Institute of International Studies at Seoul National University | 국제문제연구소 워킹페이퍼 No.7 (발간일: 2017. 5. 22.)

국가 사이버 안보 전략의 국제비교:

한반도 주변4국과 유럽 주요3국의 사례

김상배

서울대학교 정치외교학부 교수
인디애나대학교 정치학 박사
전공분야: 정보혁명과 네트워크 세계정치
대표업적: 『아라크네의 국제정치학』(2014), 『정보혁명과 권력변환』(2010), 『정보화 시대의 표준경쟁』(2007) 외 다수

초 록

최근 사이버 안보가 국가안보의 핵심적인 사안으로 인식되면서 세계 각국은 국가전략의 차원에서 사이버 안보 전략을 모색하고 있다. 이 글은 세계 주요국, 특히 한반도 주변4국으로 대변되는 미국, 일본, 중국, 러시아와 유럽의 주요3국으로 거론되는 영국, 독일, 프랑스 등 7개국의 사례를 비교 국가전략론의 시각에서 살펴보았다. 이들 국가들은 사이버 위협에 대응하기 위해서 지난 10여 년 동안 물적·인적 역량뿐만 아니라 군사적 대응태세를 지속적으로 강화해온 공통점이 있다. 그러나 사이버 안보 전략의 대내외 정책지향성이나 추진체계의 정비, 법제정의 양상 등에 있어서는 국가마다 상이한 행보를 보이고 있다. 미국과 일본으로 대변되는 서방 국가들과 중국과 러시아로 대변되는 비서방 국가들이 서로 대비되는 유형의 사이버 안보 전략을 추구하고 있으며, 영국, 독일, 프랑스 등과 같은 유럽 국가들은 그 중간지대에서 다소 복합적인 전략을 추구하고 있다. 이들 7개국의 사례는 향후 한국이 사이버 안보 전략을 모색하는 데 있어 참조할, 일종의 '일반모델'로서 함의를 가진다. 한국이 추구할 전략의 대내외적 정책지향성을 제대로 설정하고, 한국의 현실에 맞는 추진체계와 법제도를 스스로 찾아가려는 성찰과 고민이 필요하다.

I. 머리말

최근 사이버 안보가 국가전략의 관심사로 떠올랐다. 한국의 핵심 기반시설을 겨냥한 북한의 사이버 공격은 핵실험과 미사일 발사에 못지않게 중요한 위협이 아닐 수 없다. 지난 수년 동안 부쩍 거세지고 있는 미중 사이버 갈등은 사이버 안보라는 문제가 이미 두 강대국의 주요 현안이 되었음을 보여준다. 2016년 말 미국의 대선 과정에서 불거진 러시아의 해킹 논란으로 사이버 안보의 문제는 국내정치 과정의 일부가 되었다. 이러한 강대국들 간의 사이버 공방으로부터 한국도 자유로울 수 없다. 최근 들어 발생한 미국의 한반도 사드 배치를 둘러싼 논란의 와중에 중국과 러시아의 해커들이 한국을 공격하는 일이 벌어졌다. 사이버 위협에 대응하여 각국은 기술적으로 방어역량을 강화하는 외에도 공세적 방어의 전략을 제시하고 법제도를 정비하거나 국제협력을 강화하는 등의 대책 마련에 힘쓰고 있다. 그야말로 사이버 안보는 단순히 정보보안 전문가들의 기술개발 문제를 넘어서 다양한 분야를 아울러 종합적인 대응책을 마련해야 하는 21세기 국가전략의 문제가 되었다.

날로 교묘해지고 있는 사이버 공격을 막아내는 데 있어 전통안보의 대응방식은 역부족이다. 사이버 안보의 특성상 기술적으로 철벽방어를 구축하려는 단순발상은 해법이 될 수 없다. 오히려 사전예방과 사후복원까지도 고려하는 복합적인 방식이 필요하다. 정책내용 면에서 기술, 국방, 법제도, 국제협력에 이르기까지 다양한 노력이 필요하며, 추진주체 면에서도 어느 한 기관이 전담하는 모델보다는 해당 주체들이 역할과 책임을 다하는 가운데 그 상위에 총괄·조정역을 설계하는 중층모델이 적합하다. 물론 각국마다 차이는 있을 수밖에 없다. 정치와 사회와 문화의 차이가 있기 때문이고, 여타 정책이나 제도와의 관계 또는 역사적 경로의 존성의 제약을 받기 때문이다. 더 중요하게는 국가마다 사이버 위협의 기원과 성격, 그리고 각국이 처한 국제적 위상 등이 다르기 때문에 각기 상이한 해법을 모색하는 것은 당연하다. 그럼에도 지난 10여 년 동안 세계 각국이 사이버 위협에 대처하기 위해서 모색해 온 해법들은 전통안보의 경우와는 달리 좀 더 새롭고 복합적인 내용과 형식을 지니고 있는 것이 사실이다.

이 글은 세계 주요국, 특히 한반도 주변4국으로 대변되는 미국, 일본, 중국, 러시아와 유럽의 주요3국으로 거론되는 영국, 독일, 프랑스 등 7개국의 사례를 살펴보고자 한다. 사실 이 나라들은 오랫동안 한국이 정책과 제도모델을 고민하는 과정에서 일종의 '일반모델'로서 참조되었던 대표적인 나라들이다. 이들 나라들은 지금 사이버 안보 분야에서도 모델 경쟁을 하고 있다. 대략 서방 진영을 이끌고 있는 미국과 일본이 한편을 이루고, 비서방 진영의 중국과 러시아가 다른 한편에 서 있다면, 그 중간지대에 영국, 독일, 프랑스 등과 같은 유럽 국가들이 위치하는 형세이다. 이들 국가의 행보를 이해하는 것이 중요한 이유는 현 시점에서 한국이 모색할 사이버 안보 전략의 기본방향과 구성내용을 검토하고 이를 토대로 구체적인

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

실천방안을 궁리하려는 필요성 때문이다. 더 나아가 기존의 산업화 및 정보화 전략의 경우처럼 사이버 안보 분야에서도 한국이 스스로 '모델'을 개발하려는 기대 때문이기도 하다. 한국의 현실에 맞는 이른바 '한국형 사이버 안보 전략 모델'을 장차 스스로 추구해야 맞겠지만, 그 준비단계에서 세계 주요국들의 사례를 살펴보는 작업의 의미는 충분하다.

이 글은 비교 국가전략론의 시각에서 이들 7개국의 사이버 안보 전략을 비교분석하고자 한다. 사실 여태까지 국내에서 진행된 각국의 사이버 안보 전략에 대한 연구는, 새로운 전략이 발표되거나 법이 제정되면 이를 소개하고, '우리가 이만큼 부진하니 빨리 따라잡자'는 식의 개괄적 북챕터나 정책보고서가 주류를 이루었다. 주로 미국의 사례(이강규, 2011; 송은지 · 강원영, 2014)가 소개되었으며, 개괄적으로 미 · 중 · 일 · 러(조성렬, 2016; 김상배 편, 2017)나 한 · 중 · 일(김희연, 2015), 미국 · 영국 · EU(배병환 · 강원영 · 김정희, 2014) 등의 사례를 비교하거나, 좀 더 구체적으로는 일본(박상돈, 2015), 중국(양정윤 · 배선아 · 김규동, 2015; 고은송, 2016), 영국(배병환 · 송은지, 2014) 등의 사례를 탐구하는 선에 머물러 있었다. 해외연구를 보더라도 아직까지 각국의 사이버 안보 전략을 비교분석하여 이론적 함의를 도출하는 수준에는 미치고 있지 못하고, 주로 북챕터나 정책보고서 차원에서 각국의 현황을 소개하는 수준에 머물고 있는 것이 현재 학계의 엄연한 현실이다(Peritz and Sechrist, 2010; Lewis, 2015; Chang, 2014; Lindsay, et al. eds., 2015; Thomas, 2009; Nocetti, 2015; Christou, 2016).

이러한 맥락에서 이 글은 국제정치학의 개념을 원용한 비교분석의 연구를 시도해 보고자 한다. 이러한 비교분석 연구의 바탕이 되는 개념은 '네트워크 국가(network state)'에 대한 논의이다(Carnoy and Castells, 2001; 하영선 · 김상배, 2006; 김상배, 2014). 네트워크 국가는 글로벌화, 정보화, 민주화의 시대를 맞이하여 발생하고 있는, 근대 국민국가의 변환을 잡아내려는 개념 중의 하나이다. 사실 오늘날 국가의 양상은 부국강병에 주력하는 위계조직으로 개념화되던 근대 국민국가의 모델을 넘어서고 있다. 또한 오늘날 국가의 활동반경도 영토적 경계를 넘어서 그 안과 밖으로 광역화되고 있다. 이러한 과정에서 지난 수백 년 동안 이념형적 국가모델로 인식되어 온 국민국가는 변환을 겪고 있다. 그러나 국가변환의 양상은 글로벌 차원에서 획일적으로 나타나지 않고 각 국가와 지역마다 다르게 나타난다. 게다가 각 국가와 지역은 미래 국가모델을 놓고서 경합을 벌이는 양상도 나타나고 있다. 이러한 국가변환의 모델 경쟁이 사이버 안보 분야에서도 극명하게 나타나고 있으며, 이러한 양상을 제대로 읽어내는 것이 향후 미래 국가전략을 모색하는 데 있어 매우 중요하다는 것이 이 글의 인식이다.

이 글은 다음과 같이 구성되었다. 제2장은 사이버 위협에 대응하는 사이버 안보 전략의 분석틀을 각국이 추구하는 전략의 대내외적 정책지향성과 추진체계의 구성원리라는 두 가지 측면에서 마련하였다. 제3장은 서방 진영의 입장을 주도하고 있는 미국과 이에 동조하는 일

본의 사이버 안보 전략을 역량강화, 사이버 국방, 국제협력, 개인정보 보호, 추진체계의 구성 원리 등으로 나누어 살펴보았다. 제4장은 미국 주도의 질서에 도전하는 비서방 국가의 대표격인 중국과 러시아의 사이버 안보 전략을, 앞서의 미국과 일본의 사례를 살펴본 분석틀에 의거하여, 살펴보았다. 제5장은 서방 진영과 비서방 진영이 벌이는 경합구도의 중간지대에서 복합 모델을 추구하고 있는 영국, 독일, 프랑스의 사례를 검토하였다. 맺음말에서는 7개국 사례의 비교분석에서 도출된 각국 전략의 유사점과 차이점을 종합·요약하고, 이들 사례에 대한 비교분석이 한국의 사이버 안보 전략에 주는 함의와 향후 한국의 사이버 안보 전략 연구가 염두에 두어야 할 연구과제를 간략히 지적하였다.

II. 사이버 안보 전략의 분석틀

사이버 안보는 전통안보와 다른 특성을 지니고 있을 뿐만 아니라 상이한 환경을 배경으로 발생한다. 컴퓨터 시스템은 아무리 잘 설계되어도 외부로부터의 침투를 완벽히 막아낼 수 없기 때문에, 공격이 방어보다 유리한 게임인데다가 경우에 따라서는 피해여부와 피해대상 자체를 구분하기도 쉽지 않다. 사이버 공격의 주체도 국가 행위자들이라기보다는 주로 해커나 테러리스트 등과 같은 비국가 행위자들이 나서는 경우가 많으며, 사용되는 컴퓨터 바이러스나 악성코드, 공격기법 등이 '행위능력'을 지닌 중요한 변수가 되기도 한다. 따라서 누가 사이버 공격의 주범인지를 밝혀내기 어렵고, 그 범인을 밝힐 수 있더라도 매우 복잡한 인과관계에 기반을 두고 있어 공격의 주체와 보복의 대상을 명확히 판별하기 어렵다. 따라서 실제 범인을 색출하는 것만큼 누가 범인인지, 즉 무엇이 안보위협인지를 규정하는 '안보화(securitization)'의 과정이 중요한 변수가 되기도 한다. 이러한 맥락에서 이해한 사이버 공격은 마치 보이지 않는 위협으로서 '버추얼(virtual) 창'의 공격을 방불케 한다.

이러한 버추얼 창을 막아내기 위해서 필요한 것은, 철벽방어를 목표로 '벽돌집'을 짓는 전통적인 발상이 아니라 나뭇가지 하나하나를 모아서 '그물망'을 짜는 것과 같은 복합적인 발상이다. 시스템 차원의 불확실성이 커지는 상황에서, 전통안보에 대응하는 경우처럼, 국가가 나서 통제하고 자원동원을 집중하려는 위계조직의 발상은 효과적이지 않다. 다시 말해, 어느 한 주체가 나서서 집중적인 해법을 제시하기보다는 오히려 이해당사자들이 각기 책임지고 자신의 시스템을 보호하는 분산적 대책이 효과적일 수도 있다. 대응주체라는 점에서 국가 행위자 이외에도 민간 행위자도 참여하는 네트워크 모델이 필요하고, 동원하는 수단이라는 면에서도 기술과 인력, 국방의 역량을 강화하는 것뿐만 아니라 법제도 정비와 국제협력 등을 포

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

괄하는 복합적인 대응이 필요하다. 그리고 난 연후에 해당 당사자들이 담당할 수 없는 '구조적 공백'을 메워주는 총괄·조정의 역할이 빛을 발한다. 비유컨대, '네트워크 위협'에는 '네트워크 해법'을 찾아야 한다고 할까?(Christou, 2016)

이러한 맥락에서 볼 때 사이버 위협의 성격을 정확히 이해하고 이에 적합한 새로운 국가모델과 안보 거버넌스를 모색하는 것이 필요하다. 이와 관련하여 이 글의 논의는 네트워크 국가(network state)와 메타 거버넌스(meta governance)의 개념과 이론을 인식론적 뿌리를 두고 있다. 네트워크 국가란 대내적으로는 위계적 관료국가, 대외적으로는 영토적 국민국가의 모습을 하는 기존의 근대 국가모델이 글로벌화와 정보화 및 네트워크 시대의 변화하는 환경에 맞추어 자기변화와 구조조정을 해나가는 국가이다. 변화하는 국가의 모습은 중앙정부와 지방정부 내의 공조, 국가-민간기업-시민사회의 협업, 지역 및 글로벌 차원에서 진행되는 정부간 협력, 초국적 차원의 연결망 구축 등에서 다양하게 나타난다. 이렇게 다층적인 네트워크가 형성되어 작동하는 과정에서 중요한 국가의 역할은, 다양한 행위자들의 이해관계를 조정하고 협력을 이끌어내는 중심성(centrality) 제공의 역할, 즉 메타 거버넌스이다. 이러한 네트워크 국가의 메타 거버넌스는 행정조직들의 관할권의 경계를 넘어서 또는 공공영역과 사적영역의 구분을 넘어서, 그리고 국가의 경계를 넘어서 이루어진다(Jessop, 2003; 김상배, 2014).

