제1장

사이버 안보전략의 분석틀: 형성배경과 추진체계의 비교연구

김상배 | 서울대학교

I. 머리말

최근 국가안보의 핵심 영역으로 사이버 안보의 중요성이 확대되고 있으며, 세계 각국은 국가 차원에서 사이버 안보전략을 마련하고 있다. 사이버 안보의 기술적 특성상 전통안보와 같은 위협에 대응하던 조직체계와 운용방식으로는 충분한 방어에 한계가 있으며, 기술, 법제도, 국제협력 등을 통한 복합적이고 종합적인 대응전략이 필요하다. 사이버 안보의 확고한 보장을 위해서는 민간, 공공, 국방 영역이 각 분야별로 보안체계를 확립하여 대응할 필요가 있는데, 특히 최근 분야를 가리지 않고 동시 다발적으로 발생하는 사이버 공격에 대처하기 위해 민·관·군이 좀 더 긴밀하게 협력할 필요성이 제기된다. 그럼에도 세계적으로 사이버 안보전략이나 추진체계와 관련된 일반 모델이 정립되어 있지 못한 상황이며, 각국이 처한 상황에 따라 다양한 대응전략과 추진체계를 마련해 가고 있는 실정이다(김상배 2014; 2018a; 2018b; 2019; 김상배 편 2017; 2019; 김상배·민병원 편 2018).

강조컨대, 사이버 안보의 특성상 기술적으로 철벽방어를 구축하려는 단순발상만으로는 해법을 찾을 수 없으며, 사전예방과 사후복원까지도 고려하는 복합적인 대응이 필요하다. 정책내용 면에서 기술과 국방 또는 법제도와 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. 정치·사회·문화의 차이가 있기 때문이고, 여타 정책이나 제도와의 관계 또는 역사적 경로의존성의 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 다른 복합적인 내용과 형식을 지니고 있다.

이 책은 미국·일본·중국·러시아 등 한반도 주변4국은 물론 영국·독일·프랑스 등 서유럽 3개국, 에스토니아·네덜란드·핀란드·스웨덴 등 북유럽 4개국, 캐나다·호주·대만·싱가포르·이스라엘 등 아시아·태평양 지역 5개국의 사이버 안보전략과 추진체계에 대한 비교분석의 작업을 수행하였다. 각국 사이버 안보전략의 형성배경과 대내외적 정책 지향성을 비교 분석하고, 각국 사이버 안보의 추진체계 및 법제도를 비교 검토함으로써 한국에 주는 함의를 도출하고자 하였다. 이러한 과정에서 각국의 사이버 안보전략과 추진체계에 대한 유형구분을 시도하였으며, 이를 바탕으로 한국이 여태까지 취해왔고 향후 모색해 갈 전략과 제도의 방향을 가늠하고자 했다.

이 장은 크게 네 부분으로 구성되었다. 제2절은 16개국의 사이버 안보전략과 추진체계를 비교하기 위한 분석틀을 기능적 측면에서 본 대내외 정책지향성과 구조적 측면에서 본 추진주체로 나누어 제시하고, 이를 바탕으로 각국의 사례를 이론적 시각에서 유형 구분하기 위한 논의의 기초를 마련하였다. 제3절은 16개국 사이버 안보전략의 형성배경을 주변4국, 서유럽 국가, 북유럽 국가, 아태지역 국가 등의 네 그룹으로 나누어 살펴보았다. 제4절은 16개국 사이버 안보전략의 추진체계를 동일한 네 가지 그룹의 국가 사례를 통해서 살펴보았다. 제5절은 16개국 비교분석이 사이버 안보전략과 추진체계에 대한 논의에 주는 함의를 도출하였다. 끝으로, 맺음말은 이 장의 논의가 한국에 주는 함의를 지적하였다.

II. 사이버 안보전략의 분석틀

사이버 안보전략뿐만 아니라 사이버 공간전략 전반을 염두에 두고 볼 때, 각국이 취하고 있는 사이버 안보전략의 방향과 추진체계의 내용을 이론적으로 구분해서 보려는 노력이 필요하다. 이러한 이론적 구분의 작업을 통해서 각국의 사이버 안보전략 사례에 대한 유형화를 시도하는 것은 분석틀의 마련이라는 점에서 매우 유용할 것이기 때문이다. 이러한 문제의식을 바탕으로 이 절은 각국의 사이버 안보전략에서 나타나는 국가변환의 추세와 국가별 차이를 분석적으로 이해하기 위해서 두 가지의 기준을 제시하고자 한다.

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 등을 고려하여 판단하였다. 특히 사이버 안보전략의 형성배경을 파악하기 위해서 다음과 같은 질문들을 세부적으로 제기하였다. 국가 안보전략 전반에서 사이버 안보전략이 차지하는 위상, 방향, 강조점, 내용은 무엇인가? 사이버 안보 위협의 원인(예: 주적 개념)에 대한 인식과 그 실천전략과 대응태세의 특징은 무엇인가? 사이버 안보 분야에서 주변국과의 공조체제 구축 및 지역 차원의 국제협력에 참여, 그리고 국제규범 형성 과정에 대한 입장은 어떠한가?

이러한 요소들의 복합 정도를 고려하여 사이버 안보전략의 대내외 정책지향성은 크게 세 가지로 유형구분해서 이해할 수 있을 것이다. 대내외 정책지향성의 스펙트럼의 한쪽 끝에는 기술경제적 논리를 바탕으로 정보 인프라와 지적재산의 보호를 위한 글로벌 메커니즘을 지향하는 '글로벌 거버넌스(Global Governance) 프레임'을 놓을 수

있을 것이다. 다른 한편에는 정치사회적 논리를 바탕으로 내정불간섭과 국가주권의 원칙에 입각해 국내체제의 안전을 관철하려는 '국가주권(National Sovereignty) 프레임'을 위치할 수 있다. 그리고 이러한 양 극단의 중간 지대에 두 가지의 프레임이 적절한 방식으로 복합되는 일종의 '지역협력(Regional Cooperation) 프레임'을 상정해 볼 수 있다.

둘째, 국가의 구조적 측면에서 본 추진주체의 구성원리인데, 이는 주로 범정부 컨트롤타워의 설치 여부와 소재, 전담지원기관의 설치 여부, 각 실무부처의 역할과 상호 업무분장의 형태, 관련법의 제정 및 운용 방식, 프라이버시 보호의 비중 등을 고려하여 판단하였다. 특히 사이버 안보전략의 추진체계의 형식과 내용을 파악하기 위해서 다음과 같은 질문들을 세부적으로 제기하였다. 사이버 안보 분야의 업무를 조정할 컨트롤타워의 설치 여부 및 실무 전담기관과의 관계설정, 그리고 실무 전담기관의 설치 위치는 어떠한가? 사이버 안보 대응력 강화를 위한 법제도의 정비여부 및 그 형태, 즉 사이버안보법의 형태가 단일법인가 옴니버스법인가? 사이버 위협정보 공유를 위한 민관협력 시스템이나 사이버 안보와 개인정보 보호의 조화로운 발전을 추구하는 방식은 어떠한가?

이러한 요소들의 복합 정도에 따라서 볼 때, 사이버 안보전략의 추진체계는 크게 세 가지로 유형구분해서 이해할 수 있을 것이다. 추진체계 구성원리의 스펙트럼 한쪽 끝에는 범정부 컨트롤타워 또는 전담지원기관이 존재하는 '컨트롤타워 총괄형'의 추진체계를 놓을 수 있다. 다른 한편에는 실무부처들의 상위에 총괄기관을 설치하지 않고 실무부처 중의 한두 부처가 총괄하거나 또는 각 실무부처의 개별 거버넌스를 상호 간에 조정하는 '실무부처 분산형'을 위치할 수 있다. 그리고 이러한 양 극단의 중간 지대에 두 가지 유형의 추진체계가 적절한 방

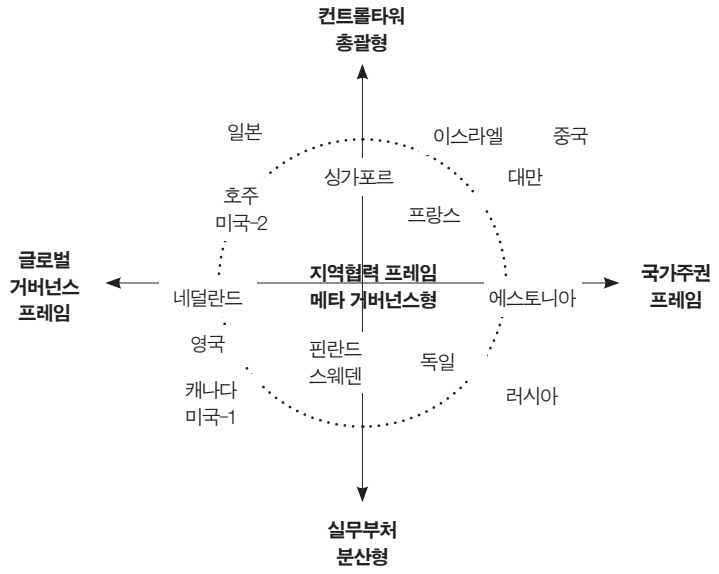

그림 1-1. 사이버 안보전략의 유형구분
출처: 김상배(2018), p.151의 응용

식으로 복합되거나 중첩되는 일종의 '메타 거버넌스형' 추진체계를 상정해 볼 수 있다.

