경북대학교 법학연구원『법학논고』
제67집 (2019.10) 311~340면.
Kyungpook Natl. Univ. Law Journal
Vol.67 (Oct 2019) pp.311~340.

사이버안보 법제도 개선 방안의 제언
: 호주의 사례를 중심으로

이 해 원*

<국문초록>

초연결 사회(hyperconnected society)의 도래로 사이버안보의 중요성이 대두되고 있음에도 불구하고 우리나라의 사이버안보 상황은 관련 법제도가 정립되지 않고 혼란스러운 상황이다. 본고는 비교법적 연구로 호주의 사례를 살펴본 후 이를 토대로 시사점을 도출하고 우리나라 사이버안보 법제도 개선 방안을 제안하였다. 본고에서 제언하는 주요 개선 방안은 다음과 같다. 첫째, 사이버안보 컨트롤 타워는 말 그대로 조정(control) 역할에 그쳐야 하며, 국가정보원은 컨트롤 타워나 전략 및 정책 수립 기능이 아닌 실무 및 지원 기능을 수행하는 것이 적절하다. 둘째, 민간과 공공 사이의 실질적인 정보 공유 및 협력을 이끌어 내기 위하여는 정보기관의 신뢰 회복이 필요하며, 이를 위하여 정보기관을 통제, 감독하는 독립적인 감독기구를 신설하는 방안에 관한 논의가 필요하다. 셋째, 사이버안보 기본법 제정이 난항을 겪고 있는 현실을 반영하여 현행 개별법 체제를 우선 체계적으로 정비하고 기본법의 제정은 장기적 과제로 추진하는 방안을 검토할 필요가 있다. 넷째, 개별법을 개정하여 정보 공유 등 사이버안보 핵심 역량을 추진하기 위한 법적 근거를 마련할 필요가 있다. 세계 초고 수준의 IT강국이라는 위상에 걸맞게 하루가 다르게 증가하고 진화하는 사이버안보 위협에 대응하기 위한 선진적인 법제도가 시급히 갖추어져야 할 것이다.

주제어 : 사이버안보, 사이버안보 거버넌스, 사이버안보법, 호주 사이버안보 사례, 독립감독기구

• 투고일 : 2019.10.02. / 심사일 : 2019.10.24. / 게재확정일 : 2019.10.25.

Ⅰ. 들어가며

정보화사회를 넘어 모든 사물과 사물이 네트워크를 매개로 상호 연결되어 통신하는 초연결사회(hyperconnected society)[1]로 급변하고 있는 오늘날 사이버

* 목포대학교 법학과 조교수/변호사.

1) 초연결사회의 개념에 관하여는 박지웅, “초연결사회의 정치경제학적 기원과 성격”,「사회경

안보(cybersecurity)[2]는 가상 공간을 넘어 현실 공간에서의 국가 안보에 직결되는 문제로서 그 중요성이 날로 부각되고 있다. 특히 대한민국은 세계 최고 수준의 정보통신기술과 인프라(infra)를 갖춘 소위 'IT 강국'으로 평가받고 있음에도 불구하고 정작 사이버안보에는 취약하다는 평가를 받고 있고,[3][4] 무엇보다 군사적 긴장관계에 있는 북한으로부터 지속적으로 사이버 공격을 받고 있는 상황이므로,[5] 사이버안보 역량 강화가 다른 어느 나라보다도 시급하다고 할 수 있다. 그럼에도 불구하고 대한민국의 사이버안보 현실은 국방, 정보통신, 금융, 전자정부 등 주요 사이버 공격 대상별로 소관 부처들이 경쟁적·산발적으로 사이버안보 관련 법제 및 정책을 추진하고 있어 다소 혼란스러운 실정이다.[6]

사이버안보 위협은 국경과 영토를 대상으로 한 기존의 물리적 군사 위협과 달리 시간과 공간의 제약을 받지 않고 사회 전 영역에 걸쳐 신속하고 광범위하며 치명적인 타격을 줄 수 있는 새로운 위협이다. 따라서 기존의 전통적인 군사 중심의 안보 전략으로는 사이버안보 위협 대응에 한계가 있을 수밖에

제평론」 제57호, 한국사회경제학회, 2018. 10., 273면.

2) 'cybersecurity'라는 영문 용어에 대응하는 국문 용어로 정보보호, 사이버보안, 사이버보호 등의 개념이 혼재되어 사용되고 있으나 본고에서는 현재 국회에 계류 중인 「국가 사이버안보에 관한 법률안」 및 「국가사이버안보법안」에서 사용하는 용어인 '사이버안보'를 사용한다. 참고로 위 법안들은 문구에 다소 차이는 있으나 사이버안보를 "사이버공격으로부터 사이버공간을 보호하여 국가 안전을 보장하고 국민의 이익을 보호하는 것"으로 개념정의하고 있다(「국가 사이버안보에 관한 법률안」 제2조 제3호, 「국가사이버안보법안」 제2조 제2호). 본고에서 사용하는 '사이버안보'의 개념 또한 이와 같다. 사이버안보의 개념에 관한 기존 연구로는 박상돈·김규동·김소정, "사이버안보 법제도의 의의에 대한 새로운 이해", 「보안공학연구논문지」 제14권 제2호, 보안공학연구지원센터, 2017. 4., 157-166면, 정필운, "사이버보안이란 개념 사용의 유용성 및 한계", 「연세 의료과학기술과 법」 제2권 제2호, 연세대학교 법학연구원 의료·과학기술과 법센터, 2011. 8., 1-25면 각 참조.

3) 국제전기통신연합(ITU)이 2017년 발표한 ICT 발전지수(ICT Development Index 2017)에 따르면 우리나라는 아이슬란드에 이어 전세계에서 2위를 차지하고 있다. ITU, *Measuring the Information Society Report 2017, Volume 1*, 2017., p.31.

4) 글로벌 보안기업 파이어아이(Fireeye)의 분석에 의하면 2015년 하반기 기준으로 한국의 사이버 공격 노출률은 37%로 세계평균인 15%, 필리핀 등 동남아시아 평균인 27%보다도 훨씬 취약한 수준이다. "IT강국 한국 사이버보안, 필리핀보다 취약", 매일경제 2016. 4. 14.자 기사.

5) 대표적인 북한의 대남 사이버 공격으로 2013년 주요 공영방송사와 금융기관 및 보안업체의 전산시스템이 마비된 3.20 사태와 2014년 원전 설계도와 매뉴얼 등이 해킹당한 한수원 사태를 들 수 있다. 정준현, "북한의 사이버공격에 대한 국가총력적 대응체계를 위한 법제 방향", 「성균관법학」 제28권 제4호, 성균관대학교 법학연구원, 2016. 12., 33-34면, 김재광, "사이버안보 위협에 대한 법제적 대응방안", 「법학논고」 제58집, 경북대학교 법학연구원, 2017. 5., 148-151면.

6) 이해원, "영국의 사이버안보 법제 변천 과정 및 시사점", 「법학연구」 제26권 제4호, 경상대학교 법학연구소, 2018. 10., 271면.

없다. 기술, 인력은 물론 법제도와 국제외교관계 등이 망라된 복합적인 대응이 필요하며, 무엇보다 공공과 민간의 유기적인 협력 체계가 갖추어져야 한다.[7] 범정부적 차원의 사이버안보 복합 대응·협력 체계를 제도적으로 뒷받침하는 관련 법제의 정비도 필수적으로 요구된다. 그러나 2006년 이후 사이버안보 역량 강화를 위한 다수의 법안이 국회에 제출되었음에도 불구하고 정보기관으로의 권력 집중, 국민의 사생활 침해, 개인정보보호 문제 등이 대두되면서[8] 이념적·정치적 문제로 비화되어 답보 상태에 머무르고 있는 실정이다. 현 20대 국회에서도 2016. 5. 20. 이철우의원 대표 발의로 「국가 사이버안보에 관한 법률안」(이하 '이철우의원안')이, 그리고 2017. 1. 3. 정부안으로 「국가사이버안보법안」(이하 '정부안')이 각 제출되었으나, 2017. 11. 29. 정보위원회 전체회의에 상정된 이후 현재까지 국회 차원의 어떠한 논의도 이루어지지 않고 있다.[9]

이러한 문제인식 하에 본고는 비교법적 연구로서 호주의 사례를 거버넌스와 법제 측면에서 각 분석하여 시사점을 도출한 후 우리나라 사이버안보 법제도 개선 방안을 제안하고자 한다. 본고에서 호주를 비교법적 분석 대상으로 삼은 이유는 다음과 같다. 호주와 우리나라는 ① 경제적 측면에서 G7으로 대표되는 글로벌 경제강국에는 포함되지 않으나 G7의 뒤를 추격하는 신흥경제국들의 그룹인 G20의 정회원국이고, ② 국제정치학적 측면에서 강대국처럼 국제체제 전반에 걸친 군사력·경제력을 가지고 있지는 않으나 지역 차원에서 동원할 수 있는 국력을 갖추고 있는 '중견국'(middle power)이며,[10] ③ 지정학적 측면에서 미국과 중국이라는 양 강대국의 대결이 치열하게 펼쳐지는 역동적인 지역인 아시아-태평양 지역에 위치하고 있고, ④ 외교적으로 미국과 안보 측면에서 굳건한 동맹을 유지하는 한편[11] 중국과도 경제적 측면에서 밀접한 우호관계를

---

7) 유사한 취지로 김도승, "국가 사이버안보의 법적 과제", 「미국헌법연구」 제28권 제2호, 미국헌법학회, 2017. 8., 110면.

8) 참여연대, "국가 사이버안보 기본법 제정(안)에 대한 의견서", 2016. 10. https://www.peoplepower21.org/Petition/1475222 (2019. 9. 14. 방문).

9) 본고 투고일 기준으로 국회 의안정보시스템(http://likms.assembly.go.kr/)에서 이철우의원안, 정부안을 각 검색한 결과 2017. 11. 29. 이후 어떠한 논의도 이루어지지 않았다.

10) 중견국의 개념 및 중견국으로서 한국과 호주간 협력의 중요성에 관하여는 김우상, "중견국 외교 협력방안 모색: 한국과 호주 중심", 「JPI 정책포럼」 제2011-31호, 제주평화연구원, 2011. 11., 3-5면 및 8-10면.