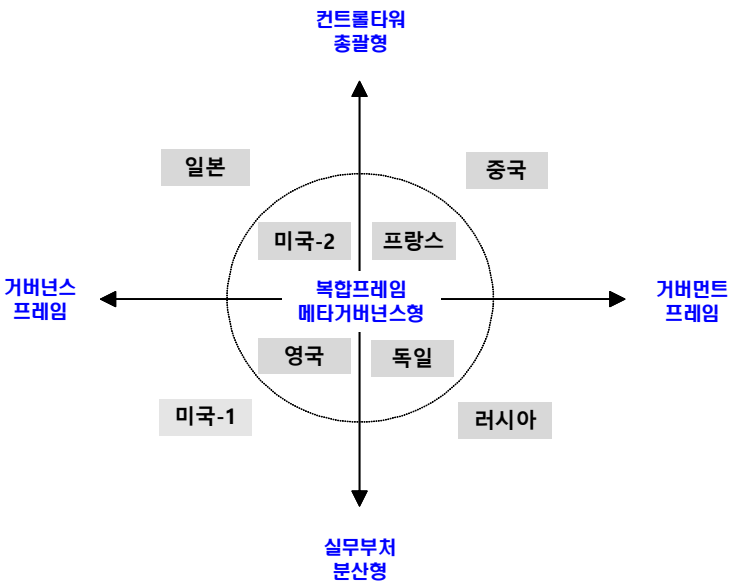
사이버 안보는 네트워크 국가의 메타 거버넌스 기능을 필요로 하는 대표적인 분야이다. 사이버 공간의 구조적 속성상 사이버 위협에 대한 예방-방어-억지-복원은, 수평적 네트워크의 형태로 활동하는 비국가 행위자들과 밀접히 협력하는 동시에 다양한 수단들을 적시적소에 유연하게 동원하는 국가의 역할이 요구되는 분야이다. 그런데 이러한 네트워크 국가와 메타 거버넌스의 역할은 국가별로 지역별로 그 진행속도와 발현형태가 다르게 나타난다. 물론 수직적 '조직'으로부터 수평적 '네트워크'로의 전반적인 변환의 추세로부터 자유로울 수 있는 나라는 없을 것이다. 그럼에도 그 변환의 추세가 수용되는 정도는 각 국가와 지역마다 다르게 나타날 수 있다. 다시 말해, 비국가 행위자들뿐만 아니라 여타 국가 행위자들을 적극적으로 네트워킹하여 대응하려는 국가가 있는가 하면, 여전히 전통적인 위계조직 모델에 기대어 새로운 위협에 대응하려는 국가도 있을 수 있다. 이러한 국가변환의 차이는 분야별로도 다르게 나타난다. 예를 들어, 전통안보 분야는 변화의 수용 정도가 느린 분야이며, 경제·문화·환경 분야는 새로운 변화를 빠르게 수용하고 있다. 이 글에서 다루는 사이버 안보 분야는 이상에서 언급한 국가변환의 추세가 빠르게 진행되는 대표적인 분야이다.

이 글은 각국의 사이버 안보 전략에서 나타나는 국가변환의 추세와 국가별 차이를 분석적으로 이해하기 위해서 두 가지의 기준을 마련하였다(〈그림-1〉). 첫째, 국가의 기능적 측면에서 본 대내외 정책지향성인데, 이는 주로 사이버 위협에 대한 기본인식과 역량강화의 전략, 사이버 국방의 전략과 역량 및 조직, 사이버 안보 분야 국제협력에 임하는 원칙, 프라이버시 보호와 국가안보 추구의 비중 등을 고려하여 판단하였다. 이러한 요소들의 복합정도에 따라서

볼 때, 사이버 안보 전략의 대내외 정책지향성은 크게 기술경제적 논리를 바탕으로 정보인프라와 지적재산의 보호를 위한 글로벌 메커니즘을 지향하는 '거버넌스 프레임'과 정치사회적 논리를 바탕으로 내정불간섭과 국가주권의 원칙에 입각해 국내체제의 안전을 관철하려는 '거버먼트 프레임,' 그리고 그 중간의 '복합 프레임'으로 나누어 볼 수 있다.

둘째, 국가의 구조적 측면에서 본 추진주체의 구성원리인데, 이는 주로 범정부 컨트롤타워의 설치여부와 소재, 전담지원기관의 설치여부, 각 실무부처의 역할과 상호 업무분장의 형태, 관련법의 제정 및 운용 방식 등을 고려하여 판단하였다. 이러한 요소들의 복합정도에 따라서 볼 때, 사이버 안보 전략의 추진체계는 크게 범정부 컨트롤타워 또는 전담지원기관이 존재하는 '컨트롤타워 총괄형'과 실무부처들의 상위에 총괄기관을 설치하지 않고 실무부처 중의 한 부처가 총괄하거나 또는 각 실무부처의 개별 거버넌스를 상호 간에 조정하는 '실무부처 분산형,' 그리고 그 중간의 '메타 거버넌스형'으로 나누어 볼 수 있다.

〈그림-1〉 사이버 안보 전략의 유형화



이러한 두 가지 분석기준으로 바탕으로 볼 때, 이 글에서 선정한 7개국의 사이버 안보 전략은 대략의 〈그림-1〉과 같이 위치지월 볼 수 있다. 미국과 일본 등으로 대변되는 서방 국가모델은 거버넌스 프레임을 지향하는 가운데 실무부처 분산형으로부터 범정부적 컨트롤타워를 설치하는 방향으로 진화하는 모델로 판단할 수 있다. 이에 비해 중국과 러시아로 대변되는 비서방 국가모델은 전반적으로 거버먼트 프레임을 지향하는 가운데 각국의 국내정치적 특

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

성에 따라서 범정부 컨트롤타워를 두거나 아니면 좀 더 비공식적인 방식으로 실무부처들의 업무를 조정하는 모델로 이해할 수 있다. 그 중간지대에 영국, 독일, 프랑스 등과 같은 유럽 국가들의 사이버 안보 전략을 설정할 수 있는데, 이들 국가는 각기 사정에 따라서 거버넌스 프레임과 거버먼트 프레임, 그리고 컨트롤타워 총괄형과 실무부처 분산형 등이 다양하게 조합되는 '복합 프레임'의 '메타 거버넌스형'이라고 볼 수 있다.

이 글에서 시도한 사이버 안보 전략의 유형 구분이 다소 도식적이라는 점은 부인할 수 없다. 이들 국가들의 전략을 서너 개의 유형을 상정하는 분석틀에 모두 담는다는 것은 무리가 없지 않다. 게다가 각국의 전략유형은 고정적인 것이 아니라 시간이 지남에 따라 진화를 거듭하고 있는 중이다. 실제로 미국의 사례는 2000년대 부시 행정부 시기의 〈미국-1〉 유형에서 2010년대 오바마 행정부의 〈미국-2〉 유형으로 진화했다. 그럼에도 이 글에서 시도한 사이버 안보 전략의 유형 구분은 비교분석의 효율성이나 실천적 함의 도출의 편의성이라는 측면에서 나름대로 유용함은 물론이다. 이하에서는 이러한 도식적 유형화의 한계를 보완하는 차원에서 7개국 사례의 구체적인 내용을 앞서 제시한 분석기준에 의거해서 하나씩 살펴보고자 한다.

III. 주변4국의 사이버 안보 전략(1): 미국과 일본

1. 미국의 사이버 안보 전략

미국에서는 1990년대에서부터 사이버 안보를 '안보화'하는 정책적 논의가 시작되었는데 2000년대 들어 9.11 테러가 발생하면서 더욱 본격화되었다. 부시 행정부는 2002년 11월 국토안보법, 12월 연방정보보안관리법(FISMA)을 제정하고 사이버 공격에 대해서 국토안보부(DHS)가 주도하는 대응체계를 갖추었다. 부시 행정부는 2003년 2월 *National Strategy to Secure Cyberspace(NSSC)*라는 전략서를 발표한 데에 이어(White House, 2003), 2008년 1월 국가안보 차원에서 사이버 안보 문제를 인식하고 대응책을 마련한 최초의 작업으로 평가받는 *Comprehensive National Cybersecurity Initiative(CNCI)*를 발표했다(White House, 2008). CNCI의 기조는 오바마 행정부에도 이어졌는데, 2009년 5월 미국 사이버 안보 전략의 근간을 형성한 전략서인 *Cyberspace Policy Review(CPR)*를 발표했다(U.S. Department of Homeland Security, 2009). CPR은 연방 정부기관에게 각기 역할과 책임을 명확히 분담하는 동시에, 사이버 안보 대응체계의 중심을 기존의 국토안보부로부터 백악관

으로 이전시켰는데, 백악관의 컨트롤타워로서 사이버안보조정관(Cybersecurity Coordinator)을 신설하였다.

이 무렵 미국의 사이버 안보 전략에는 '군사화' 담론이 강하게 가미되기 시작했는데, 이는 관련 기구의 설치와 예산증액 등으로 이어졌다. 그 중에서 가장 대표적 사례는 오바마 행정부 출범 이후 2009년 6월 창설된 사이버사령부(Cybercom)이다. 2011년 7월 국방부는 *DoD Strategy for Operating in Cyberspace*를 통해서 사이버 국방의 중요성과 능동적 방어의 필요성을 강조했다(U.S. Department of Defense, 2011). 2012년 이후 일련의 전개 과정에서 주목할 것은, 사이버 공격을 억지하기 위해서 그 진원지를 찾아 선제공격하겠다는 결연한 입장이 등장했다는 사실이다. 미 국방부는 2012년 5월 플랜-X 프로젝트를 발표했는데, 이 프로젝트는 미 국방부의 사이버 안보 전략을 증강하는 차원에서 사이버 무기 개발을 본격화하고, 전 세계 수백억 대에 달하는 컴퓨터의 위치를 식별하기 위한 사이버 전장지도를 개발하는 계획을 담고 있었다. 2012년 10월 사이버 예비군의 창설이 발표되었으며, 2013년에는 〈국방수권법(National Defense Authorization Act)〉을 통해 사이버 공간에서 군의 위상과 역할 및 권한을 강화하였다. 이러한 공세적 대응으로의 전환 구상들은 2015년 4월 발표된 *DoD Cyber Strategy*에서 더욱 구체화되었다(U.S. Department of Defense, 2015).

이러한 '안보화' 와 '군사화' 의 득세와 병행하여 미국은 국제협력의 전략도 적극적으로 추구하였다. 오바마 행정부는 2011년 5월 *International Strategy for Cyberspace(ISC)*를 발표하여 사이버 공간에서의 기본적 자유와 재산권의 존중, 프라이버시의 보호, 사이버 범죄 색출, 사이버 공격에 대한 자위권 행사 등을 위해서 국제협력이 필요하다고 역설하였다(White House, 2011). 아울러 미국은 양자 및 지역협력 차원에서 기존의 동맹을 사이버 공간에도 적용하는 전략을 추구했다. 유럽지역에서는 나토나 EU, 특히 영국과의 사이버 협력을 강화했다. 또한 아태지역에서도 일본, 호주, 한국 등과 사이버 안보 협력을 모색했다. 미국은 국제기구와 다자외교의 장에서도 사이버 안보 분야의 국제규범 형성과정에 참여했는데, 유엔 GGE나 ITU 등과 같은 기성 국제기구의 틀을 활용하기 것보다는, ICANN이나 사이버공간총회, 유럽사이버범죄협약 등과 같이 민간 이해당사자들이나 선진국 정부들이 주도하는 글로벌 거버넌스의 메커니즘에 좀 더 주력하는 모습을 보였다. 이러한 미국의 접근은, 이하에서 살펴보는 바와 같이, 중국이나 러시아로 대변되는 비서방 진영 국가들의 입장과 대립했다.