이러한 두 가지 분석기준을 바탕으로 볼 때, 이 책에서 다룬 16개국의 사이버 안보전략과 추진체계의 유형은 대략 〈그림 1-1〉과 같이 구분하여 위치시켜 볼 수 있다. 이 책의 각 장에서 자세히 설명하고 있을 뿐만 아니라 이하에서 간략히 요약하고 있는 바와 같이, 이들 16개국의 사례들은 크게 다섯 개 정도의 그룹으로 나누어 이해할 수 있다.

첫 번째 그룹은 국가주권 프레임을 지향하는 가운데 컨트롤타워 총괄형 추진체계를 갖추고 있는 국가군으로서 중국, 이스라엘, 프랑스 등이 여기에 해당한다. 두 번째 그룹은 국가주권 프레임을 지향하

는 가운데 실무부처 분산형 추진체계를 갖추고 있는 국가군으로서 러시아, 독일, 에스토니아 등이 여기에 해당한다. 세 번째 그룹은 글로벌 거버넌스 프레임을 지향하는 가운데 컨트롤타워 총괄형 추진체계를 갖추고 있는 국가군으로서 일본, 싱가포르, 호주, 미국(오바마 행정부) 등이 여기에 해당한다. 네 번째 그룹은 글로벌 거버넌스 프레임을 지향하는 가운데 실무부처 분산형 추진체계를 갖추고 있는 국가군으로서 미국(부시 행정부와 트럼프 행정부), 캐나다, 영국, 네덜란드 등이 여기에 해당한다. 마지막으로 다섯 번째 그룹은 지역협력 프레임을 지향하는 가운데 메타 거버넌스형 추진체계를 갖추고 있는 국가군으로서 핀란드, 스웨덴 등이 여기에 해당한다.

이 절에서 시도한 사이버 안보전략의 유형 구분은 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. 트럼프 시대의 미국은 다시 〈미국-1〉로 돌아가는 경향을 보이고 있다. 게다가 최근 많은 국가들이 각기 사정에 따라서 편차가 있기는 하지만, 글로벌 거버넌스 및 국가주권 프레임, 그리고 컨트롤타워 총괄형 및 실무부처 분산형 추진체계가 복합되는 형태로 수렴되는 경향을 보이고 있다. 그럼에도 이 절에서 시도한 사이버 안보전략의 유형 구분은 비교분석의 효율성이나 실천적 함의 도출의 편의성이라는 측면에서 나름대로 유용하며, 각국의 사례를 비교분석하는 기준으로서 활용 가능하다. 이상에서 도출한 비교분석의 틀을 활용하여 16개국의 사이버 안보전략의 내용과 이상에서 제시한 유형구분의 근거를 살펴보면 아래와 같다.

III. 사이버 안보전략의 형성배경

각국의 사이버 안보전략을 이해하는 데 있어 그 형성배경이나 대내외적 정책 지향성을 살펴보는 작업은 일차적으로 중요하다. 이는 주로 국가안보전략이나 국방전략의 맥락에서 온라인 공간을 중심으로 발생하는 사이버 안보의 위협을 어떻게 인식하고 사이버 안보전략의 위상을 어떻게 설정하는지의 문제로 나타난다. 이러한 인식은 대내적인 사이버 안보전략의 수립이나 이 분야에서 주변국과의 공조체제 구축 및 지역 차원의 국제협력에 참여, 그리고 글로벌 차원의 국제규범 형성 과정에 대한 입장으로도 나타난다.

1. 주변4국의 경우

미국은 자국의 정보 인프라와 지적재산의 보호를 위해서 일찌감치 사이버 안보를 강조하며 국가전략의 일부로서 사이버 안보 문제를 보는 포괄적인 전략을 추진해왔다. 더불어 억지 역량의 강화라는 명목으로 군사적인 공세전략도 병행하였다. 사실 사이버 안보 분야의 '군사화'를 선도한 나라는 미국이다. 이러한 과정에서 중국, 러시아, 이란, 북한 등 4개국의 지원을 받는 것으로 알려진 해킹의 양적 증가가 큰 영향을 미쳤다. 이러한 맥락에서 선제적 대응 개념을 도입하기도 했다. 2017년 8월에는 사이버사령부를 독자적인 지휘체계를 갖춘 10번째 통합 전투사령부로 격상시키는 조치를 단행했다. 국제협력도 양자·지역 동맹 강화를 통해 아태지역과 유럽지역에서 미국이 주도하는 사이버 안보 방위전략을 구축하려는 시도와 함께 ICANN와 같이 민간 이해당사자들이 참여하는 글로벌 거버넌스와 동시에 정부 간 프레임을

활용한 국제협력도 지향하였다. 사이버 위협정보의 공유체계를 구축하는 과정에서 프라이버시 보호를 고려하는 법제도를 마련한 것은 인상적이다. 요컨대, 미국의 대내외 정책지향성은 기본적으로 글로벌 거버넌스 프레임에 기반을 두고 있다고 보아야 할 것이다.

2010년대 접어들어 일본의 사이버 안보전략은 날로 늘어나고 있는 사이버 위협을 중대하게 인식하고 국가안보의 차원에서 적극적으로 대응하여 기존의 반응적 정책에서 선제적 정책으로, 수동적 정책에서 주도적 정책으로 변화를 꾀하였다. 특히 일본은 2013년 6월 『사이버시큐리티전략』 발표 이후 사이버 안보전략을 독자적 영역으로 설정하고 강조하고 있다. 사이버 국방전략의 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 아태지역 전략과 글로벌 거버넌스의 구상 내에서 파악할 수 있다. 또한 일본은 아세안 지역 국가들과의 협력에도 주력하고 있다. 요컨대, 일본의 대내외적 정책지향성은 대체로 미국과 같은 글로벌 거버넌스 프레임으로 파악할 수 있다.

중국의 사이버 안보전략은 자국 핵심 기반시설에 대한 사이버 공격의 위협뿐만 아니라 정치체제의 안전과 미국에 의한 국가주권의 침해(또는 미국의 기술패권)에 대한 방어적 태도를 바탕에 깔고 있다. 그러나 시진핑 시대에 접어들어 공세적인 방향으로 전략이 설정되고 있는데 이는 국방전략의 구체화나 사이버 공격을 군작전 개념의 일부로 포함시키고 사이버전을 담당하는 전략지원부대의 창설 및 사이버사령부(인터넷기초총부) 설치 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. 상하이협력기구(SCO)나 세계인터넷대회(WIC) 등이 대표적 사례이다. 요컨대, 중국의 대내외 정책지향성은 전형적인 국가주권 프레임에 기반을 두고 있다고 할 수 있다.

러시아 사이버 안보전략의 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. 최근 나토를 상대로 한 러시아의 정보전/심리전의 수행이 관건이다. 국제협력의 추구에 있어서는 유엔 정부전문가그룹(GGE)과 같은 기존의 국제기구 활동이나 지역협력체(CSTO, SCO, CIS 등)의 틀을 활용하여 주권국가들이 협의하는 사이버 안보 국제질서 모색의 선봉에 나서고 있다. 요컨대, 전반적으로 러시아 사이버 안보전략의 대내외 정책지향성은 개인권리보다는 국가주권이 강조되는 전형적인 국가주권 프레임으로 파악된다.

