제2장

미 · 일 · 중 · 러의 사이버 안보전략*

김상배 | 서울대학교

* 이 장은, 이 책에서 시도한 16개국 비교분석의 전체구도를 보여주기 위한 목적으로, 김상배(2018a)의 제5장에서 다룬 미국, 일본, 중국, 러시아의 사이버 안보전략에 대한 내용을 바탕으로 하여, 최근 미국의 변화를 살펴본 김상배(2018b)의 일부 내용을 반영하여 작성되었다.

I. 머리말

2010년대 중후반을 거치면서 사이버 안보는 중요한 국가전략적 사안으로 자리매김을 해가고 있다. 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. 적대국의 해킹이 원인으로 지목되는 가짜뉴스와 선거개입 논란이 국내정치의 쟁점이 되었다. 이러한 강대국들 간의 사이버 공방으로부터 한국도 자유로울 수 없다. 최근 들어 중국과 러시아의 해커들이 한국을 공격하는 일도 잦아졌다. 국가지원 해킹으로 의심되는 사건들 외에도 크고 작은 해킹 사건들이 공개적으로 알려지지 않으면서도 끊임없이 발생하고 있다. 이러한 다양한 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.

이러한 문제의식을 바탕으로 이 장은 세계 주요국, 특히 한반도 주변4국으로 대변되는 미국, 일본, 중국, 러시아의 사이버 안보전략과 추진체계를 살펴보았다. 사실 이 나라들은 오랫동안 한국이 정책과 제도모델을 고민하는 과정에서 일종의 '일반모델'로서 참조되었던 대표적인 나라들이다. 이들 국가의 행보를 이해하는 것이 중요한 이유는 현 시점에서 한국이 모색할 사이버 안보전략의 기본방향과 구성내용을 검토하고 이를 토대로 구체적인 실천방안을 궁리하려는 필요성 때

문이다. 더 나아가 기존의 산업화 및 정보화 전략의 경우처럼 사이버 안보 분야에서도 한국이 스스로 '모델'을 개발하려는 기대 때문이기도 하다. 한국의 현실에 맞는 '한국형 사이버 안보전략 모델'을 장차 스스로 추구해야 맞겠지만, 그 준비단계에서 주변 4개국의 사례를 살펴보는 작업의 의미는 충분하다.

이 장은 다음과 같이 구성되었다. 제2절은 사이버 안보 분야의 전략형성과 제도화를 주도하고 있는 미국의 사례를 오바마 행정부 시기의 형성과정과 트럼프 행정부 시기의 변화를 중심으로 살펴보았다. 사이버 안보전략의 형성배경과 컨트롤타워의 구성과 변화, 그리고 백악관과 구체적인 정책과 법안 제정의 노력 등을 다루었다. 제3절은 일본의 사이버 안보전략을 전략 형성, 사이버 국방, 국제협력, 추진체계, 법제정 상황 등에 초점을 맞추어 살펴보았다. 제4-5절은 미국 주도의 질서에 도전하는 비서방 국가의 대표격인 중국과 러시아의 사이버 안보전략을 앞서의 미국과 일본의 사례를 살펴본 분석틀에 준하여 살펴보았다. 맺음말에서는 주변4개국의 비교분석이 던지는 함의를 짚어보았다. 끝으로, 보론에서는 이스라엘의 사이버 안보전략과 추진체계를 추가하였다.[1]

1 이 책의 구성에 따르면 이스라엘의 사례연구는 제3부 아태지역 국가의 사례연구에서 본격적으로 다루어져야 하지만, 현실적으로 자료입수와 문헌접근이 제한되어 있는 관계로 이 장의 보론 형태로 간략히 살펴보았다.

II. 미국의 사이버 안보전략과 추진체계

1. 사이버 안보 국가전략의 형성배경

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 안보전략의 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 백악관으로 이전시켰는데, 백악관 컨트롤타워로서 사이버안보조정관(Cybersecurity Coordinator)을 신설하였다. 엄밀하게 보면 사이버안보조정관의 역할을 한 백악관 특보는 2003년부터 활동했다. 국무부에도 대외협력을 담당한 사이버조정관(Coordinator for Cyber Issues)이 국무장관 산하에 설치되었다.

