 그 골자가 동일한데, 미국 내 네트워크와 시스템 및 데이터의 안보를 강화하고, 이렇게 강화된 사이버 안보 환경에서 디지털 경제와 기술혁신을 증진하며, 국제평화와 미국의 국가안보를 보장할 뿐만 아니라, 국제 인터넷 환경과 기술 분야에서 미국의 리더십을 확대하는 등의 핵심 목표로 제시했다. 이 '전략'은 이전보다 사이버 공격에 대한 좀 더 공세적인 미국의 태도 변화를 보여줬는데, 악의적인 사이버 공격에 대응하는 국방부의 운신 폭을 넓혀줬다는 점에서 앞서 2018년 9월의 행정명령과도 맥이 닿는다(White House, 2018).

3. 실무부처 차원의 복합지정학적 대응

이러한 행정명령들과 '국가사이버전략'에 의거하여 미국 정부는 실무부처 차원에서 국가지원의 사이버 공격에 대한 다양한 대응전략을 모색하고 있다. 이러한 실무부처 차원의 대응전략은 앞서 제시한 복합지정학의 시각에서 볼 수 있는 조치들이다(〈그림 4〉 참조). 물리적 인프라 보호나 군사적 옵션까지도 포함한 공세적 대응을 취하는 국토안보부나 국방부 차원의 대응은 (고전)



〈그림 4〉 미국의 복합지정학적 대응

지정학적 시각에서 이해할 수 있는 조치이다. 사이버 공격에 대한 추적과 수사 및 기소와 제재 등의 조치를 취하는 법무부의 대응은 '안보화'로 대변되는 비판지정학적 조치로 이해할 수 있다. 이에 비해 사이버 안보와 통상이슈의 연계를 통해서 IT보안제품의 수출입 규제를 추구하는 상무부·재무부의 조치나, 사이버 안보를 위한 국제협력과 국제규범 형성을 모색하는 국무부의 정책은 비지정학적 차원에서 이해할 수 있는 조치이다. 실무부처들의 이러한 복합지정학적 대응을 좀 더 구체적으로 살펴보면 다음과 같다.

첫째, 국토안보부 차원의 대응전략과 관련하여 제일 눈에 띄는 것은 2018년 7월 31일 국토안보부가 뉴욕에서 최초로 개최한 전국사이버안보서미트(National Cybersecurity Summit)이다. 이 서미트에는 마이크 펜스 부통령, 키어스텐 닐슨 국토안보부장관 이외에 행정부과 정보기관의 고위관리 및 업계의 CEO 등이 참석하였다. 이 서미트에서 닐슨 장관은 국가핵심 기반시설의 보호 업무를 조정하기 위한 국가위험관리센터(National Risk Management

Center, NRMC)의 창설을 발표했다. 이 센터는 연방정부와 민간부문이 공동으로 국가위험 전반을 관리하기 위해 세 가지 업무를 수행하기로 되어 있다고 했다. 첫째, 국가 핵심기능에 대한 전략적 위험을 식별하고 우선순위를 선정하며, 둘째, 위험관리 전략 개발에 대한 정부 및 업계 활동을 통합하고, 끝으로, 업계부터 정부까지 동시에 작동 가능하도록 위험관리 활동의 보조를 맞추는 업무를 담당한다는 것이다. 이 센터는 국토안보부 사이버 작전의 중앙 허브인 국가사이버안보정보통합센터(NCCIC)와 긴밀히 협업해 나갈 예정이라고도 했다. 또한 닐슨 장관은 ICT공급망의 위험관리를 위한 태스크포스(TF)를 국가위험관리센터 내에 설치한다고 발표했는데, 이 TF는 글로벌 ICT공급망 관련 위험을 식별하고 관리하는 데 필요한 행동 권고사항을 개발할 예정이라고 했다.