2. 서유럽 국가들의 경우

영국의 사이버 안보전략은 핵심 기반시설의 안전을 확보하고 사이버 공격, 특히 사이버 범죄에 대응하는 역량과 정보공유 및 네트워크의 복원력을 강조하는 기조를 유지하고 있다. 민간 부문의 사이버 활동과 경제 활성화를 우선시하지만, 최근에는 국방부문에서 보복공격까지

언급할 정도로 강경한 태도를 드러내고 있다. 미국의 대테러 전쟁 수행에 공조하는 차원에서 사이버 안보 부문의 '안보화'를 추구하는 경향이 강하다. 대외적인 방어를 위해서 국방부와 외교부 산하 정보통신본부(Government Communications Headquarters, GCHQ)가 특별 프로그램을 수립하고, 사이버 부대를 창설하는 대응책을 마련하였지만, 아직 사이버사령부를 창설하는 수준에는 이르지 않고 있다. 최근에는 사후적 반응이 아닌 선제적 대응 개념을 도입하는 경향을 보인다. 국제협력의 지향성은 이른바 런던 프로세스로 알려진 사이버공간총회의 추진이나 최근 유사입장국회의 추진 등에서 드러난 바와 같이, 신뢰구축과 자발적이고 비구속적인 규범의 도출에 중점을 둔다. 요컨대, 영국의 대내외 정책지향성은 다소 복합적인 양상을 보이기는 하지만 기본적으로는 글로벌 거버넌스 프레임으로 볼 수 있다.

독일의 사이버 안보전략은 정보통신산업이나 프라이버시 보호보다는 주요 기반시설에 대한 사이버 방위에 상대적으로 더 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. 사이버 안보전략을 독자적으로 내놓고 있으며, 나토의 일원으로서 러시아와의 하이브리드전을 염두에 둔 군 역할에 대한 관심은 사이버 맞대응 부대 창설로 나타났다. 이러한 경향은 독일의 국제협력 전략에서도 나타나는데, 유럽 차원에서의 사이버 안보 협력을 위해서 외교안보뿐만 아니라 범죄예방과 단속 등의 분야에서 주체적인 역할을 자임하고 있다. 미국보다는 유럽 국가들과 협력, 국가 단위보다는 유럽 지역을 우선시하는 모델로 파악된다. 요컨대, 독일의 전략은 기본적으로 민간이 주도하여 글로벌 차원의 이슈에 참여하는 모델보다는 전통안보 분야에서 정부가 주도적 역할을 담당하는 지역협력의 국가주권 프레임에 입각하고 있는 것으로 볼 수 있다.

프랑스의 사이버 안보전략은, 대내외 정책지향성의 측면에서 볼 때, 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 신흥안보(emerging security)의 관점으로 이해할 필요가 있다. 사이버 안보전략에 대한 내용도 포괄적인 의미에서 본 국방정책의 일부 또는 사이버/디지털 전략 일부로서 나타나고 있다. 사이버 안보의 국제협력을 추진하는 방향도 글로벌 차원의 국제규범 형성 과정에 대한 참여 이외에도 유럽 차원에서 진행되는 다자간 협상에의 참여와 그 과정에서 프랑스의 역할 설정에 관심을 두고 있다. 요컨대, 프랑스의 전략은 국가주권 프레임 경향을 기본으로 하면서 글로벌 거버넌스 프레임이 복합되는 형태라고 할 수 있다.

3. 북유럽 국가들의 경우

에스토니아는 일찌감치 독자적인 사이버 안보전략을 마련하였는데, 2007년 러시아의 사이버 공격이 직접적인 계기를 제공하였다. 이후 에스토니아의 대응은 주로 군사적 접근을 취했는데, 그 기저에는 러시아에 대항하기 위해 나토라는 동맹을 활용하려는 전략적 의도가 깔려 있었다. 다시 말해 구소련 연방에서 탈피하여 독자적인 발전전략을 추구하는 과정에서 친서방적인 노선을 취하려는 구조적 상황이 에스토니아의 사이버 안보전략에 반영되었다. 이러한 군사동맹의 관점에서

사이버 안보에 접근한 에스토니아의 행보는 오프라인 공간의 국제법, 특히 전쟁법 규범을 사이버 공간의 공격 행위에 적용하여 사이버전의 교전수칙을 마련하려는 시도로 나타났는데, 그 대표적인 사례가 나토 CCDCOE(Cooperative Cyber Defence Centre of Excellence)의 총괄 하에 작성되어 2013년에 발표된 '탈린매뉴얼'이었다. 이러한 일련의 과정에서 에스토니아가 취하고 있는 사이버 안보 분야의 국제협력과 국제규범 모색의 정향성은 전통안보의 경험에서 추출된 동맹모델을 사이버 안보 분야에서 적용하려는 일종의 현실주의적 태도라고 할 수 있다. 요컨대, 에스토니아의 대내외 정책지향성은 기본적으로는 국가주권 프레임에 기반으로 두고 국제협력을 모색하는 모습으로 이해할 수 있다.

네덜란드는 사이버 공간을 안전하고 자유롭고 사회경제적 이익이 보장되는 공간으로 만들어야 한다는 인식을 바탕으로 사이버 안보전략을 독자적인 국가안보전략의 중요한 부분으로 자리매김해 왔다. 사이버 국방을 강조한 에스토니아의 경우와는 달리 네덜란드는 사이버 안보를 비(非)안보적·외교적 문제로 상정하고 접근한다. 이러한 네덜란드의 접근은 미국과 영국으로 대변되는 서방 진영과 러시아와 중국으로 대변되는 비(非)서방 진영의 사이에서 담당하고 있는 일종의 친(親)서방 외교선봉대의 역할로 나타난다. 예를 들어, 네덜란드는 영국과 헝가리, 한국에 이어 제4차 사이버공간총회를 헤이그에서 개최한 바 있으며, '사이버전(cyber warfare)에 적용 가능한 국제법'을 논한 탈린매뉴얼1.0과는 달리, 전쟁의 수준에는 미치지 않는 공격 행위에 대한 국제법 적용 문제를 다룬 탈린매뉴얼2.0을 회람한 '헤이그 프로세스'를 주도하기도 했다. 이러한 네덜란드의 행보는 자유주의적 시각에 입각하여 다중이해당사자들의 이익을 반영하는 정부 간 레짐의 모색 과정으로 이해할 수 있다. 요컨대, 네덜란드의 대내외 정책지향성은 기본적으로 정부 간 외교 네트워크를 적극적으로 활용하여 국제레짐을 추구하는 글로벌 거버넌스 프레임으로 볼 수 있다.

핀란드의 사이버 안보전략은 국방이나 외교의 관점보다는 사회의 필수 기능을 안전하게 유지한다는 관점에서 접근한다. 이러한 핀란드의 비(非)정치적 접근은 유럽과 러시아 사이에서 핀란드가 차지하고 있는 독특한 지정학적 위치에서 기인하는 바가 없지 않다. 냉전 이후 핀란드는 '핀란드화'로 불리는 '종속적 중립'을 넘어서 피(避)러, 친(親)유럽의 전략을 추구했는데, 이러한 경향이 사이버 안보 분야에도 반영된다. 이러한 과정에서 핀란드는 전통적인 비(非)나토 노선을 넘어서 나토 회원국들과의 양자 간 파트너십을 늘려왔다. 그럼에도 핀란드가 취한 사이버 안보전략은 에스토니아와 같은 사이버 국방의 맥락이라기보다는 사이버 범죄나 기술 등 분야에서 유럽 국가들과 협력하는 형태로 나타났다. 이러한 행보는 구체적으로 유럽연합 차원에서 2017년 10월 헬싱키에 유럽하이브리드위협대응센터가 설립되는 것으로 나타났다. 이러한 과정에서 드러나는 핀란드의 정책지향성은 범유럽 차원 지역공동체의 공동안보라는 맥락에서 사이버 안보를 보는 입장이며, 이는 냉전기 CSCE(Conference on Security and Cooperation in Europe) 과정에서 나타났던 역할을 했던 헬싱키 프로세스를 연상케 하는 중립모델이다. 요컨대, 핀란드의 대내외 정책지향성은 기본적으로 국가주권 프레임을 넘어서는 지역협력의 프레임으로 볼 수 있다.

스웨덴의 사이버 안보전략은 핀란드의 경우와 다소 유사한 패턴으로 이해할 수 있다. 기본적으로 스웨덴의 국방전략은 주로 러시아의 위협과 도발에 대한 대응을 상정하고 형성되었는데, 특히 2014년 러시아의 크림반도 병합 이후 스웨덴의 경계심이 더 커졌다. 이에 따라

스웨덴이 취했던 전통적인 비(非)나토 전략은 나토 회원국들과의 양자간 협력을 증대시키는 방향으로 변하고 있으며, 전통적인 군사적 중립국의 노선에도 변경 조짐이 보인다. 이렇듯 스웨덴의 사이버 안보전략이 러시아에 대한 대응이라는 맥락에서 이해되어야 하는 것은 사실이지만, 그렇다고 국방전략 일변도로만 볼 수는 없다. 좀 더 엄밀하게 살펴보면 스웨덴의 사이버 안보전략은 네트워크 보안이나 사이버 범죄 예방 및 시스템의 복원력 등까지도 고려하는 포괄적인 접근을 펼치고 있는 것으로 이해되어야 한다. 이러한 맥락에서 본 스웨덴의 사이버 안보 분야 국제협력의 기조는 아직까지는 미국을 중심으로 한 나토 동맹에의 적극적 참여보다는 자국력을 바탕으로 하는 중립전략을 모색하는 가운데 유럽 주요 국가들과의 파트너십을 늘려가고 있으며, 주변의 노르딕 국가들과 사이버 공동훈련이나 CERT협력을 벌이는 지역협의체의 틀을 활용하는 데 두어져 있다고 판단된다. 요컨대 스웨덴의 대내외 정책지향성은, 핀란드의 경우와 유사하게, 기본적으로 국가주권 프레임을 넘어서는 지역협력 프레임으로 볼 수 있다.