이 무렵 미국의 사이버 안보전략에는 '군사화' 담론이 강하게 가

미되기 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 전개과정에서 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 안보전략을 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. 아태지역에서도 일본, 호주, 한국 등과 사이버 안보 협력을 도모했다.

미국은 국제기구와 다자외교의 장에서도 사이버 안보 분야의 국제규범 형성과정에 참여했는데, 유엔 GGE나 ITU 등과 같은 기성 국제기구의 틀을 활용하기보다는, 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.

2. 사이버 안보의 추진체계 및 법제

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 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 2009

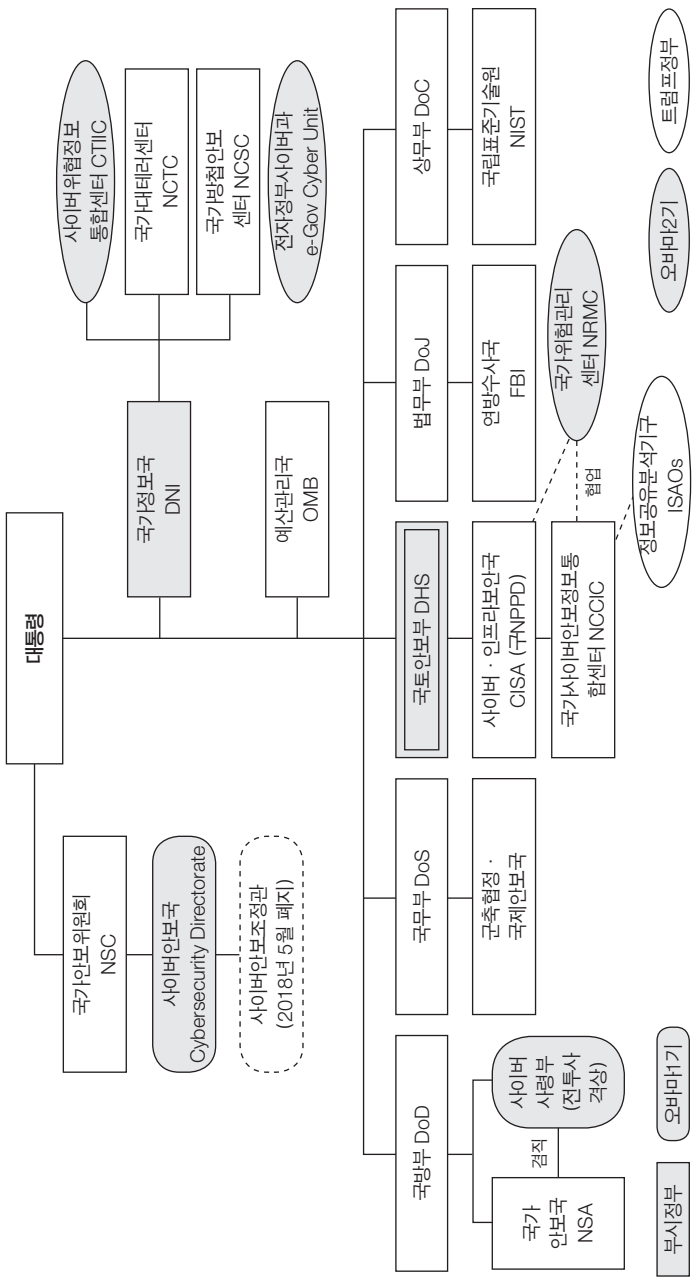

그림 2-1. 미국의 사이버 안보 추진체계
출처: 김상배(2018a), p.155를 보완 · 수정

년 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 기능을 갖추는 형태로 진화했다(〈그림 2-1〉 참조). 부시 행정부에서는 국토안보부(DHS)와 국가정보국(DNI)이 총괄 기능을 수행했다. 오바마 행정부 1기에 접어들어 국가안보위원회(National Security Council, NSC) 산하 사이버안보국(Cybersecurity Directorate) 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(Cyber Threat Intelligence Integration Center, CTIIC)가 설치되어 사이버 위협과 사고를 종합적으로 분석하여 유관기관에 정보를 제공케 했다. 국가방첩안보센터(National Counterintelligence and Security Center, NCSC)는 사이버 위협 및 공급망 보안, 주요기반시설에 관한 역할을 수행한다. 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 설치하여, 국토안보부 산하에서 민관 정보공유를 담당하는 국가사이버안보정보통합센터(National Cybersecurity and Communications Integration Center,

NCCIC)와 협력하도록 했다(김상배 2018a, 155-156).

3. 사이버 안보 컨트롤타워의 변화

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 역할을 맡아왔었다. 그의 사임이 새로이 백악관 국가안보보좌관에 강경파인 존 볼턴(John Bolton) 전 유엔대사가 취임한 지 하루 뒤에 이루어졌다는 점에서 구설수에 오르기도 했다(『뉴시스』, 2018-04-11). 보서트 보좌관 사임 며칠 후 롭 조이스(Rob Joyce) 사이버안보조정관은 사직하고 국가안보국(NSA)으로 복귀했다(*Nextgov*, April 16, 2018). 2018년 5월에는 사이버 안보 업무의 컨트롤타워 역할을 담당했던 사이버안보조정관의 직책 자체가 폐지되었다(*Hepnetsecurity*, 2018-05-16).

이러한 추진체계의 변화는 미국의 사이버 안보전략의 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 안보전략을 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 공격적인 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).

4. 행정명령과 국가사이버전략 발표