사이버 위협정보의 공유과정에서 발생하는 프라이버시와 자유의 침해 문제가 큰 논란거리였는데, 2015년 12월 위협정보의 공유를 주요 내용으로 하는 〈사이버안보법(Cybersecurity Act)〉이 최종 통과되면서 해결의 실마리를 찾았다. 사이버안보법은 단일법이 아니라 2015년 10월 상원에서 통과된 〈CISA(Cybersecurity Information Sharing Act)〉를 중심으로, 하원을 통과한 여타 법안들을 통합·조정한 수정안이다. 이 법의 제정을 통해서 사이버 안보를 위해 필요한 경우 민간 분야가 소유한 방대한 양의 개인정보를 연방 정부기관에 자발적으로

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

넘기도록 하는 정보공유체계가 구축되었다. 그 핵심 내용으로는 기관들 간의 사이버 안보 정보공유의 절차와 가이드라인 마련, 특정 개인을 식별할 수 있는 정보를 심사·삭제하는 절차 확보, 이 법에 따라 정보를 제공한 민간기관에 대한 면책 규정, 연방기관은 공유 받은 정보를 제한적으로만 사용한다는 규정 등이 포함되었다. 법안이 최초 발의된 2009년 이후 프라이버시 침해를 우려하는 정치권과 시민사회의 반대의견과 개인정보 침해에 대한 책임 부과를 우려하는 민간 기업들의 반발에 의해 법안 통과가 지연되다가 2015년에야 통과되었다.

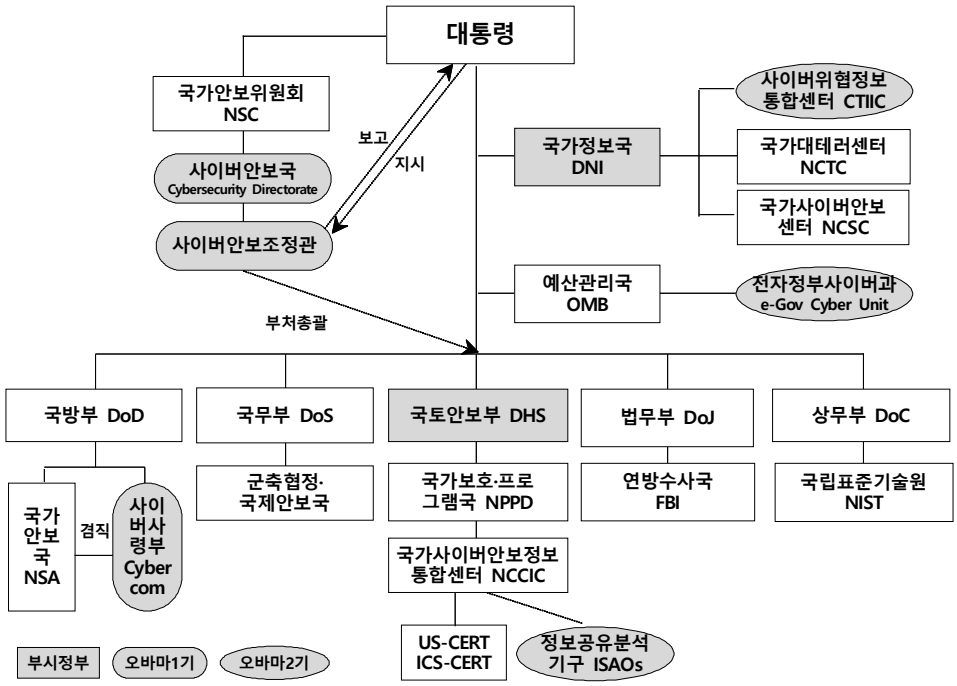
미국의 사이버 안보 추진체계는 기본적으로 연방정부의 각 기관이 각기 역할과 책임을 다하는 분산 시스템을 운영하는 가운데, 정책의 통합성을 제고하고 각 기관들의 유기적 협력을 도모하기 위한 총괄·조정 기능이 세 층위로 중첩되는 형태로 진화했다〈그림-2〉. 부시 행정부에서는 국토안보부와 국가정보국(DNI)이 총괄 기능을 수행했다. 오바마 행정부 1기에 접어들어 국가안보위원회(National Security Council, NSC) 산하 사이버안보국(Cybersecurity Directorate) 내의 사이버조정관이 국토안보부, 국가안보국, 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(Cyber Threat Intelligence Integration Center, CTIIC)가 설치되어 사이버 위협과 사고를 종합적으로 분석하여 유관기관에 정보를 제공케 했다. 예산관리국(OMB) 내에는 전자정부사이버과(E-Gov Cyber Unit)를 설치하여 연방기관의 업무를 감독·조율하게 했다. 민관협력 촉진을 위해 정보공유분석기구(Information Sharing and Analysis Organizations, ISAOs)를 설립하여, 국토안보부 산하에서 민관 정보공유를 담당하는 국가사이버안보정보통합센터(National Cybersecurity and Communications Integration Center, NCCIC)와 협력하도록 했다(신성호, 2017, p.149).

요컨대, 미국은 자국의 정보 인프라와 지적재산의 보호를 위해서 일찌감치 사이버 안보를 강조하는 전략을 추진해왔다. 더불어 억지역량의 강화라는 명목으로 군사적인 공세전략도 병행하였다. 국제협력도 양자·지역 동맹 강화와 민간 이해당사자들이 참여하는 글로벌 거버넌스의 구축을 동시에 지향하였다. 사이버 위협정보의 공유체계를 구축하는 과정에서 프라이버시 보호를 고려하는 법제도를 마련한 것은 인상적이다. 이러한 점에서 미국의 대내외 정책지향성은 기본적으로 거버넌스 프레임에 기반을 두고 있다고 보아야 할 것이다. 한편 미국에서는 실무부처들이 소관 업무를 담당하는 가운데 국토안보부가 주도하던 모델(〈그림-1〉의 좌하단)로부터 백악관이 컨트롤타워 역할을 수행하는 모델(〈그림-1〉의 좌상단)로 진화했으며, 이후에는 DNI 산하 CTIIC의 종합정보분석 역할, 전자정부사이버과의 감독·조율 역할, 국토안보부 산하 NCCIC와 ISAOs의 협력체제 구축 등의 총괄 및 지원 기능이 추가되었다. 이러한 점에서 미국의 추진체계는 실무부처의 역할을 강조하는 가운데 컨트롤타워의 총괄·조정 기능이 중층적으로 작동하는 메타 거버넌스형으로 파악할 수 있다. 그런데 2017년 들어 사이버

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

역량의 강화를 대통령 공약으로 내세운 트럼프 행정부가 출범하면서, 향후 미국의 사이버 안보 전략이 공세적인 군사화로 회귀 가능성을 안고 있다.

〈그림-2〉 미국의 사이버 안보 추진체계



출처: 임재명(2016), p.4를 부분수정

2. 일본의 사이버 안보 전략

일본은 2000년대 초반부터 'e-Japan전략'을 발표하기 시작했는데, 2006년부터는 『시큐어재팬』(2006-2009), 『정보재팬』(2010-2012), 『사이버시큐리티』(2013-) 등으로 이름을 바꾸어 가며 '정보보호 전략'을 발표했다. 2013년 6월에 이르러서는 『사이버시큐리티전략』을 발표하면서 기존의 '정보보호 전략'을 '사이버 안보 전략'으로 개명하는 인식의 변화를 보였다(情報セキュリティ政策会議, 2013a). 그 후 2015년 6월 일본연금기구에 대한 대규모 해킹 사건의 발생에 따른 충격과 2020년 개최 예정인 도쿄올림픽의 안전한 운영에 대한 우려 등이 반영되어 2015년 9월에는 기존 전략의 일부 내용을 수정하여 『사이버시큐리티전략』을 발표하기도 했다(閣議決定, 2015). 내각의 명의로 발표된 새로운 사이버 안보 전략은 자유롭고 공정한 사이버 공간의 실현을 목표로 내걸고 정보의 자유로운

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

유통, 법의 지배, 개방성, 자율성, 다양한 주체의 제휴 등을 제시하였다. 특히 컨트롤타워의 역할을 담당하는 내각사이버시큐리티센터(National center of Incident readiness and Strategy for Cybersecurity, NISC)의 기능을 강화하고, 조사 및 감시대상을 정부뿐만 아니라, 독립행정법인 및 특수법인으로 확대하는 내용을 담았다.

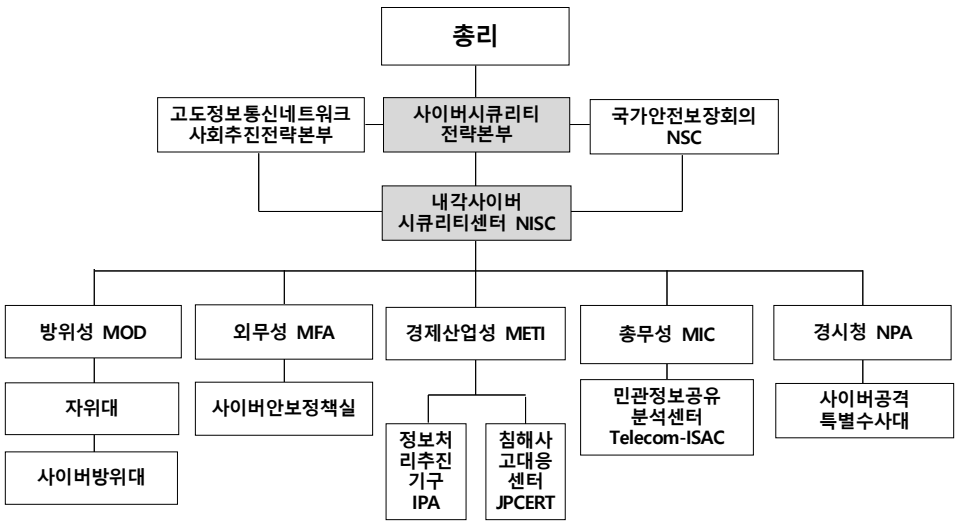
일본 방위성과 자위대는 사이버 공격에 대응하는 군사적 역량강화와 군조직 개편의 노력을 펼치고 있다. 2011년 통합막료감부 예하 지휘통신시스템부에 사이버 공간 방위대를 설치했으며, 2014년 3월 사이버 전문 인력 90명으로 구성된 사이버방위대를 새로 창설하였다. 이는 육상, 해상, 항공자위대 소속 사이버 전문 인력과 NISC의 전문 인력이 파견되어 편성된 것이었다. 이러한 조직개편의 결과로 자위대는 단순한 방어의 차원을 넘어 공격수단을 개발하고 군사작전의 일부로 사이버전을 적극 활용할 수 있는 길을 연 것으로 평가되었다(조성렬, 2016, pp.413-414). 한편 2016년 일본 『방위백서(防衛白書)』는 중국, 러시아, 북한이 일본의 핵심 기반시설을 상대로 한 사이버 공격을 벌이고 있으며, 기술적으로 더욱 교묘해지고 있다고 인식을 천명하였다(防衛省・自衛隊, 2016). 이렇듯 사이버 방어 태세를 증진시키는 노력을 펼쳐왔음에도 일본은 자원의 부족과 부처 간 조정의 어려움을 노정했으며, 좀 더 중요하게는 국가적 차원에서 사이버 안보의 위험성을 과소평가하거나 때로는 과도하게 보수적인 접근을 한다는 비판을 받기도 했다(이승주, 2017, pp.228-229).

이러한 맥락에서 2013년 2월 일본이 발표한 『사이버시큐리티국제협력전략(サイバーセキュリティ国際連携取組方針): j-initiative for Cybersecurity』는 미국을 포함한 주변국들과의 협력을 강조한 의미가 있다(情報セキュリティ政策会議, 2013b). 자국 내의 정책만으로는 모든 위협에 대응할 수 없다는 판단 하에, 타국 정부와의 협력을 통한 공조체제 구축, 국제법에 입각한 공통된 대응체계의 마련을 강조하였다. 이러한 연속선상에서 2015년 4월 미일 정상회담에서 양국은 사이버 협력이 포함된 방위협력지침 개정안에 합의했으며, 뒤이어 미일 사이버 안보 정책 실무 워킹그룹의 공동성명을 발표하기도 했다. 이러한 행보는 일본이 미국과의 협력을 통해 자체적인 사이버 안보 역량강화는 물론, 미국의 사이버 방위능력을 직접 활용하여 일본의 사이버 안보를 보장받으려는 것으로 비춰졌고, 내외신 언론에서는 이를 일본이 미국의 '사이버 우산'에 포괄되었다고 표현했다. 이러한 구도 하에서 일본은 2015년 7월 호주와 사이버 안보 협력에 합의했으며, 이밖에도 다양한 채널을 통한 양자 및 다자협력을 추구했다. 에스토니아, 영국, 프랑스, 이스라엘, 한국, EU, 인도 등과 사이버 정책대화를 진행했으며, 아세안과도 사이버 안보 협력을 강화했고, 유엔, OECD, APEC 등에서의 다자외교에도 적극적으로 임하고 있다(이승주, 2017, pp.229-236).

한편 일본은 2014년 11월 〈사이버시큐리티기본법〉을 제정하고, 2015년 1월부터 시행 중이다. 이 법은 사이버 안보 정책의 기본원칙을 규정하고, 중앙정부와 지방정부 및 기타 공공기관의 책임을 명시함으로써 사이버 안보 전략의 추진 기반을 포괄적으로 마련했다는 평가를

받았다. 특히 이 법의 제정을 통해서 일본의 사이버 안보 추진체계는 큰 변화를 맞이하였다. 그 중에서 핵심은 2015년 1월 컨트롤타워의 역할을 담당하는 사이버시큐리티전략본부와 그 산하에 전담지원기관의 역할을 수행할 내각사이버시큐리티센터(NISC)를 설치한 것이었다. 〈그림-3〉에서 보는 바와 같이, NICS는 사이버 안보의 전략안을 작성하고 국가안전보장회의(NSC)와 고도정보통신네트워크사회추진전략본부와 협력해 정부차원의 사이버 안보 정책에 대한 조정과 통제뿐만 아니라 정보 시스템에 대한 부정 활동을 감시·분석하여 대응하는 역할을 담당하고 있다(박상돈, 2015, pp.158-159). NISC가 사이버 안보 전략을 총괄·조정하는 가운데, 방위성과 자위대는 사이버 국방, 외무성은 사이버 국제협력, 경제산업성은 IT산업정책, 총무성은 통신 및 네트워크 정책, 경시청은 사이버 범죄 대응 등의 분야를 맡아서 실무부처 차원의 소관 업무를 실행하는 구도를 형성하고 있다.