4. 아태지역 국가들의 경우

캐나다의 사이버 안보전략은 2010년 CCSS(Canada's Cyber Security Strategy)에서 시작하여 2018년 NCSS(National Cyber Security Strategy)에 이르는 과정에서 독자적인 안보전략의 형체를 갖추어 갔다. 이 과정에서 드러난 주요 관심사는 사이버 공간에서의 다중이해당사자들의 권리와 자유 및 경제활동의 안전성을 보장하기 위해 연방정부의 리더십을 발휘하는 것이었다. 경제·사회·정치 분야에 광범위하게 구축되어 있는 핵심 정보통신 인프라에 대해서 가해지는 다양한 차원의 사이버 공격이 우려의 대상이었는데, 최근에는 온라인상의 지적재산에 대한 중국 해커들의 공격이 주요 관심사로 부상하였다. 그럼에도 캐나다의 사이버 안보전략은 전통적인 군사안보의 사안보다는 신흥안보의 관점에서 이해되며, 따라서 국방전략이나 안보전략이라기보다는 정보보호나 시스템의 보안전략 차원에서 자리매김 되는 것으로 보는 것이 적절하다. 한편 캐나다가 추진하는 사이버 안보 분야의 국제협력은 미국, 영국, 호주 등 이른바 파이브 아이즈(Five Eyes) 국가들과의 정보공유와 공조를 통해서 진행되고 있으며, 유엔이나 나토, G8 등과 같은 서방 진영과의 다자외교의 장에서도 활발한 활동을 펼치고 있다. 요컨대, 캐나다의 대내외 정책지향성은 기본적으로는 미국의 경우와 매우 유사한 글로벌 거버넌스 프레임으로 볼 수 있다.

호주의 사이버 안보전략은 국가안보전략이나 국방전략의 맥락보다는 전반적인 사이버 공간의 안전을 추구하는 전략의 특징을 지닌다. 특히 호주는 국제적으로 중견국 외교의 리더십을 발휘할 아이템 중의 하나로 사이버 안보 문제의 위상을 설정하고 있는 점이 눈에 띈다. 14년 만에 발간된 2017년 호주 외교백서에서도 "개방되고 자유롭고 안전한 사이버 공간을 위하여 국제사회에서의 책임을 다할 것이며, 사이버 공간에서의 악의적 행동 및 범죄를 방지하고 대응하기 위하여 다른 나라들과 협력할 것"이라고 선언한 바 있다. 이러한 연속선상에서 본 호주의 사이버 안보 분야 국제협력은 미국, 영국, 뉴질랜드 등과 같은 이른바 파이브 아이즈 국가들과의 협력을 중심으로 활발하게 진행되고 있다. 이 밖에도 인도·태평양 지역 국가들과의 네트워킹도 강화 및 확장하고 있으며, 아태지역 CERT인 APCERT에서의 활동도 벌이고 있다. 2018년 4월에는 남태평양 주변국들과 PcCSON(Pacific Cyber Security Operation Network)을 구성하여 해당 국가들의 사이버 안보

대응능력을 향상시키기 위한 지원을 벌이고 있다. 요컨대, 호주의 대내외 정책지향성은 기본적으로는 정부 간 협력을 기반으로 하는 글로벌 거버넌스 프레임에 입각해 있다고 볼 수 있다.

대만은 국제사회에서 주권국가의 지위를 인정받지 못하는 사례이지만 중국과의 관계가 갖는 독특성으로 인해 주목할 필요가 있는 경우이다. 대만에서 사이버 안보의 문제는, 중국 해커들의 사이버 공격이 빈발하고 있는 상황에서, 국가안보 문제이자 필수불가결한 국방의 문제와 직결된 것으로 인식될 수밖에 없다. 특히 양안관계의 변화에 따라서 중국으로부터 사이버 공격의 양과 질이 변화한다는 점에서 대만에서 사이버 안보의 문제는 객관적인 위협인 동시에 주관적인 '안보화'를 야기하는 정치적 쟁점으로 작동해 왔다. 그러나 대만에서 사이버 안보의 문제는 자주국방의 주요한 요소로 인식되면서 정부와 군 차원의 사이버 안보 대응체계를 강화하는 것은 물론, 미래성장과 국가브랜드의 문제로 인식되면서 사이버 안보 관련 글로벌 기술경쟁력, 산업발전에 주력하고 있다. 중국의 '하나의 중국정책'으로 인해 국제적·정치적으로 제약적 환경을 가진 대만의 사례는 대체로 다자적 외교협력과 국제규범 창출에 역할을 하고자 하는 기타 중소국가들의 사이버 안보전략과 일정한 차이를 보이며, 자체적인 군사력과 기술강국, 산업발전을 추구하는 이스라엘의 사례와 유사한 측면을 가지고 있다고 볼 수 있다. 대만의 사이버 안보 분야 국제협력은 최근 미국 트럼프 행정부와의 관계가 호전되면서 미-대만 협력이 진행되고 있지만, 대만의 주권적 지위가 지니는 특수성으로 인해서 국제기구에서의 다자외교 활동은 매우 협소할 수밖에 없는 상황이다. 요컨대, 대만의 대내외 정책지향성은 기본적으로 국가주권 프레임으로 볼 수 있다.

싱가포르의 사이버 안보전략은 국방전략이나 국가안보전략의 관점보다는 초국적 차원에서 발생하는 신흥안보 문제에 대한 대응전략의 일환으로 이해되는 경향이 강하다. 상대적으로 정치적 성격이나 가치가 탈색된 기술경제 모델로서 실용성과 효율성을 추구하는 모델이라고 할 수 있다. 싱가포르가 동남아 지역의 무역, 금융, 물류의 허브 기능을 담당하는 점을 고려할 때, 주요 정보 인프라의 안전과 복원력의 강화는 싱가포르뿐만 아니라 동남아 지역 차원에서도 매우 중요한 사안이다. 싱가포르는 이러한 명성을 유지하는 차원에서 사이버 안보를 위한 국내정책 및 지역협력에 적극성을 보이고 있으며, 사이버 범죄 분야에서도 인터폴과의 협력도 활발히 진행하고 있다. 이러한 노력을 인정받아 싱가포르의 사이버 안보 지수는 세계 1위를 차지할 정도로 높은 수준이다. 싱가포르의 사이버 안보 분야 국제협력은 아세안 지역 차원의 협력을 촉진하는 포럼을 제공하는 모델의 형태를 취하고 있는데, 아세안지역포럼(ASEAN Regional Forum, ARF)은 싱가포르가 주도적인 역할을 담당하는 동남아 지역 사이버 안보 협력 플랫폼의 대표적 사례이다. 요컨대, 싱가포르의 대내외 정책지향성은 기본적으로 국가주권 프레임을 넘어서는 지역협력 프레임으로 볼 수 있다.

이스라엘은 국방 및 안보 문제를 국가존립의 심각한 현안으로 인식하는 맥락에서 사이버 안보 문제를 인식하고 접근하고 있다. 아랍국가, 이란 등으로부터 오는 사이버 위협에 대한 인식이 사이버 안보정책의 동인으로 작동하고 있으며, 이러한 맥락에서 사이버 국방전략과의 연계성이 발생한다. 이스라엘에서는 국방이나 안보를 담당하는 부처가 아닐지라도 수행하는 업무의 궁극적인 목적은 이스라엘의 보안 및 안보 능력 강화로 연결되는 경우가 많다. 가령 경제산업부의 사이버 보안 산업 육성이나 교육부와 국방부에서 우수한 인재 양성의 궁극적인 목적은 핵심 기술과 인적 자원을 확보함으로써 국가안보를 강화

하는 데로 귀결된다. 그러나 이러한 이스라엘의 사이버 안보전략이 모두 국방전략으로 관심사에만 머무는 것은 아니고, 정부와 민간 기업 간의 균형점을 찾는 데도 주력하고 있는데, 산업과 벤처 및 대학 부문과의 연계를 통해서 국가안보와 경제번영을 동시 추구하는 국가전략을 채택하였다. 사이버 안보 분야에서 이스라엘이 취하는 국제협력 전략의 방향은 주로 미국과 협력하고 공조하는 쪽으로 설정되어 있다. 요컨대, 이스라엘의 대내외 정책지향성은 기본적으로 국가주권 프레임에 기반을 두고 있다고 보아야 할 것이다.