2017년 출범 이후 트럼프 행정부의 사이버 안보전략이 즉시 공세적으로 추진되어 러시아, 중국 등과의 관계가 악화될 가능성이 전망되었으나, 실제로 2017년에는 미러, 미중 등 강대국 관계는 다소 소강국면을 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 안보전략을 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 제

출을 지시하였다(Presidential Executive Order 13800, May 11, 2017).

트럼프 행정부의 공세적 태도 변화는 2018년 9월 15일 트럼프 대통령이 지난 수년 동안 미국 사이버 안보정책의 가이드라인을 제시했던 오바마 대통령의 정책지침 PPD-20을 폐지하는 행정명령에 서명하면서 나타났다(#Security Newspaper#, September 15, 2018). 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 목표를 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).

5. 실무부처 차원의 복합적 대응

이러한 행정명령들과 '국가사이버전략'에 의거하여 미국 정부는 실무부처 차원에서 국가지원의 사이버 공격에 대한 다양한 대응전략을 모색하고 있다. 우선, 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 행정부와 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, 국가핵심기능에 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, 이는 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 통합전투사령부로 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 공격을 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 뉴욕 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 IT제품의 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.

이 밖에도 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 실태평가와 계획보고서 제출을 지시했던 2017년 5월의 대통령 행정명령에 의거하여 2018년 5월 국무부는 '사이버위협 전략적 대응 옵션 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 정부간 활동, 비(非)국가 포럼을 통한 정책 및 기술표준 설정에의 참여, 동반자 국가들의 위협 대응을 위한 역량 구축의 지원 등과 같은 내용들이 담겼다. 이 밖에도 국무부는 다양한 사이버 안보의 국제규범 형성

과정에 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.

6. 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 추가제재 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 위협 대응 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.

III. 일본의 사이버 안보전략과 추진체계

1. 사이버 안보 국가전략 형성의 배경

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 안보전략'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 안보전략은 자유롭고 공정한 사이버 공간의 실현을 목표로 내걸고 정보의 자유로운 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, 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, 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, 229-236).

