국가전략연구위원회 이슈브리핑 32호 (발간일: 2024.9.30.)

파이브 아이즈 국가의 사이버 안보 전략: 추진체계를 중심으로[1)]

신승휴 (서울대학교)

Ⅰ. 서론

오늘날 디지털 기술이 국가의 힘과 안보에 지대한 영향을 미침과 동시에 강대국 경쟁의 한 영역으로 자리 잡게 되면서 사이버 안보 분야에서 나타나는 국제협력의 양상이 변화하고 있다. 과거 사이버 안보 국제협력이 국가별 전담기관 간 사이버 위협 관리를 위한 협조를 목표로 했다면, 최근에 와서는 기술지정학적(techno-geopolitical) 상황 가운데 동맹 차원의 연대를 구축해나가는 방향으로 그 범위가 확장되고 있다. 이러한 현상은 개별 국가의 전략 추진체계가 변화하는 추세와 맞물려 나타난다. 이미 2010년대에 접어들면서 사이버 안보는 국가전략의 맥락에서 다뤄져 왔지만, 현재는 특정 실무부처나 전담기관 차원의 정책적 대응을 넘어 '국가책략(statecraft)'의 관점에서 접근해야 할 영역으로 여겨지고 있다.

국가책략은 국가안보, 경제적 번영, 정치적 위상과 영향력 등 거시적인 차원에서 설정된 목표를 달성하기 위해 군사, 경제, 외교, 정보 등 다양한 영역의 수단을 동원하는 것으로 정의될 수 있는데,[2)] 오늘날 사이버 안보에 대한 국가적 접근 역시 범정부 차원에서 거시적 전략목표를 설정하고 이를 추구하는 과정에 다양한 정부부처와 기관의 참여를 허용한다는

1) 이 글은 2024년 9월 25일 제11차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.
2) 국가책략의 이와 같은 개념적 정의는 경제책략에 관한 볼드윈(Baldwin 1985)의 논의를 참고한 것이다. David A. Baldwin, *Economic Statecraft,* (Princeton, N.J.: Princeton University Press, 1985).

점에서 국가책략의 성격을 가진다. 즉 사이버 안보가 어느 한 이슈 분야에 국한된 문제를 넘어 범분야 기술 문제(cross-cutting technical issue)이자 체제 수준의 도전이 됨에 따라 특정 기관 차원의 대응과 협력만으로는 더는 효과적으로 대응하기 어렵게 되었기 때문이다. 따라서 범정부적 차원의 통합 대응에 대한 선호가 높아지고 있다.

그 가운데 최근 미국을 포함한 파이브 아이즈 국가(Five Eyes nation)들의 사이버 안보 국제전략은 민주주의 연대를 구축하여 사이버 안보 분야에서 발생하는 다양한 도전에 공동 대응하고자 하는 공유된 이해관계를 바탕으로 추진체계의 측면에서 높은 유사성을 드러내고 있다. 이는 '추진체계의 네트워크화' 현상으로 나타난다. 파이브 아이즈 국가들은 국가 내부적으로 다양한 주체들이 위계적이고 수직적인 거버넌스를 벗어나 이전보다 더 수평적인 관계에서 상호작용하며 사이버 안보 전략을 지원하는 추진체계를 채택하고 있다. 그 가운데 국제전략에 참여하는 주체 역시 다양해지는 현상이 나타나는데, 이는 이들 5개국이 사이버 안보 국제협력, 특히 파이브 아이즈 정보동맹(intelligence alliance) 차원의 협력에 다양한 하위주체의 참여를 허용하기 때문으로 볼 수 있다. 즉 전략의 운용조직으로서 이들 국가가 사이버 안보 분야에서만큼은 한층 더 '네트워크 국가(network state)'의 면모를 보이고 있음을 뜻한다.[3)]

Ⅱ. 사이버 안보 전략의 복합형 추진체계

최근 파이브 아이즈 국가들은 사이버 안보 전략을 추진하는 과정에서 다양한 국가 하위주체를 참여시키고 있다. 즉 위계적인 조직체로서 블랙박스화된 국가가 수직적이고 하향적인 구조에서 전략을 추진하는 방식을 따르지 않는다. 컨트롤타워가 존재하되 국가 내부적으로 다양한 하위주체들이 수직적인 거버넌스를 벗어나 이전보다 좀 더 수평적인 관계에서 상호작용하며 전략을 지원해오고 있다. 이는 이들 국가의 전략이 보이는 구조적 특징에 해당한다. 현재 파이브 아이즈 5개국은 정부부처와 기관들이 각기 담당하는 영역에서 개별적으로 사이버 보안 체계를 구축하도록 허용하되 범정부 차원의 컨트롤타워를 수립하여 사이버 안보와 디지털 기술에 대한 국가적 대응을 주도하게끔 하는 '복합형 모델'을 채택하고 있는 것으로 평가된다.[4)]

복합형 모델의 추진체계는 특정의 정부부처나 전담지원기관이 범정부 컨트롤타워가 되어 국가전략을 주도해나가는 '총괄형 모델'과, 각 실무부처나 기관이 개별적으로 거버넌스를 구축하여 이익 창출과 위험 완화를 도모하게끔 하는 '분산형 모델'이 혼합된 형태로 볼 수 있다. 이는 긴급한 대응책이나 국가적 차원의 자원 결집을 요구할 때 효과적인 총괄형 모델

3) 네트워크 국가에 관한 국제정치학적 논의는 다음의 연구를 참고할 것: 김상배 엮, 『네트워크 국가론: 미래 세계정치 연구의 이론적 기초』(파주: 사회평론아카데미, 2021).
4) 이와 같은 유형화는 주요국의 사이버 안보 전략을 정책지향성과 추진체계의 구성원리를 기준으로 구분해 분석한 김상배(2019)의 연구를 참고한 것이다.