11) 호주의 외교 및 안보관계에서 가장 큰 역할을 하는 미국과의 군사동맹(공식명칭: Security Treaty between Australia, New Zealand and the United States of America, 이하 'ANZUS Treaty')은 1951년 체결되었다. ANZUS Treaty는 본래 미국, 호주, 뉴질랜드 3국이 참여하는 조약이었으나, 1984년 뉴질랜드가 자국 영해 및 영토에서 비핵화정책

유지하는 이중전략을 취해야 하는 상황이라는 공통점을 가지고 있다. ⑤ 나아가 호주는 미국, 영국, 캐나다, 뉴질랜드와 함께 전세계를 상대로 통신감청을 실시하고 있는 '다섯 개의 눈'(Five Eyes) 동맹의 일원이며[12], ⑥ 2017년 기준으로 아시아-태평양 지역 사이버 성숙도 수준(Asia-Pacific Cyber Maturity)에서 미국의 뒤를 이어 2위를 차지할 정도로 사이버안보와 관련하여 국제적으로 높은 수준을 인정받고 있다.[13] 이상 살펴본 호주와 우리나라의 경제적, 국제정치학적, 지정학적, 외교적인 측면의 공통점, 그리고 사이버안보와 관련된 호주의 선도적 역량을 종합하면 호주의 사이버안보 거버넌스 및 관련 법제를 살펴보는 것은 우리나라 사이버안보 역량의 문제점 및 향후 개선방안을 도출함에 있어 유의미한 시사점을 제공할 수 있을 것으로 생각되나, 사이버안보와 관련된 기존의 비교법적 연구는 전통적인 연구 대상인 미국, 유럽연합, 영국, 독일, 일본, 중국에 집중되어 있고, 호주를 다룬 유의미한 연구는 찾아보기 어려운 실정이다.[14]

Ⅱ. 호주의 사이버안보 법제도

1. 거버넌스 측면

1) 개요

사이버안보 추진체계 관한 호주의 기본 방침은 새로운 정부 기관을 설치하기보다는 기존 기관들에 새로운 기능을 부여하는 한편 기존 기능을 재배치하는 방법을 택함으로써 기존 정부 조직에 중대한 변화를 주지 않는 것이다.[15]

을 채택하면서 미국의 핵잠수함 및 핵무기 탑재 항공모함의 주둔을 금지하고, 이에 대응하여 미국이 1986년 방위의무정지를 표명함에 따라 1986년 이후에는 사실상 미국과 호주 양자간 군사동맹조약이 되었다.

12) Five eyes 동맹의 개요 및 호주의 역할에 관하여는 Andrew O'Neil, "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance", *Australian Journal of International Affairs,* Vol. 71, No. 5, 2016, pp.533-539.

13) Fergus Hanson et al, "Cyber Maturity In The Asia-Pacific Region 2017", Australian Strategic Policy Institute, 2017., p.11. 위 보고서에서 한국의 사이버 성숙도는 미국, 호주, 일본, 싱가폴에 이어 5위로 평가되었다.

14) 미국, 유럽연합, 영국, 독일, 일본, 중국의 사이버안보 거버넌스 및 법제에 관하여는 기존 연구가 상당 부분 축적되어 있다. 일례로 박영철 외, "사이버보안체계 강화를 위한 정보보호법제 비교법연구", 한국인터넷진흥원, 2015. 및 양천수 외, "안전한 지능정보사회 구축을 위한 정보보호 관련 법제도 개선방안 연구", 과학기술정보통신부, 2018. 각 참조.

호주는 2016. 4. 국가 차원의 사이버안보 전략[16]을 발표하면서 사이버안보 추진체계를 개편하였고,[17] 이후 관련된 부처 및 기관들의 조직 및 기능을 일부 조정하여 복합적이고 다중적인 추진체계를 갖추고 있다. 2019. 9. 현재 호주의 사이버안보 추진체계는 정부 수반인 총리를 정점으로 다수의 부처 및 기관이 전략·정책 수립 및 실무 집행에 각 관여하는 복합적인 체계이다. ① 외교 등 국외 부문은 외무장관(Minister for Foreign Affairs) 소속의 외무부(Department of Foreign Affairs and Trade) 및 그 소속의 사이버업무 대사(Ambassador of Cyber Affairs)가, ② 안전, 치안 등 국내 부문은 내무장관(Minister for Home Affairs) 소속의 내무부(Department of Home Affairs) 및 그 소속의 국가 사이버안보 보좌관(National Cyber Security Advisor)이, ③ 국방 부문은 국방장관(Minister for Defence) 소속의 해외 통신 정보(signal intelligence) 담당 기관인 ASD(Australian Signals Directorate)[18]가 전략 및 정책을 각 담당하는 체계이다. 각 영역별로 수립된 전략·정책은 내무부가 총괄하여 국가 차원의 종합 전략을 수립, 점검하고 있다. 이렇게 수립된 사이버안보 전략·정책의 실제 집행은 ASD 소속기관인 사이버안보센터(Australian Cyber Security Centre)가 담당하며, 국가주요기반시설에 대한 사이버 공격 대응 기관인 내무부 산하 기반시설보호센터(Critical Infrastructure Centre), 사이버안보센터 소속으로 사이버안보 위협의 상시 모니터링 및 실시간 대응을 담당하는 사이버위기대응센터(Cyber Emergency Response Centre) 및 사이버안보센터 소속으로 중앙정부와 지방정부 사이, 그리고 민간과 공공 영역 사이의 정보 공유 및 협력 담당 기관인 합동사이버안보센터(Joint Cyber Security Centre)가 각 사이버안보 실무 집행의 일정 부분을 담당하고 있다.

요컨대, 호주의 사이버안보 추진체계는 국가 차원의 전략 및 정책은 내무부

15) Liam Nevil, “Cyber Security Governance in Australia”, Center for International Governance Innovation, 2018, p.13.

16) Commonwealth of Australia, *Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity*, 2016. 호주의 국가 사이버안보 전략의 주요 내용은 본고에서는 다루지 않는다.

17) Liam Nevil, *supra* note 15, p.15.

18) 호주의 정보기관은 ① Office of National Assessment(ONA), ② Australian Security Intelligence Organisation(ASIO), ③ Australian Secret Intelligence Service(ASIS), ④ Australian Signals Directorate(ASD), ⑤ Defence Intelligence Organisation(DIO), ⑥ Australian Geospatial-Intelligence Organisation(AGO)의 6개로 분산되어 있다. 이 중 ASD는 해외 통신 정보의 수집, 분석 및 호주 국내의 통신·전산 보안을 담당하는 정보기관(signal intelligence)이다.
https://www.asd.gov.au/ (2019. 9. 29. 접근) 참조.

가 총괄하여 수립 및 점검하고, 실무 집행은 국방부 소속 정보기관인 ASD 및 그 산하 기관인 사이버안보센터를 중심으로 이루어지는 체계, 즉 전략 및 정책 수립과 실무 집행이 이원화(二元化)된 체계로 파악된다. 참고로 2016. 4. 사이버안보 전략이 발표된 후 개편된 호주의 사이버안보 추진체계는 기존에 설치된 정부 부처 및 기관들의 기능을 조정하고 함께 편성(co-location)한 것으로서, 추진체계 개편에도 불구하고 기존 부처 및 기관들의 정체성, 예산, 보고 및 명령 체계(chain of command)는 기존대로 유지되고 있다고 알려졌다.[19]

2) 컨트롤 타워

2016. 4. 사이버안보 전략 발표 당시 호주의 사이버안보 추진체계는 국가 사이버안보 보좌관(총리실 소속)이 국내 정책(policy)을, 사이버 대사(외교부 소속)가 국제 관계(international engagement)를, 사이버안보센터(국방부 소속)가 집행(operation)을 각 담당하고, 국가 사이버안보 보좌관이 각 영역간의 조정을 수행하며, 국가 사이버안보 보좌관은 사이버안보센터의 수장을 겸직하는 구조였다.[20] 따라서 국가 사이버안보 전략이 수립된 2016. 4. 당시에는 정책 조정 기능 및 실무 집행 기능을 모두 가진 국가 사이버안보 보좌관이 수장으로 있는 사이버안보센터가 사실상 사이버안보의 컨트롤 타워 역할을 수행하였다고 볼 수 있다.

그러나 2016. 4. 이후 호주 정부는 사이버안보와 관련된 일련의 조직개편 및 기능조정을 실시하였다. 구체적으로 살펴보면, ① 2017. 12. 이민 및 출입국관리 기능, 국가안보 및 위기관리 기능, 대테러 조정기능 및 사이버안보 정책 기능을 수행하는 내무부를 내무장관 소속의 부처로 신설하였고,[21] ② 국가 사이버안보 보좌관을 총리실에서 내무부 소속으로, 사이버안보센터를 국방장관 직속에서 국방장관 소속 정보기관인 ASD의 하위 기관 소속으로, 핵심기반보호센터를 법무장관 소속에서 내무장관 소속으로 각 재편하였으며,[22] ③ 사이버안보 관련 호주 정부 웹사이트를 내무부 웹사이트로 이관하였고,[23] ④ 사이버안보 전략·정책 수립 및 실천 여부 점검 기능을 내무장관의 핵심 소관 업무

19) Liam Nevil, *supra* note 15, p.13.
20) *supra* note 16, p.24.
21) https://www.homeaffairs.gov.au/about-us/who-we-are/our-history (2019. 9. 14. 접근).
22) ASD 및 ACSC의 조직 개편 및 법정화는 Intelligence Service Act 2001, Part 3A.에 규정되어 있다. https://www.legislation.gov.au/Details/C2019C00018 (2019. 9. 8. 접근).
23) 일례로 호주의 국가 사이버안보 전략을 소개하는 홈페이지도 총리실에서 내무부로 이관되었다. https://cybersecuritystrategy.homeaffairs.gov.au/ (2019. 9. 26. 접근) 참조.