2. 사이버 안보 관련 법제정 및 추진체계

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 안보전략의 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 2-2〉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, 158-159). NISC가 사이버 안보전략을 총괄·조정하는 가운데, 방위성과 자위대는 사이버 국방, 외무성은 사이버 국제협력, 경제산업성은 IT산업정책, 총무성은 통신 및 네트워크

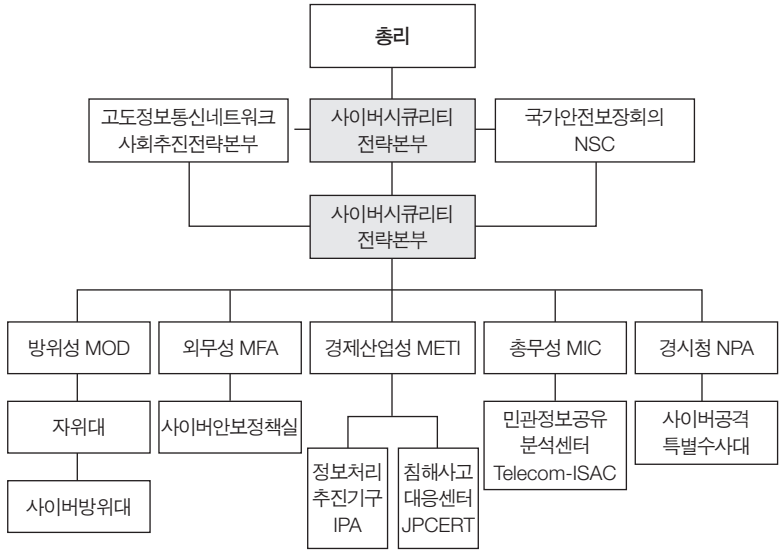

그림 2-2. 일본의 사이버 안보 추진체계

출처: 김희연(2015), p.52를 기반으로 보완하여 작성

정책, 경시청은 사이버 범죄 대응 등의 분야를 맡아서 실무부처 차원의 소관 업무를 실행하는 구도를 형성하고 있다.

IV. 중국의 사이버 안보전략과 추진체계

1. 사이버 안보 국가전략 형성의 배경

중국에서는 1990년대 후반부터 금순공정(金盾工程, Golden Project)이라는 이름으로 사이버 안보 관련 정책을 추구해 왔는데, 시진핑 체제가 본격적으로 자리를 잡으면서 좀 더 공격적으로 사이버 안보전

략을 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 왔다. 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 해당하는, 인터넷기초총부를 창설했다. 총참모부 산하 3부서는 사이버 작전을 수행하고 있는데, 지난 수년간 미국 정부기관과 기업 등을 해킹한 것으로 의심을 받고 있는 61398부대가 이 3부서 소속이다(정종필·조윤영 2017, 182-183). 2015년 10월에는 중국군이 군 개혁의 일환으로 사이버전통합사령부를 창설할 것을 천명했다(『연합뉴스』, 2015.10.26.). 그리고 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 2018년까지 중국 우전에서 개최한 세계인터넷대회(World Internet Conference)인데, 중국은 각국의 사이버 주권을 강조하며 안전한 사이버 공간의 구축을 위한 국제연대를 주창했다. 중국은 상하이협력기구(SCO), 아세안지역안보포럼(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).

2. 사이버 안보의 추진체계 및 법제

사이버 안보와 관련된 중국의 국가주권 수호의 의지는 관련법의 제정과정에서도 나타났다. 2015년 7월 중국 전국인민대표대회가 〈신국가안전법〉을 통과시키면서 사이버 공간의 테러와 해킹에 대응하는 중국

의 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(『한겨레』, 2015.7.1.).

한편 2016년 12월에는 〈인터넷안전법〉이 제정되었다. 〈인터넷안전법〉은 핵심 기반시설의 보안 심사 및 안전 평가, 온라인 실명제 도입, 핵심 기반시설 관련 개인정보의 중국 현지 서버 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 설치되었다(〈그림 2-3〉). 국무원 차원에서는 2011년 설립된 국가인터넷정보판공실은, 사이버 관련 정부 부처들이 인터넷 정보 관리를 강화하도록 지도·감독하고, 인터넷 뉴스 및 기타 업무에 대한 허가 및 감독권을 갖고 있다.