의 이점과 영역별 실무부처의 특화된 대응이 필요할 때 적합한 분산형 모델의 이점을 고루 갖추었다는 점에서 그 경쟁력을 찾을 수 있다. 물론 각국의 전략 추진체계는 총괄형 모델과 분산형 모델을 양극단에 둔 스펙트럼을 기준으로 어느 쪽에 더 가까운 성격을 보이느냐에 따라 서로 다른 유형으로 비칠 여지가 없지 않다. 또한 개별 국가 차원에서도 시기에 따라 추진체계의 구조에서 크고 작은 차이가 발견되기도 한다.[5]

그러나 이를 총괄형 모델과 분산형 모델 중 하나로 구분하기 어려운 것은 양쪽 모두 네트워크의 속성을 갖기 때문이다. 예컨대, 총괄형 모델에 좀 더 가까운 성격을 드러내는 경우라 할지라도 범정부 컨트롤타워나 특정 실무부처가 위계적인 거버넌스의 상층부에서 모든 것을 결정하고 명령을 하달하는 구조는 아니다. 그보다는 다양한 주체들의 역할을 조율하고 교류를 조정하는 중개자(borker)의 기능을 담당하는 것에 가깝다. 분산형에 더 근접한 복합형 모델의 경우에도 각각의 추진주체가 상호배타적이고 분리된 상태에서 대응책을 마련하기보다는 그들 간 거버넌스와 정책이 국가전략의 목표를 추구하는 흐름 속에서 서로 중첩되고 조화되는 '다부처 임무중심형 기능강화'의 방식으로 볼 수 있다.[6] 종합하자면, 파이브 아이즈 국가들이 채택하고 있는 사이버 안보 전략의 추진체계는 '네트워크화된 추진체계'를 의미한다. 네트워크에는 허브(hub)에 위치하는 노드(node)와 그렇지 않은 노드들이 존재하듯, 네트워크화된 추진체계에서도 중심적인 역할을 담당하는 하위주체가 존재한다.

Ⅲ. 파이브 아이즈 국가의 사례

1. 미국

미국의 경우, 사이버 안보 전략을 총괄하는 컨트롤타워는 대통령실(Executive Office of the President of the United States) 산하 국가사이버실(ONCD: Office of National Cyber Director)이 맡고 있다. ONCD는 국가안전보장회의(NSC: National Security Council) 관계자(staff)의 감독하에 대통령실 산하 관리예산실(OMB: Office of Management and Budget)과 협업하여 전략의 실행을 조정하며, 매년 NSC, OMB, 각 정부부처 및 기관과 협력하여 국가사이버안보전략의 성과를 평가해 이를 대통령 및 의회에 보고한다. AI와 관련해서도 대통령실은 그 산하에 설치된 과학·기술정책실(OSTP: Office of Science and Technology Policy)을 통해 전략의 통합성 제고와 각 정부부처 및 기관들의 협력을 총괄·조정한다.

그러나 동시에 국토안보부(Department of Homeland Security)와 그 산하의 사이버·인프라보안국(CISA: Cybersecurity and Infrastructure Security Agency), 국무부(Department of

5) 김상배, "사이버 안보전략의 분석틀: 형성배경과 추진체계의 비교연구," 김상배 엮, 『사이버 안보의 국가전략 3.0: 16개국의 전략형성과 추진체계 비교』(파주: 사회평론아카데미, 2019), pp. 52-67.
6) 김종선 외, "기정학시대에 대응한 과학기술 국제협력시스템의 고도화 방안," STEPI Insight 제323호, 과학기술정책연구원 (2024년 4월 9일).

State)와 그 산하의 사이버공간·디지털정책국(CDP: Bureau of Cyberspace and Digital Policy), 국방부(Department of Defense), 법무부(Department of Justice), 재무부(Department of the Treasury), 상무부(Department of Commerce)와 그 산하의 국립표준기술연구소(NIST: National Institute of Standards and Technology), 국가안보국(NSA: National Security Agency), 연방수사국(FBI: Federal Bureau of Investigation) 등 다양한 정부부처와 기관이 사이버 안보 문제와 디지털 기술에 대한 국가적 차원의 대응을 지원해오고 있다.[7] 특히 국토안보부의 CISA는 법집행기관 및 정보기관, 연방·주 정부, 기업 간 협력을 조율함으로써 사이버 위협으로부터 주요 기반시설을 보호하는 데 앞장서고 있다.[8]

대외적 협력 부문에서도 여러 다른 정부부처와 기관들이 협력의 주체로 등장한다. 즉 전략을 총괄하는 컨트롤타워는 ONCD가 맡고 있지만, 디지털 기술의 발달과 기술지정학적 위기로 인해 국제협력의 중요성과 범위가 더욱 증가하게 되면서 국제전략의 추진주체가 다양해지게 된 것이다. 다만 여전히 중추적 역할은 국무부가 담당한다. 바이든 행정부는 2022년 4월 국무부 산하에 CDP를 신설하였는데, CDP의 역할은 "사이버 공간 및 디지털 기술에 대한 외교정책을 주도·조정·개선함으로써 미국의 국가안보와 경제안보를 증진"하는 것으로 소개된다. 현재 그 산하에는 국제사이버공간안보(ICS: International Cyberspace Security), 국제정보통신정책(ICP: International Information and Communications Policy), 디지털자유(DFU: Digital Freedom) 부서가 운영되고 있으며. 이들 부서는 각각 안보, 경제, (자유민주주의) 가치에 초점을 맞춰 국무부와 CDP의 활동을 지원해오고 있다.[9]

한편 CDP를 이끄는 사이버공간·디지털정책 특임대사(Ambassador at Large for Cyberspace and Digital Policy)는 UN, G20 등 국제무대에서 사이버 안보에 대한 미국의 전략적 이해관계를 전달함과 동시에 주요 동맹국들과의 양자·다자 사이버 안보 협력을 강화하는 데에도 중요한 역할을 담당한다.[10] 또한 국무부 산하에는 신흥기술 전반에 걸쳐 미국의 경쟁력을 강화하고 동맹국 및 파트너국과의 협력을 증진하기 위해 신설된 핵심신기술특사실(S/TECH: Office of the Special Envoy for Critical and Emerging Technology)이 운영되고 있다. 국무부는 S/TECH를 통해 국가안보 우선순위에 따라 '통합된 기술외교전략'을 수립함으로써 미국이 AI, 양자컴퓨팅을 포함한 모든 신흥기술 분야에서 동맹 중심의 기술산업 공

---

7) White House, "One Year In: The President's National Cybersecurity Strategy is Driving Change and Protecting the Nation," (March 4, 2024). https://www.whitehouse.gov/oncd/briefing-room/2024/03/04/national-cybersecurity-strategy-one-year/ (접속일: 2024.09.07.).; White House, *National Cybersecurity Strategy Implementation Plan,* Version 2 (May 2024).

8) National Cybersecurity and Communications Integration Center, *NCCIC ICS*.

9) Department of State, "CDP Policy Units - Bureau of Cyberspace and Digital Policy." https://www.state.gov/about-us-bureau-of-cyberspace-and-digital-policy/ (접속일: 2024.09.14.)

10) US Embassy and Consulates in Brazil, "Ambassador Fick Attends G20 Digital Economy Ministerial Meeting in Brazil," (September 11, 2024). https://br.usembassy.gov/ambassador-fick-attends-g20-digital-economy-ministerial-meeting-in-brazil/ (접속일: 2024.09.15.)