한편 2018년 11월 16일 트럼프 대통령이 CISA(Cybersecurity and Infrastructure Security Agency Act)에 서명함으로써 미국 국토안보부 산하 국가보안프로그램국(NPPD)이 '사이버·인프라보안국(Cybersecurity and Infrastructure Security Agency, 이하 CISA)'으로 승격되었다. 이로써 미국의 사이버 안보 문제를 국토안보부의 CISA가 담당하게 된 것이다. CISA는 외부의 물리적 위협과 사이버 공격으로부터 기반시설의 방호하는 국가적 노력을 주도하며 정부 여러 부처와 공조할 뿐만 아니라 민간 부문과 협력하여 위협에 대처하는 임무를 맡았다. 이렇게 발족하는 CISA는 사이버 보안, 기반시설 보안, 응급 커뮤니케이션을 담당하는 세 부서로 구성되었다.

둘째, 국방부 차원에서는 사이버 작전을 위한 공세적인 대응태세를 강화하고 있다. 세계 주요국들이 사이버 공격에 능동적으로 대응하기 위해 군대를 신설하거나 확대 및 격상하는 추세 속에 미국도 2017년 8월 18일 사이버사령부를 독자적인 지휘체계를 갖춘 10번째 통합 전투사령부로 격상시키는 조치를 단행했다. 국방부는 2018년 9월 새로운 '국방부 사이버전략'을 발표했는데, 이는 2011년 7월과 2015년 9월의 '전략' 발표에 이은 세 번째였다(Department of Defense, 2018). 새로운 전략서는 공공·민간 부문에 대한 중국의 기밀정보 절취와 미국 등 서방 국가에 대한 러시아의 선거개입을 비판했다. 또한 악의적 사이버 활동의 근본적 예방을 위해 선제적 사이버 공격

을 감행할 의지도 천명하였으며, 해커에 대한 응징공격을 위한 사이버 작전 수행을 강화했다. 이러한 입장의 천명은 최근 미국이 북한을 상대로 벌인 사이버 작전과 맥을 같이 하는 것으로 평가되는데, 실제로 미국은 2014년 12월 북한의 소니 해킹에 대한 보복으로 북한 인터넷망을 10시간 동안 마비시켰으며, 북한 미사일 발사를 교란시키기 위한 전자기파 공격도 감행한 것으로 알려졌다.

한편 2018년 8월 13일 트럼프 대통령은 2019년 국방수권법(National Defense Authorization Act, NDAA)에 서명했다. 트럼프 대통령이 "현대 역사상 (미국) 군과 전사를 위해 이뤄진 가장 중요한 투자"라고 평가하기도 했던 이 법안은, 사이버 안보와 관련하여, 특히 중국의 통신장비를 정조준하고 있다. 2019년 국방수권법 889조는 미국은 중국이 소유·통제하거나 그렇다고 추정되는(believed) 기업의 통신 장비 및 서비스를 미국 행정기관이 조달 또는 계약하는 것을 금지했다. 중국의 통신장비업체 ZTE과 화웨이 같은 곳들이 해당된다. 이 같은 금지 조치는 트럼프 대통령이 국방수권법에 서명한 날로부터 1년 뒤 시행되며, 2년 뒤에는 각 행정기관의 보조금을 수령하는 기관들로까지 확대 시행될 예정이다(보안뉴스, 2018/08/20).

셋째, 법무부 차원의 대응은 중국, 러시아, 이란, 북한 해커들을 추적, 수사, 기소, 제재하는 것이었다. 2014년 5월 미 법무부가 미국 내 기관들에 대해서 해킹을 감행한 것으로 지목한 중국군 61398부대 장교 5인을 철강무역 비밀을 캐내려고 미국 회사를 해킹한 혐의로 미국에서 기소했으며, 2017년 11월에는 보유섹(Boyusec)으로 알려진 중국 IT기업에 의해 고용된 것으로 보이는 중국인 3명을 해킹 및 지적재산 도용 혐의로 기소했다(뉴시스, 2017/11/28). 2018년 10월 30일 미국 법무부는 2010년부터 2015년까지 5년간 미국과 프랑스의 우주항공 업체 컴퓨터를 해킹해 기술을 빼낸 혐의로 중국인 10명을 기소했다(MK뉴스, 2018/10/31). 한편 2018년 1월에는 러시아 군정보국(GRU) 해커 포함 정보요원 7명을 화학무기금지기구(OPCW), 미 웨스팅하우스, FIFA 등에 대한 해킹과 2016년 미 대선 개입 협의로 기소했다. 2018년 2월에는 GRU 소속 해커 13명과 단체 3곳을 기소 및 제재했다.

