연구자료 24-02

Korea Institute for International Economic Policy

주요국의 사이버안보 정책과 한국에 대한 시사점

엄준현
이보람

KIEP 대외경제정책연구원
Korea Institute for International Economic Policy

대외경제정책연구원은 세계경제환경의 변화에 따른 외부적 도전을 슬기롭게 극복하고 우리 경제의 국제적 역할과 위상을 정립하기 위해 1989년 정부 출연연구기관으로 발족하였습니다.

본 연구원은 국제거시금융, 무역통상안보, 세계지역연구, 국제개발연구 등과 관련된 문제를 조사 · 분석하고 정책수단을 개발하는 연구활동을 수행함으로써 국가의 대외경제정책 수립에 이바지하고 있습니다.

연구결과는 [연구보고서], [연구자료], [Working Paper] 등 각종 국 · 영문보고서, 웹진 [오늘의 세계경제], World Economy Brief, 학술지 *East Asian Economic Review* (*ESCI*, 한국연구재단 등재지) 등의 형태로 발간되고 있으며, 원문을 본 연구원 홈페이지(www.kiep.go.kr)에 공개하고 있습니다.

對外經濟政策研究院

KOREA INSTITUTE FOR INTERNATIONAL ECONOMIC POLICY

30147 세종특별자치시 시청대로 370
세종국책연구단지 경제정책동
T. 044-414-1114 F. 044-414-1001
www.kiep.go.kr

연 구 자 료
24-02

주요국의 사이버안보 정책과 한국에 대한 시사점

엄준현·이보람

KIEP 대외경제정책연구원
Korea Institute for International Economic Policy

연구자료 24-02

주요국의 사이버안보 정책과 한국에 대한 시사점

인 쇄 2024년 12월 26일
발 행 2024년 12월 30일
발행인 이시욱
발행처 대외경제정책연구원
주 소 30147 세종특별자치시 시청대로 370
세종국책연구단지 경제정책동
전 화 044) 414-1179
팩 스 044) 414-1144
인쇄처 (사)아름다운사람들(02-6948-9650)

정가 10,000원
ISBN 978-89-322-2514-2 94320
978-89-322-2064-2(세트)

대외경제정책연구원은 'ESG 경영' 방침에 따라
친환경 용지를 사용합니다.

국문요약

사이버안보는 군사안보, 에너지 안보, 경제안보와 같은 국가안보의 하위 개념이다. 사이버안보는 디지털화의 영향으로 국가 핵심 기반시설이 운영되는 안보 중심이 된 사이버공간을 사이버상 공격 또는 위협으로부터 방어하여 적절히 기능하게 함으로써 국가와 국민의 안전이 보장되는 상태 또는 활동이라고 정의할 수 있다. 이때 사이버공간은 '정보시스템'과 여기에 저장된 '정보'로 구성된다.

사이버안보 규범에 관한 국제적 논의 과정에서는 미국을 중심으로 한 서방 자유민주 국가와 러시아 및 중국 사이의 견해 대립이 계속되었다. 그럼에도 UN 차원에서는 정부 전문가 그룹(UNGGE)이 2004년부터 활동하고 있다. UNGGE의 제3차 보고서에서는 사이버공간에 국제법이 적용된다는 원칙을 처음 확인했고, 국가의 영역관리 책임을 노력 의무로 인정하는 등 제한적이나마 성과가 있었다.

미국 등 서방 국가는 사이버공간을 별도 영역으로 인정하는 태도를 보인다고 평가할 수 있는 한편, 현행 국제법이 사이버공간에 그대로 적용될 수 있다고 주장한다. 러시아와 중국 등 비서방 진영은 사이버공간이 별도 영역이 아니라는 태도를 보인다고 평가할 수 있는 한편, 시스템 등 물리적인 ICT 기반시설 또는 정보가 저장된 서버의 위치가 국내이면 국내법이, 외국이면 외국법이 적용될 뿐 국제법은 적용되지 않는다고 주장한다.

주요국의 사이버안보 정책을 전략과 법률로 나누어 조사한 결과는 다음과 같다. 미국의 2023년 「국가 사이버안보 전략」에 따라 민간시설에 대한 사이버안보의 최소 요건이 권고되었다. 「CISA 전략계획 2023~2025」는 핵심 네트워크에 대한 침해가 발생하기 전에 능동적으로 위협을 완화한다는 내용을 포함

한다. 또한 「2022년 핵심 기반시설 사이버사고 보고법」은 핵심 인프라 소유자에게 사이버사고 발생과 랜섬웨어 피해에 대해 각각 72시간, 24시간 내 보고의무를 부과했다. 여기서 미국 사이버안보 정책의 특징으로는 능동적 방어 전략을 택한 점, 그리고 상당수 인프라를 민간이 소유 또는 운영하는 점을 고려하여 민간과의 공조를 강화한 점을 들 수 있다.

EU는 2013년 「EU 사이버안보 전략」에서 안전하면서도 개방적인 사이버공간을 강조했으나, 2020년 동명의 전략에서는 복원력과 기술 주권을 강조했다. EU의 사이버안보 법률은 직접적인 수입 제한 조치보다는 인증 제도 또는 표시제도와 같은 간접적인 조치를 취하는 특징이 있다. 2019년 「사이버안보법」을 제정하여 다양한 사이버보안 인증 제도를 마련하고 있다. 이에 따라 2024년에는 ICT 상품에 대한 EUCC 인증 시행법이 제정되었다. 클라우드컴퓨팅 서비스, 5G 통신, AI에 대한 인증도 준비하고 있다. 또한 2024년 「사이버복원력법」은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품에 이 법에 따른 보안사항을 준수한다는 CE 표지를 부착할 법적 의무를 수입업자 또는 유통업자에 부과한다.

일본의 2022년 「국가안보전략」에서 제안된 '능동적인 사이버 방어'는 미국의 전략과 유사한 것으로 확인된다. 「경제안보추진법」을 근거로 한 기간 인프라 방호제도는 소관 부처에서 지정한 민간사업자를 대상으로 특정 중요 설비 도입 시 및 유지관리 등의 위탁 시 사전심사를 요구하며, 정부는 설비 도입 중지 명령권을 갖는다. 일본정부는 기업의 자발적 참여에 의한 인증 제도인 「IoT 제품에 대한 보안 적합성 평가제도」를 마련했다.

우리나라의 2024년 「국가 사이버안보 전략」은 자유·인권·법치 수호라는 민주적 가치를 표방한 점과 공세적 사이버 방어와 대응 전략을 도입한 점을 특징으로 볼 수 있다. 사이버안보 법률의 특징은 통합된 법률이 없이 관련 규정이 여러 법률에 흩어져 있다는 것이다. 이는 필연적으로 통합된 관리 조직의 출현을 어렵게 만든다. 그러나 클라우드컴퓨팅 등 변화하는 사이버안보 상황에 신속하게 대응하는 점은 돋보인다.

사이버안보 조치에 대한 국제통상법의 적용 가능성은 다음과 같다. 사이버안보 조치는 WTO 협정에 위반된다는 판단이 내려질 가능성이 크다. 국가안보 예외 규정을 다룬 WTO 판정례는 모두 전시 또는 국제 관계에서의 긴급상황에 관한 것이다. 평시의 조치가 국가안보 예외로 인정되려면 조치 당시에 목적을 인식했다는 주관적 증거와 실제로 군사시설 등에 간접적으로 공급한다는 증거가 있어야 한다는 견해가 있다. 패널은 당사국이 자국의 필수적 안보 이익의 보호를 위해 필요한 조치라고 신의성실하게 판단했는지를 심사할 수 있다. 국제투자중재 사건인 Seda v. Colombia에서도 결론은 같았다.

우리나라의 사이버안보 정책에 대한 시사점은 다음과 같다. 첫째, 사이버 무력공격에 이르지 않은 사이버 부당 이용 또는 사이버공격에 대해서는 자위권을 행사할 수 없다. 둘째, 공세적 방어 전략은 신중하게 추진되어야 한다. 임박한 무력공격을 대상으로 하는 선제적 자위가 국제관습법에 따라 허용된다는 견해가 있다. 그러나 임박성을 판단할 구체적 기준에 대한 논란이 있다. 셋째, 사이버공간에 대한 국가의 영역관리 책임 또는 상당 주의 의무라는 법리는 우리나라가 북한으로부터의 사이버 위협에 대응하는 데 유용하게 활용할 수 있다. 넷째,

통합된 사이버안보법을 마련할 필요가 있다.

우리나라의 통상 정책에 대한 시사점은 다음과 같다. 첫째, 주요국이 도입하는 사이버안보 조치를 지속적으로 관찰하여 우리 수출 기업이 받는 부정적 영향을 최소화해야 한다. 둘째, 우리 기업이 미국 또는 EU 시장 등에서 제3국과 경쟁할 때 사이버안보 관련 표지 및 인증 제도 등에서 유리한 위치에 설 수 있도록 우리 정부가 지원해야 한다. 셋째, 우리나라가 사이버보안 조치를 할 때는 통상규범에 저촉되지 않도록 정밀한 제도 설계와 운영이 필요하다. 넷째, 국가가 통상협정의 국가안보 예외 규정을 주장할 때도 신의칙에 따른 심사가 이루어진다.

차례

표 차례

그림 차례

글상자 차례

이 연구에서 사용한 주요 약어

약어	본말	우리말
CISA	Cybersecurity and Infrastructure Security Agency	사이버안보 및 기반시설 안보국(미국)
CRA	Cyber Resilience Act	사이버복원력법
ENISA	European Union Agency for Cybersecurity	EU 사이버안보청
NIS	Network and Information Systems Directive	네트워크 및 정보시스템 법
NRMC	National Risk Management Center	국가 위험 관리 센터
NCCIC	National Cybersecurity and Communication Integration Center	사이버안보 및 통신 통합센터
NPPD	National Protection and Programs Directorate	국가보호 및 프로그램 국

제1장 서론

1. 연구 배경 및 필요성

미국, EU, 일본 등 주요국은 사이버안보 관련 전략을 수립하고 이를 뒷받침할 자국 법령을 제정하는 등 사이버안보를 강화하기 위한 정책을 추진 중이다. 우리나라도 국가 사이버안보 전략을 2019년과 2024년에 각각 수립했지만, 국내 법률 제정은 아직 이루어지지 않고 있다.

미국은 일찍이 2003년에 「안전한 사이버공간을 위한 국가 전략」을 발표했고, 2024년에는 「국가 사이버안보 전략 이행계획」을 발표했다. 국가안보라는 일반적인 목표를 가진 국토안보부 내의 기존 조직은 「2018년 사이버안보 및 기반시설 안보국 법」에 따라 사이버안보와 기반시설 안보라는 더 구체적인 임무를 수행하는 조직으로 전환되었다. 「2022년 핵심 기반시설 사이버사고 보고법」에서는 민간에 보고의무를 부과하는 등 시기별로 다양한 사안에 대처하고 있다.

EU도 2018년에는 이른바 「EU 사이버안보법」이라고 불리는 EU 규정 제2019/881호(Regulation (EU) 2019/881)를 제정했고, 2020년에는 「EU 사이버안보 전략」을 발표했다. 이후 2024년에는 「사이버 연대법(안)」과 「사이버 복원력법(개정안)」을 제안하는 등의 노력을 기울이고 있다.

일본 역시 2014년 「사이버시큐리티 기본법(サイバーセキュリティ基本法)」을 제정하여 2015년부터 시행했다. 2021년에는 「사이버안보 전략」을 발표하여 사이버공격에 대한 안전 확보 및 우방국과의 협력 강화 추진을 천명했다. 특히 일본이 2022년 발표한 「국가안전보장전략」에는 일본은 공격받기 전 상대

방을 무력화한다는 내용의 '능동적 사이버 방어' 전략이 제시되어 있다.

우리나라는 비록 법률은 아니지만 2020년에 제정되고 2024년에 개정된 대통령령인 「사이버안보 업무규정」이 있다. 법률로는 2001년에 제정되고 2024년에 개정된 「정보통신기반 보호법」 등 분야별로 사이버안보 관련 법률이 있다.

이러한 배경에서 본고는 주요국의 사이버안보 관련 법률과 정책을 조사하고 분석함으로써, 우리나라가 사이버안보 관련 정책과 법률을 마련할 때 도움이 될 시사점을 찾고자 한다. 이 과정에서 조사하고 분석한 내용과 시사점은 우리 정부에 도움이 될 뿐 아니라 우리 기업이 해외 시장에 진출할 때도 참고가 될 것이다.

지금까지 사이버안보 분야의 다양한 주제에 대해 많은 기관과 연구자가 수행한 연구가 있다. 본 연구가 기존 연구와 비교했을 때 갖는 차별성은 본격적인 조사와 분석에 앞서 사이버안보의 개념을 정리하고 국제적 논의에서의 쟁점을 식별한 점에서 찾을 수 있다. 또한 여기서 식별된 쟁점을 바탕으로 주요국의 사이버안보 관련 전략과 법률의 동향을 조사하는 과정에서, 기존 연구에서 다루어지지 않은 최신의 진전 상황도 갱신하여 기록했다. 끝으로 본고는 주요국 사이버 정책을 통상법의 시각에서 분석한 점에서도 차별성이 있다. 구체적으로 사이버안보 조치가 통상에 영향을 미칠 때, 어떤 통상협정의 어떤 규정이 어떻게 적용될 수 있는지를 분석했다. 사이버안보 조치는 상품무역, 서비스 무역, 투자, 무역 관련 지식재산권 보호 등 통상의 다양한 분야에서 논란이 된다.

먼저 상품무역에 영향을 미칠 수 있는 사이버안보 조치는 미국 상무부가 2024년 2월 29일 발표한 커넥티드 카(connected car, ICT 기술을 이용하여 다른 차량 또는 교통 및 통신 기발 시설과 양방향 소통이 가능한 자동차)에 대한 국가안보 우려 조사 및 관련 규제 계획을 예로 들 수 있다.[1] 커넥티드 카의 운전자 감시 체계를 이용해 탑승자의 대화를 도청하거나 차량 자체를 제어할

1) 미국 상무부 홈페이지(2024), "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles"(검색일: 2024. 8. 6.).