(portfolio)에 포함시켰다. 즉 국가 사이버안보 보좌관 및 사이버안보센터의 위상은 2016. 4. 사이버안보 전략 수립 시점보다 격하된 반면, 사이버안보에 관한 내무장관의 권한은 증대된 것이다. 이와 같은 조직 및 기능 개편 이후에도 국가 사이버안보 보좌관 및 사이버안보 센터가 사이버안보 관련 다수 이해당사자들 – 특히 외교장관, 국방장관, 내무장관과 같은 내각 관료 및 관련 중앙부처들 – 의 의견을 조정하고 의사 결정을 내려야 하는 컨트롤 타워로서의 역할을 수행하고 있다고 보기 어렵다. 오히려 내무장관에게 사이버안보 관련 정책 수립 기능과 관련 조직이 집중된 점, 국가 차원의 사이버안보 전략 수립 기능이 현재 최종적으로 내무부에게 있는 점을 감안하면, 현 시점에서 호주의 사이버안보 컨트롤 타워는 내무부라고 봄이 타당하다.[24]

3) 실무기관

호주 사이버안보 전략 및 정책의 실무 집행은 ASD 및 그 산하 기관인 사이버안보센터를 통하여 이루어지고 있다. 특히 사이버안보 위협의 실시간 모니터링 및 대응 담당 기관인 사이버위기대응센터와 민관 사이의 정보 공유 및 협력을 담당하는 합동사이버안보센터가 2018. 6. ACSC 산하로 편제되면서 실무기관으로서의 사이버안보센터의 위상과 영향력은 한층 강화되었다.[25] 사이버안보센터는 사이버 범죄를 분석, 조사, 보고하고 사이버 범죄, 사이버 테러, 사이버 전쟁에 대한 국가 보안 기능과 작전에 대한 조정 등 사이버안보 관련 범정부적인 허브 역할을 수행한다.[26] 사이버안보센터는 공공 부문에 대하여는 보안 관제, 사이버안보 기술 개발 및 적용, 교육 등을 직접 실시하고 있으며, 민간 부문에 관하여는 파트너쉽(partnership)을 맺은 민간 기관으로부터 사이버안보 위협 정보를 제공받아 공유한다. 그 밖에 사이버안보센터는 사이버안보 위협 대응에 필요한 기술 지원 및 자문 제공 기능 및 중앙정부와 지방정부 사이의 사이버안보 협력 관련 창구의 기능을 담당한다. 특히 2018년 조직개편 이후 사이버안보센터는 국가사이버안보 웹사이트(cyber.gov.au)를 신규 구축하여 개인에게는 'Stay Smart Online' 프로그램을 통하여 개인이 온라인에서 자신을 보호하는 방법에 대한 간단한 도움말과 조언을 제공하고, 기업에게는 주요 위협정보, 지침 및 다양한 사이버안보 프로그램을 제공하며, 정부기관을 대상으

24) 이응용, "호주 사이버보안 정책동향", KISA Report 2018. Vol. 12., 한국인터넷진흥원, 2018., 59면도 동일한 취지이다.
25) https://www.cert.gov.au/news/cert-australia-moving-asd (2019. 9. 26. 접근).
26) 이응용, 앞의 보고서(각주 24), 55면.

로 사이버 위협에 관한 기술적 자문 및 전국 단위의 훈련프로그램 등을 제공하고 있다.[27]

사이버안보센터 외에 사이버안보 관련 주요 실무 기관으로는 에너지, 수도, 통신 등 기반시설의 보호를 담당하는 내무부 산하 기반시설보호센터가 있다. 기반시설보호센터의 기능 중 주목할 부분은 기반시설의 소유자 및 운영자와 기반시설보호센터 사이에 파트너쉽을 체결함으로써 기반시설에 관한 사이버안보 위협 관련 정보를 민관이 공유하는 네트워크(Trusted Information Sharing Network, 'TISN')를 운영하고 있다는 점이다.[28] TISN은 2003년 법무장관 주도로 설치된 정보공유 네트워크로 현재 금융, 에너지, 운송, 통신, 정부 등 기반시설별로 그룹이 설치되어 해당 기반시설을 대상으로 한 사이버안보 위협 관련 정보를 자발적으로 공유하고 있다.

4) 통제 및 감독기관

앞서 살펴보았듯이 호주의 사이버안보 추진체계는 내각 부처인 내무부가 전략 및 정책 수립을 담당하고, 정보기관인 ASD 및 그 소속 기관인 사이버안보센터가 실제 실무 집행을 담당하는 체계이다. 내각 부처인 내무부에 대한 감독은 권력분립의 일반 원칙에 따라 행정부 차원에서 소관 각료인 내무장관 및 정부 수반인 총리를 통한 통제 및 감독이, 그리고 입법부 차원에서 호주 연방의회를 통한 통제 및 감독이 각 이루어지므로 특이사항이 없다. 그런데 호주는 정보기관에 대한 통제 및 감독 장치로 우리나라와 달리 행정부와 입법부의 양 측면에서 이중의 장치를 두고 있어 이를 살펴볼 필요가 있다.

호주는 1986년 법률을 제정하여 정보기관에 대한 정부 차원의 별도의 감독기관인 '정보기관 감사관'(Inspector General of Intelligence and Security)을 설치하였다.[29] 정보기관 감사관은 중립성과 독립성이 보장되는 독립기관(independent statutory office)으로 총리의 추천을 거쳐 총독(governor general)이 임명한다.[30] 총리는 정보기관 감사관을 추천하기 위하여 호주 연방의회 야당 원내대표와 반드시 사전 협의하여야 한다.[31] 정보기관 감사관은 호주의 6대 정보기관[32]의 업무 수행이 정당한지에 관한 상시적 질문권 및 감사

27) 이응용, 앞의 보고서(각주 24), 56면.
28) https://www.tisn.gov.au/ (2019. 9. 29. 접근).
29) https://www.igis.gov.au/ (2019. 9. 25. 접근).
30) Inspector-General of Intelligence and Security Act 1986 s.6. 영연방국가에서 총독은 영연방 전체의 입헌군주인 영국 왕의 주권을 상징하는 국가 원수일 뿐 실질적인 권한은 없다.
31) Inspector-General of Intelligence and Security Act 1986 s.6(3).

권을 가지며,[33] 호주 국민은 정보기관의 부당한 업무 수행에 관하여 정보기관 감사관에게 조사를 요청할 수 있다.[34] 정보기관 감사관은 정보기관에 대한 질문 및 감사 결과에 관하여 보고서를 작성하며, 보고서의 내용 중 공공의 이익에 관한 사항으로 기밀사항이 아닌 부분은 공중에 공개할 수 있다.[35] 한편 호주 연방의회는 양원의 여야 의원이 함께 참여하는 '통합 정보위원회'(Parliamentary Joint Committee on Intelligence and Security)를 두어[36] 정보기관을 감시, 감독하고 있다. 통합 정보위원회는 우리나라 국회법상 정보위원회[37]와 유사한 조직으로 정보기관의 예산안과 결산안을 심사하고 소관 업무 집행에 관하여 필요한 사항을 보고받은 방식으로 간접적 감독권을 행사한다. 통합 정보위원회는 정보기관에 대한 감독권 행사 관련 사항 중 기밀사항을 제외한 사항을 통합 정보위원회 웹사이트를 통하여 국민에게 투명하게 공개하고 있다. 정보기관에 대한 행정부와 입법부의 이중의 통제 장치는 호주 사이버안보 실무 집행기관인 ASD 및 그 산하 사이버안보센터에도 적용되므로, 호주의 경우 정보기관이 사이버안보 실무를 담당함에 따라 발생할 수 있는 권한 오남용, 프라이버시 침해 등의 부작용을 방지할 수 있는 제도적 장치가 상대적으로 두텁게 마련되어 있다고 볼 수 있다.

2. 법제 측면

1) 개요

호주는 미국이나 일본과 달리 범정부 차원의 사이버안보 일반법 또는 기본법은 제정하지 않고 있으며,[38] 현재 일반법 또는 기본법을 제정하겠다는 움직

32) 호주의 6대 정보기관에 관하여는 각주 18 참조.
33) Inspector-General of Intelligence and Security Act 1986 s.8.
34) Inspector-General of Intelligence and Security Act 1986 s.10-14.
35) Inspector-General of Intelligence and Security Act 1986 s.8A.
36) https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security (2019. 9. 25. 접근).
37) 국회법 제37조 제1항 16호.
38) 미국의 경우 국가 사이버안보 보호법(National Cybersecurity Protection Act of 2014) 및 사이버안보정보공유법(Cybersecurity Information Sharing Act of 2015)이, 일본의 경우 사이버시큐리티기본법(サイバーセキュリティ基本法)이 사이버안보에 관한 일반법 또는 기본법이라 할 수 있다. 미국의 사이버안보 법체계에 관하여는 양천수・지유미, "미국 사이버보안법의 최근 동향 -「사이버보안 정보공유법」을 중심으로 하여 -"「법제연구」 제54호, 한국법제연구원, 2018. 6., 161-185면, 일본의 사이버시큐리티기본법에 관하여는 박상돈, "일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점

임도 찾아볼 수 없다. 기본적으로 호주는 사이버안보와 관련하여 추진체계, 중앙정부 및 지방정부의 역할, 중앙부처 및 기관간 기능과 역할 등을 규정하는 개별 법률을 제정하기 보다는 행정계획, 가이드라인 또는 민간과의 파트너쉽 등 연성적인(soft) 방법으로 접근하고 있는 것으로 알려졌다.[39] 호주의 사이버안보 법제는 사회 각 영역별, 분야별, 또는 소관 부처의 업무별 법률 중에서 사이버공간과 관련되고 국가의 안전보장에 관한 내용(감청, 수사, 정보수집, 주요시설 보호 등)과 관련된 법률들이 각 제정, 시행되는 체계로 파악된다. 호주의 실정법 중 사이버안보 관련 법률로 분류할 수 있는 주요 법률을 정리하면 <표 1>과 같다.

<표 1: 호주의 사이버안보 관련 법률>[40]

구분	명칭	개요
형사 사법 절차	Cybercrime Act 2001	사이버상의 범죄에 관한 구성요건 및 처벌을 규정한 형법
	Mutual Assistance in Criminal Matters Act 1987	국경을 초월한 범죄에 관한 사법공조 및 국제협력에 관한 법률
	Surveillance Devices Act 2004	범죄 수사를 위한 감시 장비의 설치, 컴퓨터에 저장된 데이터의 압수 수색을 위한 컴퓨터 접근 영장 신청 및 발부 등에 관한 절차를 규정한 법률
	Telecommunications (Interception and Access) Act 1979[41]	정보기관 및 수사기관이 행하는 통신검열, 감청, 장비접근 등을 규정한 법률
	Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018[42]	암호화된 통신을 통하여 이루어지는 각종 사이버 범죄 및 테러 대응력을 강화하기 위하여 ① 정보기관 및 수사기관이 통신사업자에게 자발적 또는 강제적 협조를 요청할 수 있는 권한에 관한 사항, ② 강화된 컴퓨터 접근 영장 청구 및 발부에 관한 사항, ③ 압수수색영장의 기간 및 권한을 강화하는 사항 등을 규정한 법률
정보기관 설치	Intelligence Services Act 2001	AGO(Australian Geospatial-Intelligence Organisation), ASD(Australian Signal Directorate), ASIS(Australian Secret Intelligence Service), DIO(Defence Intelligence Organisation) 등 호주 정보기관의 설치 근거에 관한 법률
	Australian Security Intelligence Organisation Act 1979	호주 국내 정보기관인 보안정보국(Australian Security Intelligence Organisation)의 설치 근거에 관한 법률

을 중심으로", 「경희법학」 제50권 제2호, 경희법학연구소, 2015. 6., 149-157면 각 참조.