〈그림-3〉 일본의 사이버 안보 추진체계



출처: 김희연(2015), p.52를 기반으로 보완하여 작성

요컨대, 2010년대 접어들어 일본의 사이버 안보 전략은 날로 늘어나고 있는 사이버 위협을 중대하게 인식하고 국가안보의 차원에서 적극적으로 대응하여 기존의 반응적 정책에서 선제적 정책으로, 수동적 정책에서 주도적 정책으로 변화를 꾀하였다. 사이버 국방 전략의 차원에서도 자위대 산하에 사이버방위대를 창설하는 등 적극적인 대응책을 모색했으며, 자체적으로 감행하기 벅찬 위험을 분담하기 위해서 전통적인 우방인 미국과의 국제협력을 강화하였다. 일본이 벌이는 사이버 안보 분야의 양자 협력이나 다자외교의 양상은 미국이 주도하는 아태

지역 전략과 글로벌 거버넌스의 구상 내에서 파악할 수 있다. 이러한 점에서 일본의 대내외적 정책지향성은 대체로 미국과 같은 거버넌스 프레임으로 파악할 수 있다. 그러나 추진주체의 구성원리라는 차원에서 일본은 미국보다는 좀 더 집중적인 형태를 갖추고 있다. 2014년 〈사이버시큐리티기본법〉 제정을 통해서 컨트롤타워의 역할을 하는 내각관방 산하의 사이버시큐리티전략본부와 전담지원기관인 NISC를 설치하여 정부기관뿐만 아니라 지방자치단체와 독립행정법인, 국립대학, 특수법인, 인가법인 등의 사이버 안보를 총괄·조정하는 체계를 갖춤으로써, 상대적으로 집중적인 컨트롤타워 총괄형을 유지하고 있는 것으로 판단된다.

IV. 주변4국의 사이버 안보 전략(2): 중국과 러시아

1. 중국의 사이버 안보 전략

중국에서는 1990년대 후반부터 금순공정(金盾工程, Golden Project)의 형태로 사이버 안보 관련 정책을 추구해 왔는데, 시진핑 체제가 본격적으로 자리를 잡으면서 좀 더 공격적으로 사이버 안보 전략을 추구하고 있다. 시진핑 주석은 2014년 2월 안전한 네트워크 구축이 향후 중국 국가이익의 핵심이 될 것이라고 전망했다(『新华网』, 2014.2.27). 이러한 기조를 이어받아 2016년 12월 중국의 사이버 안보 이념과 정책을 명확히 담은 최초의 전략서인, 『국가사이버공간안전전략(国家网络空间安全战略)』을 발표했다. 이 전략서는 사이버 주권의 중요성을 강조하면서 국가안전 유지, 정보 기반시설 보호, 사이버 문화 건설, 사이버 범죄와 테러 예방, 사이버 거버넌스 체제 개선, 사이버 안전기초 마련, 사이버 방어력 향상, 그리고 사이버 국제협력 강화 등 9개의 전략목표를 제시하였다. 특히 해킹으로 인한 국가분열이나 반란선동 기도, 국가기밀 누설 등의 행위를 중대 불법행위로 간주하고 이를 막기 위해 군사적인 수단까지 동원하겠다고 천명했다(国家互联网信息办公室, 2016).

이러한 기조는 사이버 국방 분야에서도 구체화되어 온 바 있다. 2013년 국방백서(『中国武装力量的多样化运用白皮书』)와 2015년 국방백서(『中国的军事战略白皮书』)를 통해서 기존의 방어적인 개념으로부터 사이버 공격에 대한 보복공격까지도 포함하는 '적극적 방어' 전략으로 이행을 천명한 바 있다(国务院新闻办公室, 2013; 2015). 이러한 전략의 변화는 사이버전 수행 군부대의 변천과 연동해서 이해할 필요가 있다. 중국에서는 1997년 4월 컴퓨터 바이러스 부대, 2000년 2월 해커부대(Net Force), 2003년 7월에는 4개 군구 예하에 전자전 부대가 창설되었다. 2010년 7월에는 인민해방군 총참모부 산하에, 미국의 사이버사령부에 해

당하는, 인터넷기초총부를 창설했다. 총참모부 산하 3부서는 사이버 작전을 수행하고 있는데, 지난 수년간 미국 정부기관과 기업 등을 해킹한 것으로 의심을 받고 있는 61398부대는 3부서 소속이다(정종필 · 조윤영, 2017, pp.182-183). 2015년 10월에는 중국군이 군 개혁의 일환으로 사이버전통합사령부를 창설할 것을 천명했다(『연합뉴스』, 2015.10.26). 2016년 1월에는 군구조 개혁에 따라 사이버군이 포함된 전략지원부대가 창설되어 정보수집, 기술정찰, 전자대항, 사이버 방어 및 공격, 심리전을 수행하게 되었다(『腾讯新闻』, 2016.1.1).

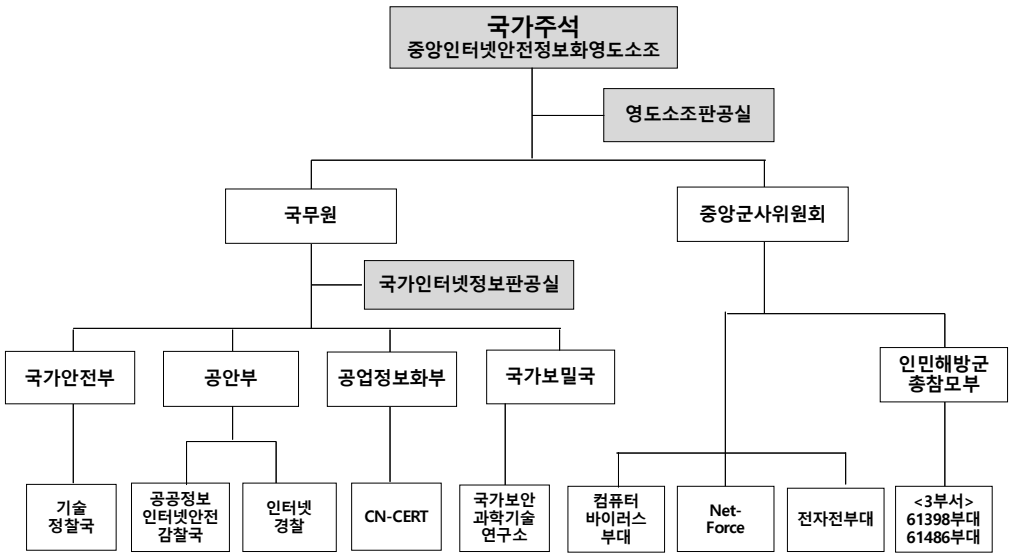
중국이 추진하는 사이버 안보 분야 국제협력 전략의 기조는 사이버 주권과 내정불간섭의 원칙을 기반으로 미국의 사이버 패권에 대항하는 국제 연합전선의 구축이다. 특히 2013년 스노든 사건 이후 중국은 글로벌 인터넷 거버넌스를 주도하는 미국을 견제하며, 중국이 중심이 되는 사이버 진영 건설을 목표로 국제협력을 강화하고 있다. 대표적인 사례가 중국이 주도하여 2014년부터 2016년까지 중국 우전에서 개최한 세계인터넷대회(World Internet Conference)인데, 중국은 각국의 사이버 주권을 강조하며 안전한 사이버 공간의 구축을 위한 국제연대를 주창했다. 중국은 상하이협력기구(SCO), 아세안지역포럼(ARF) 등과 같은 지역협력기구에서의 사이버 안보에 대한 논의에도 적극적으로 참여할 뿐만 아니라 유엔 GGE나 ITU 등과 같은 전통 국제기구의 틀을 빌어서 진행되는 국제규범 형성과정에도 적극적으로 나서고 있다. 이러한 중국의 국제협력 전략 기조는 2017년에 발표된 『사이버공간국제협력전략(网络空间国际合作战略)』에서도 강조되었다(国家互联网信息办公室, 2017).

사이버 안보와 관련된 중국의 국가주권 수호의 의지는 관련법의 제정 과정에서도 나타났다. 2015년 7월 중국 전국인민대표대회가 〈신국가안전법〉을 통과시키면서 사이버 공간의 테러와 해킹에 대응하는 중국의 주권수호 활동의 명분을 마련하였다(『보안뉴스』, 2015.7.6). 발표 직후 〈신국가안전법〉은 서방 언론으로부터 사이버 안보 강화라는 명분으로 "사회에 전방위적인 통제를 가하고... 공산당 정권의 안전을 보호하기 위한 기반" 을 마련함으로써, 외국계 기업의 활동을 통제하려 한다는 비판을 받았다(『한겨레신문』, 2015.7.1). 한편 2016년 12월에는 〈인터넷안전법〉이, 2017년 6월 1일 시행될 예정으로, 제정되었다. 〈인터넷안전법〉은 핵심 기반시설의 보안 심사 및 안전 평가, 온라인 실명제 도입, 핵심 기반시설 관련 개인정보의 중국 현지서버 저장 의무화, 인터넷 검열 및 정부당국 개입 명문화, 사업자의 불법정보 차단 전달 의무화, 인터넷 관련 제품 또는 서비스에 대한 규제 등을 주요 내용으로 하고 있다(『KOTRA 해외시장뉴스』 2016.11.28).

중국에서는 2014년 2월 공산당 정치국 및 상무위원회 산하에 국가주석을 조장으로 하는 중앙인터넷안전정보화영도소조가 신설되어 사이버 안보와 인터넷 관리 · 단속을 총괄하고 있으며, 사무기구로 중앙인터넷안전정보화영도소조판공실이 설치되어 있다(〈그림-4〉). 국무원 차원에서는 2011년 설립된 국가인터넷정보판공실이 사이버 관련 정부 부처들이 인터넷 정보관리를 강화하도록 지도 · 감독하고, 인터넷 뉴스 및 기타 업무에 대한 허가 및 감독권을 갖

고 있다. 실무부처 차원에서 국가안전부가 국내적 차원에서 사이버 안보 업무를 총괄하는 한편, 산하의 기술정찰국을 통해 사이버 보안정책을 수립하는 역할을 수행하고 있다. 공안부는 주로 국가 기밀 보호를 위한 역할을 수행하는데, 그 산하의 인터넷 경찰은 사이버 범죄 퇴치와 인터넷 반체제 운동에 대한 감시 활동을 하고 있다. 공업정보화부는 장비개발과 자주혁신을 통해 정보화를 추진하는데, 그 산하의 침해사고대응센터(CN-CERT)는 민간분야의 사이버 침해사고 조사 및 대응활동을 벌인다. 국가보밀국은 보안 감사, 보안정책 수립, 통제 감독 등 공공기관의 보안 업무 전반을 관장하고 있으며, 그 산하에 국가보안과학기술연구소를 운영하고 있다(양정윤 · 배선아 · 김규동, 2015).

〈그림-4〉 중국의 사이버 안보 추진체계



출처: 김희연(2015), p.49를 수정 · 보완

요컨대, 중국의 사이버 안보 전략은 자국 핵심 기반시설에 대한 사이버 공격의 위협뿐만 아니라 미국에 의한 국가주권의 침해에 대한 방어적 태도를 바탕에 깔고 있다. 그러나 시진핑 시대에 접어들어 공세적인 방향으로 전략이 설정되고 있는데 이는 국방전략의 구체화나 사이버전을 담당하는 전략지원부대의 창설 등을 통해서 가시화되었다. 국제협력 전략의 지향성도 미국이 주도하는 글로벌 거버넌스의 질서구축에 대항하여 중국 주도의 새로운 사이버 질서를 모색하는데, 중국의 입장에 동조하는 국가들과 지역협력과 국제기구 활동의 보조를 맞추고 있다. 최근 제정된 〈사이버안보법〉은, 미국의 경우처럼 프라이버시 보호나 자유의 보장

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

이라는 가치를 추구하기보다는, 국내사회의 통제와 외국기업에 대한 규제 등을 목적으로 한다. 이런 점에서 파악된 중국의 대내외 정책지향성은 전형적인 거버먼트 프레임이라고 할 수 있다. 사이버 안보 전략의 추진체계는 중앙인터넷안전정보화영도소조의 지도하에 작동하는 전형적인 컨트롤타워 총괄형이며, 국가안전부, 공안부, 공업정보화부, 국가보밀국 등의 각 실무부처가 사이버 안보와 인터넷 통제의 업무를 담당하고 있다.