실무부처 차원에서는 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 대응

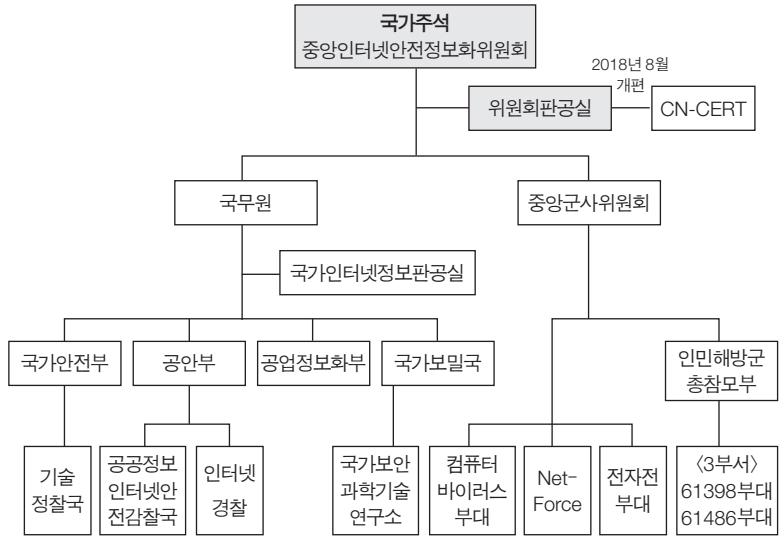

그림 2-3. 중국의 사이버 안보 추진체계

출처: 김희연(2015), p.49를 수정 · 보완

활동을 벌인다. 국가보밀국은 보안 감사, 보안정책 수립, 통제 감독 등 공공기관의 보안 업무 전반을 관장하고 있으며, 그 산하에 국가보안과학기술연구소를 운영하고 있다(양정윤·배선하·김규동 2015).

3. 사이버 안보 추진체계의 최근 변화

2018년 3월 중국공산당 중앙위원회는 『당과 국가기구 개혁 심화방안(深化黨和國家機構改革方案)』을 발표하였으며 당과 국무원의 여러 기관과 부서에 대한 개혁을 실시하였다. 중앙인터넷안전정보화영도소조는 중앙인터넷안전정보화위원회(中央網絡安全和信息化委員會)로 바꾸었다. 이와 더불어 중국 공산당은 중앙전면심화개혁영도소조, 중앙재경영도

소조, 중앙외사업무영도소조 등도 모두 위원회로 바꾸는 조치를 단행했는데, 새롭게 설치된 위원회는 관련 영역에서의 중요한 업무의 최상위급 디자인, 총체적인 업무 포석, 통합과 협조, 전면적인 추진, 그리고 감독과 시행 등 총괄적인 업무를 담당하게 되었다. 기존의 '영도소조'는 당의 공식적인 기구라기보다는 특정 업무를 효율적으로 처리하기 위한 임시적 성격이 강하며, 그 권한도 업무에 대한 논의와 협조에 그치지만, '위원회'는 당의 최고 의결기구인 당중앙위원회 산하의 공식적인 기구로 실질적인 사업 추진의 권한을 갖고 있어서, '영도소조'일 때나 '위원회'일 때나 구성원은 거의 같지만 당 안에서 기구의 공식성이나 권한이 한층 강화되었다고 볼 수 있다.