IV. 사이버 안보전략의 추진체계

사이버 안보위협에 대한 각국의 인식과 대응이 상이하게 나타나는 만큼, 이를 추진하는 각국의 정책과 제도적 사정도 각기 다르게 나타난다. 이러한 차이는 주로 범정부 컨트롤타워의 설치 여부와 소재, 전담지원기관의 설치 여부, 각 실무부처의 역할과 상호 업무분장의 형태, 관련법의 제정 및 운용 방식, 프라이버시 보호와 국가안보 추구의 비중 등에서 드러난다. 그리고 특히 역사적 맥락에서 본 각국의 행정 및 법제도의 상황 및 문화가 다르기 때문에 사이버 안보를 추진하는 구체적인 체계와 법제도를 구비하는 방식도 다르게 나타난다.

1. 주변4국의 경우

미국에서는 실무부처들이 소관 업무를 담당하는 가운데 국토안보부(DHS)가 주도하던 모델(〈그림 1-1〉의 좌하단)로부터 백악관의 사이버

안보조정관(Cybersecurity Coordinator)이 컨트롤타워 역할을 수행하는 모델(〈그림 1-1〉의 좌상단)로 진화했다. 그러나 트럼프 행정부 출범 이후에는 사이버안보조정관의 직이 폐지되고 국가안보보좌관이 컨트롤타워의 역할을 담당하는 상황이다. 이보다 더 중요하게는 정부 부처들의 시스템 자체의 사실상(*de facto*) 운용을 통해서 컨트롤타워의 역할이 작동되는 것으로 파악된다. 법제정 차원에서 볼 때 미국은 개별 실무부처의 업무를 조정하는 시스템을 갖추거나 개별법들을 집합적으로 조정하여 적용하는 일종의 메타 거버넌스형의 추진체계를 구비한 나라로서 여러 가지 부분법을 집합한 옴니버스법의 형태를 운용 중이다. 요컨대, 미국의 추진체계는 실무부처의 역할을 강조하는 가운데 컨트롤타워의 총괄·조정 기능이 중층적으로 작동하는 메타 거버넌스형으로 파악할 수 있다.

일본은 미국보다는 좀 더 집중적인 형태를 갖추고 있다. 2014년 사이버시큐리티기본법 제정을 통해서 컨트롤타워의 역할을 하는 내각관방 산하의 사이버시큐리티전략본부와 전담지원기관인 내각사이버시큐리티센터(National center of Incident readiness and Strategy for Cybersecurity, NISC)를 설치하여 정부기관뿐만 아니라 지방자치단체와 독립행정법인, 국립대학, 특수법인, 인가법인 등의 사이버 안보를 총괄·조정하는 체계를 갖춤으로써, 상대적으로 집중적인 컨트롤타워 총괄형을 유지하고 있는 것으로 판단된다. 이러한 추진체계를 실행함에 있어 필요한 각 행위주체들 간의 역할분담을 단일법 형태의 사이버시큐리티법(2014) 제정을 통해서 규정하는 것이 특징이다. 요컨대, 일본의 추진체계는 단일법 제정을 기반으로 작동하는 전형적인 컨트롤타워 설치형으로 볼 수 있다.

중국의 사이버 안보전략의 추진체계는 국가주석이 조장을 맡는

중앙인터넷안전정보화위원회의 지도 하에 작동하는 전형적인 컨트롤타워 총괄형이며, 국가안전부, 공안부, 공업정보화부, 국가보밀국 등의 각 실무부처가 사이버 안보와 인터넷 통제의 업무를 담당하고 있다. 실무전담기관은 국무원 내 국가인터넷정보판공실(사무기구)이 담당한다. 최근 제정된 〈인터넷안전법〉은, 미국의 경우처럼 프라이버시 보호나 자유의 보장이라는 가치를 추구하기보다는, 국내사회의 통제와 외국기업에 대한 규제 등을 목적으로 한다. 요컨대, 중국의 추진체계는 단일법 제정을 기반으로 작동하는 전형적인 컨트롤타워 설치형으로 볼 수 있다.

러시아의 사이버 안보 추진체계는 범정부적으로 총괄하는 컨트롤타워를 제도적으로 설치하기보다는 정보기관인 연방보안부(FSB)와 그 산하의 정보보안센터(ISC)가 주도하는 사실상(*de facto*)의 총괄 메커니즘이 작동하는 모습이다. 이러한 과정에서 연방보안부(FSB)의 컨트롤타워 역할에 주목할 필요가 있다. 연방보안부(FSB) 내 정보보안센터(ISC)가 실무전담기관의 역할을 맡고 있다. 한편 러시아에서 정보보안 관련 법제도는 아직 독립법 체계를 갖추는 데까지 나가고 있지는 않으며, 정보보안 독트린과 같은 러시아만의 독자적인 형식을 고수하고 있다. 요컨대, 러시아의 추진체계는 전반적으로 공식 컨트롤타워가 없는 실무부처 분산형의 사례로 보는 것이 맞다.

2. 서유럽 국가들의 경우

영국의 사이버 안보전략은 정부기관들의 사이버 안보 업무는 내각부가 총괄하지만 범정부 컨트롤타워가 설치된 것으로 보기는 어렵고, 사이버 안보 대응체계의 대외부문은 2016년 10월 GCHQ 산하에 신설된 국가사이버안보센터(National Cyber Security Center, NCSC)를 통해서 관련 기관들과 협력하는 체계를 운영하고 있는 것이 특기할 만하다. 국내 공공 부문은 내각부 내 사이버보안청(OCSIA)이 담당한다. 일종의 이원시스템을 이루고 있다. 최근에는 사이버 위협정보에 대한 규정을 담은 수사권 법안(investigatory Powers Bill)이 2016년에 통과됨으로써 프라이버시 보호보다는 테러와 범죄를 막는 권한강화에 무게중심을 두고 있다. 그러나 최근에는 이 법마저도 근거를 잃고 있다. 요컨대, 영국 모델은 이원모델 또는 메타모델의 성격이 없지 않지만, 굳이 따지자면 실무부처 분산형의 응용모델이라고 보는 것이 맞다.

독일의 사이버 안보 추진체계는 컨트롤타워를 따로 두기보다는 실무부처 차원에서 연방 내무부가 사이버 안보 정책 전반을 총괄하는 가운데 다른 정부기관들이 영역별로 소관 업무를 관장하는 구조이며, 그 산하의 연방정보기술보안청(BSI) 내 국가사이버방어센터(Cyber-AZ)가 전담지원기관의 역할을 한다. 사이버 안보 관련법의 형태는 IT 안보법(2015)이 있기는 하나 기본적으로 다양한 법의 옴니버스적 운영을 보인다. 연방정부와 주정부 사이에 사이버 위협정보 이전을 의무화한 점은, 이전의 사이버 안보 추진체계가 상대적으로 분산적이었기 때문에 긴급 상황에 대처하기 어려웠다는 지적을 반영한 것이다. 요컨대, 독일의 추진체계는 대체로 실무부처 분산형의 형태를 띠고 있는 것으로 파악된다.

프랑스의 사이버 안보전략은 추진체계의 구성은 전문기관으로써 총리 국방안보보좌관 산하 국가정보시스템보안국(Agence Nationale de Sécurité des Systèmes d'information, 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. ANSSI 내 정보시스템보안운영센터(COSSI)가 실무전담기관을 맡고 있다. 프랑스는 국가와 국방법전, 디지털국가 등과 같이 국방 전반을 포괄적으로 규정한 법에서 사이버 안보를 규정하고 있다. 요컨대, 프랑스의 사이버 안보 추진체계는 대체로 포괄적인 법제도를 기반으로 하여 작동하는 컨트롤타워 총괄형의 모습으로 파악된다.