39) Erica Wiking Häger, *Cybersecurity Law Overview*, Mannheimer Swartling, 2017, p.7.

40) Badu V. Shirivas, "A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains", the SANS Institute, 2015., pp.1-21을 기초로 필자가 재작성한 것이다.

41) 우리나라의 통신비밀보호법, 영국의 Regulation Investigatory Power Act(RIPA) 2000 등

기반시설 보호	The Security of Critical Infrastructure Act 2018	에너지, 수도, 항만 등 외부 세력으로부터 공격을 받아 파괴되거나 손상을 입을 경우 호주의 국가안보에 치명적인 영향을 줄 수 있는 기반시설의 보호에 관한 법률
	Telecommunication Act 1997[43]	통신사업자의 네트워크 및 통신시설 보호에 관한 법률

위 법률들 중 본고에서는 지면의 한계 및 논의의 집중 측면을 감안하여 ① 기반시설의 보호에 관한 법률[The Security of Critical Infrastructure Act 2018('CIA') 및 Telecommunications Act 1997('TA')]와 ② 가장 최근에 제정되었고 암호화된 통신(encrypted communication)에 대한 수시기관 및 정보기관의 접근에 관한 내용을 담고 있는 Telecommunications (Assistance and Access) Act 2018('TAA')을 간략히 살펴본다.

2) 기반시설 보호에 관한 법률: CIA, TA

CIA 및 TA는 에너지, 수도(water supply), 항만, 통신, 정부시설, 금융, 보건 등 외부 세력으로부터 공격을 받아 파괴되거나 손상을 입을 경우 호주의 국가안보에 치명적인 영향을 줄 수 있는 기반시설에 대하여 해당 시설의 보유자 또는 관리자에게 보호 의무를 규정하고 정부의 정보수집권 및 기타 행정권의 발동 근거를 마련하기 위하여 제정된 법률로서 우리나라의 「정보통신기반 보호법」과 입법 취지 및 목적이 매우 유사하다. CIA는 통신을 제외한 기반 시설에, TA는 통신사업자가 보호한 통신 관련 시설(네트워크, 서버, 장비 등)에 적용된다.

CIA의 주요 내용은 다음과 같이 ① 기반시설의 지정 및 등록, ② 기반시설에 대한 사업자의 보고 의무, ③ 기반시설 사업자에 대한 내무장관의 각종 권한(정보수집권, 행정명령권, 평가권)으로 정리할 수 있다.[44] 특히 주목할 점은 국가안보 관련 위협이 발생한 경우 내무장관이 발하는 행정명령에 기반시설의

과 유사한 법률이라 할 수 있다. 영국의 RIPA에 관한 개괄은 이해원, 앞의 논문(각주 6), 273-275면.

42) 엄밀히 말하여 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018은 Telecommunication Act 1997, Surveillance Act 2004, Australian Security Intelligence Organisation Act 1979, Crimes Act 1914 등 기존 법률을 개정하는 형태로 제정된 법률이다.

43) Telecommunication Act 1997은 우리나라의 「전기통신사업법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 등을 합친 것에 비견되는 통신에 관한 호주의 일반법으로 방대한 내용을 담고 있으나, 본고에서는 지면 관계상 위 법에 관한 상세한 논의는 생략하며, 기반시설보호와 관련된 내용만 언급한다.

44) Commonwealth of Australia, *Critical Infrastructure Centre Compliance Strategy,* 2016.

관리 또는 소유자가 응하지 않았을 경우 최대 52,500 호주달러의 과징금이 부과될 수 있도록 규정하여 행정명령에 일정 부분 강제력을 부여하고 있다는 점이다.

- 기반시설의 범위: 이용자 및 이용량 등의 기준에 따라 법률에 규정된 전기, 가스, 수도 시설 및 법률에 열거된 항만 시설 또는 내무장관이 기반시설로 지정한 시설(s.9-s.12, s.51)
- 기반시설의 등록: 기반시설을 소유 또는 관리하는 자는 내무장관에게 기반시설을 등록할 의무가 있음(s.19-s.23)
- 보고 의무: 기반시설을 소유 또는 관리하는 자는 기반시설의 소유 및 관리에 관한 사항 또는 기반시설의 운영에 관한 사항이 변경되면 내무장관에게 이를 보고해야 함(s.23-s.27)
- 정보수집권: 내무장관은 CIA에 따른 권한의 행사를 위하여 필요하다고 인정되는 경우 기반시설의 소유 또는 관리자에게 관련 정보를 제출할 것을 요구할 수 있음(s.37-s.40)
- 행정명령권: 내무장관은 기반시설에 국가안보 관련 위협이 발생하였고 기반시설의 소유 또는 관리자와의 협력으로는 그러한 위협에 대처할 수 없을 경우 기반시설의 소유자 또는 관리자에게 특정한 행동을 하거나 하지 않을 것을 명할 수 있음(s.32-s.35). 기반시설의 소유자 또는 관리자가 행정명령에 응하지 않을 경우 최대 52,500 호주달러의 과징금이 부과될 수 있음(s.34).
- 평가권: 내무장관은 기반시설의 보안 상황을 평가할 수 있음(s.57)

TA의 주요 내용은 CIA와 크게 다르지 않으나, CIA와 달리 기반시설의 지정 및 등록이라는 절차가 요구되지 않으며 통신사업자가 보유, 관리하는 네트워크 및 통신 설비는 모두 보호 대상이라는 점에서 차이가 있다. 모든 통신사업자는 통신에서의 보안 강화를 위한 최선의 노력을 할 의무가 있고, 이러한 의무 준수에 위배될 소지가 있는 시설이나 소프트웨어의 변경이 있다면 호주통신미디어 위원회에 사전에 통지할 의무가 있다. CIA와 마찬가지로 TA의 경우에도 내무장관이 통신사업자에게 정보수집권 및 행정명령권을 행사할 수 있다. 다만 CIA와 다른 점은 TA의 경우 호주 정보기관 중 국내 정보를 담당하는 보안정보국의 수장이 내무장관의 정보수집권 및 행정명령권을 위임받아 행

사할 수 있다는 점이다. 즉 통신 관련 기반시설의 보호와 관련하여서는 정보기관의 수장이 적법하게 정보를 수집하고 사이버안보에 필요한 명령을 발할 수 있다. TA의 주요 내용을 정리하면 다음과 같다.

- '최선의 보호' 의무: 모든 통신사업자는 통신에서의 보안 강화를 위하여 최선의 노력을 다하여 인증되지 않은 접근이나 간섭으로부터 통신설비 및 네트워크를 보호해야 함[s.312(2A)]
- 통지 의무: 모든 통신사업자는 보안 의무 준수 사항에 위배될 소지가 있는 네트워크 및 서비스의 변경 계획에 관하여 호주 통신미디어위원회(ACMA)에 미리 통지하여야 함(s.314A-s.314E)
- 정보수집권: 내무장관은 통신사업자의 보안 의무 준수 여부를 평가하기 위하여 통신사업자에게 관련 정보 및 문서의 제출을 요구할 수 있음(s.315C)
- 행정명령권: 내무장관은 총리 및 통신 관련 장관과 협의한 후 국가 안보에 해를 끼칠 위험이 있는 통신 서비스의 사용 또는 제공을 금지할 수 있고, 국가 안보 위험을 방지하기 위하여 합리적으로 필요한 특정 행동을 하거나 하지 않을 것을 통신사업자에게 명할 수 있음(s.315A-s.315B). 통신사업자가 이에 응하지 않을 경우 내무장관은 과태료를 부과할 수 있음[s.571(4)(a)]
- 내무장관의 권한 위임: 내무장관은 정보수집권 및 행정명령권을 보안정보국의 장에게 위임할 수 있음(s.315G). 보안정보국의 장은 위임받은 권한을 행사함에 있어 내무장관의 지시에 따라야 함(s.315G).

기반시설보호에 관한 CIA 및 TA의 내용 중 특히 주목할 부분은 사이버위협 정보의 공유에 관한 부분이다. CIA나 TA 모두 법률에 정부의 정보수집권한만을 규정하고 있을 뿐, 기반시설의 소유자 또는 관리자가 사이버위협 정보를 정부 또는 제3자에게 제공하거나 수집된 사이버위협 정보를 제3자에게 제공(또는 공유)하는데 필요한 법적 근거는 규정하고 있지 않다. 그럼에도 불구하고 앞서 살펴보았듯이 사이버위협 정보는 TISN을 통하여 민관에 공유되고 있는데, 이는 법률의 규정에 근거한 것이 아니라 관련 기관들 사이에 체결된 자발적인 파트너쉽에 근거한 것이다.

3) 암호화된 통신에 대한 접근: TAA

(1) 개요

암호화 기술이 보편화, 대중화되면서 테러리스트 및 범죄 조직은 감청 등을 대비하여 암호화 기술을 사용하여 통신을 하고 있다. 2017년 호주 연방 경찰의 감청 결과 90% 이상이 암호화된 통신으로 사실상 감청의 효과가 없는 상황이다.[45] 테러조직과 범죄조직이 암호화된 통신을 보편적으로 사용하게 되면서 이에 맞서는 호주 정부의 활동이 심각한 도전을 받게 되었다. 한편 통신의 암호화 문제는 다섯 개의 눈 동맹에서도 중요한 이슈로 부각되었다. 2018. 8. 29. 열린 다섯 개의 눈 동맹국들(미국, 영국, 캐나다, 호주, 뉴질랜드)의 검찰총장 및 내무장관 회담에서 암호화 통신의 불투명화(going dark) 문제가 논의되었고, 논의 결과 민관 협력 프레임워크인 '증거와 암호화된 통신에 접근하기 위한 원칙'(Statement of Principles on Access to Evidence and Encryption)에 합의하였다.[46]

이러한 문제인식 하에 2018. 8. 14. 호주 정부는 기존의 통신감청 제도 및 데이터 압수수색 제도를 강화할 수 있는 새로운 입법인 TAA에 착수하게 되었다. TAA 법안은 2018. 9. 20. 호주 하원에 제출되어 2018. 12. 6. 하원 및 상원을 통과하여 2018. 12. 8. 시행되었다. 주요 내용은 다음과 같다.