수 있다는 점을 미국 당국은 우려한다.[2]

사이버안보 조치는 서비스 무역에도 영향을 미친다. 2024년 4월 바이든 미국 대통령은 중국에 본사를 둔 바이트댄스(ByteDance)가 틱톡의 미국 사업권을 270일 이내에 매각하지 않으면 미국 내 앱스토어에서 퇴출하는 내용의 이른바 틱톡 금지법안에 서명했다.[3] 틱톡 측은 미국 헌법이 보장한 표현의 자유가 침해되었다며 미국 법원에서 다투었으나, 2024년 12월 7일 워싱턴 D.C. 항소 법원은 틱톡 금지법이 합헌이라고 결론 내렸다.[4]

2. 연구 목적과 범위

이 연구의 목적은 주요국의 사이버안보 정책을 살펴보고 우리나라에 대한 시사점을 도출하는 것이다. 이 연구는 주요국의 사이버안보 정책을 본격적으로 살펴보기에 앞서, 사이버안보란 무엇이며 사이버보안과는 무엇이 다른지 개념부터 정리한다. 사이버안보에 관한 국제적인 논의 동향은 어떠한지 살펴보고, 여기서 식별된 쟁점을 바탕으로 주요국의 정책을 조사했다. 주요국의 정책은 사이버안보 전략과 법률로 나누어 조사하고 분석했다. 주요국의 사이버안보 실행에 대한 조사에서 얻은 정보를 바탕으로 우리나라가 사이버안보 전략과 법률을 개선해 나갈 때 참고할 시사점을 도출했다.

이 연구에서 우리나라가 사이버안보 전략과 법률을 마련할 때 참고가 될 시사점을 도출하기 위해 조사 대상으로 삼은 주요국은 미국, EU, 일본으로 제한했다. 물론 사이버공간에서 해킹 등 사이버 위협의 배후 또는 주체라는 추정을 받는 국가도 연구한다면 우리나라와 기업이 대응하는 데 도움이 될 것이다. 그

2) "US expected to propose barring Chinese software in autonomous vehicles"(2024. 8. 6.).
3) 「틱톡, 강제매각법 美서 위헌소송 제기」(2024. 5. 8.).
4) 「美법원 "틱톡금지 합헌…내달 19일까지 미국內 사업권 팔아야"」(2024. 12. 7.).

러나 이러한 연구는 후속 연구를 위해 남겨두고, 이 연구에서는 연구의 목적에 집중하기 위하여 조사 대상 국가의 범위는 필요 최소한으로 줄이고, 사이버안보의 개념과 특성 및 사이버안보 조치에 대한 통상법적 분석 등 근본적인 문제에 연구 역량을 할애했다.

또한 사이버안보 조치가 통상에 영향을 미칠 때, 조치국이 안보상 예외를 주장한다면 인정될 수 있는지, 그리고 인정되기 위한 구체적인 조건은 무엇인지를 검토하는 것도 이 연구의 주요한 목적 중 하나이다. 이를 위해 안보상 예외를 다룬 WTO 판정례를 분석한다. 한편 한·미 FTA 등 일부 FTA에는 어떤 분쟁에 대해 분쟁 당사국이 필수적 안보에 관한 규정이 적용된다고 주장하면 중재판정부는 해당 사건에 이 규정이 적용된다고 판정해야 한다는 각주가 포함되어 있다. 이는 WTO 협정의 안보 예외 규정에는 없는 내용이다. 이 연구에서는 이러한 한·미 FTA의 각주가 갖는 의미가 무엇인지 검토한다. 특히 같은 형식과 문언이 포함된 FTA 등이 적용된 투자분쟁에서 이 문제를 다룬 판정례를 분석했다.

본고의 구조는 다음과 같다. 제2장에서는 사이버안보의 개념과 국제적 논의에서의 쟁점을 정리한다. 이를 바탕으로 제3장에서는 주요국의 사이버안보 정책을 전략과 법률의 두 측면에서 조사하고 분석하여 우리나라에 대한 시사점을 도출한다. 제4장에서는 사이버안보 조치에 대한 국제통상법 적용 가능성을 분석했다. 최근 등장한 디지털 통상협정에 사이버안보 조항은 있는지, 내용은 무엇이며 법적 구속력은 있는 것인지 등을 살펴본다. 그다음으로는 FTA와 WTO의 순서로 사이버안보 조치가 어떤 규정에 위반될 수 있는지, 위반된다면 안보예외를 주장하여 인정받을 수 있는 조건은 무엇인지 분석한다. 마지막으로 결론인 제5장에서는 본문에서 한 조사와 분석의 결과를 요약 및 정리하고 우리나라에 대한 시사점을 도출했다.

제2장 사이버안보 개념과 국제적 논의

주요국 사이버안보 정책에 대한 본격적인 조사와 분석에 앞서, 사이버안보의 개념을 명확히 하고 사이버안보 규범의 국제적 논의를 살펴봄으로써 사이버안보 분야의 주요 쟁점을 파악한다.

1. 사이버안보의 개념

가. 정의

'안보(安保)'는 '안전보장(安全保障)'을 줄여 이르는 말인데, 편안히 보전되거나 편안히 보전함을 뜻한다.[5] 국가안보라는 개념 아래에는 군사안보, 에너지안보, 경제안보 등 분야별 안보 개념이 있을 수 있고, 사이버안보도 이와 같은 국가안보의 하위 개념 중 하나로 볼 수 있다.

경제 분야의 안보에 관한 우리나라 기본법에는 경제안보에 관한 정의 규정이 있다. 이에 따르면 '경제안보'란 "국내외에서 발생하였거나 발생할 가능성이 있는 경제·통상·정치·외교적 상황 변화나 자연재해 등에도 불구하고 국내의 생산, 소비, 유통 등 국가 및 국민의 전반적인 경제활동에 필수적인 품목, 서비스, 기술 등이 원활히 유입되고, 부적절하게 해외로 유출되지 아니하도록 함으로써 국가의 안전보장이 유지되고 국가 및 국민의 경제활동에 지장이 초래되지 아니하는 상태"를 말한다.[6] 이러한 경제안보에 관한 우리나라 국내법의

5) 국립국어원 표준국어대사전 홈페이지(검색일: 2024. 10. 10.).

입법적 정의는 사이버안보의 개념을 파악하는 데 참고가 될 수 있다.

우리나라 국내법에는 사이버안보의 입법적 정의가 아직 없다. 다만 대통령령인 「사이버안보 업무규정」에서 사이버안보 그 자체의 정의는 아니지만, '사이버공격·위협'을 "해킹, 컴퓨터바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협"이라고 정의하고 있다.[7]

조약에서 사이버안보를 정의한 사례는 발견되지 않는다. 미국은 「2015년 사이버안보법(Cybersecurity Act of 2015)」에서 '사이버안보 목적'을 "사이버안보 위협 또는 안보 취약점으로부터 정보시스템 또는 정보시스템에 저장, 처리 또는 전송되는 정보를 보호"하는 것이라고 정의한다.[8] 외부 위협으로부터 정보시스템과 정보를 보호하는 것이 사이버안보의 개념일 수 있음을 시사한다.

EU 역시 2019년 「사이버안보법」 제2조에서 '사이버안보'를 "네트워크 및 정보시스템, 해당 시스템의 사용자 및 사이버 위협의 영향을 받는 기타 사람을 보호하는 데 필요한 활동"이라고 정의한다.[9] 미국과 마찬가지로 외부 위협이라는 요소가 포함되어 있다. EU의 정의가 미국과 다른 부분은 물적 기초를 미국이 정보시스템과 정보로 파악하는 것과 달리, EU는 네트워크 및 정보시스템으로 파악하는 점이다. 또한 EU는 미국이 정보시스템과 정보를 목적으로 규정한 것과 다르게, 해당 시스템의 '사용자' 및 사이버 위협의 영향을 받는 '기타 사람'을 보호하는 것을 목적으로 규정하여 인간 중심적인 면을 더 강조한 것으로 평가할 수 있다.

---

6) 「경제안보를 위한 공급망 안정화 지원 기본법(약칭: 공급망안정화법)」(시행 2024. 6. 27. 법률 제19828호, 2023. 12. 26., 제정) 제2조(정의).
7) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정) 제2조(정의).
8) 미국의 「2015년 사이버안보법(Cybersecurity Act of 2015)」 section 102(Definitions).
9) EUR-Lex 홈페이지(2021), "Regulation(EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA(the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation(EU) No 526/2013(Cybersecurity Act)(Text with EEA relevance)"(검색일: 2024. 12. 11.).

한편 일본은 2014년 「사이버보안 기본법」 제2조(정의)에서 '사이버시큐리티'를 "정보, 정보시스템, 정보 통신 네트워크의 안전성 및 신뢰 확보"라고 정의한다.[10] 이러한 일본 법률의 정의는 사이버안보보다는 사이버보안에 가까운 정의라고 생각된다.

이러한 내용을 바탕으로 볼 때, 사이버공격 또는 위협을 방어하여 적절한 기능이 보장되어야 할 사이버공간은 결국 '정보시스템'과 여기에 저장된 '정보'로 구성된다는 점을 알 수 있다. 따라서 이 연구에서는 사이버공간을 구성하는 그릇과 내용물이 각각 '정보시스템'과 이 정보시스템에 저장된 '정보'라고 파악하고, 주요국의 사이버안보 정책을 조사하고 분석한다.[11]

위의 내용을 종합하여, 이 연구에서는 '사이버안보(cybersecurity)'라는 용어를 '디지털화의 영향으로 국가 핵심 기반시설이 운영되는 안보의 중심이 된 사이버공간을 사이버공격 또는 위협으로부터 방어하여 적절히 기능하게 함으로써 국가와 국민의 안전이 보장되는 상태 또는 활동'으로 정의한다.[12] 짧게 말하면, 이 연구에서 사이버안보는 사이버공간의 안보이다.

나. 사이버보안과의 구별

사이버'안보'라는 용어는 사이버'보안'이라는 용어와 구별된다. 물론 사전적 정의에 따르면 '안보(安保)'는 '편안히 보전함'을 뜻하고, '보안(保安)'도 '안전을

10) e-gov 法令検索 홈페이지(2024), 「サイバーセキュリティ基本法」(검색일: 2024. 10. 11.).

11) 물론 우리나라의 「사이버안보 업무규정」은 "정보통신기기, 정보통신망 또는 이와 관련된 정보시스템"으로 규정하는 점에서 일본의 「사이버보안 기본법」과 같고, '정보통신기기'와 '정보통신망'으로 구분하지 않고 '정보시스템'만 규정한 미국의 「2015년 사이버안보법」과 차이가 있다. 이 연구에서는 정보시스템이 정보통신기기와 정보통신망을 포괄할 수 있는 개념으로 보고, 정보시스템과 정보라는 두 요소로 파악한다.

12) 이 연구에서 사용하는 사이버안보의 개념은 「공급망안정화법」 제2조(정의)에서 말하는 '경제안보' 개념과, 2024년 9월 1일 발표된 「국가 사이버안보 기본계획」에서의 '사이버공간 개념'을 참고하여 저자가 정리한 것임. 「경제안보를 위한 공급망 안정화 지원 기본법(약칭: 공급망안정화법)」(시행 2024. 6. 27. 법률 제19828호, 2023. 12. 26., 제정); 국가사이버안보센터, 「정부 합동 '국가 사이버안보 기본계획' 발표」(검색일: 2024. 9. 26.).

유지함'을 뜻하므로 큰 차이가 있다고는 할 수 없다. 특히 '보안'의 두 번째 뜻은 '사회의 안녕과 질서를 유지함'이므로 더욱 '안보'와 엄밀히 구별되기 어렵다.[13]

사이버안보, 사이버보안, 정보보호 등으로 언급되는 용어를 사이버보안이라는 용어로 통칭하면서도, 용어 사용의 다양성과 복잡성을 고려하여 단일한 개념으로 재정의하기보다는 포괄적 관점으로 접근하기도 한다.[14] 사이버보안이 디지털 시대의 핵심 기반인 동시에 국가안보에서 중요한 전략기술 부문이라는 점을 고려한 결과로, 연구의 목적에 따라서는 적절할 수 있다.

그러나 사이버'안보'와 사이버'보안'을 맥락에 따라 구별하여 사용할 필요가 있다. 사이버'안보'는 국가의 안전보장을 궁극적인 보호 법익으로 하는 개념인 반면,[15] 사이버'보안'은 비밀을 보호한다는 뜻으로 서로 구별되는 개념이다.[16] 물론 영어로는 'cybersecurity'라는 하나의 단어가 사이버안보와 사이버보안 양쪽 맥락에서 모두 사용된다. 그러나 이 용어를 우리말로 번역할 때 정확한 의미를 확인하고 구별하여 번역하는 것이 필요하다.[17]

국제연합(UN: United Nations)의 표준화 전문기구인 국제전기통신연합(ITU: International Telecommunication Union)은 'cybersecurity'를 "사이버 환경과 조직 및 사용자의 자산을 보호하는 데 사용할 수 있는 도구, 정책, 보안 개념, 보안 보호, 지침, 위험관리 접근 방식, 조치, 교육, 모범사례, 보증 및 기술의 총체"라고 정의한다. 그리고 "조직 및 사용자의 자산에는 연결된 컴퓨팅 장치, 인력, 기반시설, 애플리케이션, 서비스, 통신 시스템 및 사이버 환경에서 전송 또는 저장된 정보의 전체가 포함된다"라고 정의한다. 사이버안보의 목표는 가용성, 무결성(진정성과 부인 불가를 포함), 기밀성이라고 설명한다.[18] 이러한 정의는 사이버안보에 관한 것이라기보다는 사이버보안에 가까운

13) 국립국어원 표준국어대사전 홈페이지(검색일: 2024. 10. 10.).
14) 이재성 외(2023), p. 60.
15) 박노형(2014), p. 379.
16) 법제처 세계법제정보센터 홈페이지(2018), 「사이버안보법제 고찰」, p. 4(검색일: 2024. 10. 10.).
17) 위의 자료, p. 4.
18) ITU 홈페이지, "Definition of cybersecurity"(검색일: 2024. 7. 23.).