3. 북유럽 국가들의 경우

에스토니아의 경우 사이버안보위원회(Cybersecurity Council)가 컨트롤타워의 역할을 담당하고 있다. 사이버 안보의 실무전담기관은 2011년 국방부(Ministry of Defence)에서 경제통신부(Ministry of Economic Affairs and Communications)로 이관되었는데, 현재 사이버안보위원회의 지휘 하에 경제통신부 산하의 RIA(Riigi Infosüsteemi Amet, Estonian Information System Authority)가 실무전담기관을 맡고 있다. RIA는 국가 주요 기반시설과 주요 정보시설을 보호하고 위험 분석을 진행하며 대응책을 사전 준비하는 업무를 담당한다. RIA 내에 설치된 CERT-EE는 RIA에서 관리하는 정보통합시스템과 정부 포털을 보호하며, 에스토니아의 정보통신 네트워크에서 발생한 사건을 최대한 빠른 시간 내에 해결하는 임무를 맡고 있다. 한편 2018년 5월 에스토니아 의회는 최초로 사이버안보법(Cybersecurity Act)을 통과시켰다. 요컨대, 에스토니아의 사이버 안보 추진체계는 컨트롤타워가 총괄하는 가운데 그 산하에서 실무전담기관이 운용되는 메타 거버넌스형으로 파악된다.

네덜란드에서는 사이버안보위원회(Cyber Security Council, De Cyber Security Raad, CSR)가 사이버 안보의 컨트롤타워 역할을 맡고 있으며, 치안법무부 산하 국가사이버안보센터(NCSC)가 실무전담기관의 역할을 수행한다. NCSC의 주요업무는 사이버 위협 모니터링, 사고 대응, 위기관리, 사이버 안보 협력 플랫폼 제공 등이다. 또한 NCSC는 국가 CERT를 운영하며 정부기관과 국가 주요 기반시설에 대한 보호를 수행한다. 법제도적 측면에서는 네트워크 및 정보시스템보안법(Wet beveiliging netwerk-en informatiesystemen, Wbni)이 2018년 11월 9일 발효되었다. 동 법률에 따라 필수 서비스 운영자 및 디지털 서비스 공급자는 네트워크 및 정보시스템에 대한 보안위험을 관리, 예방 및 최소화하기 위해 적절한 조치를 취하여야 하며 보안 요구사항을 준수하여야 하고 심각한 사이버안보 침해사건 발생 시 국가사이버안보센터 및 감독기구에 보고하여야 할 의무가 발생한다. 요컨대, 네덜란드의 사이버 안보 추진체계는 컨트롤타워가 총괄하는 가운데 그 산하에서 실무전담기관이 운용되는 메타 거버넌스형으로 파악된다.

핀란드는 기본적으로 각 정부부처, 공공기관, 지자체 등이 자신의 관할 영역의 사이버 안보 문제를 직접 담당한다. 2013년 2월에 국방부 산하에 설치된 안보위원회(Security Committee)가 상설협력기구로 운용되고 있지만 이를 컨트롤타워라 볼 수는 없으며, 오히려 각 정부부처가 국가적 목표에 맞는 사이버 안보 정책을 실행한다. 사이버 안보의 실무전담기관으로는 교통통신부 산하의 핀란드교통통신국(Finnish Transportation and Communications Agency, TRAFICOM)을 들 수 있다. TRAFICOM은 기존의 핀란드통신규제국(Finnish Communications Regulatory Authority, FICORA)과 핀란드교통안전국(Finnish Transportation Safety Agency, TRAFI) 등을 통합하여 2019년 1월에

출범했다. 기존에 FICORA 안에서 사이버 보안을 담당하던 업무들은 TRAFICOM으로의 합병 이후에도 계속 수행된다. FICORA 내부 조직 중 NCSC-FI(National Cyber Security Center Finland) 역시 기존의 업무를 그대로 유지한 채 독립적인 위치를 가지고 취약점 보고 및 대응, 보안공지, 사이버위협 탐지 및 대응, 기술 지원 등의 서비스를 제공 등의 사이버보안 관련 실무 업무를 담당한다. 사이버 안보 관련법은 현재 국방부와 내무부가 함께 추진 중인 것으로 알려져 있다. 요컨대, 핀란드의 사이버 안보 추진체계는 범정부 컨트롤타워가 부재하고, 각 실무부처의 역할이 각각의 관할로 나뉘어 있는 실무부처 분산형으로 파악된다.

스웨덴은 국방부, 법무부, 민간부문 등이 권한을 갖고 사이버 안보 업무를 담당하는 추진체계를 운영하고 있으며, 별도의 컨트롤타워를 설치하고 있지는 않고 있다. 사이버 안보의 실무전담기관은 국방부 산하의 MSB(Myndigheten för samhälskydd och bereskap, Civil Contingencies Agency)가 담당하고 있다. MSB는 민간보호, 공공안전, 위기관리, 민방위 등의 책임을 지면, 사이버 안보전략서(Strategy for Information Security in Sweden 2010–2015)를 발간하기도 했다. 스웨덴 정부는 2018년 6월 IT 보안 관련법을 통과시켰으며, 이는 2018년 8월 1일에 발효되었는데, 이 법은 국가적으로 중요한 부문의 네트워크 운영자에게 적용되는데, 각 운영자들은 네트워크를 보호할 수 있는 적절한 보호 조치를 취해야 하며, 심각한 사고에 대해 관계 당국에 보고하도록 규정하였다. 요컨대, 스웨덴의 사이버 안보 추진체계는, 핀란드의 경우와 유사한 형태의 실무부처 분산형으로 파악된다.

4. 아태지역 국가들의 경우

캐나다에서는 공공안전부(Public Safety Canada, PSC)가 사이버 안보전략의 시행을 조정하는 역할을 맡고 있는데, 이는 미 국토안보부의 역할과 비슷하다. 2018년 이전에는 PSC 내의 GOC(Government Operations Centre)는 국가긴급위기대응시스템의 허브 역할을 담당하며, 그 안에 설치된 CCIRC(Canadian Cyber Incident Response Center)가 사이버 위협의 감시, 자문 제공, 국가적 대응의 지휘 등을 담당했다. 2018년부터는 캐나다 사이버안보센터(Canadian Cyber Security Center, CCSC)가 설립되며 사이버 안보 관련 사안들을 통괄하여 처리하는 구심점으로 작동한다. 사이버안보센터는 기존의 세 부서, 즉 PSC(Public Safety Canada), SSC(Shared Services Canada), CSE(Communications Security Establishment)가 담당하고 있던 사이버 안보 역할을 통합하여 책임진다. 비록 캐나다의 국가보안법이라 불리는 C-59 법안(Bil)가 입법되어, CSE(Communications Security Establishment)와 안보정보청(Canadian Security Intelligence Service)의 역할이 강조되었지만, 아직까지 캐나다에서는 사이버 안보 관련 단일법이 제정되지는 않았다. 요컨대, 캐나다의 사이버 안보 추진체계는 실무부처 분산형의 모습으로 파악된다.

호주에서는 총리가 임명한 사이버 안보 특별보좌관(Special Advisor on Cyber Security)이 컨트롤타워의 역할을 하며 사이버 안보 정책 및 전략 수립을 이끌어가면서, 각 정부 부처 및 기관에 사이버 안보 관련 목표와 우선순위를 설정하는 역할을 수행하고 있으며, 2014년 11월 출범한 ACSC(Australian Cyber Security Center)의 수장도 맡고 있다. ACSC는 사이버 안보 실무를 집행하는 실무전담기관인

데, 2018년 7월부터 통신정보수집, 감청 등을 담당하는 정보기관인 ASD(Australian Signals Directorate)의 부서로 편입되었다. ASD는 2차 대전 이후 설립된 정보기관으로 국방부의 감독을 받으며, 2018년 3월 법정기관이 되었다. 사이버 안보 관련 단일법은 아직 제정되지 않고 있는데, 법률을 제정하기보다는 정부 내의 행정계획, 가이드라인 등에 의존하려는 것으로 보인다. 요컨대, 호주의 사이버 안보 추진체계는 별도의 단일법을 제정하고 있지는 않지만 컨트롤타워 총괄형의 모습으로 파악된다.

대만에서 사이버 안보 컨트롤타워의 역할은 2001년 1월 설치되어 그 기능이 보강되고 있는 NICST(National Information and Communication Security Task force)가 담당하고 있다. NICST의 업무를 지원하기 위해서 2001년 3월 설치된 NCCST(National Center for Cyber Security Technology)가 사이버 안보 관련 기술개발과 지원을 담당하고 있다. 2016년 차이잉원 총통 취임 이후 국가안보 차원에서 사이버 안보전략이 수행되면서 사이버 안보 리더십이 격상되었는데, 2016년 8월에는 NICST의 실질적 운영을 총괄하는 실무기구로서 사이버 안보부(Department of Cyber Security, DCS)가 행정원 내에 설치되었으며, 2017년 1월에는 독립적인 사이버 안보부대인 ICEF(Information Communication Electronic Force Command)가 설치되어 사이버전에 대응하는 국방역량을 강화했다. 한편 대만은 2018년 5월 최초의 사이버 안보법인 사이버안보관리법(Cybersecurity Management Act)을 통과시켰는데, 이는 2019년 1월 발효되었다. 요컨대, 대만의 사이버 안보 추진체계는 단일법을 제정한 컨트롤타워 총괄형의 모습으로 파악된다.