(2) 통신사업자의 협조 의무

TAA의 핵심은 '암호화된 통신에 대한 호주 통신사업자의 협조 의무'를 규정하고 있다는 점이다.[47]

TAA의 제정으로 호주 통신감청법[Telecommunications (Interception and Access) Act 1979, 'TAA']에 따라 감청 권한을 가진 수사기관[48] 또는 정보기

45) The Parliament of The Commonwealth of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Explanatory Memorandum,* 2018, p.2

46) Cat Barker・Helen Portillo-Castro, "Bills Digest No. 49, 2018-19", Australian Parliament Library, 2018. 12., p.10.

47) TAA schedule 1.

48) 호주 연방 경찰(Australian Federal Police), 호주 각 주 경찰 등 총 20개 기관이다. Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979,* 2018. 11., p.6.

관(보안정보국)은 3년 이상의 징역형에 처해질 중대범죄가 행하여졌거나 행하여졌다고 믿을 만한 합리적 이유가 있는 경우이거나 국가안보 보장을 위하여 필요한 경우(이 경우는 보안정보국에 한정된다)에는 호주 통신사업자에게 가능한 기술적 지원을 요청하거나 통보할 권한을 가지게 되었다.[49] '가능한 기술적 지원'은 ① 전자적 보호수단(electrical protection)의 제거, ② 기술 정보의 제공, ③ 소프트웨어나 장비의 설치・유지・테스트, 통신장비 또는 통신서비스 접근에 대한 지원 등 정보기관이나 수사기관이 암호화된 통신에 접근하기 위하여 필요한 조치, ④ 정보기관이나 수사기관이 적법한 절차(영장이나 TAA에 따른 기술적 지원, 요청 등)에 따라 통신장비 또는 통신서비스에 접근하였다는 사실에 대한 비공개(conceal) 등을 포함하는 광의의 개념이다.[50]

정보기관과 수사기관이 TAA에 따라 통신사업자에게 요청할 수 있는 기술적 지원은 ① 기술적 지원 요청(Technical Assistance Request, 'TAR'),[51] ② 기술적 지원 통보(Technical Assistance Notice, 'TAN'),[52] ③ 기술적 역량 통보(Technical Capability Notice, 'TCN')[53]의 세 가지로 구분된다. TAR은 정보기관이나 수사기관의 장이 통신사업자에게 자발적인 기술적 지원을 '요청'하는 것으로서 강제성이 없다.[54] 그러나 TAN과 TCN은 '요청'이 아닌 '통보'(notice)로서 통신사업자의 자발적 협조를 구하는 TAR과 달리 통보에 응하지 않을 경우 제재까지 가능한 강제력 있는 행정처분이다. TAN은 보안정보국[55]이나 수사기관의 장이 통신사업자에게 기술적 지원을 해 줄 것을 통보하는 제도이다. TAN을 받은 통신사업자는 통보의 내용이 해당 통신사업자의 현재 설비나 기술 수준에서 이행가능하다면 통보대로 이행할 의무가 있다. 그러나 만약 현재 설비나 기술 수준으로 이행이 불가능하다면 해당 통신사업자는 TAN의 이행을 거부할 수 있고, 현재 설비나 기술 수준을 넘어 적극적으로 새로운 설비나 기술을 도입해야 할 의무는 없다.[56] TCN은 가장 강력한 통보로서 보안정보국[57]이나 수사기관의 장이 요청하여 검찰총장과 통신장관(Minister of

49) TAA schedule division 1, 2, 3.
50) TAA에 의해 개정된 TAA s.317E.
51) TAA에 의해 개정된 TIA s.317E-317K.
52) TAA에 의해 개정된 TIA s.317L-317RA.
53) TAA에 의해 개정된 TIA s.317S-317ZE.
54) Cat Barker・Helen Portillo-Castro, *supra* note 46, pp.21-22.
55) 다른 정보기관은 TAN을 발령할 수 없다. Cat Barker・Helen Portillo-Castro, *supra* note 46, p.22.
56) Cat Barker・Helen Portillo-Castro, *supra* note 46, p.23.
57) TAN과 마찬가지로 보안정보국이 아닌 다른 정보기관은 TCN의 발령을 요청할 권한이

Communication)이 공동으로 승인한 경우에만 발령될 수 있다.[58] TCN이 발령되면 해당 통신사업자는 그 통보의 내용대로 이행할 의무가 있으며, 현재의 설비나 기술로서 이행이 불가능하다면 새로운 설비를 설치하거나 기술을 도입해야 한다.[59] TCN은 최대 180일까지만 유효하며, TCN이 발령되면 그 적법성 및 유효성에 대한 평가가 별도의 독립 패널을 통하여 이루어지고 그 결과가 정보기관 감사관에게 보고된다.[60]

통신사업자는 TAN이나 TCN의 적법성에 대하여 정보기관 감사관에 이의를 제기할 수 있다. 만약 통신사업자가 정당한 이유 없이 TAN이나 TCN에 응하지 않을 경우 최대 10,000,000 호주달러에 달하는 과징금이 부과된다.[61]

(3) 컴퓨터 접근 영장 강화

컴퓨터 접근 영장(computer access warrant)이란 컴퓨터, 휴대전화, USB와 같은 장비를 수색하고 해당 장비에 저장된 정보를 수집할 수 있는 영장을 말한다. TAA는 컴퓨터 접근 영장을 발부받으면 해당 컴퓨터에서 이루어지는 통신의 실시간 감청을 허용하는 등 컴퓨터 접근 영장에 관한 보안정보국의 기존 권한을 확대하였고,[62] 3년 이상의 징역형에 처할 수 있는 연방 정부 차원의 범죄에 관하여는 정보기관이 아닌 수사기관도 컴퓨터 접근 영장을 발부받을 수 있도록 규정을 신설하였다.[63] 물론 보안정보국의 컴퓨터 접근 영장 발부 및 집행의 적법성에 관하여는 앞서 살펴보았듯이 정보기관 감사관 및 통합 정보위원회를 통한 이중의 감시와 통제가 이루어진다.

(4) 보안정보국의 권한 강화

TAA는 통신사의 협조 의무, 컴퓨터 접근 영장의 발부 및 집행 등 보안정보국이 TAA에 따라 행하는 권한 행사와 관련하여 보안정보국이 검찰총장에게 정보를 제공하거나 협조하도록 특정인에게 명하여 줄 것을 요청할 수 있도록 (즉, 보안정보국이 검찰총장을 통하여 간접적으로 특정인에게 자신의 정보수집

없다.

58) TAA에 의해 개정된 TIA s.317T.

59) Cat Barker · Helen Portillo-Castro, *supra* note 46, pp.23-24.

60) *Id.*

61) TAA에 의해 개정된 TIA s.3172A(3), s.570(3). 참고로 TAR은 통신사업자의 자발적 협력을 구하는 강제성 없는 요청이므로 통신사업자의 이의제기 절차가 없다.

62) TAA에 의하여 개정된 Australian Security Intelligence Organisation Act 1979 s.25(A).

63) TAA schedule 2.

에 정보를 제공하거나 협력할 것을 명하도록) 규정하고 있으며, 보안정보국에 자발적으로 협력한 자에 관하여 민사상 책임을 묻지 않도록 규정하고 있다. 이를 통하여 간접적으로 보안정보국의 정보수집 및 수사 권한이 강화되었다.[64]

Ⅲ. 시사점 및 개선 방안

1. 시사점

1) 거버넌스 관련

(1) 총괄 기능과 실무 기능의 이원화

호주의 사이버안보 거버넌스의 특징은 한마디로 '총괄 기능'(전략 및 정책 수립: 내무부)과 '실무 기능'(실제 정책 집행: 국방부 소속 ASD 산하 사이버안보센터)이 정부조직체계상 다른 기관에 각 집중되어 있는 이원화된 체계라고 할 수 있다. 이는 미국이나 일본과 같이 부처의 상위에 있는 정부 수반 직속의 범정부적 컨트롤타워를 두는 소위 '컨트롤타워 총괄형'과 다르고,[65] 영국과 같이 상호 수평적인 부처 사이에서 기능을 조정하는 소위 '실무부처 분산형'과도 차이가 있는,[66] 호주 고유의 체계이다. 이러한 추진체계는 새로운 기관을 설치하기 보다는 기존 기관들의 조직 및 기능 조정과 재배치를 통한 안정적인 조직개편을 추구해 온 호주의 전통,[67] 그리고 정치적인 고려나 소위 '부처이기주의'보다 조직, 인력, 예산 등을 고려하였을 때 사이버안보의 '총괄'과 '실무'를 가장 체계적이고 효율적으로 수행할 수 있는 추진체계가 무엇인지를 고려한, 실무적이고 현실적인 판단의 결과물로 생각된다.

특히 국가 사이버안보 전략을 발표한 2016. 4. 당시와 현재의 사이버안보 추진체계를 비교하면 중앙 부처인 내무부의 위상과 역할이 증대한 반면 국가 사이버안보 보좌관과 같은 내각 각료가 아닌 보조기관의 위상과 역할은 감소하였음을 알 수 있다. 이러한 추진체계 변화는 전략 및 정책을 효과적으로 수립하

64) TAA에 의하여 개정된 Australian Security Intelligence Organisation Act 1979 s.34AAA.
65) 김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각",「국제·지역연구」제26권 제3호, 서울대학교 국제학연구소, 2017. 9., 73-75면.
66) 김상배, 앞의 논문(각주 65), 73-75면.
67) Liam Nevil, *supra* note 15, p.15.

고 추진할 수 있는 자원(조직, 인력, 예산)을 보유한 중앙 부처가 사이버안보 전략과 정책을 총괄하는 컨트롤 타워를 맡는 것이 타당하다는 판단에서 비롯된 것으로 생각된다. 한편 사이버안보가 고도의 기술적이고 전문적인 지식을 요하는 점을 고려할 때, 사이버안보 컨트롤 타워의 변화와 관계없이 세계 제2차 대전 이래[68] 지금까지 통신 정보의 감청·수집 및 분석 기능을 담당해온 정보기관인 ASD 및 그 산하 기관인 사이버안보 센터가 일관되게 사이버안보 실무 기능을 지속적으로 담당해온 체계 또한 안정적이고 효율적이라고 판단된다.