정의로 평가할 수 있을 것이다.

또한 우리나라 국방부의 「국방 사이버보안 위험관리 지시」는 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」 제21조에 따라 무기체계 및 전력지원 체계의 사이버보안 위험을 수명주기 관점에서 관리하기 위해 국방 사이버보안 위험관리의 추진, 운영, 관리 등에 필요한 사항을 규정하기 위한 목적으로 제정되었는데,[19] '사이버보안'을 "정보 및 시스템을 사이버 위협으로부터 보호하며 피해가 발생하면 이를 복구함으로써 정보의 기밀성·무결성·가용성을 보장하는 것"이라고 정의한다.[20] 정보 자체의 보호를 뜻하기 위해 '보안'이라는 용어를 사용한 예이다.

한편 사이버안보라는 개념은 '정보시스템'과 여기에 저장된 '정보'를 보호한다는 내용을 포함하지만, 그 자체를 보호하는 것이 목적이라기보다는 국가의 안전보장을 궁극적인 보호 법익으로 한다는 점이 중요하다. 사이버공간에서의 문제를 국가안보의 문제로 파악하면서, 사이버안보라는 용어가 점차 널리 사용되기 시작했다고 보는 견해가 있다.[21]

한편 사이버'안전'은 사이버'안보'보다 더 넓은 개념으로 보는 견해도 있다. 일반적인 사이버안전이 확보되지 않으면 민감하고 특정적인 사이버안보도 지켜질 수 없기 때문이라는 점을 이유로 든다.[22] 나아가 '보안'과 '안전'의 개념이 서로 다르다는 견해도 있다. '보안(Security)'은 다양한 환경에 존재하는 가치 대상을 우연적 또는 의도적 범죄행위(보안 위험)로부터 보호하여, 질서와 안녕을 유지하는 활동(보안대책)을 뜻한다. 반면 '안전(Safety)'은 단순히 위험이 생기거나 사고가 날 염려가 없는 상태를 뜻하는 것이므로, 보안에는 있는 적극적 의미가 안전에는 내포되어 있지 않은 차이가 있다는 견해이다.[23] 그러나 우리나라의 대통령 훈령인 「국가사이버안전관리규정」에서는 '사이버안전'을

19) 「국방 사이버보안 위험관리 지시」(시행 2024. 4. 12. 국방부기타 제15호, 2024. 4. 12., 제정) 제1조(목적).
20) 「국방 사이버보안 위험관리 지시」(시행 2024. 4. 12. 국방부기타 제15호, 2024. 4. 12., 제정) 제2조(정의).
21) 김상배(2018), p. 77.
22) 법제처 세계법제정보센터 홈페이지(2018), 「사이버안보법제 고찰」, p. 4(검색일: 2024. 10. 10.).
23) 「미래 안전사회 조성을 위한 보안개념 정리 필요성과 향후 과제」(2024. 8. 30.).

"사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태"라고 정의한다.[24] 적극적 의미가 내포된 용어로서 '안전'이라는 용어를 사용한 예로 보인다. 용어의 통일적인 사용을 위해 논의를 계속하여 정비해 나갈 필요가 있다.

안보상 조치의 통상법적 저촉 여부를 분석하는 본 연구에서는 사이버안보와 사이버보안을 구별하지 않고 포괄하여 통칭하는 개념을 사용하기는 어렵다. 따라서 이 연구에서는 위에서 이미 언급한 '사이버안보(cybersecurity)'의 정의를 사용하고자 한다. 이 정의에 따르면 사이버안보는 "사이버공격 또는 위협을 방어하여, 다양한 경제·사회·문화 활동이 영위되는 자유민주주의의 근간이며 국가 핵심 인프라가 운용되는 안보의 중심인 사이버공간이 적절히 기능하게 함으로써 국가와 국민의 안전이 보장되는 상태"를 뜻한다.

더불어 사이버'안보'는 국가의 안전보장을 궁극적인 보호 법익으로 하는 개념이므로 비밀을 보호한다는 뜻인 사이버'보안'과는 구별되지만, 사이버보안이 확보되지 않으면 결국 사이버안보까지 위협받는다. 그러므로 사이버안보가 사이버보안을 포함하는 관계라고 봐야 한다.

2. 사이버안보 규범에 관한 국제적 논의

사이버안보 규범에 관한 국제적 논의의 기원은 1988년 인도가 UN 총회 결의안을 제안한 것에서 찾을 수 있다. 핵, 전자공학, 컴퓨터, 레이저 등 새로운 기술 발달로 안보 환경이 변화하고 있으므로, 관련 문제에 대한 공통된 인식을 바탕으로 문제 해결을 위한 공동의 노력을 가능하게 할 작업을 시작해야 한다는 주장이었다. 이에 따라 1988년 12월 7일 UN 총회 결의 제43/77호가 채택되었다. 이 결의는 미래의 과학 및 기술 발전, 특히 군사적 적용 가능성이 있는

24) 「국가사이버안전관리규정」(시행 2013. 9. 2. 대통령훈령 제316호, 2013. 9. 2., 일부개정) 제2조(정의).

발전을 추적하고 국제안보에 미치는 영향을 평가하여 1990년 제45차 총회에서 보고서를 제출할 것을 UN 사무총장에게 요청했다.[25] 1990년 10월 17일 UN 사무총장이 UN 총회에 제출한 보고서가 선정한 기술 분야에는 정보 기술이 핵, 우주, 물질, 생명 기술과 더불어 포함되었다.[26] UN 총회는 UN 사무총장이 제출한 보고서에 주목하여, 국제사회가 기술변화의 본질과 방향을 따르는데 더 나은 위치에 있어야 하고, UN이 이러한 목적을 위한 촉매가 될 수 있다는 점에 동의했다. 또한 '과학 및 기술의 발전과 국제안보에 미치는 영향'이라는 항목을 제47차 회의의 임시 의제에 포함하기로 했다.[27]

나아가 러시아는 1998년 9월 30일 '국제안보 차원에서 정보 통신 분야의 발달'이라는 제목의 결의안 초안이 첨부된 서한을 UN 사무총장에게 발송했다. 여기서 정보 무기(information weapons)의 발명으로, 한 국가가 다른 국가의 정보 자원과 시스템을 훼손하는 동시에 자국의 기반시설을 보호하는 정보전쟁(information war)이 등장했다고 언급했다. 따라서 국제안보 차원에서 정보 통신 분야의 발달에 관하여 UN 차원의 논의가 필요하다고 주장했다.[28] 러시아가 제안한 결의안 초안은 1999년 1월 4일 UN 총회에서 채택되었다.[29]

비록 위의 UN 결의안 제53/70호는 표결 없이 총의로 채택되었지만,[30] 이 결의안을 논의하는 과정에서 사이버안보에 관한 견해 대립이 드러났다. 미국을 중심으로 한 서방 자유민주 국가와 러시아와 중국을 중심으로 한 상하이협력기구(SCO: Shanghai Cooperation Organization) 회원국 사이에 이견이 노출된 것이다.[31]

---

25) UN 홈페이지(2024a), "The Role of Science and Technology in the context of International Security and Disarmament"(검색일: 2024. 10. 15.).
26) United Nations General Assembly(1990a), UN Doc. A/45/560(검색일: 2024. 10. 15.).
27) United Nations General Assembly(1990b), UN Doc. A/RES/45/60(검색일: 2024. 10. 15.).
28) United Nations General Assembly(1998), UN Doc. A/RES/54/49(검색일: 2024. 10. 15.).
29) *Ibid.*
30) UN 디지털도서관 홈페이지(2024), "Developments in the field of information and telecommunications in the context of international security: resolution/adopted by the General Assembly"(검색일: 2024. 10. 15.).
31) Tikk-Ringas(2012), "Developments in the Field of information and telecommunication in the context of international security: Work of the UN first Committee, 1998~2012," pp.

표 2-1. 1999년 UN 총회 결의 채택 과정에서 드러난 양 진영의 견해 대립

구분	미국 등 서방 자유민주 국가	러시아와 중국 등 상하이협력기구 회원국
국제정보안보의 개념	· 국제정보안보의 개념에서 안보는 '정보통신기반시설'만 포함해야 · 표현의 자유 원칙에 따라 '정보'는 국제정보안보의 개념에서 제외해야	· '정보통신기반시설'과 '정보'에 대한 위협의 제거와 안정성 촉진이 국제정보안보의 개념이 되어야 · 정보 자체도 무기(정보 무기)임.
정보 무기와 정보 전쟁의 개념	· 정보 무기와 정보 전쟁 미언급 · 정보 무기 관련 군축 및 비확산 논의 반대	· 정보 무기의 잠재적 위험성은 대량 살상 무기에 비견될 수 있음.
국제법적 규제의 명백한 필요성	· 민간과 군사 분야의 정보 기술 발전에 대한 국제법적 규제의 명백한 필요성 부정 · 정보 기술의 군사적 적용에는 무력 충돌법 적용 가능	· 민간 및 군사 분야의 정보 기술 발전에 대한 국제법적 규제의 명백한 필요성 인정
제1위원회의 역할	· 국제 평화와 안전에 관련된 정보안보의 일반적 측면을 다루는 제한적 기능 수행	· ICT 기술의 군사, 테러, 범죄 목적 사용을 포함한 광범위한 위협을 해결할 수 있는 적절한 포럼

자료: Tikk-Ringas(2012), "Developments in the Field of information and telecommunication in the context of international security: Work of the UN first Committee, 1998~2012," pp. 4-5(검색일: 2024. 10. 15.)의 내용을 바탕으로 저자가 표로 정리.

UN 총회 결의안이 채택된 1999년 1월 이후부터 2001년까지 미국 및 서방 국가와 중국 및 러시아 두 진영 사이의 견해 대립으로 논의가 진전되지 못했다. 이에 러시아는 2001년에 정보 안보 분야의 위협 및 이에 대응할 수 있는 협력 조치를 연구할 정부 전문가 그룹을 조직할 것을 제안했다.[32]

가. UN 정부 전문가 그룹

UN 정부 전문가 그룹(GGE: Group of Governmental Experts)[33]은 UN 총회 결의 제56/19호에 따라 2004년에 처음 설치되었다. 위 결의 제4항의 내용

4-5(검색일: 2024. 10. 15.).

32) 박노형, 정명현(2018), p. 46.

33) UN 정부 전문가 그룹의 정식 명칭은 "국제안보 차원에서 정보 통신 분야의 발전에 관한 정부 전문가 그룹(UNGGE: United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security)"임.

은 UN 총회가 사무총장에 대하여, 공평한 지리적 분포에 기초하여 사무총장 본인이 임명하는 인사로 설립될 정부 전문가 그룹의 도움을 받아, 정보 안보 분야의 존재와 잠재적 위협 및 그 해결을 위한 협력 방안을 고려하여, 전 세계적 정보통신 시스템의 보안 강화를 목적으로 하는 국제적인 개념에 관한 연구를 수행하고 그 결과에 대한 보고서를 제60차 총회에 제출할 것을 요청한다는 것이다.[34]

표 2-2. UN 정부 전문가 그룹 회의 결과

회차	보고서 채택	의의	참여국 수	우리나라 참여
1	×	국제정보안보 관련 핵심적인 사항에 대한 이견 확인	15	○
2	○	취약성, 협력 조치 등 국제안보 차원에서 정보 통신 분야의 발달을 다룸	15	○
3	○	국가의 ICT 기술 사용에 국제법이 적용됨을 명시	15	×
4	○	자발적, 비구속적 규범이 평화에 대한 위험을 낮출 수 있음을 명시	20	○
5	×	중국 등 비서방 국가들, 무력공격에 준하는 사이버공격에 대한 자위권 발동과 사이버전에 대한 국제인도법 적용에 반대 의사 표시	25	○
6	○	국제인도법을 명시적으로 언급	27	×

주: 보고서 채택은 UNGGE 회의에서 총의로 채택한 것을 뜻함. UNGGE에서 채택된 보고서는 UN 총회에 제출됨.
자료: Tikk-Ringas(2012), "Developments in the Field of information and telecommunication in the context of international security: Work of the UN first Committee, 1998~2012," pp. 6-7(검색일: 2024. 10. 15.); 박노형, 정명현(2018), pp. 49~50; United Nations General Assembly(2010), UN Doc. A/65/201; United Nations General Assembly(2013), UN Doc. A/68/98; United Nations General Assembly(2015a), UN Doc. A/70/174; United Nations General Assembly(2021a), UN Doc. A/76/135(모든 자료의 검색일: 2024. 8. 15.).

사이버안보에 관한 관심이 높아지면서, UNGGE를 구성하는 국가의 수도 증가했다. 제1차부터 제3차까지는 15개 UN 회원국의 정부 전문가가 참여했으나, 제4차 때는 20개국, 제5차에는 25개국의 정부 전문가가 참여했다. UN 안전보장이사회(이하 "안보리")를 구성하는 5개 상임이사국 전문가는 제1차부터 제5차까지 모든 UNGGE에 참여했다.[35] 우리나라는 제3차와 제6차 UNGGE에는 참여하지 못했다.[36]

34) United Nations General Assembly(1999), UN Doc. A/RES/53/70(검색일: 2024. 8. 15.).
35) 박노형, 정명현(2018), pp. 46~47.
36) 박노형, 박주희(2021), p. 176.