2. 러시아의 사이버 안보 전략

사이버 안보에 관한 러시아의 전략은, 서방 국가들의 경우와 같이, 문서로 정리되어 발표된 것이 없다. 2000년 9월에 발표된 『러시아연방 정보보안 독트린(Doctrine of the Information Security of the Russian Federation)』 정도가 있을 뿐이다(President of the Russian Federation, 2000). 러시아의 사이버 안보에 대한 관심이 본격화된 시점은 2010년 미국과 이스라엘이 스턱스넷으로 이란의 핵 시설을 공격한 이후라고 알려져 있다(『Russia포커스』, 2016.12.14). 이후 2016년 12월 푸틴 대통령은 러시아 연방보안부(FSB)가 작성한 새로운 정보보안 독트린을 승인했다(President of the Russian Federation, 2016). 신 독트린에는 러시아가 직면한 주요 위협 중 하나가 "주변국이 군사적 목적으로 러시아의 정보 인프라에 대한 영향력을 확대하는 것"이라는 우려를 표명했다. 신 독트린은 "국가 정보기관들이 주권을 훼손하고 다른 국가의 영토 보전에 손상을 입히며 세계에 불안정한 상황을 몰고 오는 사이버 심리전을 이용하고 있다"고 명시했다. 신 독트린은 법률이 아니어서 직접적인 효력은 없지만, 2013년 FSB가 마련한 법안이 뒷전으로 밀려있는 상황에서, 후속 문건이나 법률을 만드는 데 필요한 기반이 될 것이라는 평가이다(『Sputnik 코리아』, 2016.12.6).

러시아는 2002년 세계에서 처음으로 해커부대를 창설하였으며 사이버 전문 인력의 양성과 기술개발을 적극 추진하여 물리적 전쟁을 위한 지원역량으로 사이버 공격을 활용해왔다. 2008년 8월 조지아에 대한 군사작전에서 사이버전을 병행했으나 제대로 이루어지지 못했다는 자체 평가에 따라 러시아군 내에 사이버전을 전담하는 사이버전 부대를 창설하였는데, 이는 러시아가 적극적인 공세정책으로 전환하는 상징적 사건으로 이해되었다(신범식, 2017, p.260). 그 뒤 2013년에는 국방장관의 검토 지시에 따라 '사이버사령부' 창설 논의가 진행된 것으로 알려졌다. 2014년 5월에는 러시아 군지휘통신체계 보안을 위한 사이버전 부대가 창설됐다는 발표가 있었다. 이후 2015년 2월에는 『2020 러시아군 정보통신기술 발전구상』이 서명되었으며, 동년 3월에는 스마트 무기에 기반을 두고 러시아군의 사이버전 역량을 더욱 강화한다는 발표가 있었다. 또한 러시아 국방부는 2015년 10-11월 크림 반도에 독립 사이버 부대를 창설할 계획을 밝혔다(『Russia포커스』, 2015.6.26.).

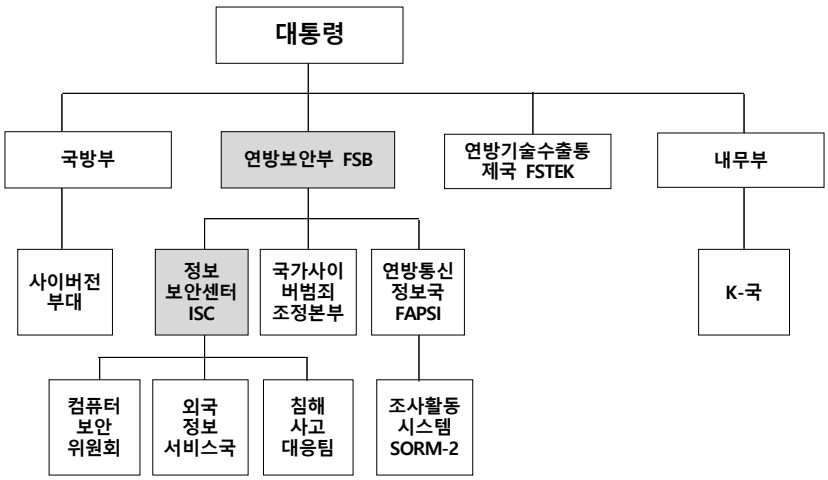
사이버 안보 국제협력과 관련하여 러시아는 스노든 사건 이후인 2013년 7월 러시아 대통령 명령으로 『2020년 국제정보안보정책기본원칙』을 발표하여 주권국가의 내정간섭을 포함한 극단주의적 목적으로 감행되는 사이버 위협에 대응하기 위한 국제협력을 강조하였다(President of the Russian Federation, 2013). 스노든 사태에도 불구하고 러시아는 미국과의 상호협력을 계속하다가, 2014년 2월 우크라이나 사태 이후 미러관계가 악화되면서 소강상태를 맞고 있다. 이에 비해 러시아와 중국의 협력은 진전되어, 2015년 5월 양국은 사이버 안보 협약을 체결하였다. 러시아는 서방 진영의 입장에 반대하여 사이버 공간에서도 국가주권이 존중되어야 한다는 주장을 펼치고 있으며, 이를 지원하는 우호세력의 확보를 위해서 집단안보조약기구(CSTO), 상하이협력기구(SCO), 독립국가연합(CIS) 등과 같은 지역협력기구 활동에 참여하고 있다. 이외에도 러시아는 브릭스(BRICS) 국가들과도 사이버 안보 분야의 공동보조를 맞추기 위한 협의도 진행해 왔으며, 유럽안보협력기구(OSCE)나 아시아안보포럼(ARF)의 사이버 안보 협의에도 적극 참여하고 있다(신범식, 2017, pp.262-266).

러시아에서 정보보안 관련 법제도의 발전은 국제적 기준에 맞추기보다는 오히려 러시아의 독자적인 발전방향을 모색해 왔다. 러시아는 1996년 2월 독립국가연합(CIS) 구성원들과 협력하여 기본형법을 채택하는 과정에서 컴퓨터 범죄에 대한 형사상의 책임을 적시하였다. 이러한 형사규정은, 타자의 컴퓨터 정보에 관한 불법적 접근, 유해 컴퓨터 프로그램의 제작, 사용 및 유포 등을 처벌하는 법적 근거가 되고 있으며, 컴퓨터 시스템 및 네트워크 운용을 위한 규정 위반에도 적용된다. 이외의 사이버 안보와 관련하여 러시아가 원용하고 있는 관련 법률로 2006년 7월 발효된 러시아 연방 법률인 〈정보, 정보기술 및 정보보호법〉을 들 수 있는데, 이는 각급 기관에서 정보시스템을 구축할 때에 보안시스템에 대한 대책을 마련하고, 이밖에도 접근이 제한된 정보의 비밀성을 지키고, 동시에 적절한 정보 접근을 실현하기 위한 법률적·기술적 조치들을 담고 있다. 그러나 아직 러시아는 독립적인 사이버안보법을 제정하지 않고 있으며, 앞서 언급한 정보보안 독트린이 이를 대체하고 있다(신범식, 2017, pp.255-256).

러시아의 사이버 안보 추진체계는 연방보안부(FSB)가 관련 기관을 총괄하는 구조로 되어 있다(〈그림-5〉). 연방보안부는 국가비밀을 포함한 주요 정보에 대한 통제와 예방 조치는 물론, 관련 기관에 대해 기술 및 암호 서비스를 제공한다. 연방보안부 산하 정보보안센터(ISC)는 통신보안 업무와 정보보호 시스템의 평가 및 인증을 총괄·조정하고, 침해사고대응팀(RU-CERT)을 운영하며, 비밀리에 공격기술을 개발하고 각급 정보를 수집하는 업무까지도 담당하고 있다고 한다. 한편 연방보안부 산하에는 국가사이버범죄조정본부라는 특수분과가 설치돼 러시아 연방기관들의 인터넷 홈페이지 보안을 담당하고 있는 것으로 알려져 있다(『Russia포커스』, 2015.6.26.). 또한 정보 및 보안기관 중에서 예산을 가장 많이 사용하는 연방통신정보국(FAPSI)에서는 조사활동시스템(SORM-2)의 프로그램을 이용해 러시아 내의 인터넷 서비스망을 통해 광범위한 정보를 수집하고 있다. 그리고 연방기술수출통제국

(FSTEK)에서는 국가정책의 시행과 부처 간 정책 조정 및 협조 그리고 정보보호 문제 등에 대한 통제 기능을 수행하고 있다(신범식, 2017, p.255). 이밖에 해킹 및 정보활동을 담당하는 내무부의 K국(Directorate K)에도 주목할 필요가 있다(조성렬, 2016, p.403).

〈그림-5〉 러시아의 사이버 안보 추진체계



출처: 조성렬(2016), p.405를 수정 · 보완

요컨대, 러시아 사이버 안보 전략의 기본방향은 정보 인프라나 지적재산의 보호보다는 러시아 정치사회체제의 안전을 확보하는 데 두어져 있었다. 그러나 2010년대 들어서 사이버 환경의 변화에 직면하여 국방전략의 관점에서 본 사이버 안보 대책들을 강조하는 방향으로 진화하고 있다. 특히 여타 국가에 비해서 일찌감치 시작한 사이버 부대의 운영이나 사이버사령부의 창설 논의 등을 통해서 적극적이고 공세적인 대책들을 마련하고 있다. 국제협력의 추구에 있어서는 기존의 국제기구나 지역협력체의 틀을 활용하여 주권국가들이 협의하는 사이버 안보 질서 모색의 선봉에 나서고 있다. 한편 러시아에서 정보보안 관련 법제도는 아직 독립법 체계를 갖추는 데까지 나가고 있지는 않으며, 정보보안 독트린과 같은 러시아만의 독자적인 형식을 고수하고 있다. 전반적으로 러시아 사이버 안보 전략의 대내외 정책지향성은 개인 권리보다는 국가주권이 강조되는 전형적인 거버먼트 프레임으로 파악된다. 한편 사이버 안보 추진체계는 범정부적으로 총괄하는 컨트롤타워를 제도적으로 설치하기보다는 정보기관인 연방보안부(FSB)와 그 산하의 정보보안센터(ISC)가 주도하는 사실상의 총괄 메커니즘이 작동하는 모습이다. 그러나 전반적으로 공식 컨트롤타워가 없는 실무부처 분산형의 사례로 보는 것이 맞다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

V. 유럽 주요3국의 사이버 안보 전략

1. 영국의 사이버 안보 전략

영국은 2009년 6월 처음으로 사이버 안보 전략을 발표한 이후, 2011년 11월 내각부(Cabinet Office) 명의로 *The UK Cyber Security Strategy*를 발표하여 공공 · 민간 · 국제 협력을 통한 안전한 사이버 공간의 구현을 강조하였다(Cabinet Office, 2011). 2013년 3월에는 정부와 업체 간의 효율적인 정보공유를 위해 *Cyber Security Information Sharing Partnership(CISP)*이라는 전략서를 발표했다(Cabinet Office, 2013). 2013년 12월에는 네트워크의 복원력 강화를 강조한, *The National Cyber Security Our Forward Plans*를 발표하였다(Cabinet Office, 2013). 2016년 11월에 이르러 영국은 사이버 안보 주무 부처인 내각부와 재무부가 주도하여 *National Cyber Security Strategy 2016-2021*라는 제목으로 새로운 전략서를 발표하였다. 이 전략서는 방어, 억지, 개발이라는 3대 목표를 설정하고 다양한 실행과제들을 제시하였으며, 국제협력의 차원에서 우방 국가들과의 양자협력과 유엔, EU, 나토 등을 통한 다자 파트너십의 구축을 강화한다는 입장을 천명하였다(Government of the United Kingdom, 2016).

영국은 2013년 새로운 사이버 부대 창설을 발표했는데, 이 부대는 정규군과 함께 임무를 맡게 되며, 컴퓨터 전문가를 비롯한 수백 명의 예비군으로 구성된다고 알려졌다. 2015년 11월 영국은 사이버군의 해킹능력 강화를 골자로 하는, *National Security Strategy and Strategic Defence and Security Review*라는 제목의 보고서를 발표하였다(Joint Committee on the National Security Strategy, 2015). 사이버 작전역량 강화의 임무는 영국 국방부와 정보기관인 정보통신본부(Government Communications Headquarters, GCHQ)가 맡았다. 앞서 언급한 2016년 *National Cyber Security Strategy*에 이르러서는, 사이버 공격 역량 향상을 위한 '사이버공격프로그램(National Offensive Cyber Programme)' 의 구축이 제시되기도 했다. 2016년 전략서는 사이버 공격으로부터 영국의 핵심 기반시설을 방어하는 것뿐만 아니라 예방 및 선제공격, 그리고 더 나아가 보복 공격까지 고려하겠다는 강력한 의지를 드러내기도 했다(Government of the United Kingdom, 2016).