(2) 연성(soft)적 민관 협력 체계

국경 중심의 전통적인 안보와 달리 사이버안보는 그 위협의 주체가 국가뿐 아니라 테러단체 등 비국가를 포함하고 그 위협의 대상도 사회 전방위적으로 광범위하게 이루어지므로 민관 사이의 정보 공유 및 협력 체계를 구축하는 것이 매우 중요하다.[69] 호주의 경우 사이버위협 정보 공유 등 민관 협력에 관한 구체적인 법률 규정이 없음에도 불구하고 사이버위기대응센터, 합동사이버안보센터, 핵심기반보호센터 등 사이버안보에 관련된 정부 기관과 사이버위협의 대상이 되는 민간 기관 사이에 협력에 관한 파트너쉽, 즉 민간과 공공의 신뢰에 기반한 자발적 협력 체계를 구축하고 있음을 주목할 필요가 있다. 일례로 현재 합동사이버안보센터와 파트너쉽을 체결한 민간 기관은 통신사, 은행, 운송회사 등 97곳에 달한다.[70] 제·개정이 어려운 법률이 아닌 파트너쉽, 즉 계약에 기반한 협력 체계는 계약법의 기본 원리에 따라 상호 합의가 있다면 언제든 협력의 내용이 변경 가능한 연성적(soft)이고 탄력적이라는 특징을 가진다.

(3) 정보기관에 대한 이중의 감시·통제 장치

호주의 사이버안보 실무를 담당하는 사이버안보센터는 정보기관인 ASD 소속으로 우리나라 국가정보원의 국가사이버안전센터와 유사한 기관이다. 우리나라의 경우 정보기관이 사이버안보, 특히 민관을 아우르는 국가 차원의 사이버안보 기능을 수행하는 것에 관하여 정보기관의 권한 비대 및 그로 인한 사생활 침해 등을 우려한 반대의 목소리가 높다.[71] 그러나 호주의 경우 정보기관

68) ASD의 전신은 1942년에 설립된 Australian-American Fleet Radio Unit Melbourne 이다. https://www.asd.gov.au/about/history.htm (2019. 9. 14. 방문).
69) 김도승, 앞의 논문(각주 7), 110면.
70) https://www.cert.gov.au/jcsc/jcsc-partners (2019. 9. 14. 방문).
71) 참여연대, 앞의 의견서(각주 8).

이 사이버안보 실무 뿐 아니라 민관 협력 및 민관간 정보공유도 담당하고 있음에도 불구하고 우리나라와 같은 논란은 제기되지 않고 있다. 특히 호주는 명문의 법률 규정이 아닌 당사자간 계약(파트너쉽)에 따라 민간이 사이버안보센터 등 정보기관에 자신이 보유한 사이버안보 위협 정보를 제공하고 있으나 이에 관하여 소위 '정보기관의 민간 사찰'과 같은 문제는 제기되지 않고 있고, 오히려 파트너쉽에 기반한 연성적 협력 체계가 강조되고 있다. 이는 정부 차원의 독립 감독 기관인 정보기관 감사관과 국회 차원의 여야 합동 감독 기관인 통합 정보위원회를 통하여 정보기관의 활동에 관한 실질적인 감시와 통제가 이루어지고 있고, 감시 및 통제의 결과 또한 보고서 형태로 국민들에게 투명하게 공개되고 있어, 결과적으로 정보기관의 권력 오남용, 개인정보 침해, 민간 사찰과 같은 부작용이 발생하기 어려운 시스템이 법제도적으로 갖추어져 있기 때문이라고 판단된다.

2) 법제 관련

(1) 분산형 개별법 체계

호주의 사이버안보 법제의 가장 큰 특징은 미국, 일본 등과 달리 사이버안보에 관한 소위 일반법 또는 기본법이 존재하지 않는다는 점이다. 앞서 언급하였듯이 호주의 사이버안보 법체계는 사회 각 영역별, 분야별, 또는 소관 부처의 업무별 법률 중에서 사이버공간과 관련되고 국가의 안전보장에 관한 내용과 관련된 법률들이 공존하는 '분산형 개별법' 체계라고 할 수 있다. Ⅱ.1.항에서 살펴보았듯이 호주는 미국이나 일본과 같은 '컨트롤타워 총괄형'이 아니라 정책과 실무가 분리된 '이원화형' 거버넌스를 채택하고 있는바, 수직적 체계를 중시하는 기본법 체계보다는 수평적 관계를 중시하는 분산형 개별법 체계가 호주와 같은 이원화형 거버넌스에 보다 부합하는 측면이 있다. 또한 사이버안보에 관한 기본법을 제정할 경우 추진체계, 인력 및 조직, 예산, 기존 법률과의 관계 등 다양한 관점을 고려한 입법 작업이 필요하고, 다양한 이해관계자들 사이의 이해충돌 문제를 조정해야 할 뿐 아니라, 정부 부처간 합의 및 국회 심사 과정에서 절차적으로도 상당한 시간이 소요되는 문제가 있는바, 이러한 현실적 문제를 고려한다면 호주와 같이 분산형 개별법 체계를 채택하고 이슈가 제기될 경우 해당 개별법을 신속히 개정하는 것이 기본법을 새롭게 제정하는 것보다 상대적으로 탄력적인 법제도에 해당할 수 있다.

(2) 정부 권한의 강화

위에서 살펴본 호주의 사이버안보 관련 주요 법률, 즉 기반시설보호 관련 법률인 CIA, TA와 암호화된 통신 접근에 관한 TAA를 살펴보면, 공통적으로 사이버안보 위협에 대응하기 위한 호주 정부의 권한이 대폭 강화되었음을 알 수 있다. 구체적으로 CIA 및 TA의 경우 호주 정부는 기반시설의 소유자 또는 관리자에게 사이버안보 관련 정보를 제공할 것을 명령할 수 있을 뿐 아니라 사이버안보에 위협이 되는 특정한 행동을 하거나 하지 않을 것을 명령할 수 있다. 2018. 12. 시행된 TAA는 한걸음 더 나아가 암호화된 통신에 관하여 호주 정부가 통신사업자에게 광범위한 범위의 기술적 지원에 관하여 자발적 협력 뿐 아니라 강제적인 협력을 요구할 수 있고 이에 응하지 않을 경우 과징금을 부과할 수 있는 등 전세계에서 유래를 찾기 어려운 강력한 권한을 규정하고 있다. 이러한 입법례가 우리나라의 실정에 부합하여 도입이 필요한지는 추가적인 연구가 필요하겠으나, CIA, TA, TAA 모두 입법 과정에서 국회 차원의 특별한 반대가 없었고, 특히 TAA의 경우 하원에 제출된 지 3개월 만인 2018. 12. 야당의 특별한 반대 없이 통과되었다는 점은 주목할 필요가 있다.[72]

2. 개선 방안

이상 살펴본 호주의 사이버안보 사례 및 그 시사점을 중심으로 우리나라의 사이버안보 법제도 개선 방안을 제안하면 다음과 같다.

1) 국가정보원의 위상 및 역할 재정립

우리나라의 현행 사이버안보 거버넌스는 ① 청와대 국가안보실이 컨트롤 타워를 담당하고 ② 국가정보원이 민·관의 사이버안보 실무를 총괄함과 동시에 대통령 훈령인 「국가사이버안전관리규정」에 따라 공공(중앙행정기관, 지방자치단체, 공공기관) 분야를 담당하고, ③ 국방부, 과학기술정보통신부, 행정안전부 등 개별 부처가 소관 분야(국방, 민간, 행정 등)를 각 담당하는 분산형 체계이다.[73] 한편 제20대 국회에 제출되어 있는 이철우의원안 및 정부안은 그 명칭

72) Cat Barker · Helen Portillo-Castro, *supra* note 46, p.2.

73) 우리나라의 현행 사이버안보 추진체계에 관하여는 기존의 연구가 상당히 축적되어 있으므로 본고에서 상세한 논의는 생략한다. 일례로 홍준호, “사이버보안 컨트롤타워 필요성에 관한 연구”, 「법학연구」 제19권 제1호, 한국법학원, 2019. 3., 238면; 김도승, 앞의 논문(각주 7), 103-104면 등.

이나 세부 기능에 다소 차이는 있으나 공통적으로 사이버안보 관련 컨트롤 타워로서 대통령 소속의 위원회를 설치하고 국가정보원장이 기본계획의 수립 및 정책 집행을 담당하는 추진체계를 규정하고 있다.[74]

현행 추진체계에 관하여는 분산형 체계로서의 한계, 즉 각 부처를 아우르는 통합적 조정기능이 부족하다는 비판이 제기되고 있다.[75] 20대 국회에 제출된 양 법안에서 제안된 추진체계, 즉 대통령 소속의 위원회를 컨트롤 타워로 두고 국가정보원장이 민관을 아우르는 사이버안보의 정책 수립 및 집행 기관이 되는 체계에 관하여는 시민단체를 중심으로 국가정보원의 권한 강화 및 그로 인한 인권 침해, 민간 사찰 우려와 같은 민감한 이슈가 제기되고 있다.[76]

정부조직 사이의 수직적 위계질서가 중시되는 우리나라의 정치적, 문화적 특성상 정부 수반이자 국가 원수인 대통령 소속의 위원회 또는 조직이 사이버안보 컨트롤 타워를 맡는 것은 상징적 의미가 있다. 특히 사이버안보는 국민의 안전 보장이라는 국가의 본질적 기능과 관련된 것이고 공공, 민간의 구분 없이 국가사회 모든 분야에 전방위적으로 관계된 문제이므로, 이러한 관점에서도 대통령 소속의 위원회 또는 조직이 최종적인 컨트롤 타워로서의 역할을 수행할 필요성이 긍정될 수 있다고 본다. 단 대통령 소속 위원회나 조직이 수행하는 컨트롤 타워의 기능은 말 그대로 조정(control), 즉 정부 부처 및 기관 사이에 이견이나 충돌이 있을 경우 이를 조정하는 기능에 국한되는 것이 타당하며 이를 뛰어넘어 사이버안보 전략이나 정책을 수립하는 것은 정부조직체계의 원리나 실제 예산, 인력, 조직, 권한 등 실행력에 비추어 볼 때 타당하지 않다고 생각한다.