또한 2016년 3월에는 이란 혁명수비대 소속 해커 7명을 2011~13년간 뉴

욕 금융시장 등 주요 금융기관, 뉴욕댐 산업제어시스템에 대한 해킹 혐의로 기소했으며, 2018년 3월에는 이란 혁명수비대 소속 해커 9명과 연구소 1곳을 기소 및 제재했는데, 미 정부기관, 유엔 등 국제기구, 민간회사 및 320개의 미국을 비롯한 각국 대학에 대한 해킹 혐의였다. 더 나아가 2018년 9월 6일 미국 법무부는 '워너크라이' 랜섬웨어 공격과 소니 픽처스, 방글라데시 중앙은행, 미 방위산업업체 록히드 마틴 등을 해킹한 혐의로 북한 해커 조직인 '라자루스'의 일원인 박진혁을 기소했다. 이와 동시에 미 재무부는 같은 혐의로 박진혁과 그가 소속된 '조선엑스포합영회사'를 독자 제재 명단에 올렸다. 미국의 독자 제재 대상에 오르면 미국 내 자산이 동결되고 미국 개인·기업과 이들 간의 거래가 금지된다.

넷째, 상무부 또는 재무부, 특히 재무부 산하 '외국인투자심의위원회(CFIUS)' 차원에서 진행된 사이버 안보 관련 IT 제품의 수출입 및 기업 인수합병 규제 조치에도 주목할 필요가 있다. 최근 가장 큰 화두는 화웨이다. 2012년 당시 미국 하원 정보위원회가 중국의 스파이 활동에 화웨이가 협조한다는 의혹을 제기한 뒤 미국 행정부에 화웨이 통신장비 구매금지를 요구했다. 2014년 ZTE와 화웨이의 설비 구매를 금지한다고 발표했으며, 2018년 1월 미국 AT&T가 중국 화웨이 스마트폰을 판매하려던 계획이 전격적으로 취소되기도 했다. 2018년 2월 미국 정보기관(CIA, FBI, NSA)들이 나서서 중국의 전자업체인 화웨이 스마트폰과 통신장비업체 ZTE의 제품을 사용하지 말라고 경고했다.

이밖에도 2014년 6월 레노버가 IBM의 x86서버 사업을 인수하는 것을 지연했다. 2017년 9월 CFIUS는 중국 펀드인 캐넌브리지가 미국의 래티스 반도체를 인수하는 것을 차단했다. DJI(드론), 하이크비전(CCTV) 등의 미국 시장 진출에 대한 우려도 제기되었으며, 2017년 7월 미국은 러시아 보안업체 카스퍼스키랩을 제재하기도 했다. 2018년 1월 알리바바 계열 앤트파이낸셜이 미국 송금서비스 기업 머니그램을 인수하는 것을 제지했다. 2018년 7월 차이나모바일의 미국 진입을 불허했다. 한편 2018년 10월 미 상무부는 미국 기업들이 중국의 D램 메모리 업체 푸젠진화와 거래하는 것을 금지했다. 푸젠진화가 기술을 훔쳤다는 것이 제재 이유였다(OBS 뉴스, 2018/10/31).

끝으로, 국무부 차원의 대응전략에도 주목할 필요가 있다. 각 분야의 실태 평가와 계획보고서 제출을 지시했던 2017년 5월의 대통령 행정명령에 의거하여 2018년 5월 국무부는 '사이버위협 전략적 대응옵션 보고서'를 제출하였다. 이 보고서는 사이버 공격이나 기타 악의적 활동에 대해서 적극 대응하겠으며, 이 과정에서 우방국과 정보공유, 공격주체의 공동지목, 대응행위의 지지선언 등과 같은 공동대응을 취하겠다고 했다. 국가 행위자들이 지원하는 사이버 공격의 성격을 고려한 맞춤형 억지전략을 개발하고 비국가 행위자에 대해서는 제재와 기소 등의 대가를 부과하는 조치를 복합적으로 활용한다고 했다.