UNGGE의 법적 성격을 말하자면, 비록 명칭은 정부 '전문가' 그룹이지만 실은 정부 '대표' 그룹이다. UNGGE 회의에서 정부 전문가의 발언은 개인적 전문성과 소신을 바탕으로 한 것이라기보다는 일반적인 UN 회의와 같이 자국의 입장을 대표하는 것이다.[37]

1) 제1차 UNGGE

2004년 설치된 제1차 UNGGE는 상당한 견해 차이로 총의에 이르지 못하여 보고서를 채택하지 못했다. 국제정보안보와 관련한 핵심적인 사항에 대해서도 참여국 사이에 서로 다른 개념을 가지고 있었다. 제1차 UNGGE의 의장을 맡은 러시아 외교관은 국제정보안보 문제는 국제사회가 직면한 새롭고 민감한 문제인데, 이를 고려하기 위한 시간은 매우 제한적이었다고 경과보고에서 언급했다.[38]

2) 제2차 UNGGE

2009년 설치된 제2차 UNGGE는 총의로 보고서를 채택하고 이를 UN 총회에도 제출했다. 제2차 UNGGE 보고서는 서론, 위협과 위험 및 취약성, 협력조치, 제안까지 크게 네 부분으로 구성되었다.

제2차 UNGGE의 보고서가 제1차 UNGGE의 보고서와 달리 채택에 성공한 원인에 대해, 미국을 중심으로 한 서방 진영도 UNGGE에서의 사이버안보 논의가 진행되어야 할 필요성을 비로소 인식했기 때문이라고 보는 견해가 있다. 서방 진영의 인식 변화 배경은 2007년 러시아로 추정되는 세력이 에스토니아에 대규모 사이버 조작을 한 것, 그리고 2008년 러시아가 조지아 침공 때 사이버공격도 병행한 것이라고 본다.[39]

---

37) 박노형, 정명현(2018), p. 52.
38) Tikk-Ringas(2012), "Developments in the Field of information and telecommunication in the context of international security: Work of the UN first Committee, 1998~2012," pp. 6-7(검색일: 2024. 10. 15.).
39) 박노형, 정명현(2018), p. 48.

표 2-3. 제2차 UNGGE 보고서의 구성과 내용

구분	주요 내용
서론	ICT 기술이 사회 모든 부분에서 사용되어 복잡한 상호 연결성을 나타냄.
	ICT 기반시설을 민간이 소유 또는 운영 시 혼란의 원인, 가해자의 신원 확인 곤란
위협과 위험 및 취약성	이중용도의 성격을 가진 ICT 기술은 전자상거래의 기초이자 동시에 안보 위협도 가능
	중요 기반시설에서 ICT 기술의 사용이 증가함에 따라 취약성이 커졌음.
	ICT 기술에 악의적 기능이 있다면, 상거래에 대한 신뢰가 약화하며 안보에 영향을 미침.
	국가마다 안보를 위한 ICT 기술 기준이 다르면, 글로벌 네트워크의 취약성이 증가하고 각국 법률과 관행의 차이로 안전하고 탄력적인 디지털 환경 구축에 어려움 겪을 것
협력 조치	상호 연결된 네트워크 관련 위험은 한 국가의 노력으로 해결 곤란. 국제적 공동 대응 필요
	현재의 보안 격차를 줄이기 위해 개발도상국의 역량구축 노력에 대한 지원 필요
제안	ICT 기술 사용에 관한 국제 규범 논의 계속, 각국의 법률, 정책, 모범사례 정보 교환 제안

자료: United Nations General Assembly(2010), UN Doc. A/65/201(검색일: 2024. 8. 15.).

3) 제3차 UNGGE

2012년 설치된 제3차 UNGGE도 총의로 보고서를 채택하고 이를 UN 총회에도 제출했다. 제3차 UNGGE 보고서는 서론, 협력, 규범 제안, 신뢰 형성 조치, 역량 구축 조치, 결론까지 여섯 부분으로 구성되어 있다. 이 중에서 규범 제안에 관한 세 번째 부분을 살펴본다. 제목은 '국가의 책임 있는 행위에 관한 규범, 규정 및 원칙에 관한 제안(Recommendations on norms, rules and principles of responsible behaviour by States)'이다. 주요 내용은 다음과 같다. 국가의 ICT 기술 사용에 현행 국제법에서 파생된 관련 규범을 적용하는 것이 국제 평화, 안보 및 안정에 대한 위험을 줄이기 위한 필수적인 조치이다. 국제법, 특히 UN 헌장은 평화와 안정을 유지하고 개방적이고 안전하며 평화롭고 접근하기 쉬운 ICT 기술 환경을 촉진하는 데 필수적이다. 주권에서 유래하는 국제규범과 원칙은 국가가 ICT 기술 관련 활동을 수행하는 데에 적용되며, 자국 영역 내의 ICT 기술 기반시설에 대한 관할권에도 적용된다. ICT 기술 보안을 해결하기 위한 국가의 노력은 「세계인권선언」 및 기타 국제기구에 명시된 인권과 기본적 자유에 대한 존중과 함께 이루어져야 한다. 국가는 자신에게

귀속되는(attributable) 국제 위법 행위(internationally wrongful acts)에 따른 국제적 의무를 이행해야 한다. 국가는 국제 위법 행위를 저지르기 위해 대리인(proxy)을 사용하지 않아야 한다. 국가는 자국의 영토가 비국가 행위자가 ICT를 불법적으로 사용하는 데 사용되지 않도록 노력해야 한다.[40]

제3차 UNGGE 보고서의 특징은 사이버공간에 국제법이 적용된다는 원칙을 처음 확인한 점이다. 또한 노력 의무로 규정된 한계는 있으나 국가의 영역관리 책임을 인정했다.

4) 제4차 UNGGE

2014년 설치된 제4차 UNGGE도 총의로 보고서를 채택하고 이를 UN 총회에도 제출했다. 제4차 UNGGE 보고서는 서론, 현존 및 임박한 위협, 규범 제안, 신뢰 형성 조치, 국제협력 및 역량구축, ICT 기술 사용에 대한 국제법 적용 방안, 결론 및 제안까지 일곱 부분으로 구성되어 있다. 이 중에서도 규범 제안에 관한 부분에는 자발적, 비구속적 규범(voluntary, non-binding norms)의 사용이 국제 평화에 대한 위험을 낮출 수 있다는 점을 재확인한다는 내용이 포함되어 있다. 다음으로 ICT 기술 사용에 대한 국제법 적용 방안에 관한 부분에도 중요한 내용이 포함되어 있다. ICT 기술 사용에 대한 국제법 적용 방안을 고려할 때 가장 중요한 국제법의 원칙은 주권 평등이다. 국가는 자국 영역 내의 ICT 기술 기반시설에 대한 관할권을 가진다. 국가는 ICT 기술을 사용하는 데 있어서 국제법, 주권 평등, 평화적 수단에 의한 분쟁 해결, 다른 국가의 내정 불개입 등의 원칙을 준수해야 한다. 국가는 인권과 기본적 자유를 존중하고 보호하기 위해 국제법에 따른 의무를 준수해야 한다.[41]

제4차 UNGGE 보고서의 의의는 사이버공간에 국제법이 적용된다는 원칙을 재확인한 것에서 찾을 수 있다. 이 원칙은 제3차 UNGGE 보고서에서 처음 인정

40) United Nations General Assembly(2013), UN Doc. A/68/98(검색일: 2024. 8. 15.).
41) United Nations General Assembly(2015a), UN Doc. A/70/174(검색일: 2024. 8. 15.).

했다. 제4차 UNGGE 보고서는 여기서 더 나아가 ICT 기술 사용에 대한 국제법 적용 방안을 고려하기 시작했다.

사이버공간에 국제법이 적용된다는 원칙은 이후 2015년 9월 미국 오바마 대통령과 중국 시진핑 주석의 정상회담, 같은 해 10월 미국 오바마 대통령과 한국 박근혜 대통령의 정상회담에서도 재확인되었다. 같은 해 11월 G20 정상회의에서도 이 점은 재확인되었다.[42]

그러나 제4차 UNGGE 보고서 채택 과정에서 대립한 두 진영 사이에 견해 차이가 노출되었다. 그중 하나가 자위권이다. 의장 초안에는 사이버 무력공격에 대한 UN 헌장 제51조에 따른 자위권 행사가 자세히 규정되었고, 자위권 행사를 허용하자는 미국의 제안도 포함되어 있었다. 그러나 중국과 러시아는 사이버공간이 평화적으로 이용되어야 한다는 이유를 들어 사이버공간에서의 자위권 행사를 반대했고, 받아들여지지 않을 때는 보고서 채택을 결렬시키겠다는 의사를 밝혔다. 프랑스와 독일도 비판적인 태도를 보였다. 이에 따라 초안에서 자위권에 관한 부분은 삭제되었다. 그러자 미국 역시 자위권이 포함되지 않으면 보고서 채택을 결렬시키겠다는 의사를 밝혔다. 이에 중국과 러시아는 유연한 접근이 가능하다고 밝히고, 최종 보고서에 자위권 인정을 우회적으로 포함하기로 합의하였다. 구체적으로는 UN 헌장이 "전체적으로(in its entirety)" 적용된다고 규정한 것이다.[43]

5) 제5차 UNGGE

2016년 설치된 제5차 UNGGE는 2017년 6월 23일 네 번째 회의에서 일부 참가국들의 반대로 보고서 채택에 실패했다. 중국을 중심으로 한 비서방 국가들이 무력공격에 준하는 사이버공격에 대한 자위권 발동과 사이버전에의 국제인도법 적용에 반대했기 때문이다.[44]

---

42) 박노형, 정명현(2018), p. 50.
43) 박노형, 정명현(2016), pp. 180~181.
44) 박노형, 정명현(2018), pp. 49~50.

6) 제6차 UNGGE

2019년에 설치된 제6차 UNGGE는 2021년 총의로 보고서를 채택하고 이를 UN 총회에도 제출했다. 제6차 UNGGE 보고서는 서론, 현존 및 임박한 위협, 규범 제안, 국제법, 신뢰 형성 조치, 국제협력 및 역량구축, 결론 및 제안까지 일곱 부분으로 구성되어 있다. 국제법에 관한 부분에서 무력 충돌(armed conflict) 상황에서만 국제인도법(International Humanitarian Law)이 적용된다고 규정했다. 국제인도법은 인도(humanity), 필요성(necessity), 비례성(proportionality), 그리고 구별(distinction)의 원칙을 포함한다는 점도 규정했다. 그러나 이러한 원칙을 국가의 ICT 기술 사용에 언제 그리고 어떻게 적용할지에 관한 추가 연구가 필요하다고 강조했다.[45]

제6차 UNGGE의 의의는 국제인도법을 보고서에 명시적으로 언급한 점에서 찾을 수 있다. 제4차 UNGGE 보고서에서는 러시아, 중국, 쿠바 등이 국제인도법 언급에 반대했기 때문에, 국제법의 핵심 원칙들만 언급한 바 있다.[46] 또 제5차 UNGGE 보고서 채택 결렬의 원인 중 하나가 사이버전에의 국제인도법 적용이었다. 따라서 국제인도법의 적용에 관한 한, 제6차 UNGGE는 제4차 UNGGE의 성과를 넘어섰고, 제5차 UNGGE 결렬의 원인이 된 사안을 극복했다고 평가할 수 있다.

다만 제5차 UNGGE 보고서 채택 결렬의 또 다른 원인은 자위권이었는데, 제6차 UNGGE도 명시적으로 자위권을 언급하지는 못하고 제4차 UNGGE와 마찬가지로 UN 헌장이 "전체적으로(in its entirety)" 적용된다고 규정했다.[47]

---

45) United Nations General Assembly(2021a), UN Doc. A/76/135(검색일: 2024. 8. 15.).
46) 박노형, 박주희(2021), p. 179, p. 183.
47) United Nations General Assembly(2021a), UN Doc. A/76/135(검색일: 2024. 8. 15.).

나. 개방형작업그룹

2017년 제5차 UNGGE 보고서 채택이 결렬되자, 2018년 10월 러시아는 개방형작업그룹(OEWG: Open-ended Working Group)의 설치를 제안했다. UN 총회는 이 제안을 받아들여 2019년부터 OEWG가 활동할 것을 결정했다. 또한 제74차 회기의 임시 의제로 "국제안보 차원에서 정보 통신 분야의 발전"을 포함할 것을 결정했다.[48] 러시아가 OEWG의 설치를 제안할 때, UNGGE의 공식 명칭에 사용된 "국제안보 차원에서 정보 통신 분야의 발전(Developments in the field of information and telecommunications in the context of international security)"이라는 문언을 그대로 사용한 것이다. 이에 따라 제6차 UNGGE는 "국제안보 차원에서 사이버공간에서 책임 있는 국가 행동의 촉진(Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)"에 관한 GGE로 변경되었다.[49]

OEWG는 UN의 후원 아래 광범위한 참여를 염두에 두고 제안되었기 때문에,[50] UN 회원국이라면 모두 참여할 수 있었다. 이러한 측면은 UN 사무총장이 공평한 지리적 분포에 기초하여 참여국을 정하는 UNGGE와 개방성에서 차이가 있다. 다만 OEWG가 개방성은 더 높지만, 효율적인 회의 진행이 가능할지에 대한 의문이 제기되었다. 약 20명으로 구성된 UNGGE도 집중적인 논의가 어려운 점이 문제점으로 지적되었기 때문이다.[51]

1) 제1차 OEWG

2019년에 설치된 제1차 OEWG는 광범위한 UN 회원국의 참여로 인해 원활한 회의 진행에 의문이 제기되었음에도, 총의로 보고서를 채택했고 이를 UN 총

48) United Nations General Assembly(2018), UN Doc. A/RES/73/27(검색일: 2024. 8. 15.).
49) 박노형, 박주희(2021), p. 176.
50) United Nations General Assembly(2018), UN Doc. A/RES/73/27(검색일: 2024. 8. 15.).
51) 박노형, 박주희(2021), pp. 177~178.

회에도 제출했다.[52] 다만 국제법에 관한 내용이 많지 않고, 그마저도 UNGGE 보고서의 내용에 비해 실질적으로 진전된 내용은 없는 것으로 평가된다.