급망과 기술 개발 생태계를 보호하고 나아가 기술 표준을 확립하도록 지원하는 것을 목표로 삼고 있다.[11]

미국의 국제전략과 관련하여 또 한 가지 주목할 점은 전략에 참여하는 정부부처와 기관들이 주로 파이브 아이즈 정보동맹을 통로로 삼아 협력을 이어오고 있다는 사실이다. NSA나 FBI 등 정보기관은 물론이거니와 국무부, 국토안보부, 법무부 등 여러 정부부처가 정보동맹의 공조체제나 이를 기반으로 한 지역·글로벌 다자협력 네트워크에 참여하고 있다. 그로 인해 과거 신호정보(SIGINT) 담당 정보기관의 공조체제에 국한되던 파이브 아이즈 정보동맹이 지금에 와서는 사이버 안보와 디지털 기술 분야 국제협력의 핵심 플랫폼으로 부상하게 되었다. 이는 사이버 안보에 대한 미국의 접근이 국가책략의 관점에서 이루어짐으로써 과거 특정 영역에 각각 묶여있던 하위주체들의 활동 범위가 경계를 허물고 확장되어가는 현상으로 볼 수 있다.

2. 영국

영국의 사이버 안보 전략은 거시적 목표를 달성하기 위해 다양한 실무부처와 기관의 참여를 기반으로 추진되어오고 있다. 2024년을 기준으로 사이버 안보에 대한 국가적 접근은 내각부(Cabinet Office)를 중심으로 정부통신본부(GCHQ: Government Communications Headquarters) 산하 국가사이버안보센터(NCSC-UK: National Cyber Security Centre)[12], 내부무(Home Office), 과학·혁신·기술부(Department for Science, Innovation and Technology), 외무·영연방·개발부(Foreign, Commonwealth and Development Office), 국방부(Ministry of Defense), 보안국(M15: Security Service) 산하 국가보호보안청(NPSA: National Protective Security Authority), 국가범죄수사청(NCA: National Crime Agency) 등 여러 정부부처와 기관의 참여를 통해 추진되고 있다.

대내적 부문에서는 사이버 범죄 대응을 전담하는 내무부와 네트워크 및 정보 시스템의 보안 수준 유지를 책임지는 과학·혁신·기술부가 사이버 안보 관련 정책을 도맡아 추진해오고 있다.[13] 다만 사이버 안보 전략을 실질적으로 총괄하는 임무는 NCSC-UK가 맡고 있는 것으로 파악되는데, 2017년까지만 해도 내각부가 그 산하에 설치된 사이버·정부보안국(CGSD: Cyber and Government Security Directorate)을 통해 사이버 안보 관련 국가 과제의 우선순위를 정하고 관련 이니셔티브를 총괄해왔으나, 2016년 NCSC-UK가 신설되면서 그 이듬해 9

11) Alexandra Kelley, "State Department Creates First Office Devoted to Emerging Technology Diplomacy," *Nextgov* (January 4, 2023). https://www.nextgov.com/emerging-tech/2023/01/state-department-creates-first-office-devoted-emerging-technology-diplomacy/381459/ (접속일: 2024.09.14.)

12) 공식적인 약칭은 NCSC이지만, 뉴질랜드 국가사이버안보센터와의 구분을 위해 본 연구에서는 NCSC-UK로 표기하였다.

13) Adam Clark, "Cybersecurity in the UK," Research Briefing, House of Commons Library (April 19, 2024), pp. 25-26.

월 CGSD의 기능이 NCSC-UK로 이전되었다. 2016년도「국가사이버안보전략」에서도 당시 새롭게 출범한 NCSC-UK가 영국의 사이버 안보 환경을 책임지는 당국(authority)으로 소개된 바 있다.[14]

한편 국제협력을 위한 전략은 주로 외무영연방개발부와 GCHQ(NCSC-UK) 그리고 국방부가 핵심 주체가 되어 전개되고 있지만, 내무부와 MI5(NPSA) 그리고 과학·기술·혁신부도 근래 대외적 협력을 점차 늘려오고 있다. 먼저, 외무영연방개발부는 국제 사이버 안보 활동을 총괄함과 동시에 NCSC-UK를 감독하는 역할을 맡고 있다. 또한 그 산하에 기술 스파이 활동과 공격을 탐지·대응하는 국가도청방지청(NACE: National Authority for Counter-Eavesdropping)을 운영하고 있으며, NACE는 NCSC-UK, NPSA 등과 협력하여 자국과 우호국 정부에 기술안보(technical security) 관련 지침 및 정책 지원을 제공한다. 한편 NCSC-UK는 사이버 안보 국제전략에서도 중심에 위치하며 다른 정부부처와 기관들을 지원해오고 있다. 따라서 대외적 협력에서도 역시 그 존재감이 두드러지는데, 2023년 11월 미국과 함께「안전한 AI 시스템 개발을 위한 가이드라인」을 도출하는 과정에서도 NCSC-UK는 핵심 주체로 기능하였다.[15] 그뿐만 아니라 파이브 아이즈 정보동맹 차원에서 중국, 러시아의 악의적 사이버 활동을 규탄하는 과정에서도 NCSC-UK는 영국 정부를 대변해오고 있다.[16]

또 다른 정보기관인 MI5 역시 NPSA를 통해 파이브 아이즈 동맹국과의 공조에 참여하고 있는데, 일례로 2023년 동맹국 정보기관들과 함께 '안전한 혁신 5대 원칙(Five Principles of Secure Innovation)'을 발표하기도 하였다.[17] 내무부도 국내 복원력 및 국토 안보를 보장하는 차원에서 사이버 방어와 허위정보 대응 역량 강화를 위한 동맹 협력에 참여해오고 있다.[18] 국방부 역시 사이버 역량 강화를 위한 동맹 차원의 협력 외에도 전략사령부(UK Strategic Command)를 통해 파이브 아이즈 동맹국들과 디지털 기술 분야 국제협력을 이뤄오고 있다.[19] 다만 국방 분야 협력 역시 다른 기관들의 협업을 요구하고 있다는 점에서 국

14) HM Government, *National Cyber Security Strategy 2016-2021* (2016), p. 10
15) National Cyber Security Centre UK, 2023b.
16) National Cyber Security Centre UK, "NCSC joins partners to issue warning about China state-sponsored cyber activity targeting CNI networks," (May 24, 2023a). https://www.ncsc.gov.uk/news/ncsc-joins-partners-to-issue-warning-about-chinese-cyber-activity-targeting-cni (접속일: 2024.09.03.).; National Cyber Security Centre UK, "UK and allies expose evolving tactics of Russian cyber actors," (Febraury 26, 2024). https://www.ncsc.gov.uk/news/uk-allies-expose-evolving-tactics-of-russian-cyber-actors (접속일: 2024.09.08.).
17) National Protective Security Authority, "Five Eyes launches the Five Principles of Secure Innovation," (October 17, 2023). https://www.npsa.gov.uk/blog/news/five-eyes-launches-five-principles-secure-innovation (접속일: 2024.09.05.).
18) Home Office, "Home Secretary meeting with 'Five Eyes' counterparts," (February 23, 2022). https://www.gov.uk/government/news/home-secretary-meeting-with-five-eyes-counterparts (접속일: 2024.09.15.)
19) UK Strategic Command, "UK hosts Five Eyes Combined Digital Leadership Forum," (May 20, 2024). https://www.gov.uk/government/news/uk-hosts-five-eyes-combined-digital-leadership-forum