한편 2018년 5월 국무부는 '국제협력 참여전략 보고서'도 제출했는데, 이 보고서에는 외교, 대외원조, 합동 군사훈련 등과 같은 정부 간 활동, 비(非)국가 포럼을 통한 정책 및 기술표준 설정에의 참여, 동반자 국가들의 위협 대응을 위한 역량 구축의 지원 등과 같은 내용들이 담겼다. 이밖에도 국무부는 다양한 사이버 안보의 국제규범 형성과정에 참여하고 있다. 최근 미국의 사이버 안보외교와 관련하여 주목을 받은 것은, 중국의 사이버 공격과 화웨이의 IT보안제품에 대한 의혹이 확산되는 분위기 속에서 이른바 '파이브 아이즈(Five Eyes)' 국가들(특히 영국과 호주, 캐나다)과의 국제공조를 추진하고 있는 현상이다.

4. 사이버 억지 및 대응 법안의 통과

이상에서 언급한 트럼프 행정부의 전략은 2018년 9월 6일 미 하원을 통과한 '사이버 억지와 대응 법안(H.R.5576)'의 내용과도 일맥상통한다. 2018년 9월 6일 미 하원은 사이버 공격에 관여한 제3국의 개인과 기관 및 정부에 추가 제재를 가하는 법안을 통과시켰다. 이 법안은 러시아, 중국, 이란, 북한 등과 같은 국가의 지원을 받는 사이버 공격을 미국에 대한 심각한 위협으로 규정하고 이에 통합적으로 대응하기 위한 체계 마련을 골자로 한다. 미국을 겨냥한 악의적 사이버 활동에 대해서 사이버 위협국 지정이나 경제적 추가제

재 및 안보 지원의 중단 등과 같은 조치를 동원해서하도 대응하겠다는 것이다. 특히 이들 법안은 북한을 적시하고 있는데 2017년 5월 발생한 사이버 공격 '워너크라이' 사태의 배후로 북한이 지목됐으며 전 세계 150여 개국에 걸쳐 컴퓨터 시스템 30만 대 이상을 감염시켰다고 지적했다. 이들 법안의 내용은 세 가지 측면에서 파악된 사이버 공격 대응 체계 구축이 핵심이다.

먼저 대통령이 해외 정부가 지원하는 악의적인 사이버 활동에 관여한 제3국의 개인 또는 기업을 '심각한 사이버 위협'으로 지정하도록 했다. 이는 테러지원국을 지정해 이들에게 제재를 부과하는 체계와 유사한데, 북한이 테러지원국에 이어 사이버 위협국으로도 지정될지 주목된다. 둘째, 좀 더 구체적으로 이들이 미국에 사이버 공격을 가할 경우 경제적 추가 제재를 부과해 대응하도록 했다. 이에 따라 대통령은 제재의 일환으로 이들 개인이나 기업이 국제금융기관으로부터 차관을 받지 못하도록 각 국제금융기구의 미국 대표에게 미국의 영향력과 투표권을 행사하도록 지시할 수 있다. 또한 사이버 위협으로 지정된 개인 또는 기업에 미국의 수출입은행이나 해외민간투자공사와 같은 미 정부기관이 보증이나 보험, 신용장 등의 증서를 발급할 수 없도록 지시할 수 있다. 끝으로, 이외에도 사이버 공격에 관여한 것으로 판단되는 제3국에 추가 제재를 부과해야 하며 이런 제재에는 미국의 인도주의와 무관한 지원과 안보 지원을 제한 또는 중단하는 조치가 포함됐다.

이러한 미국의 행보는 최근 러시아, 중국, 이란, 북한 등 국가지원 해킹에 대한 적극적인 대응의 일환으로 이해되며 미국의 독자적 위협대응 조치에 법적 근거를 제공하려는 노력으로 파악할 수 있다. 사이버 공격에 대한 사이버 맞공격을 규정하기보다는 사이버 위협국 지정, 경제제재, 안보지원중단 등의 조치를 취하는 선에 대응하려는 점이 특기할 점이다. 이는 미국과 상호의존 관계에 있는 제3국에 대해서 일정한 정도의 효과 있는 압력이 될 것이며 일종의 '비군사적 억지(non-military deterrence)'의 의미가 있을 것이다. 한편, 2018년 8월 23일 미 상원에서도 '사이버 억지와 대응 법안(S.3378)'을 발의했는데 이는 하원 법안과 거의 동일한 내용을 담고 있으며, 곧 통과될 것으로 전망되고 있다. 다만 하원법안과 달리 해외정부가 지원하는 사이버 활동에 관한 행정부의 브리핑을 요구하는 내용은 포함되지 않았다.