이러한 국가 사이버 전략을 수행하는 데 있어 영국은 국제협력의 중요성을 강조하는데, 2016년 전략서는 영국이 추구하는 사이버 외교의 방향이 사이버 공간에서 국제법의 적용을 강화하고, 자발적이고 비구속적인 규범에 대한 합의를 촉진하며, 신뢰 구축을 실천하는 데 있음을 명시했다. 또한 영국은 2011년부터 이른바 '런던 프로세스' 로 알려진 사이버공간총회

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

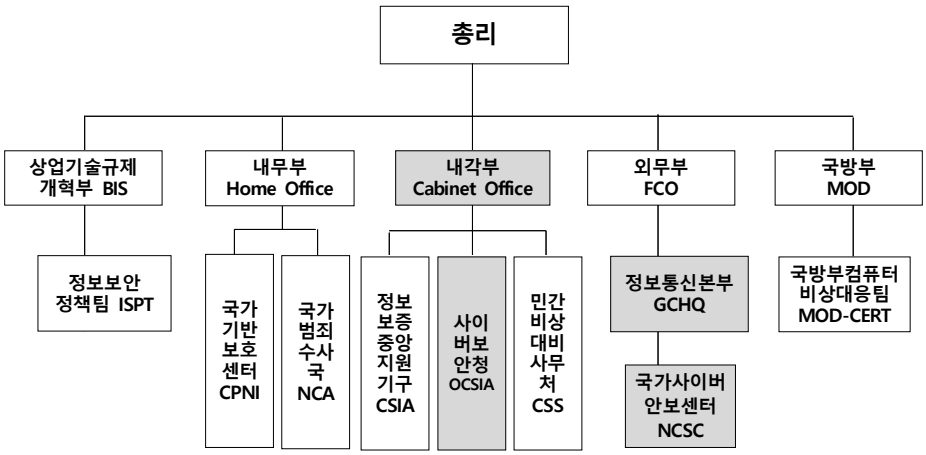
를 새로이 주도하며 자유롭고 개방적이며 평화롭고 안전한 사이버 공간에 대한 국제적인 합의를 이끌어내는 데 노력을 기울이고 있다. 또한 유엔, G20, EU, 나토, OSCE 등과 같은 기존의 국제기구와 다자외교의 프레임워크를 활용한 국제공조에도 참여하고 있다. 한편, 양자 협력의 차원에서는 2015년 1월 미국과 사이버 안보 역량 강화를 위한 양국 간 협력 프로그램의 진행에 합의했는데, 양국은 사이버 해킹에 대한 좀 더 폭넓은 대응을 위해 사이버 워게임을 합동으로 추진할 계획을 밝히기도 했다(『KISTI 글로벌 동향 브리핑』, 2015.1.21). 이러한 영미 밀월관계와 다소 모순이 될 수도 있지만, 2015년 10월 영국과 중국은 사이버 안보 협정을 체결하고 상호 간에 사이버 첩보활동을 벌이지 않겠다고 합의하기도 했다(『연합뉴스』, 2015.10.22).

한편, 영국은 2016년 11월 새로운 감시법인 〈수사권 법안(Investigatory Powers Bill)〉을 입법화했는데, 이 법은 프라이버시 침해의 여지가 상당하여 일명 '엿보기법(snooper's charter)'이라고 불렸다. 이 법은 2015년 11월 초안이 공개된 이후 프라이버시를 침해하는 법안이라는 거센 비판에 직면했었다. 그러나 파리 연쇄테러 등 유럽 대륙에서 테러가 잇따르는 가운데, 영국이 프라이버시의 침해 가능성보다는 국가안보 차원에서 본 대테러와 사이버 안보 대응체계 확립에 우선적 가치를 부여하면서 궁극적으로 법안이 통과된 것이었다. 이 법의 주요 내용으로는 인터넷 서비스 업체와 통신업체에 이용자가 웹사이트, 앱, 메시징서비스 등을 방문한 기록을 12개월 동안 보관하도록 요구하는 것이나 이들 정보에 경찰과 보안당국, 정부부처, 세관 등의 접근이 가능하고, 정보기관과 경찰이 사망, 부상, 신체적 또는 정신적 건강의 손상을 예방할 목적으로 '장비 개입'(데이터 해킹 행위)하는 행위를 허용하는 등이 담겼다(『연합뉴스』, 2016.11.30).

영국의 사이버 안보 추진체계는 내각부(Cabinet Office)가 총괄하는 형태를 취하고 있는 가운데, 해외 부문은 외무부 정보통신본부(GCHQ)가 주요 역할을 하는 일종의 이원시스템으로 되어 있다(〈그림-6〉). 내각부는 정보보증중앙지원기구(CSIA), 사이버보안청(OCSIA), 민간비상대비사무처(CSS) 등 산하 기관을 통해 사이버 안보 정책의 일관성을 제고하는 업무를 수행하고 있다. 이 중에서 2009년 설치된 사이버보안청(OCSIA)은 20개 정부부처 및 공공기관에 대한 전략방향 설정, 사이버 보안 프로그램 조정, 사이버 보안 정보인증 등의 업무를 관할한다(배병환 · 강원영 · 김정희, 2014, p.9). 이러한 내각부 총괄체제와 병행하여 영국은 대외적 사이버 안보위협에 신속하게 대처하기 위해서 정보기관들이 각기 역할을 담당하고 있다. 특히 정보통신본부는 사이버 안보 관련 정보의 수집과 암호해독 등의 업무를 수행해왔다. 2016년 10월 정보통신본부 산하에 신설된 국가사이버안보센터(National Cyber Security Center, NCSC)는 외부의 사이버 공격, 조직화된 사이버 범죄 및 테러로부터 각 부처와 민간 기업을 보호하고 침해사고에 대한 효과적인 대응과 모니터링을 실시하고 있다. 또한 정보통신본부는 내무부 보안정보부(MI5) 산하 국가기반보호센터(Center for the Protection of

National Infrastructure, CPNI), 국방부(Ministry of Defence) 등과 협력하고 있다.

〈그림-6〉 영국의 사이버 안보 추진체계



출처: 배병환 · 송은지(2014), p.9를 수정 · 보완

요컨대, 영국의 사이버 안보 전략은 핵심 기반시설의 안전을 확보하고 사이버 공격, 특히 사이버 범죄에 대응하는 역량과 네트워크의 복원력을 강조하는 기조를 유지하고 있다. 민간 부문의 사이버 활동과 경제 활성화를 우선시하지만, 최근에는 국방부문에서 보복공격까지도 언급할 정도로 강경한 태도를 드러내고 있다. 대외적인 방어를 위해서 국방부와 외교부 산하 정보통신본부가 특별 프로그램을 수립하고, 사이버 부대를 창설하는 대응책을 마련하였지만, 아직 사이버 사령부를 창설하는 수준에는 이르지 않고 있다. 국제협력의 지향성은 런던 프로세스의 추진에서 드러난 바와 같이, 신뢰구축과 자발적이고 비구속적인 규범의 도출에 중점을 둔다. 최근에는 사이버 위협정보에 대한 규정을 담은 〈수사권 법안〉이 통과됨으로써 프라이버시 보호보다는 테러와 범죄를 막는 권한강화에 무게중심을 두고 있다. 대내외 정책지향성은 복합적인 양상을 보이지만 기본적으로는 거버넌스 프레임으로 볼 수 있다. 한편 추진체계의 구성이라는 점에서 정부기관들의 사이버 안보 업무는 내각부가 총괄하지만 범정부 컨트롤타워가 설치된 것으로 보기는 어렵고, 사이버 안보 대응체계의 대외부문은 외교부 산하 정보통신본부(GCHQ) 산하의 국가사이버안보센터(NCSC)를 통해서 관련 기관들과 협력하는 체계를 운영하고 있는 것이 특기할 만하다. 이원모델 또는 메타모델의 성격이 없지 않지만, 굳이 따지자면 실무부처 분산형의 응용모델이라고 보는 것이 맞다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

2. 독일의 사이버 안보 전략

독일 사이버 안보 전략의 특징은 2011년 2월 연방 내무부(BMI)가 발표한 Cyber Security Strategy for Germany(CSSG)라는 전략서에 드러난 바 있다. 이 전략서에 의하면, 사이버 안보는 민간을 중심으로 이루어져야 하지만, 동시에 군대의 조치에 의해 보완되어야 한다고 밝히고 있다(Federal Ministry of the Interior, 2011). 이는 사이버전에서 실제 군사력의 사용을 배제하지 않는 미국의 경우와 유사하며, 예방 차원의 조치가 실제 무력 사용, 즉 자위권의 동원으로 이어질 수도 있음을 암시한다는 점에서 주목할 필요가 있다. 2016년 11월 연방 내무부에서 발표한 사이버 안보 전략도 2011년의 전략을 기반으로 수립되었는데, 그 기조가 시스템 및 시설 보호조치 중심에서 개인 및 기업 중심의 보호 및 새로운 사이버 위협 대비로 이동하였다(Federal Ministry of the Interior, 2016). 특히 2016년 사이버 안보 전략서는 4대 활동영역을 중심으로 구성되었는데, 디지털 환경에서 안전하게 스스로 결정하는 행위, 국가와 경제 분야의 공동 임무, 능률적이고 지속적인 국가 사이버 안보 아키텍처, 유럽 및 국제 사이버 안보 정책에서의 독일의 적극적 포지셔닝 등을 강조하고 있다.

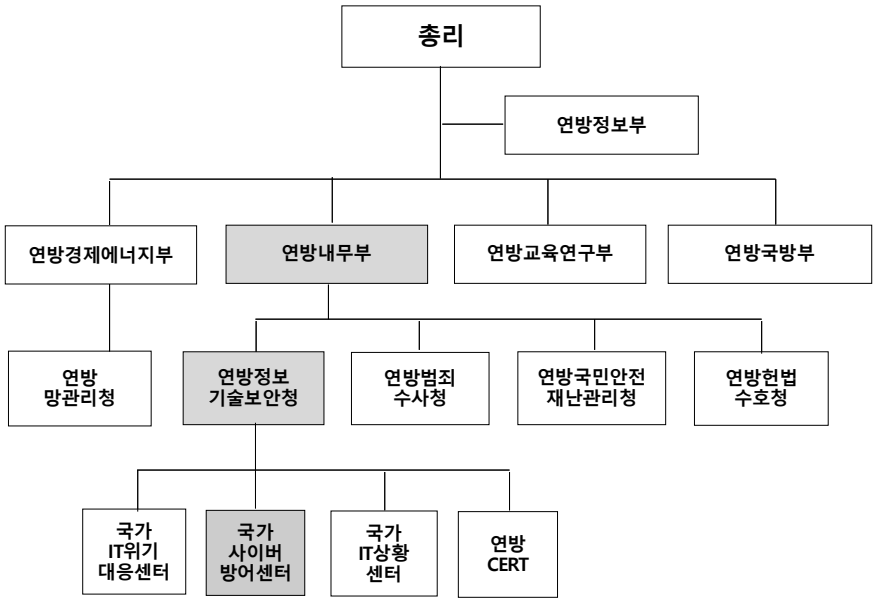
독일은 나토 국가 중에서 사이버 부대를 운영하는 첫 번째 나라로 등장하였다. 2009년 76명의 군인으로 구성된 사이버 해킹 부대를 창설했는데, 국방 차원에서 사이버 공격으로부터 국가 기반시설을 방어하기 위한 임무를 수행하였다. 이 부대를 모체로 2011년 1월에는 사이버국방센터가 신설되기도 했다. 앞서 언급한, 2016년의 독일 사이버 안보 전략서도 전반적으로 정보통신산업이나 프라이버시의 보호 측면보다는 주요 기반시설에 대한 사이버 방위 강화를 강조하였다. 이렇게 사이버 방위가 강조되면서 EU보다는 나토에서의 활동이 강조되었는데, 나토를 사이버 방위에 적극 활용하여 물리전과 사이버전이 결합된 하이브리드 위협에 맞서 억지력과 방위력을 증가시키는 것을 강조하였다. 독일이 하이브리드 전에 맞서 방위력을 증가시키고 사이버전을 군이 개입하는 군사영역으로 상정하는 점들은 러시아와 대립하고 있는 유럽 국가들의 상황을 반영한 것이기도 했다. 한편, 2017년 4월에는 사이버 맞대응 부대 창설하였는데, 1만 3,500명 규모의 부대로 확대할 예정인 것으로 보도되었다(『연합뉴스』, 2017.4.6.).

2011년 전략서는 사이버 공간을 보호하기 위해서는 국제사회의 통합성과 역량 제고를 강조하고 있다. 다만, 국제공조에서 국가 단위를 언급하기보다는 유엔, EU, 나토, G8 등 다자기구와의 협력을 강조하고 있다는 점이 특징이다(Federal Ministry of the Interior, 2011). 또한 2016년 전략서는, EU와 나토의 테두리 안에서 경찰과 사법부가 협력하고 공동으로 대외정책을 수행함으로써 유럽의 사이버 안보 정책 수립과정에서 입지를 확보할 것을 거론하고 있다. 이러한 맥락에서 독일은 유럽의 사이버범죄협약에 따라 사이버 범죄 수사를 하고 있으며, 독일의 사이버 역량을 주변국에게 지원하여 우호적인 관계를 유지하고자 양자 및 지역

협력에 주력하고 있다(Federal Ministry of the Interior, 2016). 한편 미국과의 관계는, 2013년 스노든 사건 이후 다소 소원한데, 미국의 스파이 활동에 반발하여 자국의 사이버 역량을 제고시키는 반편, 양국 간의 사이버 안보 협력에는 적극적인 태도를 드러내지 않고 있다.

그 대신 독일은 〈IT 안보법(IT Security Act)〉 제정 등을 통해 IT시스템의 보안을 제고하기 위한 조치에 나섰다. 2015년 7월부터 시행된 〈IT 안보법〉은 2011년의 사이버 안보 전략(CSSG)을 구체화한 최초의 결과물로 평가된다. 단일법이 아니라 〈연방정보기술보안청법(BSIG)〉, 〈전기통신법(TKG)〉, 〈텔레미디어법(TMG), 〈연방범죄수사청법(BKAG)〉의 규정 중 사이버 안보와 관련된 규정을 일괄 정비한 법률이다. 이 법을 통해서 독일 연방정부는 IT시스템 또는 디지털 세계의 안전과 무결성에 대한 신뢰 없이는 경제적, 사회적 잠재력을 성장시킬 수 믿음을 바탕으로, 국가가 인터넷에서의 위험과 범죄를 효과적으로 방어할 책임을 지고 있다고 강조하였다(김도승, 2017). 독일 사이버 안보 전략의 전반적 특징은 프라이버시 보호를 강조하기보다는 사이버 국가안보 강화에 치중하고 있다는 점에서 발견된다. 이러한 양상은 연방정부-주정부-지자체 간의 사이버 안보 거버넌스를 정립하는 과정에서 연방정부와 주정부 간에 위협정보 이전을 의무화한 대목에서도 드러난다.