방부를 단독 추진주체로 보긴 어렵다. 2020년 창설된 영국 국가사이버군(NCF: National Cyber Force)만 보더라도 국방부 외에 NCSC-UK와 비밀정보국(MI6: Secret Intelligence Service)이 합동 상위기관으로 자리하고 있다.[20]

AI를 포함한 디지털 기술이 국가적 관심사로 떠오르면서부터는 과학기술을 전담하는 과학·혁신·기술부의 국제적 역할이 대폭 확장되었다. 과학·혁신·기술부는 2021년 「국가AI전략」 개발을 주도한 인공지능청(OAI: Office for Artificial Intelligence)을 2024년 흡수하였고, 그해 「AI 사이버 보안 실무지침」을 발표하였다. 그보다 앞선 2023년에는 외무영연방개발부와 함께 「영국의 국제기술전략」을 발표하는 등 디지털 기술 및 핵심 공급망에 대한 영국의 국제전략을 지원해오고 있다.[21]

3. 호주

호주의 사이버 안보 전략은 복합형 추진체계 모델을 채택하고 있다. 총리내각부(Department of the Prime Minister and Cabinet)가 내무부(Department of Home Affairs)에 컨트롤타워 역할을 부여한 가운데 내무부 산하의 국가사이버안보청(NOCS: National Office of Cyber Security)과 사이버인프라보안센터(CISC: Cyber and Infrastructre Security Centre), 호주신호정보국(ASD: Australian Signals Directorate) 산하의 호주사이버안보센터(ACSC: Australian Cyber Security Centre), 외교통상부(Department of Foreign Affairs and Trade), 국방부(Defence Australia) 및 호주방위군(ADF: Australian Defence Force), 법무부(Attorney-Generals' Department), 재무부(Department of the Treasury) 등 다양한 정부부처와 기관이 사이버 안보 전략에 참여하고 있다. 그 밖에도 산업·과학·자원부(Department of Industry, Science and Resources)는 핵심기술허브(Critical Technologies Hub)를 통해 정부에 디지털 기술의 기회와 개발 및 위험에 대해 조언하는 역할을 담당하고 있다.

대외적 협력에 초점을 맞춘 국제전략 부문에서는 단연 외교통상부의 역할이 두드러진다. 외교통상부는 사이버·핵심기술 대사(Ambassador for Cyber Affairs and Critical Technology)를 통해 사이버 안보에 대한 범국가적 접근을 지원하고 국제협력을 모색해오고 있다. 2021년에는 「국제사이버핵심기술협력전략」을 수립함으로써 지역 및 글로벌 차원의 사이버 공간과 핵심기술 분야에서 '가치, 안보, 번영'의 3대 분야 국익 실현 및 국제적 기여를 위한 국가적 차원의 노력을 주도한다는 계획을 내놓기도 하였다.[22] 「국제사이버핵심기술

(접속일: 2024.09.08.).

20) *The Telegraph,* "Britain steps up cyber offensive with new £250m unit to take on Russia and terrorists," (September 21, 2018). https://www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/ (접속일: 2024.08.21.)

21) UK Government, *The UK's International Technology Strategy* (March 2023).

22) Australian Government, *Australia's International Cyber and Critical Tech Engagement Strategy* (2021b).

협력전략」에서 설정된 3대 분야의 정책 과제들은 외교통상부를 필두로 하여 총리내각부, 법무부, 호주연방경찰(Australian Federal Police), ASD 및 ACSC, 국방부, 내무부, 인프라·교통·지역개발·통신부(Department of Infrastructure, Transport, Regional Development & Communications), 산업·과학·자원부 등이 이를 지원하는 방식을 통해 추진되어오고 있다.[23]

그중에서도 ASD와 그 산하의 ACSC는 외교통상부가 추진하는 사이버 안보 국제전략의 핵심 파트너 기관으로 기능하고 있다. ACSC의 주 기능은 디지털 시스템, 데이터 및 개인정보를 보호하는 데 도움이 되는 다양한 지침과 조언을 정부와 기업에 제공함으로써 악의적인 사이버 활동에 대응하는 실질적인 대응책을 마련하는 데 있다.[24] 따라서 국제협력 측면에서 나타나는 이들 기관의 역할은 호주의 주요 협력국, 특히 파이브 아이즈 동맹국의 사이버 안보 전담기관들과 함께 악의적 사이버 위협에 대한 구체적인 해결 방안을 도출하고 이를 공표하는 활동으로 나타난다. 가장 최근 사례로는 2023년 파이브 아이즈 동맹국 및 일본, 한국, 독일의 정보기관과 함께 중국 국가안전부(国家安全部) 산하 해커조직 APT40의 악의적 사이버 작전에 관한 공동 보고서를 발표하고, 2024년에는 사이버 위협 탐지를 위한 국제적 모범사례의 공유를 주도한 바 있다.[25]

한편 내무부의 대외 부문 역할 확장에도 주목할 필요가 있다. 최근 내무부는 외교통상부, ASD 및 ACSC와 함께 국제협력의 주체로 그 역할을 확장해오고 있다. 호주 정부는 2023년 내무부 산하에 NOCS를 신설하고 이를 책임지는 '국가사이버안보코디네이터(National Cyber Security Coordinator, 이하 코디네이터)'를 새롭게 임명함으로써 사실상 내무부를 사이버 안보 전략 추진체계의 컨트롤타워로 지정하였다. 코디네이터는 국내적 차원의 사이버 대응력 및 복원력 향상을 총괄하며 그 산하에 설치된 CISC를 통해 디지털 제품 및 서비스가 안전하고 보안이 유지되며 목적에 적합한 방향으로 개발될 수 있도록 지원하고 있다.[26]

내무부 장관이 사이버 안보 장관(Minister for Cyber Security)을 겸직하고 있다는 점 역시 추진체계상 내무부의 중심적 위치를 가늠하게 한다. 이렇듯 컨트롤타워 역할을 담당하는 내무부는 최근 대외적 활동 역시 활발히 이어오고 있다. 대표적인 예로 파이브 아이즈 5개국 장관회의(Five Country Ministrial)에서 호주 정부를 대표하여 정보동맹 차원의 사이버 안보 협력을 추진하고 있다. 2018년 발발한 화웨이 사태 국면에서 중국 통신기업의 5G 장비 퇴출을 발표한 주체도 내무부 장관(당시 장관 대행)이었다는 사실 역시 주목할 만하다.[27]

---

23) Australian Government, 2021b, pp. 91-95.
24) Australian Signals Directorate, *Information Security Manual* (June 2024).
25) Australian Signals Directorate, *APT40 Advisory: PRC MSS tradecraft in action* (2023).; Australian Signals Directorate, *Best Practices for event logging and threat detection* (2024).
26) Ribeiro, 2024.
27) Michael Shoebridge, "Huawei ban part of global move to set limits on Chinese influence," *The Strategist* (August 29, 2018). https://www.aspistrategist.org.au/huawei-ban-part-of-global-move-to-set-limits-on-chinese-influence/ (접속일:2024.09.08.).