V. 맺음말

최근 사이버 공격은 양적으로 늘어났을 뿐만 아니라 질적인 패턴변화의 조짐도 보이고 있다. 사이버 공격의 목적이 다변화되고 있을 뿐만 아니라 공격수법도 다양화되고 있으며, 공격 주체의 성격도 변화하고 있다. 무엇보다도 큰 변화는 일견 일탈적 해커 집단의 소행으로 보이는 사이버 공격의 이면에 러시아, 중국, 이란, 북한 등과 같은 국가 행위자의 그림자가 짙게 깔려 있다는 사실이다. 이제 사이버 공격에 대한 대응은 민간 영역에만 맡겨 놓을 수는 없고 국가가 나서서 적극적으로 해결해야 하는 문제가 되었다. 게다가 이들 국가지원 해킹이 지정학적 갈등과 연계될 가능성이 높아졌다는 점에서 그러한 필요성은 더욱 높아졌다. 이 글은 복합지정학의 시각에서 최근 사이버 안보 분야의 변화 양상을 살펴보고, 이에 대응하는 트럼프 행정부의 사이버 안보 전략과 그 의미를 개념화하였다.

최근 트럼프 행정부의 대응은 악의적인 사이버 공격 시도에 대해 단호하게 맞대응하려는 의지를 보여주고 있다. 미국의 중간선거를 두 달여 앞둔 2018년 9월 15일 서명된 대통령 행정명령이나 사이버 공간에서도 '힘을 통한 평화 유지'를 기치로 내걸고 9월 20일 발표된 '국가사이버전략' 등이 그 사례들이다. 이러한 트럼프 행정부의 공세적인 전략은 '신냉전 시대'의 도래라는 프레임에 담겨 일견 과장되는 면모를 보이고 있다. 그러나 트럼프 행정부의 행보를 단순히 (고전)지정학으로의 회귀라는 시각에서만 볼 수는 없다. 최근 사이버 안보의 문제는 단순한 해킹공격의 탈지정학적 성격을 넘어서 국내정치 이슈의 안보화 담론과 연계되면서 비판지정학적 속내를 드러내고 있으며, 통상마찰, 데이터 안보, 심리전, 국제규범 등과 같은 다양한 세계정치 이슈들과 연계되면서 비지정학적 지평을 보여주고 있기 때문이다. 그야말로 트럼프 행정부의 전략은 사이버 안보의 복합지정학적 측면을 잘 보여주는 사례라고 할 수 있다.

이러한 트럼프 행정부의 행보를 가볍게 볼 수 없는 이유는 한국도 국가지

원 해킹의 피해를 보고 있는 비슷한 처지이기 때문이다. 러시아 해커들의 사이버 공격은 유럽 지역에서부터 중동과 중앙아시아를 지나 동북아시아에도 미치고 있다. 2018년 2월 평창 동계올림픽 개막 즈음에 발생한 해킹 공격이 그 사례 중의 하나이다. 중국지원 해커들의 공격도 한국을 겨누고 있다. '사드 보복'의 차원에서 중국주재 한국 외교공관들의 홈페이지를 해킹하거나 중국 내 한국 기업을 공격하기도 했다. 게다가 최근에는 이란의 해킹공격도 논란이다. 이란 해커들은 사우디아라비아를 공격하는 과정에서 사우디아라비아의 석유화학기업과 연관된 한국 기업도 공격한 것으로 알려졌다. 북한의 경우에도, 최근 해외로 공격의 화살을 돌려서 한국에 대한 사이버 공격이 잠잠한 듯 보이지만, 2017년 12월에는 발생한 북한 해커들의 국내 비트코인 거래소 유빗 해킹은 해당 기업의 파산이라는 큰 피해를 낳기도 했다.