사실 추진체계를 둘러싼 논란의 핵심은 국가정보원에 있다. 현행 체계에서 국가정보원은 대외적 규범력이 없는 대통령 훈령 형식의 행정규칙인 「국가사이버안전관리규정」에 따라 공공 부문의 사이버안보 정책 및 실무 권한만을 가지고 있으나, 이철우의원안 및 정부안이 국회를 통과하면 공공과 민간을 아우르는 사이버안보 정책 및 실무 집행 권한을 가지게 되는바,[77] 설사 대통령 소속의 위원회 또는 조직이 컨트롤 타워로 신설된다 하더라도 이는 명목상 조직에 그칠 위험이 크고 정책 수립과 실무 집행권한을 다 쥐고 있는 국가정보원

74) 국회 정보위원회, "국가 사이버안보에 관한 법률안(이철우의원 대표발의) 및 국가사이버안보법안(정부 제출) 검토보고", 2017. 2., 47면.
75) 김도승, 앞의 논문(각주 7), 111-112면.
76) 참여연대, 앞의 의견서(각주 8).
77) 이철우안과 정부안은 모두 국가정보원이 국가사이버안보 기본계획 및 시행계획을 각 수립·시행하도록 규정하고 있다.

이 사실상 컨트롤 타워로 군림하게 될 것이 우려되기 때문이다.

국가정보원의 조직, 인력 및 전문성을 고려할 때 공공, 민간 구분 없이 사이버안보의 '실무' - 사이버안보 위협의 탐지 및 역대응 등 - 를 국가정보원이 총괄 담당하는 것은 일응 타당한 측면이 있다. 그러나 실무 집행 차원을 넘어 이철우의원안 및 정부안이 규정한 것처럼 국가사회 전반의 사이버안보 정책 수립 권한까지 국가정보원이 가지는 것은 국가정책의 수립이 아니라 국가의 적대세력을 상정하고 그에 대한 대응 및 경쟁을 존립 이유로 삼는 정보기관의 본질에 부합하지 않는다.[78] 헌법상 국무회의에서 의결권을 행사할 수 있는 국무위원이 관장하는 행정각부 중 적절한 부처에서 국가사회 전반의 사이버안보 계획 및 정책의 최종 수립 권한을 갖는 것이 타당하다고 생각된다. 이렇게 하더라도 국가정보원의 현행 권한이나 기능이 축소된다고 보기 어렵다. 오히려 정보기관의 권한 비대화, 시민 사찰 위험 등과 같은 시민단체 및 학계의 비판에서 벗어나 정보기관 본연의 업무인 정보 수집 및 안보위협 대응 업무에 충실할 수 있을 것으로 생각된다. 호주 역시 총리와 정치적 책임을 함께하는 내각의 일원인 내무장관이 관할하는 내무부에서 국가 차원의 사이버안보 전략 및 정책을 수립하고, 정보기관인 ASD 및 그 산하기관인 사이버안보센터는 실무 집행을 전담할 뿐 사이버안보 전략 및 정책 수립의 전면에 나서지 않는다는 점을 참고할 필요가 있다.

2) 감시 및 통제 장치 신설

사이버안보의 핵심은 민간과 정부 사이의 정보 공유 및 협력이다.[79] 이를 이끌어 내기 위해서는 다른 무엇보다도 민간이 정부에 정보를 공유하고 협력하여도 정부가 이를 오남용하지 않을 것이라는 신뢰가 축적되어야 한다. 사이버안보 추진체계와 관련하여 시민단체가 제기하는 국가정보원의 권한 남용, 개인정보보호 위협, 민간 사찰 등의 문제는 사실 정보기관에 대한 뿌리 깊은 불신과 두려움에서 비롯된 것이다. 이를 간과한 채 민간을 대상으로 사이버안보 정보의 공유 및 협력을 강권하고, 나아가 법률을 통하여 제도화하더라도 실질적인 참여와 협력을 기대하기 어렵다.[80]

---

78) 한희원, "국가정보 업무의 통제와 감독체계에 대한 비교법적 고찰을 통한 법정책적 함의 연구", 「법과 정책연구」 제14권 제1호, 한국법정책학회, 2014., 6-7면.

79) 김대건・백승수・유동희, "사이버위기에 대응하기 위한 국가정보기관의 사이버위협정보 공유 역할에 대한 고찰", 「디지털융복합연구」 제15권 제6호, 한국디지털정책학회, 2017., 52면.

80) 사이버안보 관련 국가정보원에 대한 민주적・절차적 통제장치 마련이 중요하다는 취지로

민간의 신뢰를 이끌어내는 방안으로 호주의 '정보기관 감사관' 사례를 참고하여 최소한 사이버안보 관련 정보공유 및 협력에 관한 부분만이라도 객관성과 중립성이 담보되는 독립기관의 상시적 감시 및 통제를 받는 방안을 고려할 필요가 있다.[81] 현행 정부조직체계상 이론적으로는 감사원이 국가정보원에 대한 감사권을 행사할 수 있으므로 별도의 독립기관의 설치가 불필요하다는 견해도 가능하다. 그러나 헌정사를 살펴보면 실제로 감사원이 국가정보원을 감사한 경우는 정부 수립 이후 단 한 차례 밖에 없는바, 감사원의 감사기능을 통한 국가정보원의 통제는 사실상 기대하기 어렵다.[82] 물론 국회 정보위원회에서 국가정보원에 대한 감시 및 통제권을 일정 부분 행사하기는 하나 국회 위원회라는 본질상 전문성이나 상시성을 기대하기 어렵다는 한계를 노정하고 있다. 국회 정보위원회와 별도로 정부 차원에서 별도의 감시 기구를 두어 행정부와 입법부 양 쪽의 통제를 받도록 할 경우 국민의 기본권이 보다 두텁게 보장될 수 있다는 측면에서 정보기관을 감시할 제3의 독립 기구를 둘 실익을 찾을 수 있다고 생각된다. 새로운 감독 기구의 신설이 어렵다면 대안으로 독립기구인 국가인권위원회나 심의기구에서 정부조직법상 행정위원회로 개편될 것이 예정된 개인정보보호위원회에 사이버안보 관련 정보 공유 과정에서의 인권 및 프라이버시 침해 여부에 관한 조사 및 감독 권한을 부여하는 방안을 생각해 볼 수 있다.[83] 다만 기밀성과 밀행성을 본질로 하는 정보기관에 대한 광범위한 감독은 자칫 정보기관 본연의 업무 수행을 저해할 수 있으므로, 독립적 감시기구를 설치하더라도 그 기구의 설치 근거, 구성, 조사 및 감독 권한의 범위와 한계 또한 명확히 법률에 규정되고 그에 따라 적법하게 이루어져야 할 것이다.

황성기, "사이버안보 관련 법제의 문제점과 개선방향",「경제규제와 법」제12권 제1호, 서울대학교 법학연구소, 2019. 5., 50-53면.

81) 유사한 취지로 개인정보보호위원회나 국가인권위원회에서 정부의 사이버보안정책과 기술의 프라이버시 침해에 관하여 검토하도록 하자는 주장으로 김법연・권헌영, "프라이버시 보호를 위한 합리적 사이버보안법제 마련의 쟁점과제와 입법방향",「법학연구」제28권 제4호, 연세대학교 법학연구원, 2018. 12., 247면.

82) 감사원법상 감사원은 국가정보원에 대하여 회계검사 및 직무감찰이 모두 가능하나(제22조, 제24조), 국가정보원이 실질적인 감사원 감사를 받은 것은 2018년 단 한 차례에 불과하고, 그나마 감사 결과도 기밀사항이 많다는 이유로 상당 부분 비공개되었다. "사상 첫 '국정원 감사' 마무리한 감사원...국정원에 결과 통보", 서울경제 2019. 4. 14.자 기사.

83) 단 국가정보원이 대통령 소속의 정보기관이라는 점을 고려하면, 국무총리 소속이 아닌 대통령 소속 위원회로 개인정보보호위원회가 설치되도록 현재 국회 계류 중인 개인정보보호법 개정안(의안번호 2016621 인재근의원 대표발의) 제7조 제1항을 수정하는 방안을 논의할 필요가 있다.

3) 기본법 제정 추진의 재검토

사이버안보를 체계적, 효율적으로 추진하기 위해서는 범정부적 사이버안보 거버넌스 구축, 민관 협력과 소통, 정보공유와 같은 제도의 구현과 이를 뒷받침하는 법률의 정비가 필요하다. 그러나 호주 사례에서 살펴보았듯이 법률 정비를 위하여 반드시 '기본법'을 제정해야 하는 것은 아니다. 사이버안보 법제 강화 방안으로는 기본법의 제정, 기존 법률의 개정·정비, 현행 법제 운용의 정상화 등 다양한 방식이 가능하다. 어떠한 방식을 채택할 것인지는 기존 법제도의 현황 및 문제점, 정치·사회적 여건, 향후 지향점 등을 종합적으로 고려하여 상황에 맞게 탄력적으로 결정할 문제이다. 그럼에도 불구하고 우리나라는 2000년대 이후 '기본법'의 제정에 초점을 맞추어 왔고, 그 제정 추진 과정에서 국가정보원의 권한 강화, 민간 사찰 우려와 같은 정치적으로 민감한 문제가 대두되면서 결국 법 제정에 이르지 못하고 국회 회기 만료로 법안이 자동 폐기되는 악순환을 반복해왔다.

사이버안보 관련 법률이 여러 부처에 산재해있고 소관 기능도 분산되어 있는 우리나라 현실을 고려할 때 궁극적으로는 사이버안보를 통합적으로 규율하는 기본법을 제정할 필요가 있다는 점은 어느 정도 수긍할 수 있으나, 정치적으로 민감한 쟁점을 다수 포함하고 있는 사이버안보 기본법의 제정이 현 상황에서 쉽지 않다는 점을 감안하면, 기본법의 제정은 사회적 공감대가 형성되기 전까지는 장기적 과제로 지속적으로 추진하되, 기본법 제정시까지의 대안으로 현행 법률 중 사이버안보와 관련된 법률들 – 정보통신망법, 정보통신기반보호법, 「통신비밀보호법」, 「국민보호와 공공안전을 위한 테러방지법」(이하 '테러방지법') 등 – 이 병존하는 현재의 개별법 체계를 최대한 일관되고 통일성있게 정비하는 한편 현행 법제도상으로 가능한 부분은 최대한 적극적으로 시행함으로써 하루가 다르게 진화하는 사이버안보 위협에 신속하고 탄력적으로 대응할 필요가 있다.