한편 기존에는 공업정보화부 산하에 있던 국가인터넷비상센터(CN-CERT)를 중앙인터넷안전정보화위원회판공실 밑으로 이동시켰다. CN-CERT의 핵심 업무는 직능부문에 대한 조기 경비와 인터넷 데이터 지원 등이 있으며, 크게는 은행, 전기 등 인터넷 시스템을 지키는 것에서부터 작게는 피싱 사이트를 식별하여 개인의 정보안전을 보호하는 업무를 담당한다. 뿐만 아니라 CN-CERT는 인터넷과 정보안전의 기술연구에도 일정한 역할을 하고 있다. 이러한 CN-CERT의 소속 변화는 중앙인터넷안전정보화위원회와 공업정보화부 사이에서 서로의 직권 배분가 더욱 뚜렷하고 명확해진 것으로 평가할 수 있다. 중앙인터넷안전정보화위원회는 국가 인터넷 안보를 지키는 데 관련 직능을 더욱 강화시켰다. 그리고 2018년 8월 15일 중앙인터넷안전정보화위원회가 주관하고 CN-CERT가 주최한 제15회 중국 인터넷 안전 연례회의(中国互联网安全年会)가 베이징 국가회의센터에서 개최되었는데, 이는 CN-CERT가 인터넷안전정보화위원회의 지도를 받고 있는 상하관계에 놓여 있음을 보여주는 일이었다.

V. 러시아의 사이버 안보전략과 추진체계

1. 사이버 안보 국가전략 형성의 배경

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 밀려 있는 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 못

했다는 자체 평가에 따라 러시아군 내에 사이버전을 전담하는 사이버전 부대를 창설하였는데, 이는 러시아가 적극적인 공세정책으로 전환하는 상징적 사건으로 이해되었다(신범식 2017, 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 아세안지역안보포럼(ARF)의 사이버 안보 협의에도 적극 참여하고 있다(신범식 2017, 262-266).

2. 사이버 안보의 추진체계 및 법제

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, 255-256).

러시아의 사이버 안보 추진체계는 연방보안부(FSB)가 관련 기관을 총괄하는 구조로 되어 있다(〈그림 2-4〉). FSB는 국가비밀을 포함한 주요 정보에 대한 통제와 예방 조치는 물론, 관련 기관에 대해 기술

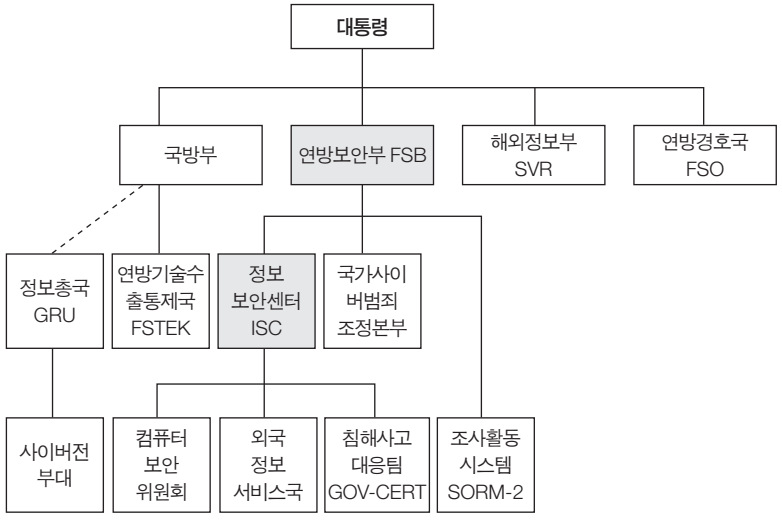

그림 2-4. 러시아의 사이버 안보 추진체계

출처: 조성렬(2016), p.405를 수정 · 보완

및 암호 서비스를 제공한다. FSB 산하 정보보안센터(ISC)는 통신보안 업무와 정보보호 시스템의 평가 및 인증을 총괄·조정하고, 침해사고대응팀(GOV-CERT)을 운영하며, 비밀리에 공격기술을 개발하고 각급 정보를 수집하는 업무까지도 담당하고 있다고 한다. 한편 FSB 산하에는 국가사이버범죄조정본부라는 특수분과가 설치돼 러시아 연방기관들의 인터넷 홈페이지 보안을 담당하고 있는 것으로 알려져 있다(『Russia포커스』, 2015.6.26.). 정보 및 보안기관 중에서 예산을 가장 많이 사용했던 연방통신정보국(FAPSI)는 2003년 해체되고, 그 기능이 연방보안국(FSB) 이외에도 해외정보국(SVR), 연방경호국(FSO) 등으로 이관되었다. FSB는 조사활동시스템(SORM-2)의 프로그램을 이용해 러시아 내의 인터넷 서비스망을 통해 광범위한 정보를 수집하고 있다. 그리고 국방부 산하 연방기술수출통제국(FSTEK)에서는 국가정책