이러한 국가지원 해킹에 대응하는 과정에서 트럼프 행정부의 복합지정학적 대응은 큰 참고가 된다. 먼저 여태까지는 북한의 사이버 공격이 주요 위협이었다면 최근에는 해킹 공격의 기원이 다변화되고 있다는 점을 인식해야 한다. 대북전략의 차원에서 (고전)지정학적으로만 대응하려는 관성을 탈피할 필요가 있다. 이외에도 시급하게 보완하고 개선할 문제들이 산적해 있다. 그러나 최근 한국의 행보가 그리 밝지만은 않다는 것이 문제이다. 2014년 말 한수원 해킹 사건을 계기로 설치되었던 사이버안보비서관 직이 최근 폐지되면서 컨트롤타워의 약화에 대한 우려가 높다. 오랫동안 공을 들여온 '국가사이버안보전략'은 아직도 발표되지 못하고 있으며, 현재 국회에 계류 중인 '국가사이버안보법'이 가까운 미래에 통과될 가능성도 그리 높지 않다. 이러한 상황에서 청와대, 국정원, 국방부, 과기정통부, 경찰청, 검찰청 등이 추진하는 사이버 안보의 거버넌스를 효과적으로 작동시킬 과제가 제기된다.

요컨대, 최근 사이버 안보는 좁은 의미의 해킹 문제를 넘어서 거시적인 국가안보의 문제가 되었다. 양질전화와 이슈연계 및 지정학적 임계점을 넘어서 명실상부한 국제정치적 문제가 되었다. 무엇보다도 국가지원 해킹의 형태로 나타나고 있는 사이버 공격의 최근 양상이 현란한 변화를 보이고 있다. 사이버 공격의 양적·질적 변화와 더불어 이를 방어하는 국가적 차원의 대응책도 예전보다 훨씬 더 복합적인 구도에서 마련될 필요성이 있다. 이제 사이버 안

보의 문제는 컴퓨터 시스템의 보안 문제에만 그치는 것이 아니라 산업경쟁력과 통상마찰, 선거개입과 심리전, 국제협력과 규범형성의 문제가 되었다. 현재 사이버 공간이 우리 삶에 미치는 복합적인 영향을 생각해 보면, 이러한 사이버 안보의 복합지정학적 성격은 점점 더 강화될 가능성이 크다. 이러한 시대적 변화에 발맞춰가는 사이버 안보의 국가전략에 대한 좀 더 본격적인 고민이 필요하다.

투고일자: 2018-11-12 심사일자: 2018-12-03 게재확정: 2018-12-05

참고문헌

2012.「미-이란 사이버 전쟁 중…'사이버 진주만' 공격 위험」.『보안뉴스』 10월 15일
2015.「'세계는 사이버전쟁 중'…러, 스마트 무기 기반 준비태세 강화」.『Russia Focus』 6월 26일.
2016.「美, 이란 사이버공격 준비했다…핵 협상 실패 대비」.『국민일보』 2월 17일.
2016.「중국의 대미 사이버공격 급감…'시진핑 군 개혁도 영향'」.『연합뉴스』 6월 21일.
2016.「한일, 28일 북한발 사이버 공격 대응 첫 양자협의」.『연합뉴스』 10월 28일.
2017.「YT '오바마, 北 핵·미사일 무력화 위한 사이버戰 실시'…'北 미사일 잇단 실패로 성공하는 듯했지만 결국 실패'」.『조선일보』 3월 5일.
2017.「러 '정보 게릴라전' 맞서…美·EU 사이버 연합군 뜬다」.『매일경제』 4월 12일.
2017.「美 사이버 교란 작전 '레프트 오브 론치'에 北미사일 잇단 실패?」.『조선일보』 4월 18일.
2017.「정부간 사이버스파이 중단 합의, 효과 있나」.『ZDNet Korea』 5월 11일.
2017.「'국가주도 사이버 공격' 러·중·북·이란 실태는」.『MK뉴스』 5월 16일.
2017.「英, 워너크라이 랜섬웨어 공격 배후로 北 지목」.『연합뉴스』 6월 16일.
2017.「미 '북 포함 사이버 위협국 대가 치를 것'」.『Radio Free Asia』 7월 31일.
2017.「이란, 한국 정유사 1년 이상 북한식 해킹공격…정부는 뭐하고 있나?」.『월간조선』 11월호
2017.「美 법무부, 해킹·지적재산권 도용 혐의로 중국인 3명 기소」.『뉴시스』 11월 28일.
2017.「HBO 해킹한 이란인, 알고 보니 이란 정부 해커」.『보안뉴스』 12월 7일.
2017.「백악관 '워너크라이 사이버 공격은 북한 소행' 첫 공식 지목」.『연합뉴스』 12월 20일.
2018.「우크라이나는 러시아 해커들의 훈련장이다」.『보안뉴스』 1월 3일.
2018.「러시아의 해킹 그룹 소파시, 활동 영역을 동쪽으로 넓힌다」.『보안뉴스』 2월 21