마지막으로, 국방부도 디지털 기술의 발달을 고려하여 사이버 안보 역량 강화를 위한 국제협력을 추진해오고 있다. 이러한 맥락에서 2022년 「국방사이버안보전략」과 「국방정보통신기술전략」 발표를 통해 사이버 안보와 정보통신기술 분야에서 국제협력을 확장해나갈 의지를 드러냄과 동시에 동맹국과의 사이버 안보 파트너십 및 상호운용성을 여러 방면에서 강화하고 있다.[28] 특히 오커스의 첨단기술역량 부문 협력(필러2 협력)을 통해 사이버, AI, 양자 컴퓨팅 기술을 포함한 8개 기술 분야에서 공동개발을 추진하면서 자국과 오커스 협력국의 기술산업 간 연결성을 강화하는 노력 역시 전개해오고 있다.[29] 한편 국방부는 호주 외교안보 분야 싱크탱크인 호주전략정책연구소(ASPI: Australian Strategic Policy Institute)를 지원하고 있는데, 2001년 호주 정부가 설립한 ASPI는 2021년부터 매년 사이버를 포함한 핵심기술 분야 정책포럼인 시드니 대화(The Sydney Dialogue)를 개최해오고 있기도 하다.

4. 캐나다

캐나다의 사이버 안보 전략 추진체계는 통신보안기구(CSE: Communications Security Establishment)와 그 산하에 설치된 캐나다사이버안보센터(CCCS: Canadian Centre for Cyber Security)를 사실상 컨트롤타워로 삼고 있다. 「국가사이버안보전략」과 「국가사이버안보 실천계획 2019-2024」가 발표된 2010년대 말까지만 해도 컨트롤타워의 역할은 공공안전부(Public Safety Canada)와 그 산하의 캐나다사이버사고대응센터(CCIRC: Canadian Cyber Incident Response Centre)가 담당해왔지만, 2018년 2월 CSE의 CCCS가 설립되면서부터 점진적으로 그 기능과 책임이 CCCS로 이전되었다.[30] 캐나다 정부 역시 CCCS가 사이버 안보의 전문 기술 자문과 지침 및 서비스를 제공하는 단일 통합 기관으로 설립되었음을 분명히 한 바 있다.[31]

한편 공공안전부와 CCCS 외에도 외교부(Global Affairs Canada), 캐나다보안정보국(CSIS: Canadian Security Intelligence Service), 연방경찰(RCMP: Royal Canadian Mounted Police), 캐나다보안정보국(CSIS: Canadian Security Intelligence Service), 혁신·과학·경제개발부(Innovation, Science and Economic Development Canada), 천연자원부(Natural Resources Canada), 국방부(Department of National Defence) 등 다양한 정부부처와 기관들도 각기 전

---

28) Defence Australia, *Defence Cyber Security Strategy* (August 2022).; Defence Australia, *2022 Defence Information and Communications Technology Strategy* (August 2022).

29) Defence Australia, "AUKUS Defence Ministers' Joint Statement," (April 9, 2024). https://www.minister.defence.gov.au/statements/2024-04-09/aukus-defence-ministers-joint-statement (접속일: 2024.09.09.).

30) 유인태, "캐나다 사이버 안보와 중견국 외교: 화웨이 사례에서 나타난 안보와 경제·통상의 딜레마 속에서," 『문화와 정치』 제6권 2호 (2019), p. 276.

31) Public Safety Canada, "National Cyber Security Strategy 2019-2024: Report on the Mid-term Review," (June 27, 2022). https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx#s4 (접속일: 2024.09.09.).

담하는 분야에서 역할과 책임을 다하고 있다.[32] 재정위원회(Treasury Board) 역시 자국 정부의 사이버 대응 역량과 디지털 자원 보호를 강화하는 목적에서 2024년 「정부사이버안보전략」을 수립·발표하기도 하였다.[33] 반면에 총리실(Office of the Prime Minister)의 경우, 사이버 안보를 위한 국가전략의 수립을 관련 정부부처에 지시하는 것 외에는 전략의 수립 및 추진 과정에서 특별히 그 존재감을 드러내지 않는다.

캐나다의 전략에서 대외적 차원의 협력을 모색하는 일은 '사이버 공간에 대한 국제전략 프레임워크' 이니셔티브를 담당하는 외교부가 전담해오고 있다. 외교부는 2018년 국제사이버협력실무그룹을 출범시키고 그 이듬해 사이버 안보 전담 부서를 내부에 설치하는 등 국제협력을 추진하기 위한 토대를 마련하였다. 비록 현시점까지 발표되진 않았으나 국제사이버전략을 수립하기 위한 노력 역시 전개해오고 있는 것으로 알려졌다.[34] 그 밖에도 캐나다가 사이버 안보 관련 국제회의를 주최하거나 국제기구와 같은 다자포럼에서 사이버 안보에 대한 자국의 이해관계와 가치를 알리는 일은 모두 외교부가 중심이 되어 추진되고 있다. 한편 외교부는 자국을 대표해 동맹 차원에서 외국 정부의 악의적 사이버 활동을 규탄하는 일에도 적극적으로 나서고 있는데, 이러한 활동은 쟁점화된 이슈의 성격에 따라 CSE와의 분업을 통해 이루어진다.[35]

일찍이 CSE는 파이브 아이즈 동맹국의 정보기관들과 함께 국제적으로 쟁점화된 악의적 사이버 공격의 책임소재를 파악하고 이를 대외적으로 알리는 데 힘써왔다. 그리고 이러한 협력의 양상은 2020년을 기점으로 더욱 강화되기 시작하였다. 근래에 와서는 권위주의 국가의 정부가 배후에 있는 것으로 추정되는 사이버 위협을 경고하고 구체적인 대응 방안을 안내하는 일에도 힘쓰고 있다.[36] 그러한 맥락에서 2022년 발간한 「국가사이버위협평가」 보고서를 통해 중국, 러시아, 이란, 북한의 사이버 작전이 캐나다에 심각한 위협이 되고 있음을 경고하기도 하였다.[37] 국방부(Department of National Defence) 역시 외교부와의 협업을 통해 사이버 안보 국제전략에 참여해오고 있는데, 이는 주로 핵심 동맹국들과의 사이버 연

32) Public Safety Canada, "Public Safety Canada 2023 Summer – Issues Book," (November 23, 2023). https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20231123-2/06-en.aspx (접속일: 2024.09.15.).