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

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. 이러한 문제의식을 바탕으로, 이 장은 사이버 위협에 대응하는 전략과 제도를 마련하고 있는, 한반도 주변4개국, 즉 미국·일본·중국·러시아의 사례를 비교의 시각에서 살펴봄으로써 향후 한국이 사이버 안보 분야에서 모색할 국가전략의 방향을 가늠하고자 하였다.

이들 국가가 지난 10여 년 동안 추진해온 사이버 안보전략을 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 장에서 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 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 안보전략의 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 '글로벌 거버넌스 프레임'의 국가들이 있는가 하면, 정부 주도로 정치 논리를 앞세워 자국체제의 이데올로기를 고수하려는 '국가주권 프레임'을 강조하는 국가들도 있으며, 이 두 프레임이 형성하는 스펙트럼의 중간지대에 위치하는 '복합 프레임'의 정책을 펴는 국가들도 있다. 이 장의 분석에 따르면, 이러한 차이는 대략 미국과 일본으로 대변되는 서방 진영의 프레임과 중국과 러시아로 대변되는 비서방 진영의 프레임의 대립 구도로 나타난다.

사이버 안보의 추진체계 측면에서 본 각국의 차이도 간과할 수 없다. 대체로 사이버 안보 정책을 담당하는 기관의 설치나 이를 지원하는 법을 제정하는 추세이다. 이 글에서 다룬 국가들은 형태와 명칭이 다르지만, 미국의 DHS, 일본의 NISC, 중국의 '위원회,' 러시아의 FSB, 영국의 NCSC 등과 같이 사이버 안보전략을 총괄 수행하는 기관들을 설치하고 있다. 그러나 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), 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)도 있다.

이들 국가의 사례에 대한 비교분석은 한국의 사이버 안보전략에 주는 일반론적 함의를 던진다. 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 위협도는 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

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

김상배. 2018a.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』, 한울엠플러스.

김상배. 2018b. "트럼프 행정부의 사이버 안보전략: 국가지원 해킹에 대한 복합지정학적 대응."『국제·지역연구』 27(4), pp.1-35

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

『뉴스1』, 2018-09-21. "美 '사이버위협에 공격적 대응'…北·中·러 등 겨냥."

『뉴시스』, 2017-11-28. "美 법무부, 해킹·지적재산권 도용 혐의로 중국인 3명 기소."

『뉴시스』, 2018-04-11 "트럼프 핵심참모 또 백악관 떠나… 보서트 국토안보 보좌관 사임."

『보안뉴스』, 2018-08-20, "中 통신장비 정조준 美 국방수권법, 韓 5G 장비 수출 '기대'."

송은지. 2016. "이스라엘의 사이버보안 정책 및 시사점: 인력양성 및 산업육성 정책을 중심으로."『정보통신방송정책』 28(18), 정보통신정책연구원, pp.1-18

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

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

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

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

『조선일보』, 2018-08-20. "볼턴 '중국·북한도 美 중간선거 개입 우려'."

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

『MK뉴스』, 2018-10-31. "이번엔 미 법무부가 중 압박."

『OBS 뉴스』, 2018-10-31. "서방, 중 패권 핵심 'IT굴기' 봉쇄 박차."

Department of Defense. 2018. *DoD Cyber Strategy*. United States of America.

『Hepnetsecurity』, 2018-05-16. "White House Eliminates Cybersecurity Coordinator Role."

『Nextgov』, April 16, 2018. "White House Cybersecurity Coordinator Leaving Office."

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.

Presidential Executive Order 13800. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." May 11, 2017.

『Security Newspaper』, September 15, 2018. "New Trump's Executive Order against Possible Election Intervention."

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, and Openness in a Networked World*. May.

White House. 2018. *National Cyber Strategy of the United States of America*. September, 2018.

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.