일.
2018.「美 보안업체 '북한 해커 집단 리퍼가 전세계 위협'」.『뉴스1』 2월 22일.
2018.「美 정보기관 '평창 개막식 해킹 北위장 러시아 총정보국 소행'」.『중앙일보』 2월 25일.
2018.「中, 남중국해 갈등에 美 기업 해킹 공격 재개 파이어아이」.『뉴시스』 3월 16일.
2018.「이란 해커, 미국 등 전세계 300개 대학 해킹」.『연합뉴스』 3월 27일.
2018.「한반도는 사이버 전쟁 중, 한국군의 사이버 옵션은?」.『중앙일보』 4월 6일.
2018.「트럼프 핵심참모 또 백악관 떠나…보서트 국토안보 보좌관 사임」.『뉴시스』 4월 11일.
2018.「시리아 사태에 보복 경고…사이버전 옮겨붙는 미러 '신냉전'」.『디지털타임스』 4월 17일.
2018.「中 해커, 日 정부 북핵 정보 얻으려 방산업체 해킹」.『조선일보』 4월 23일.
2018.「아세안정상회담 '사이버 보안협력' '남북정상회담지지'」.『HaninPost Indonesia』 5월 7일.
2018.「北, 북미회담 접촉 중에도 '사이버 해킹 돈벌이 여전」.『뉴스핌』 5월 10일.
2018.「미국 '핵협정 탈퇴', 이란 해커 사이버 테러 위험 늘어」.『전자신문』 5월 14일.
2018.「북한 사이버 공격에 미국서 수출된 컴퓨터 사용돼」.『VOA뉴스』 6월 7일.
2018.「중국 해커, 미 해군 협력업체로부터 수중전 데이터 614GB를 훔쳤다」.『IT World』 6월 14일.
2018.「중국 해킹집단, 美·亞 인공위성 사업자 등 겨냥 사이버 공격」.『연합뉴스』 6월 20일.
2018.「대만, 중국의 사이버 공격에 시달려…'차이잉원 집권 후 급증'」.『연합뉴스』 6월 25일.
2018.「무역전쟁 이어 사이버 해킹 의심…美는 '中 전방위 압박' 화력 집중」.『한국일보』 6월 25일.
2018.「캄보디아 '총선 앞둔 중국의 해킹 공격 조사」.『연합뉴스』 7월 16일.
2018.「볼턴 '중국·북한도 美 중간선거 개입 우려'」.『조선일보』, 8월 20일.
2018.「中 통신장비 정조준 美 국방수권법, 韓 5G 장비 수출 '기대'」.『보안뉴스』 8월 20일.
2018.「'일대일로' 연관된 중국발 사이버 공격 흐름 포착」.『KINEWS』 9월 1일.
2018.「美 '사이버위협에 공격적 대응'…北·中·러 등 겨냥」.『뉴스1』 9월 21일.
2018.「FT '아시아·태평양 국가들, 중국의 사이버 공격에 공세적 대응'」.『연합뉴스』 10월 4일.
2018.「펜스 '중국, 트럼프 아닌 대통령 원해', 中 '뜬구름잡는 소리'」.『연합뉴스』 10월 5일.
2018.「이번엔 미 법무부가 중 압박」.『MK뉴스』 10월 31일.
2018.「서방, 중 패권 핵심 'IT굴기' 봉쇄 박차」.『OBS 뉴스』 10월 31일.
김상배. 2015.「사이버 안보의 복합 지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계」.『국제·지역연구』 24권 3호, pp. 1-40.
_____. 2018.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』, 한울엠플러