33) Treasury Board of Canada, "Government of Canada releases its first Enterprise Cyber Security Strategy," (May 22, 2024). https://www.canada.ca/en/treasury-board-secretariat/news/2024/05/government-of-canada-releases-its-first-enterprise-cyber-security-strategy.html (접속일: 2024.09.15.)

34) Public Safety Canada, 2022.

35) Governmant of Canada, "International cyber policy," (December 20, 2023c). https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=eng#a1 (접속일: 2024.09.10.)

36) Canadian Centre for Cyber Security, "CSE and its Canadian Centre for Cyber Security release advisory on People's Republic of China state-sponsored cyber threat," (May 24, 2023). https://www.cyber.gc.ca/en/news-events/advisory-peoples-republic-china-state-sponsored-cyber-threat (접속일: 2024.09.10.).

37) Communications Security Establishment, *National Cyber Threat Assessment 2023-2024* (2022), pp. 12-15.

합작전 역량을 증진하거나 위협정보 및 모범사례를 공유하는 방식으로 전개되고 있다. 다만 원래 국방부 산하에 존재했던 CSE가 독립적인 기관으로 분리되었기 때문에 사이버 안보 국제협력에 관한 국방부의 기능과 책임은 군사 분야에만 한정되는 방향으로 변화했을 것으로 추측해볼 수 있다.

5. 뉴질랜드

여느 파이브 아이즈 동맹국과 마찬가지로 뉴질랜드의 사이버 안보 전략 역시 복합형 추진체계를 통해 수립·전개되어오고 있는 것으로 평가된다. 먼저 총리내각부(Department of the Prime Minister and Cabinet)가 컨트롤타워의 위치에서 사이버 안보에 대한 국가전략을 수립하고 이를 총괄하는 역할을 맡고 있다. 총리내각부는 그 산하의 국가안보정책국(NSPD: National Security Policy Directorate)을 통해 국가안보 관련 정책을 조정하고 정보 및 보안 또는 대테러를 위한 입법 과정을 주도해오고 있다. NSPD 내부에 설치된 국가사이버정책실(NCPO: National Cyber Policy Office)은 사이버 안보 분야 정부 자원 활용에 대한 자문 제공을 포함하여 정책의 개발을 지원함과 동시에 사이버 안보 전략의 추진 과정을 감독한다.[38] 2024년 초 뉴질랜드 정부가 새로운 사이버 안보 전략의 수립을 계획하고 있다는 소식 역시 총리내각부 대변인의 입을 통해 전달되기도 하였다.[39]

한편 국가안보·정보장관(Minister of National Security and Intelligence)을 겸직하는 총리는 정책 우선순위에 따라 통신장관(Minister for Media and Communications)에게 사이버 안보 전략 전반과 CERT NZ에 대한 책임 및 권한을 '할당(allocate)'해왔다.[40] 따라서 통신장관은 정부를 대표하여 「사이버안보전략 2015」와 「사이버안보전략 2019」를 발표한 바 있으며, 사이버 안보 정책과 CERT NZ에 대한 책임 권한 역시 행사해왔다. 또한 사이버 안보 분야 민관협력이나 호주와의 양자 협력을 강화하는 과정에서도 총리와 함께 핵심적인 역할을 담당해오기도 하였다.[41]

전략의 목표와 방향성을 결정하는 일이 총리내각부의 역할이라면, 그간 실질적인 전략의 실행을 담당해온 주체는 정부통신보안국(GCSB: Government Communications Security Bureau)과 그 산하에 설치된 국가사이버안보센터(NCSC-NZ: National Cyber Security Centre)[42]로 볼 수 있다. 특히 NCSC-NZ가 CERT NZ의 기능을 통합한 이후로는 GCSB의 역

38) New Zealand Government, "National Cyber Policy Office," (September 16, 2020a). https://www.dpmc.govt.nz/our-business-units/national-security-group/national-security-policy/national-cyber-policy-office (접속일: 2024.09.10.)

39) Dileepa Fonseka, "NZ drafts new cybersecurity strategy, will it match Australia's bold one?," *BusinessDesk* (May 14, 2024). https://businessdesk.co.nz/article/policy/nz-drafts-new-cybersecurity-strategy-will-it-match-australias-bold-one (접속일: 2024.09.10.).

40) 2017년 출범한 CERT NZ는 현재 NCSC-NZ로 흡수되었다.

41) 사이버 안보와 관련한 통신장관의 구체적 역할은 다음을 참고할 것: New Zealand Government, *Briefing to Incoming Minister responsible for cyber security policy* (November 2018).

할이 점차 커지는 양상을 보이고 있다. GCSB는 사이버 보안 사고에 대한 보고 경로와 대응 방식을 통합하는 '선도 기관'으로 기능하며, GCSB 국장은 정보보안(information security)에 대한 정부의 전략을 총괄하는 정보보안책임자(GCISO: Government Chief Information Security Officer) 직책을 겸하고 있기도 하다. 또한 뉴질랜드가 새로운 기술의 위험과 기회에 발맞춰 국가적 역량을 강화할 수 있도록 지원해오고 있다.[43]

일례로, 화웨이 사태 국면에서 GCSB는 자국 기업이 5G 공급자를 선정할 때 '전자통신법(TICSA)'을 앞세워 적극적으로 개입하는 양상을 보이기도 하였다. TICSA법은 통신 관련 기업이 새로운 기술을 도입하는 과정에서 정보기관의 보안 권고를 수용하도록 마련된 제도였고, 이를 토대로 GCSB는 자국 기업의 화웨이 장비 도입을 사실상 차단하였다.[44] 이를 종합적으로 고려할 때, 현시점을 기준으로 뉴질랜드에서는 총리내각부와 GCSB가 서로 다른 층위에서 사이버 안보 전략을 이끌어가고 있는 것으로 평가해볼 수 있다.