사이버공간에서 UN 헌장을 포함한 국제법의 적용 가능성과 분쟁의 평화적 수단을 통한 해결이 재확인되었다. 또한 국가 사이의 의견 교환과 UN에서의 논의를 위한 '특정 국제법 주제(specific topics of international law)'를 식별함으로써, 사이버공간에서의 국제법 적용 방안에 관한 공통의 이해가 깊어질 수 있다고 결론 내렸다. 역량구축을 위한 중립적이고 객관적 노력이 추가적으로 필요하다는 결론도 내렸다.[53]

표 2-4. 개방형작업그룹 회의 결과

회차	기간	의의	참여국 수	우리나라 참여
1	2019~21	UNGGE 2013년과 2015년 보고서의 결론 재확인(2021. 3.)	62	○
2	2021~25	2024년 7월 8차 회의까지 개최	진행 중	○

주: 제1차 개방형작업그룹 참여국 수는 보고서 초안에 의견 등을 제출한 국가를 기준으로 산정한 것임.
자료: United Nations General Assembly(2021b), UN Doc. A/AC.290/2021/CRP.2; United Nations General Assembly(2021c), UN Doc. A/75/240; OEWG 홈페이지(2024), "Open-Ended Working Group on Information and Communication Technologies"(모든 자료의 검색일: 2024. 8. 15.).

2) 제2차 OEWG

2020년 12월 31일 UN 총회는 2021년부터 2025년까지 활동할 제2차 OEWG를 설치한다는 내용의 결의안을 채택했다. 참여한 UN 회원국들이 필요하다고 간주하면, 하위 주제별 그룹을 구성하거나 기업과 비정부기구 및 학계를 포함한 다른 이해관계자가 참여하도록 결정할 수 있다는 내용이 포함되었다.[54] 제2차 OEWG는 2021년부터 활동을 시작하여, 2024년 7월 8차 회의까지 개최했다.[55]

52) United Nations General Assembly(2021b), A/AC.290/2021/CRP.2(검색일: 2024. 8. 15.).
53) 박노형, 박주희(2021), p. 178.
54) United Nations General Assembly(2021c), UN Doc. A/75/240(검색일: 2024. 8. 15.).
55) OEWG 홈페이지(2024), "Open-Ended Working Group on Information and Communication

한편 이러한 OEWG와 비교할 때 UNGGE는 2021년 제6차 UNGGE 이후 현재까지 새로운 활동이 없는 것으로 보인다. 제6차 UNGGE가 2019년에 설치되고 2021년 총의로 보고서를 채택하여 UN 총회에도 제출한 이후, 제7차 UNGGE를 설치한다는 UN 총회의 결의는 아직 없다. 따라서 당분간은 OEWG가 사이버안보 분야의 국제적 논의의 주요 장이 될 것으로 전망된다.

3. 사이버안보 분야의 주요 쟁점

가. 사이버공간의 별도 영역성 인정 여부

1) 사이버공간 별도 영역성 인정 견해

미국 등 서방 국가는 사이버공간(cyberspace)을 별도 영역으로 인정하는 태도를 보이는 것으로 평가할 수 있다. 국가 차원에서 이 문제에 대해 명시적으로 견해를 밝힌 사례는 찾기 어렵지만, 국제사회 논의, 국내 전략과 법률 동향 등에서 나타나는 국가실행을 바탕으로 추정할 수 있다. 위에서 이미 살펴본 것처럼, UN에서 UNGGE의 정식 명칭은 "국제안보 차원에서 정보 통신 분야의 발전에 관한 정부 전문가 그룹"이었다. 그러나 2018년 러시아가 OEWG의 설치를 제안하면서 "국제안보 차원에서 정보 통신 분야의 발전에 관한"이라는 문언을 사용하자, 제6차 UNGGE부터 "국제안보 차원에서 사이버공간에서 책임 있는 국가 행동의 촉진에 관한 정부 전문가 그룹"으로 공식 명칭을 변경했다.[56] 명칭에 '사이버공간'이라는 용어를 사용한 것이다. 물론 UNGGE에 참여한 전문가는 출신 국가의 입장을 공식적으로 대표할 자격을 부여받지 않았다. 한편 미국은 2003년 자국의 사이버안보 전략을 최초로 발표했는데, 명칭에

Technologies"(검색일: 2024. 8. 15.).
56) 박노형, 박주희(2021), p. 176.

'사이버공간'이라는 용어가 포함되었다. EU도 2020년 사이버안보 전략을 발표하는 보도자료에서 '사이버공간'이라는 용어를 사용했다. 일본 역시 2015년 발표한 「사이버보안 전략」에서 '사이버공간'이라는 용어를 사용했다. 우리나라도 2019년 「국가 사이버안보 전략」은 물론 2024년 「국가 사이버안보 전략」에서도 '사이버공간'이라는 용어를 사용했다.

사이버공간의 별도 영역설을 지지하는 견해는 학계에도 있다. 이때는 사이버공간을 ICT 기술을 사용하여 상호 의존적이고 상호 연결된 네트워크를 통해 정보를 생성, 저장, 수정, 교환 및 활용하기 위해 전자 장치와 전자기 스펙트럼을 사용하는 독특하고 고유한 특성을 가진 정보 환경 내에 있는 전 지구적 영역으로 본다.[57] 국내 학계에도 비슷한 견해가 있다. 물리력 중심의 전통 사회와 달리, 데이터 전송을 통해 비물리적으로 연결되고 제어되는 현대사회가 하나의 사이버 생태계라고 보는 시각이다.[58]

2) 사이버공간 별도 영역성 부정 견해

러시아, 중국 등은 사이버공간이 별도 영역이 아니라는 태도를 보이는 것으로 평가할 수 있다. 국가 차원에서 이 문제에 대해 명시적으로 견해를 밝힌 사례는 찾기 어렵지만, 국제사회 논의, 국내 전략과 법률 동향 등에서 나타나는 국가실행을 바탕으로 추정할 수 있다. 러시아가 2018년 제안하여 설치된 제1차 OEWG가 채택하고 총회에 제출한 보고서에는 '사이버공간'이라는 용어가 등장하지 않는다. 대신 'ICT 기술의 사용(use of information and communications technology)'이라는 용어를 사용한다.[59]

---

57) Ishikawa and Kryvoi(2003), p. 8. 원문을 소개하면 다음과 같다. "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

58) 정준현(2021), 안종만, 안상준 편저, p. 47.

59) United Nations General Assembly(2021b), UN Doc. A/AC.290/2021/CRP.2(검색일: 2024. 8. 15.).

사이버공간의 별도 영역설을 부정하는 견해는 학계에도 있다. 이 견해는 사이버공간이 육지, 바다, 하늘, 우주에 이은 다섯 번째의 독립된 영역이 아닌 단지 관념상의 공간일 뿐이라고 주장한다. 부정설이 제시하는 몇 가지 근거는 다음과 같다. 첫째, 사이버공간은 장비나 인력을 배치할 수 없으므로, 바다나 우주 등과 같은 다른 네 영역과 달리 실존하지 않는 가상의 공간이라는 것이다. 사이버공간의 목표물에 대해 조치하려면 결국 이것이 저장된 시스템을 목표로 할 수밖에 없는데, 시스템에 대한 조치는 더 이상 사이버공간에서의 행위라 보기 어렵다는 것이다. 둘째, 사이버공간은 네 영역 어딘가에 위치한 대상에 영향을 미치는 수단일 뿐 별도의 영역이 아니라는 것이다. 하늘과 우주조차도 비록 모호할 수는 있지만 경계가 있다. 그러나 사이버공간은 경계가 있다기보다는 오히려 나머지 네 영역 중 어딘가에 위치할 뿐이라는 말이다.[60]

사이버공간을 유지하는 데 필수적인 서버, 통신망, 전력망 등은 하나 또는 그 이상의 국가 영역, 공해(high seas), 또는 우주 등 물리적인 공간 어딘가에는 위치할 수밖에 없으므로, 부정설의 지적도 타당한 측면이 있다. 그러나 사이버공간의 목표물에 대해 조치하려면 결국 이것이 저장된 시스템을 목표로 할 수밖에 없다는 주장에는 동의하기 어렵다. 시스템 자체를 파괴하기 위한 공격 외에도, 정보를 훼손·멸실·변경·위조하여 무결성을 침해하는 방식으로 조치의 목적을 달성할 가능성이 있기 때문이다.

3) 국가실행

사이버공간이 다른 영역과 독립된 별도 영역이 아니라는 견해를 UNGGE 또는 OEWG에서 유지하는 국가도, 자국에서의 국가실행을 보면 사이버공간을 별도의 영역으로 인정하는 듯한 모습도 발견된다. 예컨대 중국 국무원은 2029년 7월 24일 '신시대 중국 국방'이라는 백서를 발표했는데, 이 문서에는 중국의 우주와 더불어 '사이버공간'에서의 국가안보 이익을 수호한다는 표현이 있다.[61]

60) Delerue(2020), pp. 11-12.

사이버공간의 별도 영역성을 인정하는 견해를 취하는 미국은 이와 부합하는 국가실행을 보인다. 미국 국방부는 2009년 사이버사령부 창설을 공식 발표했다.[62] 미국 사이버사령부는 '사이버공간 영역(cyberspace domain)'에서 진화하는 위협에 대응하고, 전 세계에서 적대국의 능력을 약화한다고 소개한다.[63]

UN 총회도 제목에 '사이버공간'이라는 용어를 사용한 결의안을 2019년과 2020년에 각각 채택했다.[64] 이 두 결의안의 제목은 같은데, '국제안보 맥락을 고려한 사이버공간에서의 책임 있는 국가 행동 증진'이 그것이다.

우리 국회에서도 사이버안보에 관한 법률안으로 2020년과 2021년에 각각 제안되었다가 회기 만료로 폐기된 두 법안 모두 '사이버공간'을 정보통신망의 정보 처리 영역으로 정의하는 규정을 두었다.[65] 대한민국 대통령실 역시 2024년 9월 1일 「국가 사이버안보 기본계획」을 발표했는데, 여기서 "대한민국의 사이버공간은 다양한 경제·사회·문화 활동이 영위되는 자유민주주의의 근간이며, 국가 핵심 인프라가 운용되는 안보의 중심"이라고 언급하면서, '사이버공간'이라는 용어를 사용한다.[66]

나. 사이버공간에 대한 국제법 적용 여부

사이버공간의 별도 영역성 인정 여부는 사이버공간에 대한 국제법 적용 여부에도 영향을 미친다. 사이버공간이 육지, 바다, 하늘, 우주와 같은 별도 영역이라고 인정하게 되면, 이러한 사이버공간에 국제법이 적용된다고 인정할 가능

61) 중화인민공화국 중앙인민정부 홈페이지(2019), 「新时代的中国国防」(검색일: 2024. 8. 15.).
62) 「美국방부, 사이버사령부 창설 공식 발표」(2009. 6. 24.).
63) 미국 사이버사령부 홈페이지(2024), "U.S. Cyber Command CODE"(검색일: 2024. 8. 15.).
64) United Nations General Assembly(2019), UN Doc. A/RES/74/28; United Nations General Assembly(2020), UN Doc. A/RES/75/32(모든 자료의 검색일: 2024. 8. 15.).
65) 대한민국 국회 의안정보시스템(2020), 「[2101220] 사이버안보 기본법안(조태용 의원 등 27인)」; 대한민국 국회 의안정보시스템(2021a), 「국가사이버안보법안(김병기 의원 등 13인)」(모든 자료의 검색일: 2024. 8. 19.).
66) 국가사이버안보센터(2024), 「정부 합동 '국가 사이버안보 기본계획' 발표」(검색일: 2024. 9. 26.).

성이 크다. 물론 별도 영역이라고 하여 반드시 국제법만이 적용되는 것은 아니다. 우주 공간에는 국제법이 적용된다. 그러나 바다는 국제법이 적용되는 공해(high seas)도 있지만, 국내법이 적용되는 영해(territorial sea)도 있다. 사이버공간이 별도의 영역이라고 보는 견해는 사이버공간의 성격을 우주와 비슷한 것으로 보고, 국제법이 적용된다고 주장한다. 반면 사이버공간이 별도 영역이 아니라고 보는 견해에 따르면 국제법은 적용되지 않는다. 시스템 등 물리적인 ICT 기반시설 또는 정보가 저장된 서버의 위치가 국내이면 국내법이, 외국이면 외국법이 적용될 뿐이다.

1) 사이버공간에 대한 국제법 적용 긍정 견해

미국을 중심으로 한 서방 자유민주 국가는 전시인지 평시인지와 무관하게 현행 국제법이 사이버공간에 그대로 적용될 수 있다고 주장한다.[67] 학설 중에도 사이버공간에 적용될 국제법이 현재는 없으므로, UN 헌장과 국제관습법이 적용된다고 보는 견해가 있다.[68] 이 견해에 따르면 사이버공간에 국제법이 적용된 결과는 다음 여섯 가지로 정리된다.

첫째, 다른 국가에 대한 국가의 사이버공격은 무력을 사용하는 것이므로 (ⅰ) 중대한 재산 피해, (ⅱ) 인명 사상, (ⅱ) 핵심 기반시설의 기능에 대한 심각한 방해를 초래하거나 초래할 합리적인 가능성이 있는 경우, UN 헌장 제2조 제4항[69]과 국제관습법에 따라 금지된다. 다만 여기서 '초래할 합리적인 가능성이 있는 경우(reasonably likely to cause)'는 예방적 자위권(anticipatory self-defense) 등을 인정하는 견해에서 요구하는 조건을 충족해야 한다. 이에 대해서는 후술한다.

---

67) 박노형, 김효권(2021), pp. 64~65.
68) Roscini(2014), p. 115.
69) UN 헌장 제2조. "국제연합과 그 회원국은 제1조에 명시된 목적을 추구함에 있어서 다음의 원칙에 따라 행동한다. 4. 모든 회원국은 자국의 국제 관계에 있어서 어떠한 국가의 영역 보전 또는 정치적 독립에 반하거나 국제연합의 목적에 부합하지 않는 그 밖의 어떠한 방식의 무력 위협이나 행사도 삼간다."

둘째, 중대한 인명 및 재산상 피해 등을 초래하지 않는 사이버공격은 타국에 대한 '위법한 간섭(unlawful intervention)'에는 해당하지만, '무력 사용(use of force)'은 아니다.