스.
지상현, 콜린 플린트. 2009.「지정학의 재발견과 비판적 재구성」.『공간과 사회』통권 1호, pp. 160-199.
2018. “White House Cybersecurity Coordinator Leaving Office.” *Nextgov*, April, 16.
2018. “White House Eliminates Cybersecurity Coordinator Role.” *Helpnetsecurity*, May, 16.
2018. “New Trump’s Executive Order against Possible Election Intervention.” *Security Newspaper*, September 15.
Castells, Manuel. 2000. *The Rise of the Network Society*. 2nd edition. Oxford: Blackwell.
Coats, Daniel R. 2017. *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, Statement for the Record by the Director of National Intelligence, May 11.
Department of Defense. 2018. *DoD Cyber Strategy*. United States of America.
Dodds, Klaus. 2001. “Politics Geography III: Critical Geopolitics After Ten Years.” *Progress in Human Geography*, 25(3): pp. 469-484.
Gilpin, Robert. 1981. *War and Change in World Politics*. Cambridge: Cambridge University Press.
Hansen, Lene and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly*, 53(4): pp. 1155-1175.
Ikenberry, G. John. 2014. “The Illusion of Geopolitics: The Enduring Power of the Liberal Order.” *Foreign Affairs*, 93(3): pp. 80-90.
Kelly, Phil. 2006. “A Critique of Critical Geopolitics.” *Geopolitics*, 11: pp. 24-53.
Mead, Walter Russell. 2014. “The Return of Geopolitics: The Revenge of the Revisionist Powers.” *Foreign Affairs*, 93(3): pp. 69-79.
Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: The MIT Press.
_____. 2010. *Networks and States; The Global Politics of Internet Governance*. Cambridge and London: MIT Press.
Ó Tuathail, Gearóid. 1996. *Critical Geopolitics*. Minneapolis, MN: University of Minnesota Press.
Ó Tuathail, Gearóid and John Agnew. 1992. “Geopolitics and Discourse: Practical Geopolitical Reasoning in American Foreign Policy.” *Political Geography*, 11(2): pp.190-204
Organski, A.F.K. and Jack Kugler. 1980. *The War Ledger*. Chicago: University of Chicago Press.
Presidential Executive Order 13800. 2017. “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” May 11.
White House. 2017. *National Security Strategy of the United States of America.*

December.
_____. 2018. *National Cyber Strategy of the United States of America*. September.

Cybersecurity Strategies of the Trump Administration:
Complex Geopolitical Responses to State-sponsored Hacking

Sangbae Kim
Professor, Dept. of Political Science and Diplomacy
Seoul National University

The latest cyber attacks are not only increasing in quantity, but also changes in the patterns of the attacks—diversifying its targets and adopting various methods. A major change is likely to be linked to geopolitical conflicts as state actors such as Russia, China, Iran and North Korea intervene behind the cyber attacks, which have been previously attempted by deviant hacker groups. The U.S. Trump administration is showing strong will to launch counterattacks against such illegitimate hacking attacks. The Trump administration's cybersecurity strategies, which have shown a tendency to attack by even mentioning the use of military options, has been exaggerated by mobilizing a framework called the advent of the "New Cold War era." However, understanding the latest cybersecurity strategies under the Trump administration only in the context of enhancing physical attacks might overlook the unique nature of cybersecurity issues and the complexity of corresponding strategies. The recent cybersecurity issues have been linked to various international politics such as trade friction, data security and psychological warfare, and has evolved to seek multilateral international norms beyond national strategies of one nation or bilateral relations between nations. Relying on this perception, this paper looks at the recent changes in cybersecurity from the perspective of "complex geopolitics" and conceptualizes cybersecurity strategies of the Trump administration and its implications.

Keywords: Cybersecurity, Trump Administration, Complex Geopolitics, State-sponsored Hacking, National Strategies

김상배. 서울대학교 정치외교학과 교수
서울시 관악구 관악로 1 서울대학교 사회대 정치외교학부
sangkim@snu.ac.kr