싱가포르의 사이버 안보전략은 2015년 총리실 직속으로 설치되었으며 행정편제상으로는 통신정보부의 관리를 받는 사이버안보청(Cyber Security Agency of Singapore, CSA)을 중심으로 추진된다. CSA의 설치로 인해 이전에는 SingCERT(Singapore Computer Emergency Response Team), IDA(Info-communication Development Authority), SITSA(Singapore Technology Security Authority) 등의 3개 부서로 산재되었던 사이버 안보 기능이 하나로 통합되었다. CSA는 사이버 안보 정책의 개발, 주요 정보 인프라의 핵심 서비스의 보호, 대규모 사이버 사고에 대한 정책 조정 등의 업무를 담당한다. 싱가포르는 2018년 2월 사이버 안보 법안을 통과시켰는데, 이 법안은 CSA와 통신정보부의 주도로 작성된 것으로 사이버 안보를 적극적으로 실천할 수 있는 법적 프레임워크의 의미를 갖는다. 사이버안보위원장직(Commissioner)을 신설하여 사이버 안보 관련 사고를 조사할 수 있는 권한을 부여하고, 주요 정보 인프라 소유자들이 시설 보호를 위해 능동적인 조치를 취하도록 하는 등 한층 선제적이고 능동적인 사이버 안보 프레임워크를 수립하였다. 요컨대, 싱가포르의 사이버 안보 추진체계는 단일법 제정을 바탕으로 한 컨트롤타워 총괄형의 모습으로 파악된다.

이스라엘의 경우에는 총리실 산하 국가사이버국(National Cyber Bureau, NCB)이 사이버 안보의 컨트롤타워 역할을 담당하고 있다. NCB는 사이버 공격 대응, 보안 산업 투자촉진, 대학 R&D·교육·산업·경제 성장 엔진으로 사이버 기술 개발, 국제협력 등 모든 사이버 안보 관련 업무를 총괄한다. 한편 총리실 산하 국가사이버보안국(National Cyber Security Authority, NCSA)이 실무전담기관의 역할을 담당하고 있다. 2014년 총리실 산하에 사이버보안 관할 전담기관(NCSA)이 독립적으로 설치된 것은 이스라엘이 설정한 사이버 안보 이슈의 중요도를 가늠케 한다. NCSA는 공공기관, 각종 정부 기관 및

장관실, 중요 부문, 사회 기반 시설, 국방 산업 등은 물론 민간 기업과 국민 개인이 최대한의 보안을 누리게 하는 책임을 지고 있다. 이들 기관과의 업무연계 속에서 경제산업부, 국방부 등의 실무기관이 사이버 안보 업무를 담당한다. 요컨대, 이스라엘의 추진체계는 별도의 법을 제정하고 있지는 않지만 정부기구 내에서 명시적인 컨트롤타워를 설치한 유형으로 파악할 수 있다.

V. 16개국 비교분석의 함의

이 책에서 시도한 비교분석의 함의를 도출하기 위해서 앞서 제기했던 질문들을 다시 한 번 환기해 보자. 사이버 안보전략의 대내외적 정책 지향성과 관련하여, 우선적으로 제기했던 질문은 각국의 국가안보전략 전반에서 사이버 안보전략이 차지하는 위상과 방향 및 강조점은 무엇인가의 문제였다. 좀 더 구체적으로 국방전략과의 관련 속에서 사이버 안보위협의 원인에 대한 인식과 이에 대응하는 실천전략과 대응태세의 특징은 무엇이며, 주변국들과의 사이버 안보 공조체제의 구축양식이나 지역 차원의 국제협력에의 참여형태 및 글로벌 차원의 국제규범 형성 과정에 대한 외교적 입장에 대해서도 탐구하였다. 한편 사이버 안보전략의 추진체계와 관련하여, 사이버 안보 분야의 업무를 총괄하는 컨트롤타워와 실무를 맡은 실무전담기관의 설치 여부 및 양자의 관계설정은 어떠하며, 사이버 안보의 대응력 강화를 위해 마련된 법제정의 여부 또는 관련법의 존재형태 등에 대해서도 문제를 제기하였다. 이 장에서는 16개국을 다섯 그룹으로 구분하였으며, 그러한 구분의 근거가 되는 내용을 개괄하여 살펴보았다. 이러한 분석을 바탕으로 도출되는 16개국 비교분석의 함의는 다음과 같은 여섯 가지로 요약된다.

첫째, 모든 국가들이 점점 더 사이버 위협의 문제를 국가안보의 시각에서 인식하고, 이에 대한 대비책을 한층 강화하고 있다는 사실이다. 물론 각국별로 국가안보전략 전반에서 사이버 안보전략이 차지하는 위상과 방향 및 강조점 등은 다르게 나타난다. 그럼에도 사이버 안보의 전략적 우선순위를 높이고 이를 실현하기 위한 물적·인적 역량의 강화와 법제도 정비에 박차를 가하고 있다는 공통점이 있다. 이 책에서 살펴본 각종 전략서나 기구의 설치 및 법 제정 등의 사례는 이러한 추세를 잘 보여준다. 또한 이들 국가는 모두 사이버 안보의 문제를 단순한 '안보화'의 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. 그런데 여기서 주목할 점은 이러한 인식과 실천이 모두 동일한 형태의 추진체계 도입이나 법제도의 제정으로 수렴하고 있지는 않다는 사실이다. 아무리 사이버 공격의 피해 가능성이 높더라도 모든 국가들이 집중적인 형태의 컨트롤타워를 설치하거나 단일법 형태의 사이버 안보 관련법을 제정하는 형태로 반영하지는 않고 각국의 사정에 적합한 다양한 형태의 추진체계와 법을 도입하고 있다.

둘째, 국방전략 전반의 맥락에서 사이버 안보 위협의 원인을 어떻게 인식하고 있으며, 이에 대비한 구체적인 대응전략을 어떻게 갖추고 있느냐의 문제는 사이버 안보전략의 중요한 관건이다. 이와 관련하여 북유럽 및 서유럽 국가들의 사이버 안보전략은 러시아의 사이버 위협을 전통적인 군사적 위협과 더불어 매우 심각하게 인식하고 있다. 특

히 에스토니아, 핀란드, 스웨덴 등이 그러하고, 독일, 영국 등도 러시아를 사이버 공격의 주적으로 상정한다. 아태 지역 국가들의 사이버 안보전략에서 중국도 주요 사이버 위협으로 상정된다. 중국을 주적으로 삼는 가장 대표적인 사례는 대만이다. 미국과 일본도 중국의 사이버 위협에 대응한다는 명문으로 사이버 안보전략을 강화해 왔다. 이들 국가의 국내정치에서 사이버 안보는 개관적으로 실재하는 위협인 동시에 주관적으로 구성되는 '안보화'의 변수이다. 사이버 안보의 군사적 성격과 함께 산업기술적 측면을 강조한 민군겸용기술의 시각에서 접근하는 시도는 이스라엘과 대만에서 두드러진다. 이들 국가에게 사이버 안보 문제는 기술경쟁력과 국가브랜드를 의미한다. 한편 싱가포르, 프랑스, 캐나다 등은, 전통안보의 군사적 위협보다는, 신흥안보의 초국적 위협이라는 관점에서 사이버 안보에 접근하고 있으며, 핀란드와 스웨덴은 좀 더 포괄적인 의미에서 이해한 사회안보(societal security)의 차원에서 사이버 안보의 문제를 본다. 군사보다는 외교의 관점이 더 많이 가미된 사이버 안보전략의 추진 국가로는 네덜란드와 호주가 있다.