4) 정보 공유 등 사이버안보 핵심 역량의 법적 근거 마련

사이버안보 역량 강화의 핵심은 민간과 정부의 정보 공유와 협력이다. 그러나 현행 법률은 이에 관한 법적 근거, 관련 절차 및 개인정보보호와 같은 사항이 매우 미흡하다. 일례로 정보통신기반보호법을 살펴보면 민관 정보공유 및 협력에 관한 근거조항으로는 '정보공유·분석센터를 둘 수 있다'는 단 1개의 조항만을 두고 있어(제16조) 정보공유의 절차, 공유되는 정보의 내용 및 범위와 한계, 공유정보의 오남용 방지 장치와 같은 사항에 관한 법적 규율이 사실

상 공백(空白)인 상태이다. 반면 정보통신기반보호법에 대응하는 호주의 CIA 및 TA의 경우 민간에 대한 정부의 정보수집권 및 행정명령권을 규정하는 등 민관 정보 공유 및 협력에 관하여 우리나라에 비하여 상대적으로 상세한 규정을 두고 있고, 법률은 아니지만 민간과 공공의 신뢰에 기반한 파트너쉽을 통하여 사이버위협 정보를 민관이 활발히 공유하고 있다. 호주의 사례에 비추어 볼 때 정보통신기반보호법이나 정보통신망법을 개정하여 사이버안보 위협 정보의 민관 공유에 관한 원칙, 공유 및 분석 절차, 분석 결과의 환류, 개인정보보호에 관한 사항의 법적 근거를 규정하거나, 최소한 민관과 공공의 협력에 기한 파트너쉽을 촉진할 수 있는 근거 조항(민간에 대한 재정적 지원, 사이버위협 정보 제공에 관한 민간의 면책 등)을 두는 등 개별법의 정비 방안을 고민할 필요가 있다. 한편 하루가 다르게 진화하는 신종 사이버 공격에 대한 대응 체계를 강화하는 차원에서 호주의 TAA와 유사하게 통신사업자에게 암호화된 통신에 대한 자발적 지원이나 협조 의무를 규정할 필요에 관하여도 논의를 시작할 필요가 있다.

Ⅳ. 마치며

모든 사물과 사물이 네트워크로 연결되어 상호 통신하고 사회의 모든 활동이 네트워크를 매개로 한 가상 공간에서 이루어지는 초연결사회의 도래를 눈앞에 두고 있다. 이러한 사회적 변화 속에서 국가 안보의 패러다임도 국경·영토와 같은 기존의 전통적인 물리적 공간에서의 안보를 뛰어넘어 가상 공간에서의 안보로 진화하고 있다. 사이버안보 위협은 기존의 물리적 안보위협과 달리 군사력과 같은 재래식 전력을 요하지 않고, 시공간의 제약을 받지 않으며, 공격을 받았다는 사실 여부를 확인하기도 어렵고, 일단 공격이 성공하면 사회 전 영역에 치명적이고 광범위한 타격을 가할 수 있다는 등의 특징을 가지고 있어, 다른 어느 분야보다도 신속하고 체계적인 범국가적 대응 체계를 갖출 것이 요구된다. 그럼에도 불구하고 아직까지 사이버안보를 뒷받침할 수 있는 법제도는 미비한 상황이며, 국회 계류 중인 정부안과 이철우의원안에 대하여는 제대로 된 논의조차 이루어지지 않고 있는 것이 우리의 현실이다. 이처럼 사이버안보 법제도가 교착(deadlock) 상태에 빠진 주된 이유는 국가정보원의 위상과 역할을 둘러싼 정치적·사회적 갈등에 있다. 국회에 제출된 사이버안보 법

제도 개편방안은 정보기관이 공공과 민간을 아우르는 컨트롤타워를 맡는 한편 실무 집행도 전담하는 구조로서 정보기관의 권한 비대화 우려 및 그로 인한 민간 사찰과 사생활 침해 논란에서 자유로울 수 없다는 내재적 한계를 가지고 있다. 논란과 우려를 불식시키기 위해서는 국가정보원이 컨트롤타워를 맡는 추진체계가 타당한지, 사이버안보 '기본법'의 제정이 필요한지 등에 관한 근본적인 고민과 진지한 논의가 필요하다. 본고에서 살펴본 호주의 사례에서 알 수 있듯이 사이버안보 컨트롤타워와 실무집행기관을 각 분리하는 이원화된 추진체계도 얼마든지 상정할 수 있으며, 사이버안보에 관련되어 기존에 제정, 시행중인 개별법을 탄력적으로 개정함으로써 사이버안보 위협에 신속하게 대응할 수 있는 측면이 있기 때문이다. 아무쪼록 국가정보원을 둘러싼 소모적인 논쟁에서 탈피하여 대한민국이 세계 최고 수준의 IT 강국이라는 위상에 걸맞은 혁신적이고 선도적인 사이버안보 체계를 하루속히 갖추기를 희망한다.

[참고문헌]

김대건・백승수・유동희, “사이버위기에 대응하기 위한 국가정보기관의 사이버위협정보 공유 역할에 대한 고찰”, 「디지털융복합연구」 제15권 제6호, 한국디지털정책학회, 2017.

김도승, “국가 사이버안보의 법적 과제”, 「미국헌법연구」 제28권 제2호, 미국헌법학회, 2017. 8.

김법연・권헌영, “프라이버시 보호를 위한 합리적 사이버보안법제 마련의 쟁점과제와 입법방향”, 「법학연구」 제28권 제4호, 연세대학교 법학연구원, 2018. 12.

김상배, “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각”, 「국제·지역연구」 제26권 제3호, 서울대학교 국제학연구소, 2017. 9.

김재광, “사이버안보 위협에 대한 법제적 대응방안”, 「법학논고」 제58집, 경북대학교 법학연구원, 2017. 5.

김우상, “중견국 외교 협력방안 모색: 한국과 호주 중심”, 「JPI 정책포럼」 제2011-31호, 제주평화연구원, 2011. 11.

박상돈, “일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로”, 「경희법학」 제50권 제2호, 경희법학연구소, 2015. 6.

박상돈・김규동・김소정, “사이버안보 법제도의 의의에 대한 새로운 이해”, 「보안공학연구논문지」 제14권 제2호, 보안공학연구지원센터, 2017. 4.

박지웅, “초연결사회의 정치경제학적 기원과 성격”, 「사회경제평론」 제57호, 한국사회경제학회, 2018. 10.

양천수・지유미, “미국 사이버보안법의 최근 동향 - 「사이버보안 정보공유법」을 중심으로 하여 -”「법제연구」 제54호, 한국법제연구원, 2018. 6.

이해원, “영국의 사이버안보 법제 변천 과정 및 시사점”, 「법학연구」 제26권 제4호, 경상대학교 법학연구소, 2018. 10.

정준현, “북한의 사이버공격에 대한 국가총력적 대응체계를 위한 법제방향”, 「성균관법학」 제28권 제4호, 성균관대학교 법학연구원, 2016. 12.

정필운, “사이버보안이란 개념 사용의 유용성 및 한계”, 「연세 의료과학기술과 법」 제2권 제2호, 연세대학교 법학연구원 의료・과학기술과 법센터, 2011. 8.

한희원, “국가정보 업무의 통제와 감독체계에 대한 비교법적 고찰을 통한 법정책적 함의 연구”, 「법과 정책연구」 제14권 제1호, 한국법정책학회, 2014.

황성기, “사이버안보 관련 법제의 문제점과 개선방향”, 「경제규제와 법」 제12권

제1호, 서울대학교 법학연구소, 2019. 5.
홍준호, “사이버보안 컨트롤타워 필요성에 관한 연구”, 「법학연구」 제19권 제1호, 한국법학원, 2019. 3.

국회 정보위원회, “국가 사이버안보에 관한 법률안(이철우의원 대표발의) 및 국가 사이버안보법안(정부 제출) 검토보고”, 2017. 2.
박영철 외, “사이버보안체계 강화를 위한 정보보호법제 비교법연구”, 한국인터넷진흥원, 2015.
양천수 외, “안전한 지능정보사회 구축을 위한 정보보호 관련 법제도 개선방안 연구”, 과학기술정보통신부, 2018.
이응용, “호주 사이버보안 정책동향”, KISA Report 2018. Vol. 12., 한국인터넷진흥원, 2018. 12.
참여연대, 국가 사이버안보 기본법 제정(안)에 대한 의견서, 2016. 10.
청와대 국가안보실, “문재인 정부의 국가안보전략”, 2018. 12.
청와대 국가안보실, “국가사이버안보전략”, 2019. 4.

Erica Wiking Häger, *Cybersecurity Law Overview,* Mannheimer Swartling, 2017.
ITU, *Measuring the Information Society Report 2017, Volume 1*, ITU, 2017.

Andrew O’Neil, “Australia and the ‘Five Eyes’ intelligence network: the perils of an asymmetric alliance”, *Australian Journal of International Affairs,* Vol. 71, No. 5, 2016.
Badu V. Shirivas, “A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains”, the SANS Institute, 2015.
Cat Barker・Helen Portillo-Castro, “Bills Digest No. 49, 2018-19”, Australian Parliament Library, 2018. 12.
Fergus Hanson et al, “Cyber Maturity In The Asia-Pacific Region 2017”, Australian Strategic Policy Institute, 2017.
Liam Nevil, “Cyber Security Governance in Australia”, Center for International Governance Innovation, 2018.

Commonwealth of Australia, *Australia’s Cyber Security Strategy,* 2016.

Commonwealth of Australia, *Critical Infrastructure Centre Compliance Strategy*, 2016.

Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, 2018. 11.

The Parliament of The Commonwealth of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Explanatory Memorandum*, 2018.

[Abstract]

Proposal of Enhancing National Cybersecurity Legal Framework: Focusing on Case Study of Australia Cybersecurity

Lee, Hae-Won*

Despite the importance of cybersecurity is emerging in the era of hyperconnected society, the national capability including the policy, strategy and legal system of responding cybersecurity threats is still insufficient. This paper reviews Australia's case by comparative law research, draws implications, and suggests ways to improve the Korean cyber security legal framework. The main improvement measures suggested in this paper are as follows First, the cybersecurity control tower should literally be a control role, and the National Intelligence Service('NIS') is appropriate to carry out practical and support functions, not the control tower or strategy and policy making functions. Second, to restore substantial information sharing and cooperation between the private sector and the public, it is necessary to restore the trust of the NIS. To this end, it is necessary to establish an independent supervisory agency that controls and supervises the NIS. Third, it is necessary to review the current individual law system in a systematic way and to consider the establishment of the 'cybersecurity basic law' as a long-term task. Fourth, it is necessary to prepare a legal basis for promoting cyber security core competencies such as information sharing by amending individual laws. In line with its status as the world's most advanced IT powerhouse, advanced legal systems are urgently needed to cope with the ever-increasing and evolving cyber security threats.

Keywords : cybersecurity, cybersecurity governance, cybersecurity law, australia cybersecurity case study, independent supervisory agency

* Assistant Professor/Attorney at Law, Department of Law, Mokpo National University.