〈그림-7〉 독일의 사이버 안보 추진체계



출처: 김도승(2017), p.29를 수정 · 보완

연방제 국가인 독일은 연방 내무부과 그 산하의 연방 정보기술보안청(BSI)을 중심으로 연방 경제에너지부, 연방 교육연구부, 연방 국방부 등이 사이버 안보와 관련된 역할을 분담하는 형태를 취하고 있다(〈그림-7〉). 연방 정보기술보안청(BSI)은 기술 업무뿐만 아니라, 사법적 임무 수행 지원, 테러정보 수집 및 평가, 정보보안 관련 자문 등 광범위한 사이버 안보 업무를 총괄·집행하고 있다. 연방정보기술보안청 산하 국가사이버방어센터(Cyber-AZ)는 여러 기관에서 동시에 사고가 발생할 경우 위기대응을 주도하며 연방정부를 포함한 모든 주체들을 총괄하는 역할을 담당한다. 또한 2016년 전략서에 의해서, 연방 정보기술보안청 내에 모바일 사고대응팀(MIRTs)이 신설되어 보안 사고의 기술적 처리를 위한 신속하고 유연한 대응을 지원하도록 했다. 이외에도 내무부 산하의 연방범죄수사청(BKA)은 사이버 범죄를 수사하며 특별수사기관(QRF)을 설립하고, 연방헌법수호청(BfV)은 연방정부 차원에서 외국 정보기관 및 극단주의자와 테러리스트들의 활동을 모니터링하고 있다.

요컨대, 대내외 정책지향성이라는 차원에서 볼 때, 독일의 사이버 안보 전략은 정보통신산업이나 프라이버시 보호보다는 주요 기반시설에 대한 사이버 방위에 상대적으로 많은 관심을 기울이고 있다. 사이버 위협의 원인으로서 러시아를 상정할 수밖에 없는 독일의 상황이 사이버전을 포함한 하이브리드 위협에 맞서 군사 담론과 정책이 주도하는 국가사회적 분위기를 창출한 것으로 판단된다. 이러한 경향은 독일의 국제협력 전략에서도 나타나는데, 유럽 차원에서의 사이버 안보 협력을 위해서 외교안보뿐만 안라 범죄예방과 단속 등의 분야에서 주체적인 역할을 자임하고 있다. 이렇게 파악된 독일의 전략은 거버먼트 프레임에 입각하고 있는 것으로 볼 수 있다. 한편 독일의 사이버 안보 추진체계는 연방 내무부가 사이버 안보 정책 전반을 총괄하는 가운데 다른 정부기관들이 영역별로 소관 업무를 관장하는 구조이며, 그 산하의 연방 정보기술보안청과 국가사이버방어센터가 전담지원기관의 역할을 한다. 연방정부와 주정부 사이에 사이버 위협정보 이전을 의무화한 점은, 이전의 사이버 안보 추진체계가 상대적으로 분산적이었기 때문에 긴급 상황에 대처하기 어려웠다는 지적을 반영한 것이지만, 대체적으로 독일의 추진체계는 실무부처 분산형의 형태를 띠고 있다.

3. 프랑스의 사이버 안보 전략

2008년과 2013년 프랑스의 『국방 및 국가안보 백서(Défense et Sécurité Nationale)』는 사이버 안보를 국가적 우선과제로 제시하고 사이버 공격에 대한 예방과 대응을 강조하였다(President of the French Republic, 2008; 2013). 2015년 10월에는 유럽의 '디지털 전략 자율성을 위한 로드맵'의 선두주자를 목표로 한, 『국가디지털안보전략(Stratégie Nationale pour la Sécurité du Numérique)』을 발표했는데, 이는 2010년대로 넘어오면서 국가적 우선과제로 채택된 사이버 안보를 추진하는 총괄적 국가전략이 수립됨

을 의미했다(Premier Ministre, 2015). 이 전략은 사이버 공간에서의 '안전한 디지털 전환'을 위한 전략 목표를 제시하고, 이를 달성하기 위한 세부 과제들을 지적하였다. 특히 프랑스는 역량 강화를 통한 사이버 안보 및 디지털 경제의 신뢰성 강화를 전략의 가장 큰 목표로 설정하였다. 이외에도 사이버 안보와 경제적 역동성 간의 적절한 균형을 유지함으로써 통한 국제 경쟁력을 높일 것을 주문했으며, 프랑스 시민의 프라이버시 보호를 주요 이슈로 다루어야 한다고 강조했다. 특히 디지털 서비스에 위탁된 데이터의 사용을 감시하기 위한 '디지털 신원 확인 로드맵(road map for digital identity)'을 수립하고자 한 것이 눈에 띈다.

2011년 프랑스 국방부는 사이버 국방 전략의 일환으로서 사이버 위기시 조정역을 맡는 사이버방어담당총관(Officier général chargé de la cyberdéfense)을 신설하였으며, 2014년에는 『사이버방위정책(Pacte Défense Cyber)』 발표하였다(Ministre de la Défense, 2014). 이 문건에서는 사이버 국방 정책과 관련하여 정보시스템 보안 수준 강화 및 국방부와 안보 관련 기관의 적극적인 대책 강구, 미래 국방태세 강화를 위한 기술 · 학문 · 작전수행 · 연구개발 강화와 산업기반 지원, '브레타뉴 단지'로 알려진 사이버 안보 협력단지 조성계획 등이 제시되었다. 프랑스 국방부는 2016년 12월에도 사이버 안보 강화를 주된 내용으로 하는 국방정책을 발표했는데, 사이버 공격에 응전하고 이를 제압할 수 있는 공격력을 갖춘 별도의 군조직 추진, 국방인력 중 사이버전 병력 3,200명 확보, 국방예산 연간 약 5천억 투자, 사이버 안보 예비군 제도 운영 등의 내용을 담았다.

프랑스는 미국과의 사이버 안보 협력에는 큰 관심을 보이지 않고 있는데, 미국이 적개념으로 상정하는 러시아나 중국보다는 중동의 이슬람 세력들이 벌이는 테러와 사이버 공격을 더욱 위협적인 것으로 인식하고 있기 때문이다. 실제로 프랑스는 2015년 파리 테러 등의 위협에 대응하는 대내외적 대책 마련에 적극 나섰다. 예를 들어, 프랑스는 2015년 『국가디지털안보전략』에서 '유럽의 디지털 전략 자율성을 위한 로드맵' 작성을 제안하였고 이를 위한 교육과 국제협력을 강조한 바 있다. 구체적으로는 EU의 주요 사이버 안보 원칙과 정책의 동일성 및 회원국 간 결속을 중시하고, 표준화 및 인증, 연구개발, 디지털 기술에 대한 신뢰 구축을 목표로 하는 유럽의 '디지털 전략의 자율성을 위한 로드맵'을 수립하였다. 또한 이 전략서는 대외적으로 EU 전체에 걸친 네트워크 및 정보시스템 보안 향상을 위해 주요 사이버 위기에 대한 대응을 위한 다자간 협력을 강조했는데, 국제적 영향력 강화를 위해 국제법 준수와 유엔과 유럽안보협력기구(OSCE)에서의 다자간 협상에 참여를 주문하였다(유지연, 2017).

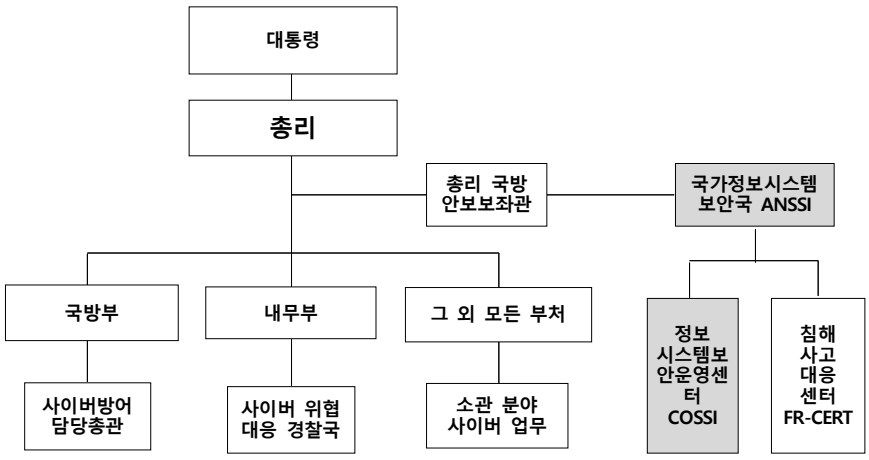
프랑스에서는 〈국방법전(Code de la Défense)〉이 민간영역과 공공영역 전체에 대해서 가해지는 사이버 위협에 대한 대응책을 규율하고 있다. 사이버 안보에 관한 국가의 권한, 민간의 의무, 신고제도 등 구체적인 내용을 규정하고 있는데, 여기서 한 가지 주의할 점은 〈국방법전〉은 국방부 및 군조직에만 한정되는 것이 아니라 대통령과 총리를 필두로 하는 국가 전

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

체의 국방업무 전반을 아우르는 일반 법령이라는 사실이다. 한편 2016년 10월 발표된 〈디지털공화국법〉은 프랑스 정부가 국가행정 영역뿐 아니라 다양한 산업 분야에 걸쳐 정보화를 활용한 사회적 개혁을 단행하고자 추진하고 있는 사회 정보화 정책을 담은 법률이다. 데이터와 지식의 유통, 디지털사회 권리 보호, 디지털 접근권 등에 대한 규정을 담고 있다. 특히 디지털 사회의 권리 보호와 관련된 내용으로 사이버 공간과 프라이버시 보호에 대한 내용을 규율하고 있는데, 열린 공간으로서 사이버 공간에서의 권리 보호는 인터넷 중립성, 데이터의 이동성과 회수, 플랫폼 신뢰성과 소비자 정보 등으로 구성된다(김도승, 2017).

프랑스의 사이버 안보 추진체계는 총리를 사이버 안보에 대한 권한과 책임을 지는 주체로 하여 총리 국방안보보좌관 소속의 국가정보시스템보안국(Agence Nationale de Sécurité des Systèmes d' information, ANSSI)이 사이버 안보 업무를 총괄하는 컨트롤타워의 역할을 하는 구조로 되어 있다(〈그림-8〉). 국가정보시스템보안국은 2009년 창립되었는데 2013년 조직의 지위가 격상되었고, 2015년 10월에는 발표된 국가디지털안보전략을 통해서 그 역할이 더욱 강화되었다. 국가정보시스템보안국은 국가 공공기관의 정보시스템 보안에 영향을 미치거나 위협하는 사이버 위기에 대응하고 이를 해결하기 위해 조치를 취하고 있는데, 그 산하에 정보시스템보안운영센터(Le Centre Opérationnel de la Sécurité des Systèmes d' Information.: COSSI)와 침해사고대응센터(FR-CERT)를 두고 있다. 한편 실무부처 차원에서는 내무부 산하의 경찰국이 사이버 범죄 대책을 맡고 있다고 할 수 있는데, 2014년에 사이버 위협에 대한 대응을 담당하는 경찰국장직이 신설되었다.

〈그림-8〉 프랑스의 사이버 안보 추진체계



출처: 김도승(2017), p.52와 유지연(2017), p.27을 수정 · 보완

요컨대, 프랑스의 사이버 안보 전략은 러시아나 중국과 같은 국가 행위자로부터의 위협보다는 중동지역 이슬람 세력을 더 심각한 위협으로 인식하고 대응하는 과정에서 형성되었다. 따라서 프랑스가 국방 차원에서 구축한 사이버 방위의 시스템은 전통적인 군사안보의 시각에서 본 대응이라기보다는 국가업무 전반을 강조하는 신흥안보의 관점으로 이해할 필요가 있다. 사이버 안보의 국제협력을 추진하는 방향도 글로벌 차원의 국제규범 형성과정에 대한 참여이외에도 유럽 차원에서 진행되는 다자간 협상에의 참여와 그 과정에서 프랑스의 역할 설정에 관심을 두고 있다. 이런 점에서 볼 때, 프랑스의 전략은 거버먼트 프레임 경향을 기본으로 하면서 거버넌스 프레임이 복합되는 형태라고 할 수 있다. 추진체계의 구성은 전문기관으로써 국가정보시스템보안국(ANSSI)이 총리를 보좌하며 총괄·조정 기능을 담당하고, 각 실무부처들은 소관 업무에 속하는 사이버 안보 관련 사항에 대응하는 구조이다. 2009년과 2013년 두 차례에 걸쳐서 범정부 컨트롤타워로서의 국가정보시스템보안국의 지위와 역할이 강화되면서 점점 더 컨트롤타워 총괄형의 모습을 갖춰가는 것으로 판단된다.

VI. 맺음말

최근 사이버 공격이 단순한 컴퓨터 보안과 정보보호의 문제가 아니라 국가안보의 문제로 인식되면서 이에 대응하는 각국의 전략도 군사, 외교, 경제, 정치, 사회 등을 아우르는 총체적인 국가전략으로서 이해되기 시작했다. 게다가 끊임없이 진화하는 복잡한 환경을 배경으로 발생하는 사이버 공간의 위협은 그 성격상 전통안보의 경우와는 크게 달라서 예전과 같은 단순발상을 넘어서는 새로운 안보 거버넌스를 요구하고 있다. 이 글의 서두에서 사이버 안보 분야의 대응양식을 보이지 않는 버추얼 창에 대응하는 그물망 방패의 구축이라고 비유한 것은 바로 이러한 이유 때문이다. 이러한 문제의식을 바탕으로, 이 글은 사이버 위협에 대응하는 그물망 방패의 구축에 나서고 있는, 세계 주요국, 특히 미국, 일본, 중국, 러시아, 영국, 독일, 프랑스 등 7개국의 사례를 비교 국가전략론의 시각에서 살펴봄으로서 향후 한국이 사이버 안보 분야에서 모색할 국가전략의 방향을 가늠하고자 하였다.