셋째, 사이버 안보 국제협력과 외교전략의 추진이라는 관점에서 주변국과의 공조체제를 어떻게 구축하고 있으며, 지역 차원의 국제협력에는 어떻게 참여하고, 더 나아가 글로벌 차원의 국제규범 형성 과정에 대해 어떠한 입장을 취하느냐의 문제도 사이버 안보전략의 지향성을 이해하는 중요한 관건이다. 에스토니아, 일본, 이스라엘, 대만 등은 동맹협력의 관점에서 사이버 안보에 접근한다. 그 이면에는 미국이 주도하는 사이버 안보 분야의 동맹전략이 있다. 영국, 캐나다, 호주 등과의 파이브 아이즈 동맹도 매우 중요한 국제협력의 형식이다. 영국과 네덜란드는 서방 진영의 우방국들이 형성하는 정부 간 네트워크의 틀을 빌어 사이버 안보의 국제협력 전략을 추구한다. 이에 대항하여 중국과 러시아가 주도하는 정부 간의 지역협력체의 사이버 안보 협력에도 주목해야 한다. 한편 핀란드, 독일, 프랑스 등은 유럽연합 차원에서 사이버 안보의 국제협력을 추진하고 있으며, 스웨덴은 유럽연합보다는 작은 범위에서 노르딕 국가들의 지역협력을 주도하고 있다. 아세안 지역협력을 주도하는 싱가포르의 전략이나, 남태평양 지역협력의 맹주 역할을 하는 호주의 사례에도 주목해야 한다.

넷째, 일견 컨트롤타워를 두는 것이 전반적인 추세로 파악되고 있을지라도, 사이버 안보를 추진하는 각국의 체계, 특히 각국의 사이버 안보 컨트롤타워의 현황과 거버넌스 아키텍처는 각기 다르게 나타나고 있다. 각국의 정부기구의 성격에 따라서 컨트롤타워에 해당하는 공식적(*de jure*) 기구를 설치하는 경우, 즉 중국의 중앙인터넷안전정보화위원회, 일본의 사이버시큐리티전략본부, 프랑스의 국가정보시스템보안국(ANSSI), 호주의 사이버안보특별보좌관, 네덜란드의 사이버안보위원회(CSR), 이스라엘의 국가사이버국(NCB), 대만의 국가정보통신안보태스크포스(NICST) 등과 같은 경우도 있지만, 싱가포르의 사이버안보청(CSA)처럼 독립기관을 설치하여 컨트롤타워의 역할을 맡기거나, 사실상(*de facto*)의 컨트롤타워 역할을 하는 정부기능이 있는 경우, 즉 미국 오바마 2기의 사이버안보조정관, 러시아의 정보보안부(FSB), 독일의 연방내무부 등과 같은 경우도 있으며, 굳이 법제도적 접근을 하지 않고 운영의 묘를 살려서 이원시스템이 작동하는 경우, 즉 영국의 내각부 내 사이버보안청(OCSIA)과 외교부 내 정보통신본부(GCHQ)의 이원 시스템과 같은 경우도 있다. 결국 사이버 안보에 대처하는 방식에는 획일적으로 공식적 컨트롤타워를 설치하는 것만이 능사는 아니고, 경우에 따라서 관련 기관들의 역할을 조율하면서 운영

의 묘미를 살리는 부분도 중요하다.

다섯째, 대체로 사이버 안보 정책을 담당하는 실무전담기관(주로 NCSC)의 설치하는 추세이지만, 이러한 실무전담기관의 유무 및 설치 위치가 나라마다 조금씩 다르다. 다시 말해, 실무전담기관을 컨트롤타워에 두느냐, 아니면 사이버 안보전략을 총괄 수행하는 실무기관들을 설치하고 그 안에 두느냐 등의 문제는 나라마다 다르다. 컨트롤타워 산하에 실무전담기관이 설치된 경우로는 일본 총리 산하 사이버시큐리티전략본부 내 내각사이버시큐리티센터(NISC), 중국 국무원 내 국가인터넷정보판공실(사무기구), 프랑스 국가정보시스템보안국(ANSSI) 내 정보시스템보안운영센터(COSSI), 호주 ACSC(사이버안보특별보좌관이 수장을 맡음, 2018년 7월부터 ASD의 부서로 편입), 대만 NICST 내의 NCCST(2016년 이후 DCS), 이스라엘 NCB 산하(?)의 NCSA 등의 사례를 들 수 있다. 사이버 안보전략을 총괄 수행하는 실무기관들에 설치되는 경우로는 미국 국토안보부(DHS) 산하 CISA내의 NCCIC, 영국 외교부 산하 정보통신본부(GCHQ) 내 국가사이버안보센터(NCSC), 독일 연방내무부 산하 연방정보기술보안청(BSI) 내 국가사이버방어센터(Cyber-AZ), 러시아 연방보안부(FSB) 내 정보보안센터(ISC), 에스토니아 경제통신부 내의 RIA, 네덜란드 치안법무부 내의 NCSC, 핀란드 교통통신부 산하의 FICORA(2019년 1월 TRAFICOM으로 병합), 스웨덴 국방부 산하의 MSB, 캐나다 공공안전부 내 CCIRC 등을 사례로 들 수 있다.

끝으로, 사이버 위협에 효과적으로 대응하기 위한 법제도를 제정하는 문제에 있어서도, 최근 미국, 일본, 중국 등 주요국들이 모두 사이버 안보와 관련된 국내법을 제정하는 추세이지만. 모든 나라가 획일적으로 단일법 제정을 도모하는 것은 아니고 각 나라의 사정에 따라

필요한 법을 어떤 내용과 형식으로 제정·운영할 것인가가 다르다. 범정부 차원에서 정책을 관장하는 컨트롤타워를 설치하고 그 업무를 지원하는 단일법을 제정하는 나라(일본 사이버시큐리티법, 중국 인터넷안전법, 에스토니아의 사이버안보법, 네덜란드의 사이버안보법, 대만 사이버안보관리법, 싱가포르 사이버안보법)가 있는가 하면, 국가와 국방 전반을 포괄적으로 규정한 법에서 사이버 안보를 규정하는 나라(프랑스 국방법전과 디지털국가법)도 있고, 실무부처들이 각기 소관 영역의 법으로 사이버 안보 업무를 담당하는 나라(독일 IT안보법, 핀란드, 스웨덴, 이스라엘)도 있으며, 새로이 법을 제정하지 않고 대통령 명령이나 독트린에 의거해서 정책을 추진하는 나라(러시아의 사례)도 있다. 이상의 양식들을 적절히 아울러서 개별 실무부처의 업무를 조정하는 시스템을 갖추거나 개별법들을 집합적으로 조정하여 적용하는 일종의 메타 거버넌스형의 추진체계를 구비한 나라(미국 CISA, 영국 수사권법, 캐나다, 호주)도 있다.

VI. 맺음말

이들 16개국의 사례에 대한 비교분석은 한국의 사이버 안보전략에 주는 일반론적 함의를 던진다. 사실 이들 국가의 사례는 사이버 안보전략 분야의 세계적인 선도국들로서 한국에게는 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. 이러한 맥락에서 볼 때 사이버 위협의 성격을 정확히 이해하고 한국의 현실에 적합한 사이버 안보의 추진체계 모델을 모색하는 것이 필요하다. 이러한 맥락에서 볼 때, 향후 연구과제로 한국과 유사한 처지에 있는 사례를 살펴본 작업의 유용성이 있다. 그럼에도 궁극적으로 필요한 것은 한국의 현실에 맞는 사이버 안보전략을 스스로 고민하는 성찰적 노력일 것이다.

특히 이상의 비교분석은 한국의 사이버 안보 추진체계 정비와 관련하여 중요한 시사점을 준다. 이상의 내용을 종합해서 판단해 볼 때, 사이버 안보의 경우는 기본적으로 각 부문이 알아서 사이버 안보의 대응체계를 마련하고 그러한 체계의 추진과정에서 발생하는 문제들을 컨트롤타워(또는 조종타워)의 차원에서 대응하는 이원적 시스템이 적합한 것으로 판단된다. 이는 추진체계의 구조상으로는 분산형의 구조를 갖추면서도 추진체계가 운영되는 과정에서 필요에 따라서 집중형 거버넌스를 도입하는 형태이다. 사실 사이버 안보 분야에서는 전통안보에 대응하는 경우처럼, 국가가 나서서 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 포괄하는 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 한다.

참고문헌

김상배. 2014.『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』, 한울.
김상배. 2018a.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』, 한울.
김상배. 2018b. "트럼프 행정부의 사이버 안보전략: 국가지원 해킹에 대한 복합지정학적 대응."『국제·지역연구』27(4), pp.1-35.
김상배. 2019. "동아태 사이버 안보 거버넌스: 국제협력과 지역규범의 모색." 김상배·신범식 편.『동북아 신흥안보 거버넌스: 복합지정학의 시각』, 사회평론
김상배 편. 2017.『사이버 안보의 국가전략: 국제정치학의 시각』, 사회평론.
김상배 편. 2019.『사이버 안보의 국가전략 2.0: 국제규범의 형성과 국제관계의 동학』, 사회평론.
김상배·민병원 편. 2018.『사이버 안보의 국제정치학적 지평: 전략과 외교 및 규범』, 사회평론.