뉴질랜드의 사례에서 한 가지 흥미로운 지점은 내무부(Department of Internal Affairs)의 제한적 역할이다. 이웃 국가인 호주와 달리 뉴질랜드의 사이버 안보 전략에서는 내무부의 존재감이 크지 않다. 통신장관이 사이버 안보 관련 정책을 수행할 때 일차적으로 협조해야 할 대상 중에서도 내무장관(Minister of Internal Affairs)은 포함되지 않는다.[45] 최근에는 그 기능이 더욱 축소되는 경향마저 나타난다. 2024년 5월 내무부는 정부개인정보보호책임자(GCPO: Government Chief Privacy Officer)를 비롯하여 그 산하의 정보보안 관련 주요 직책들을 없애는 방안을 발표하였다. 그간 GCPO는 개인정보 보호에 대한 범정부적 접근 방식을 제공하는 역할을 담당하며 공공 서비스가 개인정보를 안전하게 수집하고 합법적으로 관리하도록 지원해왔는데, 디지털 기술의 발달로 인해 개인정보 보호의 중요성이 증대하는 상황에서 내무부가 그와 같은 결정을 발표함으로써 적지 않은 논란이 일기도 하였다.[46]

사이버 안보 분야 국제협력을 모색하는 일은 외교통상부(Ministry of Foreign Affairs and Trade)와 GCSB가 담당한다. 이들 기관은 뉴질랜드가 위치한 남태평양 지역의 사이버 복원력 증진을 위한 지역 차원의 다자협력을 주도하는 행보를 보이고 있다. 외교통상부는 호주 외교통상부와 함께 남태평양 지역의 사이버 위기에 대응하는 공동 역량을 강화하는 한편 아시아태평양경제협력체(APEC), 아세안(ASEAN), 남태평양도서국포럼(PIF) 등 다자협의체를 통해 남태평양 지역 사이버 안보에 대한 뉴질랜드의 인식과 이해관계를 알리는 데 힘쓰고 있다.[47]

---

42) 공식적인 약칭은 NCSC이지만, 영국 국가사이버안보센터(NCSC-UK)와의 구분을 위해 본 연구에서는 NCSC-NZ로 표기하였다.

43) Government Communications Security Bureau, *GCSB Strategy 2023-27* (2023), p. 4.

44) Chris Keall, "GCSB bans Spark from using Huawei gear for its 5G mobile upgrade," *NZ Herald* (November 28, 2018). https://www.nzherald.co.nz/business/gcsb-bans-spark-from-using-huawei-gear-for-its-5g-mobile-upgrade/5APETBE7J2AF74YL6JZQP25GGE/ (접속일:2024.09.10.).

45) New Zealand Government, 2018, p. 5.

46) Radio New Zealand, "DIA proposes cutting eight roles relating to information security, union says,"

GCSB 역시 자체적으로 내놓은 전략서에서 남태평양 지역이 직면한 사이버 안보 문제에 대해 자국 정부가 더 깊은 통찰력을 갖출 수 있도록 지원하는 한편 지역 사이버 복원력을 증진하는 데에 기여하는 것을 핵심목표로 소개하기도 하였다.[48] 대외정보 수집을 담당하는 뉴질랜드안보정보청(NZSIS: New Zealand Security Intelligence Service)도 간첩행위, 내정간섭, 폭력적 극단주의, 테러리즘 등의 위협을 차단하고 남태평양 지역 안보를 증진하기 위해 '데이터 및 디지털 기술 활용'을 3대 활동 분야 중 하나로 설정하여 외부 환경에 대한 자국 정부의 이해와 의사결정을 지원해오고 있다.[49] 최근에는 GCSB와 함께 '공동 목적을 위한 성명(GCSB-NZSIS Joint Statement of Common Purpose)'을 발표하여 악의적 사이버 활동에 대응할 수 있는 보안 대책을 마련해나갈 의지를 드러내기도 하였다.[50]

IV. 5개국 추진체계 비교

앞서 제Ⅲ장에서 살펴본 것처럼, 파이브 아이즈 5개국은 모두 국가책략의 관점에서 사이버 안보 전략을 수립·추진함에 따라 다양한 정부부처와 기관의 참여를 허용하는 복합형 추진체계를 채택해오고 있다. 물론 5개국의 전략 추진체계에서는 크고 작은 차이도 발견된다. 이들 국가는 모두 복합형 추진체계를 사이버 안보 전략에 적용하고 있지만, 아래 [표 1]에서 보이는 바와 같이 '컨트롤타워의 위치'와 '국제협력 참여 주체'를 기준으로 차이를 가진다.

먼저, 추진체계상 컨트롤타워를 담당하는 정부기관이 다르다. 미국의 경우 대통령실 산하의 ONCD가 전략목표를 설정하고 부처별 대응을 조정하는 컨트롤타워 역할을 담당하지만, 동시에 국무부와 국토안보부의 역할과 권한도 매우 크다. 영국은 내각부가 컨트롤타워의 위치에서 사이버 안보에 대한 국가전략을 수립하지만, 실질적인 전략 수행은 GCHQ와 그 산하의 NCSC-UK가 중심이 되어 이루어진다. 한편 캐나다에서는 과거 공공안전부에 있던 컨트롤타워의 기능이 현재는 CSE와 그 산하의 CCCS로 이전된 상태이다. 반면에 호주는 총리내각부를 대신하여 내무부가 사실상 컨트롤타워의 역할을 수행하며 가장 큰 영향력을 행사하는 주체로 활동한다. 뉴질랜드의 경우 사이버 안보를 전담하는 정보기관인 GCSB의 역할이 두드러지지만, 여전히 총리내각부가 컨트롤타워 역할을 수행하는 추진체계를 채택하고 있다.

47) Australian Government, "Australia and New Zealand: Pacific cyber cooperation," (November 16, 2018). https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-and-new-zealand-pacific-cyber-cooperation (접속일: 2024.09.11.)
48) Government Communications Security Bureau, 2023.
49) New Zealand Security Intelligence Service, *NZSIS Strategy 2024-2029* (2024).
50) Government Communications Security Bureau, "GCSB-NZSIS Joint Statement of Common Purpose."

[표 1] 파이브 아이즈 국가 전략의 추진체계

국가	복합형 추진체계의 세부 유형	국제전략 참여 주체
미국	'정부수반-정부부처 중심' 추진체계	▲대통령실, △국무부, △국토안보부, △NSA, FBI, 국방부, 법무부
영국	'정부수반-정보기관중심' 추진체계	▲내각실, △GCHQ 및 NCSC-UK, △외무·영연방·개발부, 국방부, MI5, △과학·혁신·기술부
호주	'정부부처 중심' 추진체계	▲내무부, △외교통상부, △ASD 및 ACSC, 국방부, 산업·과학·자원부
캐나다	'정보기관 중심' 추진체계	▲CSE 및 CCCS, 공공안전부, 외교부, 천연자원부, 국방부
뉴질랜드	'정부수반 중심' 추진체계	▲총리내각부, GCSB 및 NCSC, 외교통상부, NZSIS, 국방부

▲는 사실상의 컨트롤타워를, △는 핵심 수행기관을 의미함.

이를 유형화해보자면, 대통령실이나 총리내각부가 직접 컨트롤타워의 역할을 수행하는 국가는 '정부수반 중심(head of government-centred)'의 복합형 추진체계를 통해 사이버 안보 전략을 전개하고 있는 것으로 볼 수 있다. 컨트롤타워의 기능을 정부부처 단위의 하위주체에 부여한 국가의 전략 추진체계는 '정부부처 중심(government department-centred)'의 복합형 추진체계로 구분이 가능하다. 대내적 치안을 전담하는 내무부나 국제협력을 담당하는 외무부 등 특정 정부부처의 사이버 안보 관련 권한과 역할이 눈에 띄게 큰 경우도 이에 해당한다. 마지막으로, 사이버 안보 분야에 특화된 정보기관이 국가전략의 수행을 총괄하며 다른 정부부처 및 기관별 대응을 조정한다면, 그 국가는 '정보기관 중심(intelligence agency-centred)'의 복합형 추진체계를 통해 사이버 안보 전략을 전개하는 것으로 유형화해 볼 수 있다. 복합형 추진체계의 이와 같은 세부 유형들은 서로 명확히 구분되기보다 어느 정도 중첩되어 나타날 수 있다.

한편, 파이브 아이즈 국가들은 사이버 안보 국제협력에 다양한 정부조직을 참여시킨다는 점에서 비슷하지만, 그중에서도 특히 주도적인 역할을 담당하는 주체가 누구인가에 따라 다소 차이를 드러낸다. 미국과 영국 그리고 호주의 경우에는 각각 국무부, 외무·영연방·개발부, 외교통상부가 사이버 안보 국제전략의 중심축이 되어 대외적 협력을 주도해오고 있다. 이들 국가에서는 사이버 안보에 특화된 정보기관의 역할도 매우 중요하지만, 여전히 국제협

력의 구체적인 분야를 설정하거나 다자협의체에서 자국 정부를 대변하여 전략적 이해관계를 전달하는 주체는 외교 전담 부처이다. 캐나다와 뉴질랜드의 경우에도 역시 대외적 협력의 모색은 각각 외교부와 외교통상부가 담당하지만, 미국과 영국 그리고 호주의 사례와 비교할 때 이들 외교 전담 부처의 활동은 다소 제한적으로 나타난다. 예컨대, 뉴질랜드의 경우 크라이스트처치 콜과 같은 글로벌 차원의 이니셔티브는 총리가 직접 관장하는 반면 외교통상부의 활동은 주로 남태평양 지역 차원의 다자협력에 집중되는 경향이 나타난다.

다만, 이러한 차이에도 불구하고 5개국 전략의 추진체계는 다음의 공통된 특징적 현상을 보인다는 점에서 점차 일치되는 방향으로 나아가고 있다고 평가해볼 수 있다. 첫째, 대내적 치안 부문을 담당하는 정부부처의 대외적 활동이 증가한 것이다. 국토안보부나 내무부와 같은 정부부처가 비단 사이버 안보의 대내적 위협 요인뿐만 아니라 국제적 맥락에서 나타나는 위협 요인에도 주목하게 되면서 동맹 차원의 협력에 대한 참여를 점차 확대해오고 있다. 이는 일차적으로 내정 전반을 담당하는 정부부처가 애초에 대내적으로 행사할 수 있는 행정권력과 국가안보적 권한이 크기 때문에 비롯되는 현상으로 볼 수 있지만, 또 한편으로는 사이버 안보에 대한 국가적 접근이 국가책략의 관점에서 이루어짐에 따라 네트워크화된 추진체계 안에서 다른 정부조직들과 높은 연결성을 가지는 국토안보부나 내무부의 활동 범위가 더욱 확장된 것으로 해석해 볼 수 있을 것이다.

둘째, 전통적으로 대외협력을 전담해온 외교 전담 부처의 기술안보 분야 역할이 강화된 것이다. 물론 과거에도 국무부나 외교통상부와 같은 외교 전담 부처는 글로벌·지역 안보 문제에 대한 개입을 담당해왔다는 점에서 언제나 안보적 기능을 가져온 것으로 볼 수 있지만, 사이버 공간이 새로운 전략영역으로 부상하고 디지털 기술이 급격히 발달함에 따라 사이버 안보가 동맹 협력의 주된 의제가 되면서 그 활동이 기술안보 분야로까지 확대되는 양상을 보이고 있다. 그 결과 과학기술 분야를 전담하는 실무부처가 별로도 존재함에도 불구하고 외교 전담 부처가 기술안보에 대한 국가적 대응에서 중요한 역할을 담당하는 현상이 목격되고 있다. 물론 현재 캐나다나 뉴질랜드의 경우에는 외교 전담 부처의 존재감이 미국이나 영국 또는 호주의 사례에 비추어 볼 때 상대적으로 덜 드러나지만, 이는 이들 국가가 비교적 뒤늦게 동맹 차원의 국제협력을 모색하기 시작하였기 때문에 나타나는 '시차' 정도로 해석해볼 수 있을 것이다.

마지막으로, 정보기관의 공조 기능이 확장된 현상에도 주목할 필요가 있다. 이들 정보기관은 자국 및 동맹국에 대한 외부로부터의 위협 정보를 수집·분석·가공·공유하는 데 특화되어 있어 이미 국제협력에 대한 참여 역사가 길다. 그러나 사이버 안보가 중요해지고 정보동맹이 사이버 안보에 특화된 작전조직(operational grouping)이자 제도(arrangement)로 발전하게 되면서 5개국의 정보기관 역시 새로운 형태의 위협에 대한 대외적 인식 및 정보의 공유를 촉진하고 나아가 집단적 대응을 적극적으로 지원하는 주체로 떠올랐다. 현재 파이브아이즈 5개국에서 정보기관과 그 산하에 설치된 사이버 안보 및 디지털 기술 전담 기관은 각국을 대표하여 정보동맹 차원의 협력에 참여하는 주체이기도 하다. 그리고 그 협력의 범

위는 단순히 위협정보를 공유하는 수준을 넘어 특정 이슈에 대한 인식의 공유를 촉진하고, 국제적 공동대응의 필요성을 알리며, 디지털 기술의 글로벌 표준, 원칙, 규범을 제시하는 것을 아우르는 수준으로 확대되었다. 2010년대 중반에 접어들면서 이들 정보기관의 기능과 활동이 5개국의 외교·국방 정책을 통해 본격적으로 수면 위로 드러나기 시작한 것도 이러한 맥락에서 이해될 수 있는 부분이다. **/끝**

<참고자료>

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.