이들 국가가 지난 10여 년 동안 추진해온 사이버 안보 전략을 살펴보면 뚜렷한 공통점을 찾을 수 있다. 무엇보다도 모든 국가들이 점점 더 사이버 위협의 문제를 국가안보의 시각에서 인식하고, 이에 대한 대비책을 한층 강화하고 있다는 사실이다. 사이버 안보의 전략적 우선순위를 높이고 이를 실현하기 위한 물적·인적 역량의 강화와 법제도 정비에 박차를 가하고 있다. 이 글에서 살펴본 각종 전략서의 발표나 기구의 설치 및 법 제정 등의 사례는 이러한 추세를 잘 보여준다. 또한 이들 국가는 모두 사이버 안보의 문제를 단순한 '안보화' 의

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

차원을 넘어서 '군사화' 하는 경향을 보이고 있다. 사이버 위협에 대한 군사적 대응태세의 강화는 군 차원의 사이버 역량강화, 사이버전을 수행하는 부대의 창설과 통합지휘체계의 구축, 사이버 자위권 개념의 도입, 사후적 반응이 아닌 선제적 대응 개념의 도입 등에서 나타나고 있다.

그러나 이들의 사이버 안보 전략의 내용을 좀 더 자세히 살펴보면, 그 대내외적 정책지향성이라는 측면에서 본 차이도 무시할 수 없다. 민간 주도로 기술경제적 인프라와 지적재산 및 사회적 권리의 보호를 중시하는, 이른바 거버넌스 프레임의 국가들이 있는가 하면, 정부 주도로 정치 논리를 앞세워 자국체제의 이데올로기, 또한 국가주권의 논리를 강조하는, 이른바 거버먼트 프레임의 국가들도 있으며, 이 두 프레임이 형성하는 스펙트럼의 중간지대에 위치하는 복합 프레임의 정책을 펴는 국가들도 있다. 이 글의 분석에 따르면, 이러한 차이는 대략 미국과 일본으로 대변되는 서방 진영의 거버넌스 프레임과 중국과 러시아로 대변되는 비서방 진영의 거버먼트 프레임의 대립 구도로 나타나고, 영국, 독일, 프랑스 등의 유럽 국가들은 그 중간지대에 위치하는 양상으로 나타난다.

사이버 안보의 추진체계 측면에서 본 각국의 차이도 간과할 수 없다. 대체로 사이버 안보 정책을 담당하는 기관의 설치나 이를 지원하는 법을 제정하는 추세는 유사하지만, 어떤 기관을 어떻게 설치하고, 필요한 법을 어떤 내용과 형식으로 제정·운영할 것인가에 대해서는 국가들마다 다르다. 범정부 차원에서 정책을 관장하는 컨트롤타워를 설치하고 그 업무를 지원하는 단일법을 제정하는 국가가 있는가 하면(일본, 중국, 프랑스), 실무부처들이 각기 소관 영역에서 사이버 안보 업무를 담당하거나(독일), 새로이 법을 제정하지 않고 대통령 명령이나 독트린에 의거해서 정책을 추진하는 나라(러시아)도 있으며, 이 두 양식을 아울러서 개별 실무부처의 업무를 조정하는 시스템을 갖추거나 개별법들을 집합적으로 조정하여 적용하는 일종의 메타 거버넌스형의 추진체계를 구비한 국가(미국, 영국)도 있다.

이러한 논의를 토대로 이 글은 〈그림-1〉에서 제시한 유형화를 뒷받침하기 위해서 각국의 사례를 검토하고 이들을 대략 세 그룹으로 구분하였다. 첫째, 미국과 일본 모델로서 정책지향성은 기본적으로 거버넌스 프레임을 지향하는 가운데 추진추계는 컨트롤타원의 설치와 운영과정에서 메타 거버넌스를 모색하는 유형이다. 둘째, 중국과 러시아 모델로서 정책지향성은 거버먼트 프레임에 기반을 두고 있으며 각기 정치사회적·법제도적 특성에 맞추어 컨트롤타워 총괄형과 실무부처 분산형을 선택적으로 채택하는 유형이다. 끝으로, 유럽의 주요3국의 모델인데, 영국, 독일, 프랑스 등의 정책지향성과 추진체계는 각국의 정치적·제도적 특성에 맞춘 복합 프레임과 메타 거버넌스형을 추구한다. 물론 이들 모델은 결코 각국의 유형을 규정하는 고정된 것이 아니고 앞으로도 계속 진화할 가능성이 있는 유동성을 지니고 있다.

이들 국가의 사례에 대한 비교분석은 한국의 사이버 안보 전략에 주는 일반론적 함의를 던진다. 사실 이들 국가의 사례는 사이버 안보 전략 분야의 세계적인 선도국들로서 한국에게

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

는 일종의 '모델' 로서의 의미가 있다. 그러나 이들이 아무리 이 분야의 선도국이라 할지라도, 그 어느 나라도 한국이 그대로 베낄 수 있는 벤치마킹의 사례는 아니다. 각국의 정치·사회·문화와 역사적 경로의존성이 다르고, 각기 당면한 사이버 위협의 종류와 이들을 둘러싼 국제안보 환경의 성격이 다르기 때문이다. 향후 연구과제로 비교분석의 사례를 늘리려는 시도는 부분적 유용성이 있을 수 있다. 예를 들어, 이 분야에서 눈에 띄는 행보를 보이고 있는 호주, 에스토니아, 네덜란드, 싱가포르, 이스라엘 등과 같은, 이른바 중견국의 사례들을 살펴볼 필요가 있다. 그럼에도 궁극적으로 필요한 것은 한국의 현실에 맞는 사이버 안보 전략을 스스로 고민하는 성찰적 노력일 것이다.

오늘날 한국의 사이버 안보 현실을 보면, 인터넷 인프라 강국이라고 하면서도 사이버 안보는 취약국임을 자탄하게 된다. 북한발 사이버 공격, 최근에는 중국과 러시아의 사이버 공격마저 증가하여 사이버 위협도은 세계적으로 유례가 없을 정도로 높은데, 관련 법제도는 제대로 구비되지 못한 상황이다. 컨트롤타워의 설치와 사이버 안보 관련법의 제정을 둘러싸고 과잉 안보화와 과잉 정치화 담론 사이에서 표류하고 있기 때문이다. 게다가 대외적인 차원에서도 미중 사이버 갈등의 틈바구니에 낄 가능성이 다분하다. 글로벌 차원에서도 서방 진영과 비서방 진영의 사이에서 중견국의 이익을 주장하는 외교적 목소리를 내기도 쉽지 않다. 이러한 상황인식을 바탕으로 볼 때, 지금 우리에게 시급히 필요한 것은, 한국이 추구할 전략의 대내외적 정책지향성을 제대로 파악하고, 한국의 현실에 맞는 추진체계의 구축과 법제정에 대한 정치사회적 합의를 도출하는 일이다.

참고문헌

고은송. 2016. "중국의 사이버 안보 전략: 안보화 이론의 시각." 『신흥권력과 신흥안보: 미래 세계정치의 경쟁과 협력』 사회평론, pp.284-328.

김도승. 2017. "주요국 사이버 안보 법체계." 서울대학교 국제문제연구소 사이버 안보 세미나 발표자료. 4월 7일.

김상배. 2014. 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 한울.

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

김희연. 2015. "한중일 침해사고 대응체계 비교에 관한 연구: 사이버보안 법규, 대응기관, 대응절차를 중심으로." 『정보보호학회지』 25(2), pp.43-57

박상돈. 2015. "일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로." 『경희법학』 50(2), pp.144-175.

배병환 · 강원영 · 김정희. 2014. "영국의 사이버보안 추진체계 및 전략 분석." *Internet & Security Focus*, August.

배병환 · 송은지. 2014. "주요국 사이버보안 전략 비교 · 분석 및 시사점: 미국, EU, 영국의 사이버보안 전략을 중심으로." 『정보통신방송정책』 26(21), pp.1-26

송은지 · 강원영. 2014. "미국 오바마 정부 2기의 사이버보안 강화정책." *Internet & Security Focus*, September.

신범식. 2017. "러시아의 사이버 안보 전략과 외교." 김상배 편. 『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.241-277.

신성호. 2017. "미국의 사이버 안보 전략과 외교." 김상배 편. 『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.138-176.

양정윤 · 배선아 · 김규동. 2015. "중국 사이버 역량 현황 연구." 국가보안기술연구소.

유지연. 2017. "유럽 주요국의 사이버 안보 전략." 서울대학교 국제문제연구소 사이버 안보 세미나 발표자료. 4월 7일.

이강규. 2011. "세계 각국의 사이버 안보 전략과 우리의 정책 방향: 미국을 중심으로." 『정보통신방송정책』 23(16), pp.1-27.

이승주. 2017. "일본의 사이버 안보 전략과 외교." 김상배 편. 『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.211-240.

임재명. 2016. "사이버 보안: Intro." 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 7월 4일.

정종필 · 조윤영. 2017. "중국의 사이버 안보 전략과 외교." 김상배 편. 『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.177-210.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

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

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

Cabinet Office, UK. 2011. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* November.

Cabinet Office, UK. 2013. *Cyber Security Information Sharing Partnership(CISP).* March.

Cabinet Office, UK. 2013. *The National Cyber Security: Our Forward Plans.* December.

Carnoy, Martin, and Manuel Castells. 2001. "Globalization, the Knowledge Society, and the Network State: Poulantzas at the Millennium." *Global Networks.* 1(1), pp.1-18.

Chang, Amy. 2014. *Warring State China's Cybersecurity Strategy.* Center for a New American Security.

Christou, George. 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,* Palgrave Macmillan UK.

Federal Ministry of the Interior. 2011. *Cyber Security Strategy for Germany 2011. (Cyber-Sicherheitsstrategie für Deutschland 2011)* February

Federal Ministry of the Interior. 2016. *Cyber Security Strategy for Germany 2016. (Cyber-Sicherheitsstrategie für Deutschland 2016)* November.

Government of the United Kingdom. 2016. *National Cyber Security Strategy 2016-2021.* November.

Jessop, Bob. 2003. *The Future of the Capitalist State.* Cambridge: Polity Press.

Joint Committee on the National Security Strategy, UK. 2015. *National Security Strategy and Strategic Defence and Security Review 2015.* House of Lords and the House of Commons, UK.

Lewis, James Andrew. 2015. *U.S.-Japan Cooperation in Cybersecurity.* A Report of the CSIS Strategic Technologies Program. CSIS.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford and New York: Oxford University Press.

Ministre de la Défense. 2014. *Cyber Defense Policy (Pacte Défense Cyber)*

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

November.

Nocetti, J. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs*, 91(1), pp.111-130.

Peritz, Aki J. and Michael Sechrist. 2010. *Protecting Cyberspace and the US National Interest*. Belfer Center for Science and International Affairs. Harvard Kennedy School.

Premier Ministre. 2015. *French National Digital Security Strategy (Stratégie Nationale pour la Sécurité du Numérique)*. October.

President of the French Republic. 2008. *The French White Paper on Defense and National Security (Défense et Sécurité Nationale, 2008)*.

President of the French Republic. 2013. *French White Paper: Defence and National Security (Défense et Sécurité Nationale, 2013)*.

President of the Russian Federation. 2000. *Information Security Doctrine of the Russian Federation*. September.

President of the Russian Federation. 2013. *Basic Principles for State Policy of the Russian Federation in the Field of International Information Security*. July.

President of the Russian Federation. 2016. *Information Security Doctrine of the Russian Federation*. December, 5.

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.

U.S. Department of Defense. 2011. *Department of Defense Strategy for Operating in Cyberspace*. July.

U.S. Department of Defense. 2015. *The DoD Cyber Strategy*. April.

U.S. Department of Homeland Security. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. May.

White House. 2003. *The National Strategy to Secure Cyberspace*. February.

White House. 2008. *The Comprehensive National Cybersecurity Initiative*. January.

White House. 2011. *International Strategy for Cyberspace: Prosperity, Security,*

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

and Openness in a Networked World. May.

国家互联网信息办公室(국가인터넷정보판공실). 2016. 『国家网络空间安全战略(국가사이버공간안전전략)』 12月 27日.

国家互联网信息办公室(국가인터넷정보판공실). 2017. 『网络空间国际合作战略(사이버공간국제협력전략)』 3月 1日.

国务院新闻办公室(국무원신문판공실). 2013. 『中国武装力量的多样化运用白皮书(중국군사역량다양화운용백서)』.

国务院新闻办公室(국무원신문판공실). 2015. 『中国的军事战略白皮书(중국국방전략백서)』.

閣議決定(각의결정). 2015. 『サイバーセキュ…リティ戦略(사이버시큐리티전략)』. 9月 4日.

防衛省・自衛隊(방위성・자위대). 2016. 『防衛白書(방위백서)』. 防衛省・自衛隊.

情報セキュリティ政策会議(정보시큐리티정책회의). 2013a. 『サイバーセキュリティ戦略(사이버시큐리티전략)』, 6月 10日.

情報セキュリティ政策会議(정보시큐리티정책회의). 2013b. 『サイバーセキュリティ国際連携取組方針(사이버시큐리티국제협력전략): j-initiative for Cybersecurity』 10月 2日.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr