사이버안보연구, 3집 1호 2026 여름, 131-172

미일 사이버안보 협력의 전개와 한국의 정책 과제

0301-131172

연원호 | 현대자동차그룹

논문접수일 2026년 5월 13일 | 논문심사일 2026년 6월 10일 | 게재확정일 2026년 6월 17일

논문 요약

본 연구는, 첫째, 2013년 미일 사이버대화 출범 이후 미일 사이버 안보 협력이 어떠한 경로로 진화해 왔는지 그 전개 과정을 정리하고, 둘째, 2023년 이후 가속화된 준제도화 전환의 다섯 흐름을 분석하며, 셋째, 그 흐름이 한국 정부의 사이버안보 정책에 가하는 조정 압력과 정책적 시사점을 도출한다. 분석 결과 미일 사이버협력은 정책 협의기(2013~2018), 능력 강화기(2019~2022), 준제도화 전환기(2023~2026)의 세 시기를 거치며 그 폭과 깊이를 누적적으로 확장해왔음을 알 수 있다. 특히 2023년 이후의 변화는 ① 일본의 능동적 사이버 방어(ACD: Active Cyber Defense) 법제화, ② 정보·위협 공유의 고도화, ③ 미일 방어적 사이버작전(DCO: Defensive Cyber Operations) 협력, ④ 민관 협력과 핵심 인프라 보안, ⑤ 미·일·필리핀과 한미일을 잇는 다자 네트워크화의 다섯 흐름이 동시에 진행되며 미일 협력을 인도태평양 사이버안보 네트워크의 허브로 변환시키고 있다는 점에서 주목할 만하다. 본 연구는 이러한 흐름이 한국에 가하는 조정 압력을 정리하고, 북한 사이버위협·중국계 APT·해저케이블의 세 사례를 통해 이를 구체화한 뒤 단기·중기·장기 정책 과제를 종합한다. 결론적으로 한국은 일본 모델을 단순 이식할 것이 아니라, 우리의 위협 환경과 법제 전통, 산업구조에 맞는 “한국형 통합 사이버안보 모델”을 단계적으로 구축할 필요가 있다.

주제어 미일 사이버안보 협력, 능동적 사이버 방어, 한미일 협력, 사이버안보 정책

Ⅰ. 서론

미일 사이버안보 협력은 지난 10여 년간 가장 빠르게 진화한 동맹 협력 분야 중 하나다. 2010년대 초까지만 해도 외교부 중심의 선언적 협의에 가까웠으나, 오늘날 미일 사이버협력은 법제·조직·작전·민관·다자 네트워크를 포괄하는 준제도화된 안보협력 단계로 올라섰다. 일본은 2022년 국가안보전략을 통해 "사이버안전보장 분야에서의 대응능력을 구미 주요국과 동등 이상"으로 끌어올린다는 목표를 명시했고(내각관방 2022), 이를 위해 능동적 사이버 방어, 통신정보 활용, 공격자 서버 무해화, 통합조정조직 설치를 일관되게 추진해왔다(내각관방 2024). 미국 또한 중국계 행위자의 중요 인프라 사전배치 활동을 반복적으로 공개하며, 사이버 위협을 전통적 간첩행위가 아니라 위기 시 파괴·교란을 준비하는 안보 문제로 규정하고 있다(NSA et al. 2023; CISA et al. 2024). 이 두 흐름이 만나는 지점에서 미일 협력은 빠르게 고도화되었고, 그 파급효과는 한미일 협력의 제도 설계와 한국의 국내 정책 선택에 직결되고 있다.

본 연구가 던지는 질문은 단순하다. 미일 사이버안보 협력은 어떤 경로로 발전해왔으며, 그 흐름은 한국 정부의 사이버안보 정책에 어떠한 조정 압력을 가하는가다. 한국이 직면한 사이버 위협이 미일이 직면한 위협과 상당 부분 겹친다는 점에 그 출발점이 있다. 북한의 가상자산 탈취와 IT 노동자 침투, 중국계 행위자의 통신·정부망 사전배치, 해저케이블·클라우드 등 핵심 인프라의 취약성은 한국에도 동일하게 작용하는 위협이다. 그러나 미국과 일본이 이러한 위협에 대응해 구축해 온 협력 구조는 한국의 분산된 법제와 부처별 운영 체계와는 상당한 격차를 보인다. 따라서 미일 협력의 전개 흐름을 살피는 일

은 우리가 한국의 위협 환경에 맞는 협력 모델을 설계하기 위한 중요한 기준점이 된다.

본고의 시각은 두 가지 점에서 기존 연구와 구별된다. 첫째, 본고는 미일 협력을 단발성 회의체의 누적이 아닌, 시기별로 진화해 온 누적적 제도화 과정으로 본다. 이를 위해 Ⅱ장에서는 2013년 사이버대화 출범부터 2026년 보안 클라우드 협력까지를 세 시기로 나누어 정리한다. 둘째, 본고는 학술적 이론화보다 정책적 시사점 도출에 무게를 둔다. 본 연구가 한국 정부의 사이버안보 정책 수립자에게 직접 활용될 수 있는 진단과 권고를 목표로 하기 때문이다.

본고의 구성은 다음과 같다. Ⅱ장에서는 미일 사이버협력의 시기별 전개를 정책 협의기, 능력 강화기, 준제도화 전환기의 3단계로 정리한다. Ⅲ장에서는 2023년 이후의 준제도화 전환을 법제·조직, 정보 공유, 방어적 작전, 민관·공급망, 다자 네트워크의 다섯 가지 흐름으로 분석하고, 각 흐름이 한국에 가하는 조정 압력을 함께 진단한다. Ⅳ장에서는 북한 사이버위협, 중국계 APT[1], 해저케이블의 세 사례를 통해 한국이 직면한 위협을 구체화하고, 미일 협력이 주는 시사점을 이 위협 환경 위에서 재구성하여 한국 정부의 정책 과제와 한국형 통합 사이버방위 모델의 윤곽을 제시한다. 마지막으로 Ⅴ장에서는 결론과 본 연구의 한계를 정리한다.

한 가지 미리 밝혀둘 점은, 사이버안보가 공급망·기술 보호·투자 심사·수출통제·금융제재와 결합되는 "경제안보화" 차원의 분석은

1) Advanced Persistent Threat: 지능형 지속 위협. 문장에서 말하는 "중국계 APT"는 중국과 연계된 것으로 의심되는 국가 지원형 해킹 그룹을 의미함.

별도의 후속 연구에서 다루며, 본고에서는 협력의 역사적 전개와 한국 정부에 대한 정책적 시사점에 초점을 둔다는 점이다. 두 흐름이 분리되어 있는 것은 아니나, 한정된 분량 안에서 깊이 있는 분석을 위해 본고에서는 미일 협력의 "역사적 흐름과 한국에 대한 정책적 시사점"이라는 단일 축에 집중하고자 한다.

자료는 일본 외무성·내각관방·내각사이버시큐리티센터(NISC: The National Center of Incident Readiness and Strategy for Cybersecurity)·국가사이버통괄실(NCO: National Cybersecurity Office), 미국 백악관·국무부·국가안보국(NSA: National Security Agency)·사이버안보 및 기반시설보호국(CISA: Cybersecurity and Infrastructure Security Agency), 한국 국가안보실·국가사이버안보센터(NCSC: National Cyber Security Center), 한미일 공동성명 등 공식 1차 자료를 중심으로 활용했다. 보조자료로는 CSIS, RAND Corporation, RUSI, 대외경제정책연구원(KIEP) 등의 보고서와 일부 학술 문헌을 활용했다. 분석 기간은 2013년 미일 사이버 대화 출범부터 2026년 3월 미일 정상회담까지로 설정하되, 분석의 무게는 2023년 이후의 변화에 두었다.

Ⅱ. 미일 사이버안보 협력의 시기별 전개와 일본의 정책 변화

미일 사이버안보 협력은 단번에 오늘의 모습을 갖춘 것이 아니다. 약 13년에 걸쳐 협의 → 능력 → 제도화의 단계로 점진적으로 진화해 왔으며, 각 단계는 직전 단계에서 누적된 자산 위에 새 층위를 쌓는 방식으로 진행되었다. 본 장에서는 이를 정책 협의기(2013~2018), 능력

강화기(2019~2022), 준제도화 전환기(2023~2026)의 세 시기로 나누어 정리한다. 시기 구분은 미일 양국 정부의 공식 문건과 정책 결정의 변곡점을 기준으로 한 것이며, 시기별로 협력의 성격, 주요 행위자, 핵심 의제, 가시적 성과가 어떻게 달라져 왔는지를 보여주는 데 그 목적이 있다.

1. 정책 협의기 (2013~2018)

미일 사이버안보 협력의 공식 출발점은 2013년 5월 양자 사이버대화 출범이다. 이 협의체는 일본 외무성과 미국 국무부를 중심으로 양국의 사이버 정책을 정기적으로 조율하기 위한 기구로 출범했고, 이후 거의 매년 개최되며 미일 협력의 외교적 중추로 자리잡았다. 같은 해 일본은 사이버안보 기본법 제정 작업을 본격화했고, 2014년 11월 사이버시큐리티기본법이 성립했다. 2015년에는 내각사이버시큐리티센터(NISC)가 정식 출범하면서 일본 정부 차원의 사이버 정책 조정 기구가 마련되었다.

이 시기 미일 협력의 또 다른 축은 미일 방위협력지침의 개정이다. 2015년 4월 개정된 동 지침은 사이버를 동맹 협력의 영역으로 명시적으로 포함시켰고, 사이버 공격에 대한 정보공유와 방위 협력을 양국 합의 사항으로 규정했다. 한편 같은 해 미국은 사이버사령부의 통합전투사령부 격상 작업에 착수하기 시작했고, 일본 자위대 또한 사이버방위대를 단계적으로 확대하기 시작했다.

학술적으로 이 시기는 일본의 사이버안보가 정보보호의 영역에서 안보화의 영역으로 이동하기 시작한 전환의 시기로 평가된다. Kallender and Hughes(2017)는 이러한 변화를 일본이 “사이버 강국

(cyber power)"으로 부상하는 안보화-군사화 과정으로 분석했다. Matsuzaki(2016)는 일본 방위성과 자위대의 사이버안보 강화 노력이 처음부터 미국 사이버사령부 모델 등 미국의 선례를 명시적 참조점으로 삼아 추진되었음을 잘 보여준다. RAND가 2016년 발간한 미일 동맹 컨퍼런스 결과물(Harold et al., 2016) 또한 이 시기 미일이 사이버를 본격적인 안보 의제로 끌어올리는 정책 지형을 보여주는 핵심 자료라고 할 수 있다.

이 시기 협력의 특징은 두 가지로 정리할 수 있다. 첫째, 협력의 초점이 외교·국방 채널에서의 정보교류와 정책 조율에 머물렀다는 점이다. 협의 채널 정비가 우선이었고, 구체적 작전 협력이나 민관 통합은 본격화되지 않았다. 둘째, 비록 이 시기 인식의 전환이 시작되었지만, 일본의 국내 제도가 여전히 사이버안보를 정보보안의 하위 분야로 다루는 단계였기 때문에, 미일 협력의 공통 기반 역시 정보보안 협력 수준에 머물렀다는 점이다. 한마디로 말해, 이 시기는 미일 사이버 협력의 "틀을 짜는 단계"였다고 평가할 수 있다.

2. 능력 강화기 (2019~2022)

2019년부터 2022년까지의 시기는 미일이 사이버안보 협력을 본격적으로 능력 차원으로 끌어올린 단계라고 할 수 있다. 가장 결정적인 사건은 2019년 4월 미일 안보협의위원회(2+2)에서 사이버 공격이 일정 조건 하에 미일 안보조약 제5조[2]의 적용 대상이 될 수 있음을 확

2) "각 당사국은 일본국의 시정(施政)하에 있는 영역에 있어서, 어느 한 쪽에 대한 무력 공격이 자

인한 것이다(일본 외무성 2019). 이것은 사이버 위협이 동맹의 군사적 방위 의무와 연결될 수 있음을 처음으로 명시한 결정으로, 미일 협력을 "협의"에서 "방위"의 단계로 한 차원 격상시켰다는 점에서 주목할 만하다. 결국 이 결정은 사이버 공격에 대한 동맹의 대응 의무를 정치적으로 확립한 것으로, 이후 협력의 모든 후속 진전을 가능케 한 정치적 토대로 작용했다.

이 시기 일본의 자위대 사이버 부대는 단계적으로 확대되었고, 2022년 3월에는 자위대 사이버방위대가 출범하며 약 540명의 인력을 갖춘 통합 부대로 정비되었다(Bae 2026). 다만 이 같은 조직 확대에도 불구하고 일본의 사이버 역량은 여전히 미국·영국 등 주요 사이버 강국에 비해 인력 규모와 작전 경험 면에서 제한적이라는 평가가 가능하다. 바로 이 한계 때문에 일본은 2022년 국가안보전략에서 사이버안보 대응능력을 "구미 주요국과 동등 이상"으로 끌어올리겠다는 목표를 제시했고, 이후 ACD 도입과 NISC 개편을 추진하게 되었다(내각관방 2022). 따라서 2019~2022년의 능력 강화는 완성된 작전능력의 확보라기보다, 미일 동맹과 연동 가능한 국내 사이버 방위역량을 구축하기 위한 전환 단계로 이해할 필요가 있다. 한편 미국에서는 사이버사령부의 통합 작전 교리 개정과 "지속적 관여(persistent engagement)[3]" 개념의 도입이 이뤄졌고, 이러한 미측의 교리 변화는 자연스

국의 평화 및 안전을 위태롭게 하는 것임을 인정하고, 자국의 헌법 상의 규정 및 절차에 따라 공통의 위험에 대처하도록 행동할 것임을 선언한다..."

3) 미 사이버사령부가 2018년 비전 문서 「Achieve and Maintain Cyberspace Superiority」를 통해 정식화한 작전 개념으로, 위협 발생 후 대응하는 수세적 자세에서 벗어나 평시부터 적대 행위자와 지속적·선제적으로 대치한다는 발상. 같은 해 국방부 사이버전략의 '전방 방어(defend forward)' 개념과 짝을 이루며, 미군 네트워크 외부에서 위협을 사전 차단하는 작전의

럽게 미일 간 작전·교리 차원의 정합성 논의로 이어졌다. 그 결과 양국은 비공개 작전 차원의 조율을 점진적으로 강화했고, 사이버 부대 간 인력 교류와 합동 훈련도 본격화되기 시작했다.

특히 2022년은 일본 사이버안보 정책의 결정적 전환점으로 기록될 만하다. 12월 일본 정부는 새 국가안보전략을 발표하며 "사이버안전보장 분야에서의 대응능력을 구미 주요국과 동등 이상"으로 끌어올린다는 목표를 명시하고, 능동적 사이버 방어 도입과 NISC의 발전적 개편을 핵심 정책 과제로 제시했다(내각관방 2022). 이 결정은 사이버안보를 정보보안의 하위 영역에서 국가안보의 통합 정책 영역으로 재정의한 의미 있는 사건이었다. 이때부터 일본의 사이버안보 논의는 외교·방위·산업·통신·통신비밀 보호의 영역을 가로지르는 범정부 의제로 자리잡게 된다.

요약하면, 이 시기 미일 협력의 본질적 특징은 양국이 공동의 위협 인식을 공식적으로 정립했다는 점이다. 다시 말해 사이버 공격을 단순한 정보 침해가 아니라 동맹 차원의 안보 위협으로 다루기 시작했고, 일본 또한 이를 국내 제도 변화의 출발점으로 받아들였다. 이 시기에 누적된 정치적·제도적 합의가 곧 다음 단계인 준제도화 전환의 직접적 토대로 작용하게 된다.

3. 준제도화 전환기 (2023~2026)

2023년 이후 미일 사이버협력은 가속도를 내며 준제도화 단계로

교리적 기반으로 기능함.

진입했다. 이 시기의 특징은 크게 세 가지로 요약할 수 있다. 첫째, 일본의 능동적 사이버 방어(ACD: Active Cyber Defense) 법제화와 국가사이버 통괄실(NCO: National Cybersecurity Office) 출범으로 협력의 국내 제도 기반이 본격적으로 갖춰지기 시작했다. 둘째, 양자 정상회담과 2+2가 사이버안보를 동맹의 핵심 의제로 격상시켰다. 셋째, 사이버안보 관련 다자 네트워크가 미일 양자 관계를 허브로 외연이 확장되고 있다. 사건의 밀도가 높고 변화의 폭이 큰 시기인 만큼, 본 절에서는 연도별 주요 사건을 요약하는 방식으로 정리한다.

먼저 2023년 9월 발표된 BlackTech[4] 관련 미일 합동 사이버 권고는 양국이 중국계 행위자의 라우터 펌웨어 침투를 공동으로 분석·공개한 첫 본격적 사례 가운데 하나로(NSA et al. 2023), 정보공유와 위협 귀속의 동맹화가 작전 차원에서 진행되고 있음을 보여주는 상징적 사건이었다. 같은 시기 미국 정부는 Volt Typhoon[5] 등 중국계 APT의 중요 인프라 사전배치 활동을 반복적으로 공개했고(CISA et al. 2024), 일본 정부 또한 유식자회의(有識者会議)를 가동해 ACD의 구체적 설계 작업에 본격적으로 착수했다(내각관방 2024).

2024년은 미일 협력이 가시적 성과로 결실을 맺기 시작한 해다. 4월 미일 정상 공동성명은 정보·사이버안보 협력 심화와 ICT 영역의 복원력·핵심 기반시설 보호 강화를 공식화했다(일본 외무성 2024a). 6월에 개최된 제9차 미일 사이버대화는 양국의 국내 사이버정책, 양자

4) 미국·일본 정부가 중국 연계 해킹조직으로 지목한 사이버 첩보 그룹으로, 네트워크 장비를 악용해 동아시아 및 미국의 정부·기업을 장기간 침해하고 정보수집 활동을 수행한 것으로 알려짐.

5) 미국 등 서방 정부가 중국 연계 해킹조직으로 지목한 사이버 위협 그룹으로, 통신·에너지·교통 등 중요 기반시설에 장기 잠복하며 정보수집 및 유사시 교란 가능성을 노린 것으로 평가됨.

협력, 역내 협력, 역량배양, 악성 행위 대응을 포괄적으로 다뤘다(일본 외무성 2024b). 특히 7월의 미일 2+2는 제로트러스트[6], 방어적 사이버 작전(DCO) 협력, 연합연습에서의 사이버 방어 개념 반영을 명시하며 사이버안보를 동맹 억지력의 운영 수단으로 격상시켰다는 점에서 주목할 만하다(일본 외무성 2024c). 11월에 발표된 일본 관방 유식자회의 권고는 ACD 법제의 구체적 골격을 "관민연계 강화", "통신정보 활용", "접근·무해화"의 세 축으로 한층 정교화했다(내각관방 2024).

2025년은 일본 국내 제도 변화의 결정적 해다. 5월 ACD 관련법이 성립했고(내각관방 2025), 7월에는 NISC가 국가사이버안보실(NCO)로 확대·개편되었으며(국가사이버통괄실 2025), 12월에는 새 사이버전략을 통해 향후 5년간의 국가적 대응 목표를 제시했다[7]. 한편 6월에 개최된 제10차 미일 사이버대화는 이러한 변화를 양자 협력 차원에서 재확인하며 정보공유 기반 강화를 핵심 과제로 명시했다(일본 외무성 2025a). 같은 해 1월 한미일은 북한 가상자산 탈취 대응 공동성명을 발표했고(미국 국무부 2025a), 8월에는 일본 NCO와 경찰청(NPA: National Policy Agency)이 참여한 다국가 합동 권고에서 중국계 APT의 통신·정부·교통·숙박·군사 인프라 침투를 공개했다(NSA et al. 2025). 9월 한미일 외교장관 회의 공동성명은 북한 사이버위협 외교실무그룹의 지속과 공공·민간 협력 심화를 재확인했다(미국 국무부 2025a).

그리고 2026년 3월 미일 정상회담은 협력의 범위를 데이터 인프라

6) 제로트러스트(Zero Trust)는 "아무것도 신뢰하지 말고, 모든 것을 검증하라(Never trust, always verify)" 라는 원칙에 기반한 사이버보안 모델.

7) 일본은 향후 5년간 능동적 사이버방어를 축으로 사이버 대응능력을 서방 주요국과 동등 이상으로 끌어올리고, 방어·억지-사회 전반 회복력-인재·기술 생태계를 함께 강화하겠다는 목표를 제시.

차원으로까지 확장한 또 하나의 변곡점이라고 할 수 있다(백악관 2026). 양국은 정부데이터를 위한 보안·주권형 클라우드 플랫폼 개발을 통해 정보공유·계획·조정을 개선하겠다고 발표했다. 이러한 합의는 정보공유 협력이 더 이상 단순한 위협 인텔리전스의 교환에 머무는 것이 아니라, 정부데이터 처리 기반의 공동 설계로까지 확장되었음을 의미하는 결정이다.

〈표 1〉 미일 사이버협력의 시기별 특징 비교

구분	정책 협의기 (2013~2018)	능력 강화기 (2019~2022)	준제도화 전환기 (2023~2026)
핵심 의제	협의 채널 정비, 정보교류	협의에서 방위로 전환 사이버 부대 강화	동맹 사이버안보 체계 구축
주요 행위자	외교 채널 중심	외교+방위 채널 통합	범정부: 외교·방위·산업·정보·수사
협력 범위	정보보안 정책 협의	동맹 방위와 사이버 부대 협력	법제·조직·작전·민관·다자 통합
대표 성과	미일 사이버대화 출범, 일본 사이버보안기본법	동맹 5조 적용 합의, 일본 자위대 사이버방위대 출범	ACD 법제화, NCO 출범, DCO 협력, 보안 클라우드, 다국가 협력
협력의 성격	협의 위주	능력 강화	준제도화

이 시기의 변화는 단발성 사건들의 나열이라기보다 누적적·구조적 전환으로 이해할 필요가 있다. 기존 제1·2기 협력이 "협력의 틀과 능력의 정렬" 단계였다면, 제3기 협력은 "법제·조직·작전·민관·다자가 결합된 운영 가능한 동맹 사이버안보 체계"의 구축 단계라 할 수 있다. 그리고 이 전환의 가장 큰 함의는, 미일 협력이 단순한 외교적 협의 중심의 단계에서 벗어나, 국내 제도를 갖춘 파트너십을 전제로 작동하는 단계로 이동했다는 것이다.

Ⅲ. 2023~2026 미일 협력 확대의 다섯가지 흐름과 한국에의 시사점

Ⅱ장이 미일 사이버협력의 시기별 전개를 큰 흐름으로 정리했다면, 본 장에서는 2023년 이후 가속화된 준제도화 전환을 다섯 흐름으로 나누어 살펴보고, 동시에 각 흐름이 한국 정부에 가하는 정책적 조정 압력을 함께 검토한다. 다섯 가지 흐름이란 △ 법제와 조직 △ 정보·위협 공유 △ 방어적 사이버작전 △ 민관 협력과 핵심 인프라 보안 △ 다자 네트워크화를 말한다. 이들 흐름은 별개로 진행된 것이 아니라 상호 연결된 묶음으로 작동했으며, 그 결과 미일 협력은 양자 동맹 차원의 사이버 의제 조율에서 출발해, 인도태평양 사이버안보 협력 네트워크를 뒷받침하는 핵심 축으로 발전하고 있다.

한국은 이미 2024년 국가 사이버안보 전략을 통해 자유·인권·법치의 가치 수호, 공세적 사이버 방어 및 대응, 글로벌 공조체계 구축, 핵심 인프라 복원력 강화를 내세웠다(국가안보실 2024). 그러나 한국의 사이버안보 법체계는 통합된 기본법 없이 여러 법률과 규정에 분산되어 있으며, 이러한 분산 구조는 통합 관리조직과 법적 권한 배분을 불분명하게 만들고 있다. 2025년 범부처 정보보호 종합대책은 1,600여 핵심 IT 시스템 점검, 상시 취약점 탐지, 소비자 중심 사고 대응, 정보보호 예산·인력 확보, 산업·인력 육성을 제시했고(과학기술정보통신부 외 2025), 국가사이버안보센터는 2025 연례보고서 발간, 국가망보안체계(N²SF) 구축, 2026년 Locked Shields 참가 등 운영능력 강화 움직임을 보이고 있다(국가사이버안보센터 2025). 그러나 이러한 변화는 여전히 개별 대응책의 성격이 강하다. 그 결과 미일이 형성하고 있는 '법제·조직·작전·민관·다자가 결합된 운영 가능한 동맹 사이버체계'

와의 격차가 영역별로 서로 다른 양상과 깊이로 드러나고 있다. 본 장은 이 격차의 성격과 폭을 다섯 흐름 각각의 차원에서 진단한다.

1. 법제와 조직: ACD 법제화와 NCO 출범과 한국 법제의 격차

미일 협력 확대의 가장 중요한 기반은 일본의 제도 변화다. 2022년 국가안보전략에서 출발한 ACD 도입과 NISC 개편은 2024년 11월 유식자회의 권고를 거쳐 2025년 5월 ACD 관련법 성립으로 결실을 맺었다(내각관방 2022; 내각관방 2024; 내각관방 2025). 새 법제의 골격은 크게 네 가지로 요약할 수 있다. 첫째, 중요 인프라 사업자의 도입 설비 신고와 사건보고 의무다. 둘째, 정부의 통신정보 분석 권한이다. 셋째, 일정 조건 아래 공격자 서버에 대한 접근·무해화 조치다. 넷째, 독립적 감독장치 설치다. 2025년 7월에는 NISC가 NCO로 확대·개편되었고(국가사이버통괄실 2025), 전술한 바와 같이 2025년 12월에는 새 사이버전략이 향후 5년간의 국가적 대응 목표를 제시했다.

이러한 일본의 제도화는 미일 협력의 작동 조건 자체를 바꿔놓고 있다. 과거 협력이 외교당국 간 정책협의와 정보교류에 머물렀다면, ACD 법제와 NCO 출범 이후에는 민간 인프라 사업자의 보고의무, 정부의 통신정보 분석, 일본 경찰·자위대와의 역할분담, 독립적 감독체계 설계가 동맹 협력의 하부 구조로 편입되었다. 다시 말해, 미일 협력은 더 이상 "협의할 사안"이 아니라 "상호 운용 가능한 국내 체계를 갖춘 파트너십"을 전제로 움직이게 된 것이다.

한국이 받는 압력은 이 지점에서 가장 직접적이다. 한국은 통합된 사이버안보 기본법이 부재한 채 여러 법률과 규정에 권한이 분산되어 있어, 사건보고의 임계치(기준), 위협정보 공유 절차, 제한적 통신

데이터 활용의 근거, 독립적 감독장치의 설계가 모두 명문화되지 않은 상태다. 조직 측면에서도 관계부처 협의 구조는 존재하나 NCO에 상응하는 상설 통합조정기구는 마련되어 있지 않다. 따라서 미일 협력의 흐름은 한국 정부에 단순한 전략 갱신이 아닌 법제·조직 결합의 재설계를 요구한다. 다만 한국의 헌법적 통신비밀 보호 전통과 개인정보 법제의 특성을 감안하면, 일본 ACD 법제의 단순 이식은 적절치 않으며, "보고-분석-대응-감독"의 4단계 구조를 한국 법제 전통 위에서 재구성하는 작업이 요구된다.

2. 정보 공유: 정보·위협 공유의 고도화와 상호 운용성 요구

2024년 4월 미일 정상 공동성명은 정보·사이버안보 협력을 심화하고 ICT 영역의 복원력과 중요 기반시설 보호를 강화하겠다고 명시했다(일본 외무성 2024a). 이 문구는 단순한 선언적 표현에 그치지 않았다. 2024년 6월 제9차, 2025년 6월 제10차 미일 사이버대화는 양국의 국내 사이버정책, 양자 협력, 역내 협력, 역량배양, 악성 행위 대응을 포괄적으로 다뤘고(일본 외무성 2024b; 일본 외무성 2025a), 2026년 3월 미일 정상회담은 한 걸음 더 나아가 양국 정부데이터를 위한 보안·주권형 클라우드 플랫폼 개발을 통해 정보공유·계획·조정을 개선하겠다고 밝혔다(백악관 2026). 정보공유의 대상이 단순 위협 인텔리전스에서 정부데이터 처리 기반과 디지털 인프라 설계에까지 확장된 것이다.

이러한 흐름의 함의는 명확하다. 정보공유는 기술적 상호운용성 없이는 작동하지 않고, 정보공유가 작동하려면 상대국이 신뢰할 수 있는 보안성·감독체계·기밀보호 체계를 갖추어야 한다. 따라서 정보

공유 강화는 필연적으로 보안 클라우드, 보안심사, 제로트러스트, 인력보안, 공급망 관리 등 인접 정책영역의 정합성을 동반할 수밖에 없다. 다시 말해, 미일 사이버협력 확대는 정보공유 자체보다 정보공유를 가능하게 하는 제도 인프라의 상호조정을 더 깊게 요구하고 있다는 점에 주목해야 한다.

한국의 정보공유 체계는 분야별·기관별로 부분적 채널이 존재하나, 표준화된 분류·공유·기밀보호 체계가 갖춰져 있다고 보기 어렵다. 한미·한일·한미일 협력에서 한국이 동등한 노드로 기능하려면 위협 인텔리전스의 표준화된 분류체계, 정부데이터 보호 등급, 인증·평가 프레임이 마련되어야 한다. 특히 2026년 미일이 추진하는 보안·주권형 클라우드 플랫폼은 향후 한미일 정보공유의 기술적 전제조건으로 작동할 가능성이 크다. 한국형 보안·주권형 정부 클라우드와 제로트러스트 전환은 단순한 디지털정부 정책이 아니라 동맹 정보공유에 참여하기 위한 기본 조건으로 다뤄져야 한다.

3. 작전 협력: 방어적 사이버작전 협력의 부상과 한미일 운영 의제

2024년 7월 2+2 「미일 안보협의위원회 공동성명」은 양국의 사이버협력이 새 단계에 접어들었음을 보여주는 상징적 문서다(일본 외무성 2024c). 이 성명은 사이버 및 정보 보안이 동맹의 미래 능력 발전에 기초적 중요성을 가진다고 규정하고, 제로트러스트 아키텍처를 통한 복원력 강화, 중요 인프라 사이버보안 향상, 미일 방어적 사이버작전 협력 증진, 양자 연합연습(combined exercise)에서의 사이버 방어 개념 확대를 명시했다. 또한 지휘통제 개편과 양국 사이버·데이터·정보보안 강화가 더 깊은 상호운용성의 조건이라고 밝혔다. 여기서 우리가

반드시 주목해야 할 점은 미일이 "사이버 정책 협력"이 아니라 "동맹 억지력 강화 수단으로서의 사이버 운용 협력"을 공식화했다는 사실이다.

이러한 정책 차원의 전환은 학술 문헌에서도 확인되기 시작했다. Rashley, Shives and Huntley(2025)는 상륙작전을 지원하는 미일 합동 사이버 작전을 분석하면서, 미일이 외교 협의에 그치지 않고 실제 작전계획 수준에서 양국 사이버 부대의 통합 운용을 준비하고 있음을 보여준다. 이 연구는 2024년 7월 2+2 공동성명이 명시한 "방어적 사이버작전 협력"과 미일 "연합연습에서의 사이버 방어 개념 반영"이 단순 선언이 아니라 작전 교리와 부대 편성 차원의 변화를 동반하고 있음을 시사한다.

이 흐름은 한국에 두 가지 신호를 준다. 하나는 한미일 안보협력에서 앞으로 사이버안보가 부속 의제가 아닌 본류의 작전·억지 의제로 취급될 가능성이 크다는 점이다. 다른 하나는 한국이 향후 한미일 또는 다자 연습에서 사이버 방어 개념, 위기 시 정보공유, 지휘통제 연동방식에 대해 보다 구체적 입장을 요구받게 될 것이라는 점이다.

그러나 한국의 현행 체계는 군·정보·민간 축이 분리되어 운영되는 경향이 강하다. 미국 또는 일본과 연동이 가능한 운영개념을 정립하려면 합참·국방부·국가정보원·과기정통부·NCSC가 공유하는 공동상황판, 그리고 분석·대응·대외공조 전반을 관통하는 일원화된 의사결정 절차가 함께 갖춰져야 한다. 따라서 미일의 방어적 사이버작전(DCO: Defensive Cyber Operations) 협력 제도화는 한국에게 법제와 운영을 분리해서 볼 수 없게 만드는 변화라고 할 수 있다.

4. 민관·인프라: 민관 협력과 핵심 인프라 보안의 확장

일본 ACD 법제의 핵심은 국가기관의 단독 역량이 아니라 민관 공동 대응 생태계 구축에 있다. 민관연계 강화, 중요 인프라 사업자의 도입 설비 신고와 사건보고, 분석정보·취약점 정보의 공유, 통신정보 활용의 법적 근거 부여는 모두 민간 인프라 사업자를 국가안보형 사이버방위 체계 안으로 끌어들이는 장치다(내각관방 2024). 그리고 이 흐름은 한국이 사이버안보를 더 이상 "기업 자율영역"이 아니라 "국가-민간 공동 책임 영역"으로 재정의해야 함을 강하게 시사한다.

핵심 인프라 보안의 의미도 한층 넓어졌다. 미일 디지털경제 대화(U.S.-Japan Dialogue on Digital Economy)는 2024년 초 안전하고 신뢰할 수 있는 글로벌 해저케이블 네트워크의 중요성을 재확인했고, 미국 싱크탱크 CSIS는 일본과의 협력 확대가 인터넷 핵심 인프라(public core), IoT 보안 기준, 안전한 소프트웨어 개발, 법집행 협력으로까지 확장되어야 한다고 지적한다(Komiyama, 2025). 이러한 논의는 미일 협력의 미래가 군사부문만이 아니라 의료기기, 자동차, 통신장비, 클라우드, 해저케이블, 소프트웨어 구성목록(SBOM: Software Bill of Materials)[8] 등 산업 전반으로 번질 가능성이 크다는 점을 시사한다.

한국이 받는 압력도 바로 이 지점에서 커진다. 한국은 2025년 범부처 정보보호 종합대책으로 민관 보안 협력 강화에 착수했으나, 통신·플랫폼·클라우드 사업자가 국가안보 체계 안에서 어떤 위치에 자리

8) 하나의 소프트웨어를 만들 때 사용된 모든 구성 요소 목록. 예: 오픈소스 라이브러리, 서드파티 모듈, 버전 정보, 의존성 등

하는가에 대한 법적·제도적 정의는 아직 미완성 상태다. 특히 한국은 일본보다 민간 통신·플랫폼·클라우드 시장의 집중도가 높고 글로벌 사업자보다 국내 사업자의 비중이 크다는 점이 차별적 조건으로 작용한다. 따라서 한국은 민간 사업자에게 보고 의무를 부여하되, 동시에 위협 인텔리전스 공유, 법적 안전지대, 산업·기술 지원을 결합한 "균형 잡힌 동반자" 구조를 설계해야 한다. 사이버안보를 더 이상 "기업 자율영역"이 아니라 "국가-민간 공동 책임 영역"으로 재정의하는 과제다.

5. 다자 네트워크화: 미일에서 미일+α로

미일 협력은 더 이상 양자 차원에 머무르지 않는다. 2024년 10월 미·일·필리핀 사이버-디지털 대화는 사이버 보안사고 대응팀(CERT: Computer Emergency Response Team) 간 협력, Open RAN, 해저케이블, 그리고 사이버 역량배양을 다루며 미일 협력을 제3국 디지털 안보 지원과 연결했다(일본 외무성 2024d). 2025년 9월 한미일 외교장관회의 공동성명도 북한 사이버위협 관련 삼자 외교실무그룹의 지속과 공공·민간 협력 심화를 재확인했다(미국 국무부 2025a). 2025년 8월 중국계 APT 대상 13개국의 합동 권고[9]에는 일본 NCO와 NPA가 동참했다(NSA et al. 2025). 이러한 사례들은 미일 협력의 초점이 "양자동맹 내부의 사이버 역량 정비"에서 "동맹을 허브로 한 다자 사이버안보

9) 13개 참여국: 미국, 호주, 캐나다, 뉴질랜드, 영국, 체코, 핀란드, 독일, 이탈리아, 일본, 네덜란드, 폴란드, 스페인

네트워크 구축"으로 확장되고 있음을 보여준다.

이 과정에서 일본은 Quad, NATO, 유럽 파트너들과의 협력을 통해 사이버 의제의 외연을 확장하고 있다(RUSI 2024). 2024년 Quad 외교장관 공동성명은 사이버안보를 실질협력 분야로 재확인했고, 일본 외무성은 일본-영국, 일본-EU, 일본-NATO 사이버대화를 정례화하고 있다.

따라서 한국이 보는 미일 협력은 단순한 양자 동맹의 문제가 아니라, 인도태평양과 유럽을 잇는 사이버 안보 네트워크의 중심축 형성이라는 관점에서 이해할 필요가 있다. 이러한 관점 전환은 한국의 외교적 선택을 "한미일"에 한정하는 것이 아니라, "미일+α" 네트워크의 어느 노드와 어떤 의제로 연결될 것인가를 결정하는 문제로 확장시킨다. 한국은 한미일과 NATO 훈련 참가를 확대하고 있으나, 어느 다자 채널에 어느 의제로 진입할지에 대한 전략적 좌표 설정은 아직 명료하지 않다. 특히 군사적 사이버 협력에서 한국은 미일에 비해 정치적 제약이 크지만, 산업·표준·통신복원력 영역에서는 한국 기업과 정부의 자산이 충분한 만큼 의제 주도 가능성이 더 크다고 판단된다.

6. 종합: 영역별 격차의 비대칭성

상기 다섯 가지 흐름은 별개의 사건이 아니라 누적적·구조적 전환의 다섯 단면이며, 한국에 가하는 압력 또한 영역별로 분리되어 작동하기보다 결합된 형태로 작용한다. 표 2는 다섯 가지 흐름 각각에서 일본 및 미일 협력의 동향, 한국의 현재 위치, 그리고 한국에 대한 직접 함의를 비교한 것이다.

한국과 미일의 격차는 영역별로 균질하지 않다. △ 법제와 통합조

정조직 차원의 격차가 가장 크고, △ 운영·민관 차원에서는 2025년 종합대책 이후 일정한 진전이 있으며, △ 다자 외교 차원에서는 한국이 비교적 새로운 자산을 형성할 여지가 있다. 이러한 비대칭성은 Ⅳ장 2절의 정책 제안에서 우선순위 설정의 출발점이 된다.

다만 이러한 압력이 한국의 위협 환경에서 어떻게 구체적으로 작동하는지를 보여주려면, 추상적 차원의 영역별 진단에 머무르지 않고 실제 위협의 양상을 살펴볼 필요가 있다. 다음 Ⅳ장에서는 한국이 당면한 세 위협 영역을 사례로 분석하고, 이를 바탕으로 한국 정부의 정책 과제를 도출한다.

〈표 2〉 미일 협력 확대와 한국의 위치 비교

항목	일본 및 미일 협력 동향	한국의 현재 위치	한국에 대한 직접 함의
법적 근거	ACD 관련법으로 보고·정보활용·무해화·감독 구조 제도화	전략은 있으나 통합 기본법 부재, 규정 분산	포괄적 법률 또는 법률 패키지 필요
통합조정 조직	NISC를 NCO로 개편하여 중추화	관계부처 협의 구조는 있으나 상설 통합조정 명확성 부족	국가 차원 컨트롤타워 실질화 필요
방어적 작전협력	2+2에서 DCO, 제로트러스트, 연습 반영 공식화	군·정보·민간 축 분리 경향	한미일 연동 가능한 운영개념 정립 필요
정보공유 기반	보안 클라우드, 정보보호 강화, 상호운용성 강조	분야별·기관별 공유체계 존재하나 파편화	공공 데이터 및 위협정보 공유 표준화 필요
민관 거버넌스	중요 인프라 보고의무, 분석정보 공유 강화	2025 종합대책으로 강화 중	법적 안전지대와 인센티브 설계 필요
핵심 인프라	해저케이블, Open RAN, 장비·클라우드 보안 중시	통신·클라우드·플랫폼 중심의 후속대응 단계	통신망·케이블·라우터·클라우드 통합점검 필요

항목	일본 및 미일 협력 동향	한국의 현재 위치	한국에 대한 직접 함의
다자 네트워크	한미일·미일필·Quad·NATO로 확장	한미일과 NATO 훈련 참가 확대 중	한국의 규범·훈련·역량수출 전략 구체화 필요

Ⅳ. 한국이 직면한 위협과 정책 과제

Ⅲ장이 미일 협력의 다섯 흐름과 한국에 대한 영역별 조정 압력을 분석했다면, 본 장은 그 압력이 한국의 실제 위협 환경에서 어떻게 나타나는지를 세 가지 사례를 통해 살펴보고, 이를 바탕으로 한국 정부가 무엇을 해야 하는지를 정리한다. 먼저 한국이 당면한 세 위협 영역을 사례로 분석한 뒤, 이를 바탕으로 한국형 통합 사이버방위 모델의 윤곽을 정책 과제 차원에서 제시한다.

1. 한국이 당면한 위협

한국은 미일과 동일한 위협 환경에 노출되어 있으나, 그 결합 방식과 강도는 다소 다르다. 북한이라는 일상적·표적적 위협, 중국계 행위자의 통신·정부망 사전배치 위험, 그리고 해저케이블과 같은 핵심 디지털 인프라의 취약성은 미일이 직면한 위협과 상당 부분 겹치면서도, 한국 고유의 위협 구조를 형성한다. 본 절은 이 세 영역에서 미일 협력이 한국과 어떻게 교차하고 있는지를 사례를 통해 살펴본다. 세 사례는 Ⅲ장에서 분석한 다섯 흐름이 현실의 위협 지도 위에서 교차하는 지점을 보여준다는 점에서 의미를 가진다.

가. 북한 사이버위협: 가상자산 탈취와 연합형 위협관리의 필요성

한국이 직면한 북한 사이버위협의 핵심은 단순한 해킹이나 정보탈취가 아니라, 정권 차원의 외화 확보, 제재 회피, 군사·핵 개발 자금 조달, 사회기반 교란 가능성이 결합된 복합 안보위협이라는 점에 있다. 특히 북한의 가상자산 탈취와 IT 노동자 침투는 금융·수사·외교·제재·민간 보안이 결합된 복합 위협으로 나타나고 있으며, 피해 범위도 정부기관이나 방산기업에 국한되지 않고 가상자산 거래소, 금융기관, 클라우드 사업자, 민간기업으로 확대되고 있다(미 재무부 2023; 미 법무부 2025; MSMT 2025). 한국은 북한 사이버위협의 직접 표적이자 반복적인 공격 대상이 되어 왔지만, 역설적으로 위협의 일상성 때문에 대응이 부처별·사건별로 쪼개질 위험이 있다.

이러한 위협에 대응하기 위해 한미일은 2023년 말부터 북한 사이버활동 전담 삼자 외교실무그룹을 가동했고(미국 국무부 2023), 2024년과 2025년에 후속 회의를 이어갔다(미국 국무부 2025b). 2025년 1월에는 북한의 가상자산 탈취와 공공·민간 협력에 관한 공동성명이 발표되었고, 2025년 9월 한미일 외교장관 공동성명은 북한 사이버위협 외교실무그룹의 지속과 공공·민간 협력 심화의 중요성을 재확인했다(미국 국무부 2025a). 이러한 일련의 조치는 북한 위협을 단순한 대북 사이버 사건이 아니라, 외교·제재·금융·민간 보안이 결합된 "연합형 위협관리 의제"로 끌어올린 것이라고 평가할 수 있다.

한국에 주는 시사점은 분명하다. 대북 사이버 대응은 군과 정보기관 중심의 사건 대응만으로는 충분하지 않으며, 가상자산 거래소, 통신사, 클라우드 사업자, 금융기관, 수사기관, 제재 집행기관이 함께 참여하는 통합 대응 체계로 확장되어야 한다. 특히 다국적제재모니터링팀(MSMT)의 2025년 보고서가 지적하듯이 북한 IT 노동자와 가상

자산 탈취 대응은 기술대응만으로 해결되지 않으며, 신원 검증, 자금 세탁 추적, 민간 신고, 우방국 공조가 결합되어야 한다. 북한 사이버 위협은 한국이 가장 먼저 통합형 사이버위협 관리체계를 구축해야 하는 실질적 압력으로 작용하고 있다.

나. 중국계 APT: 통신망·경계장비 침투와 공급망 보안 리스크

한국이 직면한 중국계 APT 위협의 핵심은 단순한 정보탈취가 아니라, 통신망·네트워크 장비·데이터센터·클라우드 등 디지털 운영기반에 장기간 잠복해 위기 시 교란 가능성을 높이는 데 있다. 한국은 반도체·자동차·배터리·금융 등 주요 산업의 디지털 의존도가 높고, 통신·플랫폼·클라우드 인프라가 국가경제와 안보 운영에 깊게 연결되어 있다. 따라서 라우터·방화벽·VPN 등 경계장비 침투, 계정정보 탈취, 로그 은폐, 공급망 취약점 악용이 결합될 경우 피해는 개별 기관의 보안 사고에 그치지 않고 산업기밀 유출, 통신망 교란, 위기 시 대응능력 저하로 이어질 수 있다(NSA et al. 2023; CISA et al. 2024; NSA et al. 2025; 국가안보실 2024; 과학기술정보통신부 외 2025).

미일 협력 확대를 가장 강하게 밀어 올린 동인도 다름 아닌 중국계 행위자의 장기 잠복형 침투다. 2023년 9월 미국과 일본 정부는 BlackTech가 다국적 기업의 해외 지사 라우터를 거점 삼아 본사 네트워크에 은밀히 침투해 왔다고 경고했다(NSA et al. 2023). 또한 2024년 2월 미국 정부는 Volt Typhoon이 통신, 에너지, 교통, 수도 분야의 중요 인프라에 장기간 잠복해 위기 시 파괴·교란을 준비할 수 있다고 밝혔다(CISA et al. 2024). 2025년 8월에는 일본 NCO와 NPA까지 참여한 다국가 합동 권고가 중국계 APT가 전 세계 통신·정부·교통·숙박·군사 인프라 네트워크를 표적으로 삼고 있다고 공개했다(NSA et

al. 2025). 이 세 사건은 중국계 위협이 단발성 침투가 아니라 공급망, 통신망, 경계장비, 운영기반을 겨냥한 구조적 침투라는 점을 분명히 드러낸다.

한국에 대한 함의는 세 가지로 정리할 수 있다. 첫째, 네트워크 장비와 통신사, 데이터센터, 클라우드의 경계보안(외부 침입을 차단하는 방어선, perimeter security)과 계정·로그 정책(접근 권한 부여와 이용 기록 관리 규칙)을 국가안보 관점에서 재설계해야 한다. 둘째, 소프트웨어·장비 공급망 보안은 조달과 산업정책의 일부로 들어와야 한다. 셋째, 중국계 APT 대응은 기술 대응만이 아니라 외교적 책임 규명, 동맹 차원의 정보공유, 산업 규제, 통신정책까지 연결된다는 점에 주목해야 한다. 일본이 ACD와 NCO를 통해 이 문제를 국가 차원으로 끌어올린 이상, 한국의 통신·플랫폼·클라우드·반도체 생태계는 더 높은 보안 기준을 요구받을 가능성이 크다.

다. 해저케이블·통신망 보안: 한국 디지털 인프라의 구조적 취약성

한국의 해저케이블·통신망 보안 문제는 단순한 통신사업자 설비 관리의 문제가 아니라, 국가 차원의 데이터 흐름, 클라우드 접속, 금융·산업 활동, 위기 시 지휘통제 기능과 직결되는 핵심 인프라 안보 문제다. 한국은 국제 데이터 트래픽과 클라우드 서비스, 반도체·자동차·금융 등 주요 산업의 디지털 연결성이 높고, 통신·플랫폼·클라우드 기능이 소수 대형 사업자와 주요 거점에 집중되어 있다. 따라서 해저케이블 절단, 라우팅 교란, 랜딩스테이션[10] 침해, 네트워크 장비 공

10) 해저케이블이 육지에 도착해 지상 통신망과 연결되는 육상 접속 시설. 바닷속 광케이블이 국

급망 취약점이 결합될 경우 개별 통신 장애에 그치지 않고 국가경제와 안보 운영 전반에 영향을 미칠 수 있다(미국 국무부 2024b; STEPI 2024/2025; 산업통상자원부 2023).

이러한 문제의식은 최근 미일 및 미·일·필리핀 협력에서도 확인된다. 미국의 『국제 사이버·디지털 전략 보고서(United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future)』는 해저케이블이 세계 디지털 트래픽의 95% 이상을 운반한다고 설명했으며(미국 국무부 2024a), 2024년 "해저 케이블 안보와 복원력" 관련 원칙은 24개국과 EU, NATO의 지지를 받았다. 같은 해 미일 디지털경제 대화는 안전하고 신뢰할 수 있는 글로벌 해저케이블 네트워크의 중요성을 재확인했고, 미·일·필리핀 사이버-디지털 대화는 CERT 협력, Open RAN, 해저케이블, 역량 배양을 묶어 논의했다(일본 외무성 2024d). 일본 외무성의 『2024 개발협력 백서』는 미국·호주와 함께 동(東)미크로네시아 해저케이블 사업을 추진 중이라고 명시한다(일본 외무성 2024e). 다시 말해, 미일은 해저케이블을 단순 개발협력 인프라가 아닌 안보·통신·표준 전략의 일부로 다루고 있다는 점을 알 수 있다.

한국에 대한 시사점은 명확하다. 해저케이블 보안은 단순한 통신 설비 관리 문제가 아니라, 통신망 복원력, 경로 다변화, 랜딩스테이션 보호, 클라우드 지역분산, Open RAN 및 코어망 보안을 함께 다루는 국가 핵심 인프라 의제다. 특히 한국은 해상교통로와 국제 데이터 허브 의존도가 높고, 대형 통신·플랫폼 기업이 집중된 구조를 지니므

가 통신망·데이터센터·인터넷망으로 이어지는 관문 지점.

로, 케이블의 물리적 절단·라우팅 교란·해저케이블이 상륙하는 해외 거점에서의 국제 공조 실패·네트워크 장비 공급망 취약점이 결합될 경우 경제적 충격이 클 가능성이 있다. 따라서 우리는 미일 모델을 참고하되, 통신정책·해양안보·과기정책·산업정책을 연결하는 별도의 "공공핵심 디지털 인프라 보호전략"을 마련해야 할 것이다.

세 사례에서 공통적으로 드러나는 점은 사이버안보의 핵심 대상이 개별 시스템에서 공공핵심 인프라와 공급망 전체로 이동하고 있다는 사실이다. 또한 미일은 양자 협력을 다자 권고와 다자 인프라 협력으로 외연을 확장하면서, 위협 대응의 단위 자체를 '단일 정부의 사이버 대응'에서 '동맹 네트워크 차원의 대응 체계'로 옮겨가고 있다. 한국은 위협 인식 자체는 미일과 다르지 않지만, 대응의 제도화 수준과 다자 네트워크에 참여하기 위한 제도적 기반에서는 여전히 격차를 보인다.

2. 한국 정부 정책 과제

한국의 대응 방향은 "일본 추격"이 아니라 "한국형 통합 사이버방위 모델 구축"이 되어야 한다. 일본 ACD가 우리에게 주는 가장 큰 교훈은 능동성 그 자체가 아니라, 능동성을 떠받치는 △법적 근거 △민관보고 △감독장치 △조정조직 △국제협력의 결합이다. 동시에 한국은 일본과 세 가지 구조적 조건에서 다르다. 첫째, 한국은 북한이라는 일상적·표적적 위협에 더 직접적으로 노출되어 있어 위협 비대칭성을 직접 반영하는 대응 설계가 필요하다. 둘째, 한국의 헌법적 통신비밀 보호 전통과 개인정보 법제는 통신정보 활용에 대한 정치적·법적 민감성이 일본보다 높아, 사법적 통제와 감독장치의 정교화가 더 깊

게 요구된다. 셋째, 한국은 민간 통신·플랫폼·클라우드 시장의 집중도가 높고 글로벌 사업자보다 국내 사업자의 비중이 커, 민관 책임의 설계 방식이 일본과 다를 수밖에 없다. 따라서 일본 모델은 학습 자료이지 이식 모델이 아니다.

가장 시급한 과제는 법제와 거버넌스의 재설계다. 한국은 통합된 사이버안보 기본법 없이 여러 법률과 규정에 권한이 분산되어 있어, 미일 협력이 요구하는 "상호 운용 가능한 국내 체계"의 기준을 충족하지 못하고 있다. 따라서 통합적 사이버안보 기본법 또는 이에 준하는 법률 패키지가 마련되어야 한다. 여기에는 첫째, 중요 인프라 사업자의 사건보고와 취약점 보고 의무, 둘째, 정부의 제한적 교차국경 트래픽 데이터 활용 요건과 절차, 셋째, 독립적 감독·사후통제 기구, 넷째, 민관 정보공유의 면책 범위, 다섯째, 국가위기 시 부처 간 지휘조정 메커니즘이 포함되어야 한다. 일본 ACD법이 제시하는 "보고-분석-대응-감독"의 4단계 구조는 유효한 참조점이라고 할 수 있으나(내각관방 2025; Bae 2026), 한국에서는 통신비밀보호법 체계와 개인정보법제 위에서 사법적 통제 절차와 독립적 감독장치를 일본보다 더 정교하게 설계해야 하며, 면책 범위는 좁고 명확하게 규정해야 한다.

조직 차원에서는 NCO와 같은 단일 컨트롤타워를 즉시 만드는 것보다, 부처별 권한은 유지하되 위기 대응·정보공유·국제 공조 차원의 운영체계를 표준화하는 "운영 통합" 접근이 보다 현실적이다. 국가안보실, 국가정보원, 과학기술정보통신부, 국방부, 경찰청, 금융위원회의 권한을 일거에 통합하는 것은 정치적·법적 비용이 크기 때문이다. 대신 국가 차원의 사이버 통합조정센터를 상설화하되, 정보기관 중심 모델과 민간보안 중심 모델을 분리하지 않고 상호연동시키는 설계가 필요하다. 위기 시 공동상황판, 분석·대응·대외공조의 일

원화, 한미일 정보공유의 기술적 상호운용성을 갖추기 위한 인증·평가 체계가 그 핵심 구성요소가 된다. 한국형 보안·주권형 정부 클라우드와 제로트러스트 전환, SBOM·구성요소 투명성 기준, N²SF 확산 역시 단순한 디지털정부 정책이 아니라 동맹 정보공유의 진입 자격으로 다뤄져야 한다.

민관 협력의 재정의는 한국 모델의 가장 차별적인 영역이 될 가능성이 크다. 한국의 민간 통신·플랫폼·클라우드 시장 집중도가 일본보다 높고 국내 사업자 비중이 크다는 점은 "국가-민간 공동 책임"의 설계 방식을 일본과 다르게 만든다. 한국 모델은 민간 사업자에게 사건보고와 분석정보 공유의 의무를 부여하되, 동시에 위협 인텔리전스 공유, 법적 안전지대, 산업·기술 지원을 결합한 "균형 잡힌 동반자" 구조를 설계해야 한다. 통신망, 케이블 랜딩스테이션, 라우터·스위치 등 네트워크 장비, 클라우드 관리 시스템, 소형 통신기지국, 핵심 클라우드 소프트웨어(SaaS)에 대한 고강도 모의점검을 즉시 상설화하고, 분야별 사건 심각도 분류와 민관 핫라인을 통일하는 작업은 입법 절차와 별개로 곧바로 가동될 수 있다.

위협별 통합 대응 체계는 앞 절에서 살핀 세 영역에서 우선 구체화될 수 있다. 북한 사이버위협 대응은 군·정보기관 중심의 사건 대응에 머물러서는 안 되며, 외교·금융·수사·정보기관과 가상자산 거래소·통신사·클라우드 사업자를 연결하는 상설 합동분석반을 중심으로 재편되어야 한다. 이 분석반은 단순 정보공유 채널이 아니라 위협 인텔리전스, 자금흐름 추적, 외교·제재 정보, 민간 신고를 결합한 통합 분석-대응 단위가 되어야 하며, 한미일 외교실무그룹과 직접 연결되어야 한다. 중국계 APT 대응은 네트워크 장비와 통신사, 데이터센터, 클라우드의 경계보안과 계정·로그 정책을 국가안보 관점에서 재

설계하고, 소프트웨어·장비 공급망 보안을 조달과 산업정책의 일부로 끌어들이는 작업을 동반한다. 해저케이블·통신망 보안은 국가적 복원력, 라우팅 다변화, 해저케이블 양륙 시설(landing station) 보안, 클라우드 지역분산, Open RAN 및 코어망 보안을 묶는 "공공핵심 디지털 인프라 보호전략"으로 구체화될 필요가 있다. 한국은 해상교통로와 국제 데이터 허브 의존도가 높고 대형 통신·플랫폼 기업이 집중된 구조를 지니므로, 케이블 절단, 라우팅 교란, 양륙 시설을 매개로 한 국제 협력 실패, 라우터 공급망 취약점이 결합될 경우 경제적 충격이 크다는 점에 주목해야 한다.

사이버안보 다자외교는 영역별 자산 우위를 외교 자본으로 전환하는 차별화 전략으로 설계되어야 한다. 한국은 군사적 사이버 협력에서 미일에 비해 정치적 제약이 크지만, 산업·표준·통신복원력 영역에서는 한국 기업과 정부의 자산이 우위에 있다. 이 비대칭을 토대로 (1) 군사 협력은 한미일에서 한국이 북한 대응과 훈련 분석 부담을 능동적으로 분담하는 방식으로, (2) 산업·표준 협력은 제3국 지원을 통해 의제 형성자로, (3) 규범 협력은 NATO·EU와의 기존 협력 채널을 활용하되, 한국 주도의 인도태평양 사이버 규범 포럼을 별도로 추진해 의제 발신국으로서의 역할을 강화할 필요가 있다. 이를 위해서는 외교부·국방부·과기정통부·국정원·NCSC 등이 동일한 '의제 지도'를 공유하고, 한국이 매년 선제 발의할 다자 의제 목록을 갱신·관리해야 한다. 이것은 한국이 다자 사이버외교에서 추종자가 아닌 의제 설정자로 자리잡기 위한 최소 조건이다.

생태계 전략은 이상의 과제를 떠받치는 기반이다. 일본이 ACD 법제와 NCO를 구축하면서 맞닥뜨리는 과제도 인력 부족과 산업 생태계의 취약성이다(Komiyama 2025). 한국 또한 화이트해커를 단기적 사

건 대응에 활용하는 방식에서 벗어나, 국방·정보·민간·학계·산업을 아우르는 국가 차원의 사이버 전문인력 풀을 구축해야 한다. 산업적으로는 보안 클라우드·네트워크 장비·공급망 검증·양자내성암호·AI 보안 분야의 산업육성이 필요하며, 외교적으로는 인도태평양 지역 국가들에 대한 사이버 역량배양 외교를 동시에 추진해야 한다(대외경제정책연구원 2025). 이 영역에서 한국은 일본의 추격자가 아니라 인도태평양 사이버 역량배양의 주도적 공여국으로 자리매김할 잠재력을 갖고 있다.

이상의 과제들은 단기·중기·장기로 단계화될 수 있다. 핵심 인프라 사건보고와 상황공유의 통합, 대북 사이버 통합 분석반의 구성, 통신·케이블 랜딩스테이션·라우터·클라우드의 고강도 모의점검 상설화는 1~2년 내 즉시 가동이 가능하며, 입법을 기다리지 않고도 추진할 수 있다. 통합적 사이버안보 기본법 또는 법률 패키지의 마련, 사이버 통합조정센터의 상설화, 보안·주권형 정부 클라우드와 제로트러스트 확산은 3~5년의 입법·예산·기관 조정을 필요로 한다. 그리고 국가 차원의 사이버 전문인력 풀과 연구생태계의 구축, 해저케이블·Open RAN·공급망 보안 외교의 본격화는 5년 이상의 장기 과제다. 다만 세 시간축은 순차적인 것이 아니라 동시에 출발하되 가시화 시점이 다를 뿐이다. 단기 운영 통합이 중기 입법의 정치적 기반을 만들고, 장기 생태계 투자가 중기 거버넌스의 인적 토대를 형성하는 누적적 관계속에서 함께 작동해야 한다.

한국형 통합 사이버방위 모델의 본질은 일본 ACD를 부분적으로 변형해 옮겨오는 작업이 아니다. 위협 비대칭성·통신비밀 보호 전통·시장 집중 구조라는 한국의 조건 위에서, 능동성과 절제, 통합과 분권, 동맹 정합성과 자율성을 동시에 충족시키는 독자적 설계 논리

를 구축하는 작업이다. 미일 협력은 한국에 분명한 제도적 기준을 요구하고 있지만, 그 기준을 충족하는 경로까지 일본을 따라야 할 이유는 없다.

〈표 3〉 단기·중기·장기 정책 제안

기간	제안	중점 주체	실무 포인트
단기	핵심 인프라 사건보고·상황공유 통합	국가안보실, NIS/NCSC, 과기정통부, 금융위, 경찰	분야별 임계치 통일, 민관 핫라인, 통신·클라우드 긴급점검
	대북 사이버 통합 분석반 구축	외교·금융·수사·정보기관, 거래소, 통신사	IT 노동자·가상자산 탈취·제재정보 결합
중기	포괄적 사이버안보 기본법 또는 법률 패키지 마련	국회, 국가안보실, 법무·과기·국방·정보기관	보고의무, 데이터 활용, 감독장치, 면책·책임 규정
	사이버 통합조정센터 상설화	국가안보실, NIS/NCSC, 국방부, 과기정통부	위기 시 공동상황판, 분석·대응·대외공조 일원화
	보안·주권형 정부클라우드와 제로트러스트 확산	디지털정부 부처, NCSC, 각 부처 CISO[<?>]	기밀 수준별 분리, 상호운용성, 감사 추적성 확보
장기	국가 사이버안보 인력 육성 및 연구생태계 구축	교육·국방·정보·민간기업	군-민 전환 트랙, 전문인증, 실전훈련 정례화
	해저케이블·Open RAN·공급망 보안 외교 강화	외교부, 과기정통부, 산업부	인도태평양 역량배양, 표준·조달 연계, 기업 해외진출 지원

V. 결론

본 논문은 미일 사이버안보 협력이 2013년 정책 협의기에서 출발해 2019년 능력 강화기를 거쳐 2023년 이후 준제도화 전환기에 진입하는 13년의 누적적 진화 과정을 정리하고, 그 흐름이 한국 정부에 가하는 정책적 조정 압력을 분석했다. 분석의 결론은 다음 세 가지로 요약할 수 있다.

첫째, 미일 협력은 더 이상 외교 협의의 누적이 아니라 "운영 가능한 동맹 사이버체계"의 구축 단계로 진입했다. 일본의 ACD 법제와 NCO 출범, 미일 2+2의 DCO 합의, 보안 클라우드 협력, 다국가 합동 권고는 이 변화를 단계적으로 보여주는 지표다. 둘째, 미일 양자 협력은 인도태평양 사이버 네트워크의 허브로 확장되고 있다. 미·일·필리핀, 한미일, Quad, NATO와의 연결은 미일 협력을 "양자 동맹"이 아니라 "사이버안보 네트워크의 중심축"으로 재정의하고 있다. 셋째, 한국은 이러한 변화에 대해 일본 모델의 단순 이식이 아닌, 우리의 위협 환경, 법제 전통, 산업 구조에 맞춘 "한국형 통합 사이버방위 모델"을 구축할 필요가 있다. 그 모델의 윤곽은 단기적 운영체계 통합, 중기적 법제·거버넌스 재설계, 장기적 인력·산업·외교 생태계 구축의 시간축 위에서 차별화되어야 할 것이다.

이러한 분석은 미일 사이버안보 협력이 일본의 전반적 안보력 강화 흐름과 분리되어 있지 않다는 점도 보여준다. 일본의 ACD 법제화, NCO 출범, 방어적 사이버작전 협력, 민관 인프라 보안 강화는 일본의 안보력 강화가 전통적 군사력 증강에 국한되지 않고, 법제·조직·정보·민간 인프라·동맹 운용을 결합한 통합 안보역량 강화로 확장되고 있음을 보여준다. 동시에 사이버안보 협력은 미일 안보협력

일반과도 구별되는 특징을 갖는다. 전통적 안보협력이 병력 배치, 작전계획, 억지태세를 중심으로 전개되었다면, 사이버안보 협력은 국내법제, 통신정보 활용 근거, 민관 보고체계, 보안 클라우드, 핵심 인프라 복원력 등 비군사적 제도 기반을 동맹 상호운용성의 핵심 조건으로 끌어올린다. 이 점에서 본 연구는 미일 안보협력의 진화를 사이버 공간의 제도화·운영화라는 관점에서 조명하고, 한국이 한미일 및 인도태평양 사이버안보 네트워크에 참여하기 위해 갖추어야 할 국내 제도적 조건을 제시했다는 점에서 의의를 갖는다.

따라서 미일 협력의 흐름을 정확히 읽고 한국의 정책 좌표를 재설정하는 일은, 앞으로 정부·학계·산업이 함께 축적해 나가야 할 중장기 정책연구 과제라고 할 수 있다.

〈참고문헌〉

국가안보실. 2024.『국가 사이버안보 전략』(2월 1일 발표). https://ksaem.or.kr/wp-content/uploads/2024/02/240201_참고자료_국가사이버안보전략.pdf

국가사이버안보센터. 2025.「국가망보안체계(N²SF) 보안가이드라인 1.0」(9월 9일 공개, 9월 30일 NCSC 홈페이지 게시). https://ncsc.go.kr/.

과학기술정보통신부·국가안보실·금융위원회·개인정보보호위원회·국가정보원·행정안전부. 2025.「범부처 정보보호 종합대책」(10월 22일 발표). 정책브리핑: https://www.korea.kr/news/policyNewsView.do?newsId=148952831.

대외경제정책연구원. 2025.『주요국의 사이버안보 정책과 한국에 대한 시사점』. https://www.kiep.go.kr/gallery.es?mid=a10101010000&bid=0001&list_no=11761&act=view

산업통상자원부. 2023.「데이터센터 수도권 집중 완화 방안」(3월 9일 발표). https://www.motir.go.kr/attach/down/095a2dda9c864e1d90d751f7668a1117/213638f7ef310dbf2e490ce19bc71ad3

조원선·이광호·최해옥·이승윤·이현익·김가은. 2024.『기술안보 관점의 디지털 인프라 복원력 강화 방안 – 해저케이블 사례를 중심으로 –』. 과학기술정책연구원, 기초연구 2024-05. https://www.stepi.re.kr/site/stepiko/report/View.do?cateCont=A0203&cbIdx=1292&reIdx=327

「사이버안보 업무규정」(대통령령 제34287호, 2024년 3월 5일 일부개정, 2025년 1월 1일 시행). 국가법령정보센터: https://law.go.kr/LSW//lsInfoP.do?lsId=013942.

Bae, Sunha. 2026. “South Korea’s Integrated Cyber Defense Framework: Active Cyber Defense and Reactive Responses.” CSIS Strategic Technologies Program https://www.csis.org/analysis/south-koreas-integrated-cyber-defense-framework-active-cyber-defense-and-reactive

CISA, NSA, FBI et al. 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" (Volt Typhoon 권고, AA24-038A) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CSIS Japan Chair. 2026. "Deepening Strategic Alignment: Priorities for the U.S.-Japan Alliance" https://www.csis.org/analysis/deepening-strategic-alignment-priorities-us-japan-alliance.

Harold, Scott W., Martin C. Libicki, Motohiro Tsuchiya, Yurika Ito, Roger Cliff, Ken Jimbo, and Yuki Tatsumi. 2016. *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/conf_proceedings/CF379.html.

Jensen, Mikkel Storm. 2023. "Entrapment Risk or Entanglement Nuisance." *Cyber Defense Review* (Spring).

Kallender, Paul, and Christopher W. Hughes. 2017. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace." *Journal of Strategic Studies* 40(1-2): 118-145. DOI: 10.1080/01402390.2016.1233493.

Komiyama, Koichiro. 2025. "Norms in New Technological Domains: What's Next for Japan and the United States in Cyberspace." CSIS Strategic Japan White Paper. https://www.csis.org/analysis/norms-new-technological-domains-whats-next-japan-and-united-states-cyberspace.

Lewis, James A. 2026. "Active Cyber Defense in the Korean Context." CSIS. https://www.csis.org/analysis/active-cyber-defense-korean-context.

MSMT(Multilateral Sanctions Monitoring Team). 2025. *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology*

Worker Activities. https://msmt.info/Publications/detail/MSMT%20Report/4221

Nakasone, Paul M. 2019. 'A Cyber Force for Persistent Operations.' *Joint Force Quarterly 92*. https://cs.brown.edu/courses/cs180/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf

NSA, FBI, CISA, NPA, NISC. 2023. "People's Republic of China-Linked Cyber Actors Hide in Router Firmware" (BlackTech 공동 권고) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a.

NSA et al. 2025. "NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations" https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/.

RUSI. 2024. "Cyber Capabilities in the Indo-Pacific: Shared Ambitions, Different Means?" https://www.rusi.org/explore-our-research/publications/commentary/cyber-capabilities-indo-pacific-shared-ambitions-different-means.

RAND Corporation. 2019. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*. https://www.rand.org/pubs/research_reports/RR2961.html.

RAND Corporation. 2024. *Integrated Deterrence as a Defense Planning Concept*. https://www.rand.org/pubs/research_reports/RRA1844-1.html.

Rashley, Harrison, Timothy Shives, and W. Huntley. 2025. "Supporting Amphibious Forces with Partnered U.S.-Japan Cyber Operations." *European Conference on Cyber Warfare and Security* 24(1).

The White House(백악관). 2026. "Fact Sheet: President Donald J. Trump

Strengthens U.S.-Japan Alliance for the Benefit of All Americans" https://www.whitehouse.gov/fact-sheets/2026/03/fact-sheet-president-donald-j-trump-strengthens-u-s-japan-alliance-for-the-benefit-of-all-americans/.

U.S. Cyber Command. 2018. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.* https://www.cybercom.mil/portals/56/documents/uscybercom%20vision%20april%202018.pdf

U.S. Department of Justice(미 법무부). 2025. "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes." June 30. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

U.S. Department of State(미국 국무부). 2023. "Inaugural United States-Japan-Republic of Korea Trilateral Diplomatic Working Group Meeting on Democratic People's Republic of Korea Cyber Activities" https://2021-2025.state.gov/inaugural-united-states-japan-republic-of-korea-trilateral-diplomatic-working-group-meeting-on-democratic-peoples-republic-of-korea-cyber-activities/.

U.S. Department of State(미국 국무부). 2024a. *United States International Cyberspace and Digital Policy Strategy* https://2021-2025.state.gov/briefings-foreign-press-centers/the-united-states-international-cyberspace-and-digital-policy-strategy/.

U.S. Department of State(미국 국무부). 2024b. "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World." September 26. https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-

a-globally-digitalized-world/

U.S. Department of State(미국 국무부). 2025a. "Joint Statement from the Trilateral Meeting of the United States of America, Japan, and the Republic of Korea in New York City" https://www.state.gov/releases/2025/09/joint-statement-from-the-trilateral-meeting-of-the-united-states-of-america-japan-and-the-republic-of-korea-in-new-york-city.

U.S. Department of State(미국 국무부). 2025b. "Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration" https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/joint-statement-on-cryptocurrency-thefts-by-the-democratic-peoples-republic-of-korea-and-public-private-collaboration/

U.S. Department of the Treasury(미 재무부). 2023. "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities." May 23. https://home.treasury.gov/news/press-releases/jy1498

国家サイバー統括室 (국가사이버통괄실, National Cyber Office). 2025.「サイバー安全保障に関する取組(能動的サイバー防御の実現に向けた検討など)」https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html.

外務省(일본 외무성). 2019.「日米安全保障協議委員会(『2+2』)共同発表」https://www.mofa.go.jp/region/n-america/us/security/scc/joint1904.html.

外務省(일본 외무성). 2024a.「日米首脳共同声明:『未来のためのグローバル・パートナー』」("Japan-U.S. Joint Leaders' Statement: 'Global Partners for the Future'") https://www.mofa.go.jp/na/na1/us/pageite_000001_00259.html

外務省(일본 외무성). 2024b.「第9回日米サイバー対話」("The 9th Japan-U.S. Cyber Dialogue") https://www.mofa.go.jp/press/release/

pressite_000001_00394.html.

外務省(일본 외무성). 2024c.「日米安全保障協議委員会(『2+2』)共同発表」("Joint Statement of the U.S.-Japan Security Consultative Committee ('2+2')") https://www.mofa.go.jp/region/n-america/us/security/scc/index.html

外務省(일본 외무성). 2024d.「第1回日米比サイバー・デジタル対話」("The 1st Japan-U.S.-Philippines Cyber-Digital Dialogue") https://www.mofa.go.jp/press/release/pressite_000001_00661.html.

外務省(일본 외무성). 2024e.『開発協力白書 2024年版』(Development Cooperation White Paper 2024) 중 동(東)미크로네시아 해저케이블 사업 관련 서술. https://www.mofa.go.jp/policy/oda/page22e_000976.html.

外務省(일본 외무성). 2025a.「第10回日米サイバー対話」("The 10th Japan-U.S. Cyber Dialogue") https://www.mofa.go.jp/press/release/pressite_000001_01381.html.

サイバーセキュリティ戦略本部(사이버시큐리티전략본부). 2025.「サイバーセキュリティ2025」https://www.nisc.go.jp/pdf/council/cs/dai44/44shiryou1.pdf.

内閣官房(내각관방). 2022.「国家安全保障戦略」(国家安全保障戦略について). https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html.

内閣官房サイバー安全保障体制整備準備室(내각관방 사이버안전보장체제정비준비실). 2024.「サイバー安全保障分野での対応能力の向上に向けた提言」(능동적 사이버 방어 도입을 위한 유식자회의 최종 제언) https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf; 일람: https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html.

内閣官房サイバー安全保障体制整備準備室(내각관방 사이버안전보장체제정비준비실). 2025.「サイバー対処能力強化法案及び同整備法案について」(ACD 관련 신법·정비법 설명자료)「重要電子計算機に対する不正な行為による被害の防止に関する法律」(관련 법령) https://www.cas.go.jp/jp/seisaku/

cyber_anzen_hosyo_torikumi/index.html.
松﨑みゆき(Matsuzaki, Miyuki). 2015.「サイバーセキュリティに関する防衛省・自衛隊の課題」. https://npi.or.jp/research/data/note-matsuzaki20150422.pdf

The Evolution of U.S.-Japan Cybersecurity Cooperation and Policy Tasks for Korea

Yeon, Wonho | Hyundai Motor Group

This paper (1) traces the evolution of U.S.–Japan cybersecurity cooperation since the launch of the bilateral Cyber Dialogue in 2013, (2) analyzes the five trends driving the quasi-institutionalization that has accelerated since 2023, and (3) derives both the adjustment pressures these trends impose on Korean cybersecurity policy and the resulting policy implications. The analysis finds that U.S.–Japan cyber cooperation has expanded cumulatively in scope and depth through three stages: policy consultation (2013–2018), capability-building (2019–2022), and quasi-institutionalization (2023–2026). The post-2023 transformation is particularly notable in that five trends are unfolding simultaneously—(i) Japan's legislation on Active Cyber Defense (ACD), (ii) the advancement of intelligence and threat information sharing, (iii) U.S.–Japan cooperation on Defensive Cyber Operations (DCO), (iv) public–private collaboration and critical infrastructure security, and (v) multilateral networking linking the U.S.–Japan–Philippines and Korea–U.S.–Japan channels—together transforming bilateral cooperation into a hub of the Indo-Pacific cyber network. The paper identifies the adjustment pressures these trends place on Korea, illustrates them through three case studies—DPRK cyber threats, China-linked APT activity, and submarine cable security—and synthesizes short-, medium-, and long-term policy tasks. In conclusion, rather than simply transplanting the Japanese model, Korea should gradually establish a "Korean-style integrated cybersecurity model" tailored to its threat environment, legal tradition, and industrial structure.

Keyword U.S.-Japan cyber cooperation, Active Cyber Defense, Korea-U.S.-Japan cooperation, cybersecurity policy,