셋째, 사이버 부당 이용(cyber exploitation)은 국제법에 따라 금지되지 않는 때에는 타국에 대한 부당한 간섭 또는 주권 침해에 해당하겠지만, UN 헌장 제2조 제4항에 따른 무력행사는 아니다.[70]

넷째, UN 헌장 제2조 제4항 및 국제관습법에 따른 사이버 자위권 또는 물리적 자위권(kinetic self-defense)은 국가 또는 비국가 행위자의 사이버공격이 '규모와 효과(scale and effects)'의 측면에서 무력공격에 해당해야 행사될 수 있다.[71]

표 2-5. 사이버 작전과 기타 사이버 관련 활동의 다양한 유형

구분	타국 주권 침해	간섭	무력 사용
중대한 재산 피해 또는 인명 사상을 초래하거나 초래할 합리적인 가능성이 있는 사이버공격			○
국가 핵심 기반시설(NCI: National Critical Infrastructure)의 기능에 대한 심각한 훼손으로 물리적 피해를 초래하지 않는 사이버공격			○
기타 사이버공격		○	
사이버 부당 이용(cyber exploitation)	○		
타국의 반군 단체에 사이버 무기 및 훈련 제공			○
제3국에 대한 침략행위에 사용될 목적으로 자국의 사이버 기반시설을 타국의 처분에 놓이게 하는 조치			○

자료: Roscini(2014), p. 116.

여기서 말하는 '규모와 효과(scale and effects)'라는 무력공격 판단 기준은 니카라과 사건에서 국제사법재판소(ICJ: International Court of Justice) 재판부가 제시했다. 무력공격(armed attack)은 정규군이 국경을 넘어 행하는

70) Roscini(2014), p. 115.
71) *Ibid.*

행동뿐 아니라, 비정규군을 파병하여 정규군에 의해 수행된 실제 무력공격(actual armed attack)에 해당할 만큼 중대성(gravity)을 갖는 무력 행위를 수행한 것도 포함한다고 재판부는 판단했다. 규모와 효과에 따라 단순한 국경 사건(mere frontier incident)이 아니라 무력공격으로 분류될 수 있다고 설명했다. 그러나 무기 및 병참 제공 또는 기타 지원은 무력공격에 해당하지 않고, 타국의 내정 또는 외무에 대한 간섭에 이를 수는 있다고 재판부는 덧붙였다.[72]

글상자 2-1. 보복(retorsion)

'보복(retorsion)'은 적법하나 비우호적인 성격의 조치를 말한다. 외교관계 단절, 여행금지, 원조 중단 등 다양한 형태가 있을 수 있다. 피해국은 위법한 활동에 책임이 있는 상대국에 보복 조치를 할 수 있다. 보복은 적법한 행위뿐 아니라 국제법 위반 행위 또는 무력공격에 대해서도 할 수 있다. 그러므로 위법한 조치이지만 위법성이 배제(조각)되는 '대항조치(countermeasures)'와 구별된다.[73]

자료: Delerue(2020), pp. 424-425, p. 437.

글상자 2-2. 대항조치(countermeasures)

'대항조치(countermeasures)'는 국제법상 중요성에도 불구하고 일반적인 정의는 없다. 다만 학설 중에는 "피해국이 타국의 위법행위를 중지시키고 또 이미 발생한 위법행위에 대한 완전한 손해배상을 얻어내기 위하여 의무 위반국에 부담하는 국제 의무를 이행하지 않는 것"을 뜻한다고 보는 견해가 있다. 무력 사용에 대한 일반적 금지가 없던 전통 국제법에서는 '복구(reprisal)'라는 용어로 사용되던 개념이다. 무력 사용이 금지된 현대 국제법을 고려하여 UN 국제법 위원회(ILC: International Law Commission)가 국가책임초안 제3부 제2장(대항조치)을 규정하면서 '대항조치'라는 중립적인 표현을 선택한 것이다. 다만 국가책임초안 제50조 제1항 c호에서는 여전히 '복구'가 언급된다. 대항조치이든 복구이든 자력구제(self-help)의 한 형태이다.[74] 대항조치의 법적 성격은 불법적이지만 평화적인 일방적 대응이다. 구체적인 형태의 예로는 특정 조약의 적용을 중지시키는 조치, 경제 제재를 부과하는 조치 등을 들 수 있다.[75] 대항조치는 처벌이나 보복이 아니라, 국제 의무를 위반하는 상대방 국가가 국제 의무를 준수하도록 유도하기 위한 목적으로 취해져야 한다. 따라서 상대국이 위법행위를 중지하고 손해를 배상하면 대항조치는 즉시 종료되어야 한다.[76]

자료: 김대순(2022), p. 798; Delerue(2020), p. 433, p. 437.

72) Military and Paramilitary Activities in and against Nicaragua(Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, para. 195.
73) Delerue(2020), pp. 424-425.
74) 김대순(2022), p. 798.

다섯째, 무력공격에 해당하지 않는 사이버 작전(cyber operation)에 대한 자위권은 사건의 축적(accumulation of events)과 예방적 자위권(anticipatory self-defense)에 관한 원칙에 따른 한계 내에서만 행사될 수 있다. 나머지 경우에 대한 합법적인 대응 수단으로는 보복(retorsion) 조치, 무력공격의 수준 아래의 사이버공격을 포함하는 비강제적인 대항조치(non-forcible countermeasures), UN 안보리 회부가 있다.[77]

표 2-6. 사이버 작전에 대한 구제 조치

구분	보복 (retorsion)	비강제적 대항조치	자위권 행사	UN 안보리 회부
사이버 부당 이용(cyber exploitation)	○	○		○
중대한 재산 피해 또는 인명 사상을 초래하는 무력공격의 규모와 효과에 이르는 사이버공격	○	○	○	○
국가 핵심 기반시설(NCI: National Critical Infrastructure)의 기능에 대한 심각한 훼손으로서 무력공격의 규모와 효과에 이르는 사이버공격	○	○	○	○
무력공격에 이르지 않는 사이버공격	○	○		○

자료: Roscini(2014), p. 116.

여섯째, 사이버 작전(cyber operation)에 대한 자위권(self-defense) 행사를 주장하기 위한 증거의 기준은 물리적 무력공격에 대한 자위권 행사 주장에 사용되는 증거의 기준과 다르지 않다. 일반적으로 '명백하고 설득력 있는 증거(clear and convincing(or compelling) evidence)'가 필요하다.[78] '명백하고 설득력 있는 증거'라는 기준은 1957년 노르웨이 공채 사건 본안 판결에서 ICJ 재판부가 언급했다.[79]

75) Delerue(2020), p. 433, p. 437.
76) 김대순(2022), p. 801.
77) 위의 자료.
78) Roscini(2014), p. 116.
79) Certain Norwegian Loans(France v Norway), Merits, Judgment, 6 July 1957, ICJ Reports 1957, Separate Opinion of Judge Sir Hersch Lauterpacht, p. 39.

2) 사이버공간에 대한 국제법 적용 부정 견해

러시아와 중국을 중심으로 한 상하이협력기구 회원국은 사이버공간에는 이 영역의 특수한 성격을 고려한 별도의 조약 또는 국제관습법 등 국제법이 적용되어야 한다고 주장한다.[80] 대표적인 예로는 러시아와 중국 등이 2011년 UN 총회에 제출한 '정보 안전을 위한 국제 행동 규약(International Code of Conduct for Information Security)'을 들 수 있다. 이 규약은 총 13개 규정으로 구성된다. 사이버공간이라는 용어를 사용하지 않고, '정보 공간(information space)'이라고 표현했다. 또한 이 공간이 국제 공역이 아니라 각국이 이 공간에 대해 배타적 관할권을 갖는다는 점을 강조하는 모습을 보인다. 예컨대 규약 제1항은 "자발적으로 이 규약에 서명한 각국은 주권, 영토보전, 정치적 독립에 관하여 UN 헌장을 준수한다"고 규정한다. 또한 제5항은 "각국은 ICT 상품 및 서비스에 대한 국가의 독립적 통제권을 저해하지 않도록 노력해야 한다"고 규정한다.[81]

앞서 살펴본 것과 같이, 2016년 설치된 제5차 UNGGE가 2017년에 보고서 채택에 실패했던 원인은 미국을 중심으로 한 서방 진영과 러시아와 중국을 중심으로 한 비서방 진영 사이의 견해 대립이 주된 원인이었다. 이러한 견해 차이는 2018년 OEWG 설치가 제안되고 2019년부터 활동을 개시한 배경이라고 평가할 수도 있다.

다. 사이버 무력공격에 대한 예방적 자위권 인정 여부

1) 사이버 무력공격과 예방적 자위권의 개념

'공격'은 전쟁을 뜻하는 무력 충돌(armed conflict)에 적용되는 국제법에서 사용하는 개념이다.[82] '공격'과 '무력공격'은 국제법에서 서로 다른 의미를 갖는 전문 용어이다. 국제법에서 국가가 무력을 사용하는 것을 규율하는 법제는

80) 박노형, 김효권(2021), p. 65.
81) United Nations General Assembly(2015b), UN Doc. A/69/723(검색일: 2024. 10. 17.).
82) 박노형, 정명현(2014), pp. 66~67.

크게 무력 사용법(jus ad bellum - law on the use of force)과 무력 충돌법(jus in bello - law in war)으로 나뉜다. 무력 사용법은 무력 충돌이 존재하지 않는 평시에 국가의 무력 사용이 언제 적법할 수 있는지 판단하는 법체계이다. 그리고 자위권은 무력 사용법의 대표적인 규율 대상이다. 한편 무력 충돌법은 무력 충돌이 이미 존재하는 상황에서 지켜져야 할 법규이다. 무력 충돌법의 주요 내용에는 비례성의 원칙, 민간인 보호 등이 있다. 그러므로 자위권에 관해서는 '사이버공격'이 아닌 '사이버 무력공격'이라는 용어를 사용해야 한다.

니카라과 사건에서 ICJ 재판부는 정규군이 아닌 무장단체가 다른 국가의 영토에 파견되어 정규군과 같은 규모와 효과로 작전을 수행했다면, 단순한 국경사건(frontier incident)이 아닌 무력공격(armed attack)으로 분류될 수 있다고 보았다. 하지만 무기와 병참의 제공 및 기타 지원의 형태는 무력공격에 포함되지 않는다고 판단했다.[83] 비록 니카라과 사건에서 사이버 무력공격이 다루어진 것은 아니지만, 규모와 효과를 강조한 점에서 사이버 무력공격에 대해서도 시사점이 있다.

사이버 무력공격(cyber armed attack)에 대한 입법적 정의는 국제조약은 물론, 우리나라를 포함한 주요국 국내법에서도 발견하기 어렵다. 「탈린 매뉴얼(Tallinn Manual)」에도 이 용어에 대한 정의 규정은 없지만, 규칙 제73조에서 "'사이버 무력공격'이 발생했거나 임박하였으면 자위권이 발생한다"고 규정한다. 사이버 무력공격에 사용된 위성을 물리적으로 파괴하기 위해 위성을 겨냥한 방어 무기를 사용하는 사례를 들 수 있다.[84] 그러므로 사이버 무력공격도 전통적인 무력공격과 마찬가지로 자위권 발생의 근거가 된다고 볼 수 있다.

여기서 「탈린 매뉴얼」은 사이버전(cyber warfare)에 관한 대표적인 국제법 연구로서 2013년에 출간되었다. 연구와 출간을 에스토니아의 수도 탈린시(市)

83) Military and Paramilitary Activities in and against Nicaragua(Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, para. p. 195.
84) Schmitt(2016), p. 274, p. 415.

에 있는 NATO 합동 사이버 방위센터(CCDCOE: Cooperative Cyber Defence Centre of Excellence)가 지원했다. 개인 자격으로 참여한 국제법 전문가와 기술전문가 25명이 3년 동안 참여하여, 95개 규칙(rule)과 각 규칙에 대한 주석(commentary)을 마련했다. 미국 사이버사령부, 국제적십자위원회, 그리고 NATO도 참관단을 파견했다. 그러나 탈린 매뉴얼도 한계가 있다. 법적인 효력이 있는 법 문서가 아닐뿐더러, NATO와도 공식적으로는 무관하다. 또한 미국, 영국, 독일, 그리고 캐나다의 군사 교본(manual)만을 참조하여 작성된 것으로서 서방 편향성이 있다는 지적을 받는다.[85]

더불어 우리나라 대통령령인 「사이버안보 업무규정」은 '사이버공격'에 관한 정의 규정이 있으므로 참고할 만하다. 물론 위에서 살펴본 것과 같이 사이버공격과 사이버 무력공격은 국제법에서는 엄연히 다른 용어이지만, 국내 법령 등에서는 이러한 측면보다는 구체적인 규율 대상에 집중한다. 우리나라 「사이버안보 업무규정」은 '사이버공격'을 "해킹, 컴퓨터바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위"라고 정의한다.[86] 이 규정의 목적은 「국가정보원법」에 따른 국가정보원의 직무 중 사이버안보 업무의 수행에 필요한 사항을 규정하는 것이다.[87] 이 직무에는 「군사기밀 보호법」에 규정된 죄에 관한 정보, 국제 및 국가 배후 해킹조직 등 사이버안보 관련 정보 등이 포함된다.[88] 「사이버안보 업무규정」은 정보통신 '기기'도 대상으로 포함한 점을 특징으로 볼 수 있다. 사이버공격의 효과 또는 결과가 비단 사이버공간 내의 것으로 제한될 필요가 없음을 알 수 있다.

다음으로 예방적 자위(anticipatory self-defense)는 무력공격이 예상되면 아직 무력공격이 발생하지 않았다고 하더라도 조치하는 것을 뜻한다.[89] 예방적

85) 박노형, 정명현(2014), pp. 68~69.
86) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정) 제2조(정의).
87) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정) 제1조(목적).
88) 「국가보안법」(시행 2024. 1. 1. 법률 제17646호, 2020. 12. 15., 전부개정) 제4조(직무) 제1항.
89) DeWeese(2015), pp. 83-84.

자위와 관련된 여러 용어와 개념이 명확하게 정의되고 상호 포함관계가 확립되었다고 보기는 어렵다. 그래도 본고에서는 예방적 자위권은 아래와 같은 세 가지 하위 유형의 자위권을 포함하는 상위 개념으로 정의한다.

첫째, 차단적 자위(interceptive self-defense)는 무력공격은 착수되었지만 아직 결과가 발생하지 않았을 때 행사하는 자위 조치이다. 이때 무력공격은 임박한 것이 아니라 실재하는 것이다. 1941년 12월 일본군이 미국 하와이의 진주만 군항을 공격하고자 전투기를 출격시킨 후에, 미군 항공기나 함정이 군항이 공격받기 전에 해상에서 이를 격퇴하는 것을 가정한 가상 사례를 들 수 있다. 이때라면 일본에 무력공격을 가한 미국의 행위에 책임을 묻기 어렵다.[90]

둘째, 선제적 자위(pre-emptive self-defense)는 아직 개시되지 않았으나 임박한(imminent) 무력공격을 대상으로 하는 자위 조치이다. 여기서 '임박한'은 "최초 무력공격에 합리적으로 인접(reasonably proximate to the initial armed attack)"해야 한다는 뜻이다.[91]

셋째, 방지적 자위(preventive self-defense)는 장래에 발생할 가능성이 있는 무력공격을 대상으로 하는 자위 조치이다. 미래의 불확실한 시점(at some indeterminate point in the future)에 발생할 수 있는 무력공격을 대상으로 한다고 보는 견해가 있다.[92] 방지적 자위권은 자위권의 범위를 지나치게 확대하는 측면이 있으므로 인정하기 어렵다는 비판이 많다.

2) 예방적 자위권의 인정 근거

우선 국제조약이 예방적 자위권의 근거가 될 수 있는지 살펴본다. 자위권 등의 전통적인 일반 국제법 주제를 규율하는 일반적인 조약 중 대표적인 것으로는 UN 헌장을 들 수 있다. UN은 2011년 이후 회원국이 193개에 달하는 측면

90) Dinstein(2011), p. 203. 원문을 소개하면 다음과 같다. "reaction to an event that has already begun to happen even if it has not yet fully developed in its consequences."
91) DeWeese(2015), p. 88.
92) *Ibid.*, p. 86.

에서 보편적인 국제기구라고 볼 수 있기 때문이다.[93] 나아가 UN 헌장은 UN 헌장에 따른 의무와 그 밖의 국제협정상 의무가 상충하는 때에는 UN 헌장의 의무가 우선한다는 명시적인 규정까지 두고 있다.[94]

이러한 UN 헌장은 UN 회원국의 무력 사용을 포괄적으로 금지한 것으로 평가된다.[95] 유일한 두 가지 예외는 (ⅰ) 개별 또는 집단 자위권(제51조)과 (ⅱ) 안보리 결정(제39조)에 따른 집단적 안보 체제에서의 무력 사용이다.[96]

자위권에 관한 UN 헌장 제51조는 "무력공격이 발생하면(if an armed attack occurs)" UN 회원국이 UN 안보리가 국제 평화와 안보를 유지하는 데 필요한 조치를 취할 때까지 자국의 자위권 또는 집단 자위권을 행사하는 것을 금지하지 않는다.[97] 무력공격의 발생이라는 조건에서 '발생'이 현재 시제로 규정되어 있는 점과 UN 안보리의 조치가 있을 때까지 자위권 행사가 금지되지 않는 시간에 제한이 있는 점이 특징이다.

이러한 UN 헌장 제51조의 자위권 규정을 근거로 예방적 자위권이 허용되는지에 대해서는 학자들 사이에 견해가 대립한다. 먼저 예방적 자위권은 인정되지 않는다고 보는 견해는 제51조의 문언, UN 헌장의 대상과 목적, 준비 문서 등을 근거로 제시한다. 이에 따르면 UN 헌장의 목적 중 하나는 국가의 무력 사용을 가능한 한 UN의 통제 아래에 두는 것이었다. 따라서 자위권에 관한 국제관습법은 UN 헌장으로 대체되었다고 본다. 미국 조지워싱턴 대학의 스타니미르 알렉산드로프(Stanimir Alexandrov) 교수가 이러한 견해를 취하는 대표적인 학자

93) UN 홈페이지(2024b), "Growth in United Nations membership"(검색일: 2024. 11. 17.).
94) UN 헌장 제103조.
95) UN 헌장 제2조 제4항. "모든 회원국은 자국의 국제 관계에 있어서 어떠한 국가의 영역 보전 또는 정치적 독립에 반하거나 국제연합의 목적에 부합하지 않는 그 밖의 어떠한 방식의 무력 위협이나 행사도 자제해야만 한다(All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations)." 국문 번역본에는 "삼간다"라고 되어 있으나, 법정 의무(shall refrain)인 점을 고려하여 저자가 번역을 수정했음.
96) UN 헌장 제39조. "안전보장이사회는 평화에 대한 위협, 평화의 파괴 또는 침략행위의 존재를 결정하고, 국제 평화와 안보를 유지하거나 이를 회복하기 위하여 권고하거나, 제41조 및 제42조에 따라 어떤 조치를 할지 결정한다."
97) UN 헌장 제51조.

이다. 영국 옥스퍼드 대학의 이언 브라운리(Ian Brownlie) 교수, 이스라엘 텔아비브 대학의 요람 딘스타인(Yoram Dinstein) 교수, 미국 노트르담 대학교의 메리 엘렌 오코넬(Mary Ellen O'Connell) 교수도 이를 지지한다.[98]

표 2-7. UN 헌장 제51조

Charter of the United Nations Article 51	UN 헌장 국문본 제51조
Nothing in the present Charter shall impair the inherent right of individual or collective self-defence **if an armed attack occurs** against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.	국제연합 회원국에 대하여 **무력공격이 발생한 경우,** 이 헌장의 어떠한 규정도 안전보장이사회가 국제 평화와 안보를 유지하는 데 필요한 조치를 할 때까지 개별적 또는 집단적 자위의 고유한 권리를 침해하지 않는다.
Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.	자위권을 행사하면서 회원국이 취한 조치는 즉시 안전보장이사회에 보고되며, 이 조치는 이 헌장상 안전보장이사회가 국제 평화와 안보의 유지 또는 회복을 위하여 필요하다고 인정하는 조치를 언제든지 취할 안전보장이사회의 권한과 책임에 어떠한 영향도 미치지 않는다.

주: UN 헌장의 정본은 영어본, 프랑스어본, 스페인어본, 러시아어본, 중국어본 이상 5개임.
자료: 법제처 국가법령정보센터 홈페이지(2024), 「국제연합헌장 및 국제사법재판소규정」(검색일: 2024. 11. 17.).

이러한 견해와 달리 UN 헌장의 규정은 기존 국제관습법에서 인정되던 자위권의 내용에 어떠한 변경을 가하는 것이 아니라, 자위권 행사에 추가적인 안전장치를 제공하는 것뿐이라고 해석하는 견해도 있다. 이러한 견해를 취하는 대표적인 학자로는 영국 케임브리지 대학의 데릭 보웻(Derek W. Bowett) 교수를 들 수 있고, 미국 예일 대학교의 마이레스 맥두걸(Myres McDougal) 교수, ICJ 소장을 역임한 미국 존스 홉킨스 대학교의 스티븐 슈웨벨(Stephen Schwebel) 교수도 이를 지지한다.[99]

98) Eenma(2005), p. 4.

이렇듯 예방적 자위권이 UN 헌장에 따라 인정되는지에 대해 학설이 대립하는 가운데, ICJ는 예방적 자위권을 명시적으로 인정한 사례도 없고 부정한 사례도 없다. 자위권을 다룬 ICJ의 주요 판결로는 1998년 니카라과 사건(Nicaragua v. United States), 2003년 이란과 미국 사이의 석유 플랫폼 사건(Oil Platforms), 2006년 콩고민주공화국(DRC)과 우간다 사이의 콩고 영토 내 무력 활동 사건(Armed Activities on the Territory of Congo)을 들 수 있는데, 이 사건들에서는 예방적 자위권이 쟁점으로 부상하지는 않았다. 예컨대 니카라과 사건에서 ICJ는 "분쟁의 양 당사국은 무력공격이 이미 발생한 때의 자위권에 대해서만 다투었고, 무력공격의 임박한 위협에 대한 대응의 적법성의 문제는 제기되지 않았다. 따라서 이 문제에 대해서는 어떠한 견해도 표명하지 않는다"라고 언급했다.[100] 결국 예방적 자위권이 조약, 그중에서도 대표적인 조약이라 할 수 있는 UN 헌장에 따라 인정되는지는 명확하지 않다는 것이 결론이라 할 수 있다. 이를 다룬 ICJ 판정례가 없는 데다가 학설은 대립하기 때문이다.

다음으로 국제관습법이 예방적 자위권의 근거가 될 수 있는지 살펴본다. 예방적 자위권이 아닌 일반적 자위권에 대해서는 일찍부터 널리 인정되었다. 예컨대 1837년 미국과 영국 사이에 발생한 캐롤라인 호(the Caroline) 사건은 영국을 상대로 반란을 일으킨 캐나다 반군을 지원하던 미국 증기선 캐롤라인 호를 영국군이 공격한 사건이다. 영국이 자위권 행사에 따른 공격이었다고 주장하자, 미국 국무장관 대니얼 웹스터(Danial Webster)는 주미 영국 대사에게 보낸 서한에서 자위권 행사로 인정되기 위해 충족되어야 할 조건을 언급했다. 이것은 훗날 웹스터 공식(Webster Formula) 또는 캐롤라인 심사 기준(Caroline Test)으로 국제법 학계에서 불리며, 국제관습법에 따른 자위권으로

99) *Ibid.*, pp. 4-5.

100) Military and Paramilitary Activities in and against Nicaragua(Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, para. 194.

인정되기 위한 조건으로 자리 잡았다. 이에 따르면 자위권은 (ⅰ) 무력 사용의 필요성(necessity of the use of armed force)과, (ⅱ) 직면한 위협에 대한 비례성(proportionality to the threat being faced)이라는 두 가지 조건을 충족해야 한다.[101]

이러한 웹스터 공식 또는 캐롤라인 심사 기준을 실제 무력공격(actual armed attack), 즉 이미 개시된 무력공격에 대해서만 자위권이 인정된다고 좁게 해석한다면 예방적 자위는 허용되지 않을 것이다. 그러나 무력공격의 대상이 되는 국가가 지리적으로 대단히 좁은 국가여서 상대국의 무력공격이 성공적으로 마무리되기 전에 대응할 시간이나 기회가 거의 없을 때도 있을 수 있다. 또는 오늘날은 다양한 첨단 무기로 인해 매우 빠른 속도로 공격의 결과가 발생하는 점을 고려하면, 무력공격이 실제로 개시될 때까지 기다려 자위권을 행사하기보다는 임박한(imminent) 무력공격에 대해 예방적 자위권을 허용해야 한다는 주장이 설득력이 있을 수도 있다. 문제는 '합리적이고도 명백하게(reasonably and evidentially)' 임박한 무력공격이 있었는지에 대한 판단이다.[102]

이와 관련하여 임박성(imminence) 기준의 의미 등에 대한 학계의 견해 불일치는 여전하지만, 국제관습법에 근거해서는 선제적 자위권이 인정된다고 보는 학자가 대부분이라는 견해도 있다. 이 견해는 방지적 자위권에 대해 학계가 대체로 부정적인 태도를 보이는 것과 달리, 선제적 자위권에 대해서는 지지하는 견해가 다수라고 주장하며 십여 명 이상의 저명한 학자와 다양한 국제연구소 등의 입장을 근거로 제시한다.[103]

국제관습법에 따른 예방적 자위권에 대해 ICJ가 명시적으로 확인한 사례는 없다. 예컨대 콩고 영토 내 무력 활동 사건에서도 ICJ 재판부는 우간다가 예상되는 공격에 대한 무력 사용이 아니라고 주장한 점을 지적했다. 재판부는 니카라과 사건에서도 무력공격의 임박한 위협에 대한 대응의 적법성 문제가 제기되

101) Eenma(2005), p. 5.
102) Shaw(2017), pp. 866-867.
103) O'Meara(2022), pp. 8-9.

지 않아 이에 대한 의견 표명을 하지 않았음을 언급하면서, 이 사건에서도 의견 표명을 하지 않겠다고 밝혔다.[104]

비록 임박한 무력공격이 무엇을 의미하는지 논란은 있지만, 국제관습법에 근거하여 선제적 자위권이 인정된다는 견해가 더 유력한 것으로 보인다. 그러므로 예방적 자위권을 주장할 때는 이를 허용하는지 해석 논란이 있는 UN 헌장을 근거로 하기보다는 국제관습법을 근거로 하는 것이 유리할 것으로 보인다.

라. 사이버공간 관련 상당 주의 의무 적용 여부

1) 일반 국제법에서 국가의 영역관리 책임

국가의 영역관리 책임은 국가가 영토, 영해, 영공 등 자국의 주권이 미치는 영역을 상당한 주의를 다하여 관리하여, 다른 국가에 위해가 가해지지 않도록 예방하거나 적절한 조치를 해야 한다는 의무를 뜻한다. 이러한 의무의 법적 근거는 국제관습법이다. 국가의 영역관리 책임을 명시적으로 인정한 국제조약은 환경법 영역에서는 발견되지만, UN 헌장 등 보편적인 조약에서는 찾아보기 어렵다. 그러나 국제관습법에 따른 의무라는 점은 여러 사건에서 확인되었다. 예컨대 1928년 팔마스 섬(Island of Palmas) 사건에서 상설중재재판소(PCA: Permanent Court of Arbitration)는 국가의 영토주권에는 자국 영역 내에서 다른 국가의 권리를 보호해야 한다는 의무도 따른다고 언급했다. 여기서 다른 국가의 권리에는 영토에 대한 불가침, 자국민에 대해 주장할 수 있는 국가의 권리 등이 포함된다.[105] 또한 1949년 코르푸 해협(Corfu Channel) 사건에서 ICJ 재판부는 "다른 국가의 권리에 반하는 행위에 자국 영토가 사용되도록 허용하지 않을 모든 국가의 의무"가 인정된다고 보았다.[106]

---

104) Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, ICJ Reports 2005, para. 143.

105) Island of Palmas Case(United States v. Netherlands), Permanent Court of Arbitration, Arbitral Award, 2 RIAA 829(4 April 1928), p. 839.

이러한 국가의 영역관리 책임은 더 구체적으로는 위해 금지 원칙(no harm principle)과 예방 원칙(principle of prevention)과도 관련이 있다. 우선 위해 금지 원칙 관련, 캐나다 트레일 제련소의 가스가 미국 워싱턴주에 피해를 준 트레일 용광로(Trail Smelter) 사건에서 미국과 캐나다 양국의 합의로 설치한 임시 중재판정부(ad hoc arbitration)는 국제법 원칙에 따라 어떤 국가도 다른 국가에 손해를 입힐 수 있는 방식으로 영토를 사용하거나 사용을 허용할 권리가 없다고 결론 내렸다.[107] 이 판정에서 확인된 위해 금지 원칙은 국제환경법의 기본원칙을 규정한 1972년 스톡홀름 선언과 1992년 리우선언에 반영되었다.[108] 다음으로 예방 원칙 관련, 2010년 펄프 공장(Pulp Mill) 사건에서 ICJ는 예방 원칙은 자국 영역에 대한 국가의 상당 주의(due diligence) 의무에서 유래하며, 국제환경법 분야에서 국제관습법의 지위를 가진다고 언급했다.[109]

2) 사이버공간 관련 상당 주의 의무 적용 여부

일반 국제법에서 인정되는 '국가의 영역관리 책임' 또는 국제환경법 분야에서 인정되는 '국가의 상당 주의 의무'가 사이버공간에도 적용되는지는 중요한 의미가 있다. 피해국이 사이버공격을 한 개인 또는 단체의 배후에 있는 국가에 책임을 물으려면, (ⅰ) 사이버공격의 주체, (ⅱ) 그 배후국이 해당 개인 또는 단체를 지시 또는 통제했다는 사실을 증명하여 사인의 행위를 국가로 귀속시키는 것이 필요하다. 그러나 상당 주의 의무에 의하면, 어느 국가의 영역에서 사이버

106) Corfu Channel(United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment, ICJ Reports 1949(19 April 1949), p. 22. 원문을 소개하면 다음과 같다. "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."

107) Trail Smelter Case(United States of America v. Canada), Reports of International Arbitral Awards, vol. 3(1941), p. 1965.

108) 박노형, 김효권(2021), p. 68.

109) Pulp Mills on the River Uruguay(Argentina v. Uruguay), Judgement, ICJ Reports 2010, para. 101.

공격이 발생했는지만 증명하면 그 국가에 대해 피해국이 책임을 물을 수 있다. 상당 주의 의무는 국가 책임 귀속에 관한 법리보다 증명의 대상이 적고 난도 역시 상대적으로 낮다.[110]

이를 반영하듯, 「탈린 매뉴얼」 제6조는 국가가 자신이 통제하는 영토 또는 사이버 기초 설비가 다른 국가에 부정적인 결과 등을 초래하는 사이버 조작에 이용되는 것을 허용하지 않도록 상당한 주의를 다해야 한다고 규정한다.[111]

그러나 UN 등 국제사회에서의 논의는 순탄하지 않아 보인다. 국가가 자국 영역이 비국가 행위자가 국제적 위법행위를 하는 데 사용되지 않음을 보장하도록 "마땅히 노력해야 한다(should seek)"라는 문언은 제3차,[112] 제4차,[113] 제6차 UNGGE 보고서에 포함되었지만,[114] 모두 법적 의무는 아니다. 원인은 UNGGE 보고서에서 상당 주의를 법적 의무로 규정하는 안에 미국 등 일부 국가가 반대했기 때문이다. 사이버공격에 이용될 수 있는 사이버 기반시설이 많은 선진국으로서는 상당 주의 원칙이 법적 의무가 되었을 때 책임이 커질 것을 우려했다고 풀이된다. 그러나 이러한 미국 등의 입장은 고정불변이 아니라, 의무화 찬성으로 변화하고 있는 것으로 보인다.[115]

우리나라는 북한과 대치하고 있다는 특수성이 있다. 우리나라에 가해지는 사이버 위협의 출처는 상당 부분이 북한으로 추정된다. UN 안보리 보고서에 따르면, 2023년 북한 해커 집단이 암호화폐를 탈취한 사건은 총 17건이고 피해액은 7억 5,000만 달러(약 1조 원)에 달한다. 2024년 11월 우리나라 경찰도 2019년 암호화폐거래소 업비트를 해킹하여 보관 중이던 가상화폐 이더리움을 탈취한 주체가 북한 해커 집단이라는 점을 확인했다고 발표했다.[116]

---

110) 박노형, 김효권(2021), p. 75.
111) Schmitt(2016), p. 415.
112) United Nations General Assembly(2013), UN Doc. A/68/98(검색일: 2024. 8. 15.).
113) United Nations General Assembly(2015a), UN Doc. A/70/174(검색일: 2024. 8. 15.).
114) United Nations General Assembly(2021a), UN Doc. A/76/135(검색일: 2024. 8. 15.).
115) 박노형, 김효권(2021), p. 72.
116) 「이더리움 580억 탈취, 北 소행…"북한 어휘 '혈한 일' 발견"」(2024. 11. 21.).

그런데 북한이 인터넷에 접속하기 위해서는 위성 인터넷을 사용하지 않는 한, 중국 또는 러시아를 통할 수밖에 없다. 만약 북한이 중국 또는 러시아 등 제3국의 영토 내에 거점을 마련하고 해킹 활동을 한다면, 우리나라는 국제관습법에 따른 영역관리 책임 또는 상당 주의 의무를 근거로 해당 국가에 조치 및 재발 방지를 요구할 수 있다.

예컨대 2014년 11월 말, 미국의 영화제작사인 소니 픽처스 엔터테인먼트는 북한 체제를 풍자하는 영화의 개봉을 앞두고 해킹 공격을 받았다. 2014년 12월 19일 FBI는 해킹의 배후가 북한 정부라는 조사 결과를 공개했다. 특정 코드, 암호화 알고리즘, 데이터 삭제 방법, 손상된 네트워크의 측면에서 2013년 한국의 은행과 언론사를 상대로 한 해킹과 비슷하다는 점을 근거로 제시했다. 또한 공격에 사용된 데이터 삭제 악성코드의 소스코드에 북한 기반시설과 관련이 있다고 알려진 여러 인터넷 프로토콜(IP) 주소가 데이터를 직접 입력하는 방식으로 입력된 점도 들었다.[117]

이후 2014년 12월 23일부터 24일까지 북한의 인터넷 접속이 끊어졌다.[118] 북한의 인터넷 접속이 이틀 만에 복구된 점은 국가가 지원한 해킹 공격에 의한 것은 아니라는 방증이라고 미국 인터넷 업계는 보았다. 또한 미국이 중국에 대해 중국 인터넷을 사용하는 북한의 서버 등을 폐쇄하고 중국 내에서 활동하는 북한 해커를 파악하여 추방하라고 요구했다고 보도했다.[119] 북한은 동남아, 아프리카 등에 제3국 거점을 마련하여 해킹을 계속하리라는 예상도 있다. 그러므로 우리나라가 제3국에 시정 조치를 요구할 때, 국가의 영역관리 책임 또는 상당 주의 의무는 중요한 근거가 될 수 있다.

117) "FBI Accuses North Korea in Sony Hack"(2014. 12. 19.).
118) 「북한 인터넷이 끊기자 종북 댓글도 줄었다?」(2014. 12. 26.).
119) "North Korea's Internet links restored amid U.S. hacking dispute"(2014. 12. 23.).

4. 소결

'사이버안보'는 사이버공격 또는 위협을 방어하여, 사이버공간이 적절히 기능하게 함으로써 국가와 국민의 안전이 보장되는 상태라고 정의할 수 있다. 그리고 '사이버공간'은 '정보시스템'과 여기에 저장된 '정보'로 구성된다는 점을 알 수 있다.

한편 사이버'안보'는 국가의 안보를 궁극적인 보호 법익으로 하는 개념으로 비밀을 보호한다는 뜻인 사이버'보안'과는 구별된다. 그러나 사이버보안이 확보되지 않으면, 결국 규모와 효과의 측면에서 사이버안보까지 위협받게 되는 때가 있을 수 있으므로 두 개념은 무관하다기보다는 포함관계로 보아야 할 것이다. 예컨대 가정용 인터넷 공유기가 해킹당하는 것은 사이버보안의 문제에 머물 수 있다. 그러나 수백만 가구의 인터넷 공유기가 해킹되어 인터넷 서비스 공급업체의 서버를 공격하면 국가안보의 문제가 될 수 있다. 2016년 미국 동부에서 발생한 미라이 봇넷(Mirai Botnet) 사건이 대표적인 사례이다.

사이버안보 규범에 관한 국제적 논의는 전자공학, 컴퓨터 등 새로운 기술이 발달하자 일찍이 1988년부터 UN 총회에서 시작되었다. 그러나 이후 사이버안보 논의에서 미국을 중심으로 한 서방 자유민주 국가와 러시아와 중국을 중심으로 한 상하이협력기구 회원국 사이에 견해 대립이 계속되었다. 이에 러시아가 2001년 정부 전문가 그룹(UNGGE) 조직을 제안하여, 2004년부터 UNGGE가 활동을 시작했다. 제1차 보고서는 채택되지 못했다. 제2차 보고서는 협력 필요성 및 모범사례 교환 등을 언급했다. 제3차 보고서는 사이버공간에 국제법이 적용된다는 원칙을 처음 확인했고, 국가의 영역관리 책임을 노력 의무로 인정했다. 제4차 보고서는 사이버공간에 국제법이 적용된다는 원칙을 재확인했다. 그러나 사이버공격에 대한 자위권 허용 여부에 관한 견해에는 대립이 있어, UN 헌장이 전체적으로 적용된다고 규정했다. 제5차 보고서는 채택되지 못했다.

제6차 보고서는 무력 충돌 상황에서만 국제인도법이 적용된다고 언급했으나, 이 원칙을 국가의 ICT 기술 사용에 어떻게 적용할지 연구가 필요하다고 강조했다.

2017년 제5차 UNGGE 보고서 채택이 결렬되자, 2018년 10월 러시아가 개방형작업그룹(OEWG) 설치를 제안했고, UN 총회는 2019년부터 활동하도록 결정했다. 제1차 OEWG는 2021년 보고서를 제출했으나 UNGGE 보고서의 결론을 재확인하는 등 실질적으로 진전된 내용은 없는 것으로 평가된다. 2021년부터 2025년까지 2차 OEWG가 활동 중이다.

한편 국제적 논의 과정에서 식별된 사이버안보 분야의 주요 쟁점은 (i) 사이버공간의 별도 영역성 인정 여부, (ii) 사이버공간에 대한 국제법 적용 여부, (iii) 사이버 무력공격에 대한 예방적 자위권 인정 여부, (iv) 사이버공간 관련 상당 주의 의무 적용 여부이다.

첫째, 미국 등 서방 국가는 사이버공간을 별도 영역으로 인정하는 태도를 보이는 것으로 평가할 수 있다. 반면 러시아, 중국 등 비서방 국가는 사이버공간을 별도 영역으로 인정하지 않는 태도를 보인다고 평가할 수 있다, 러시아 등은 '사이버공간'이라는 용어 대신 'ICT 기술의 사용'이라는 용어를 사용한다.

둘째, 미국을 중심으로 한 서방 자유민주 국가는 사이버공간의 성격을 우주와 비슷한 것으로 본다. 따라서 현행 국제법이 사이버공간에 그대로 적용될 수 있다고 본다. 반면 사이버공간이 별도 영역이 아니라고 보는 러시아와 중국을 중심으로 한 상하이협력기구 회원국은 시스템 등 물리적인 ICT 기반시설 또는 정보가 저장된 서버의 위치가 국내이면 국내법이, 외국이면 외국법이 적용될 뿐 국제법은 적용되지 않는다는 태도를 보인다.

셋째, 사이버 무력공격에 대한 예방적 자위권 인정 여부에 관한 ICJ 판정례는 없고, 학설이 대립한다. 사이버공격(cyber attack)이라는 용어에서 '공격'은 전쟁을 뜻하는 무력 충돌(armed conflict)에 적용되는 국제법에서 사용하는 개념이다. 그리고 예방적 자위(anticipatory self-defense)는 무력공격이

예상되면 아직 무력공격이 발생하지 않았다고 하더라도 조치하는 것을 뜻한다. UN 헌장 제51조는 "무력공격이 발생하면(if an armed attack occurs)" UN 안보리 조치가 있을 때까지 자위권 행사를 허용한다. 현재형으로 규정된 문언을 근거로 예방적 자위가 금지된다고 보는 견해가 있다. 반면 UN 헌장의 규정은 기존 국제관습법에서 인정되던 자위권의 내용에 어떠한 변경을 가하는 것이 아니라, 자위권 행사에 추가적인 안전장치를 제공하는 것뿐이라고 해석하는 견해도 있다. 비록 임박한 무력공격이 무엇을 의미하는지 논란은 있지만, 국제관습법에 근거할 때 예방적 자위권이 인정된다는 견해가 설득력이 있다. 그러므로 사이버 무력공격에 대한 예방적 자위권을 주장할 때는 국제관습법을 근거로 주장하는 것이 유리할 것이다.

넷째, 국가의 영역관리 책임 또는 국제환경법 분야에서 인정되는 국가의 상당 주의 의무의 사이버공간 적용 여부에 대해 미국은 과거에 반대했다. 그 결과 제6차 UNGGE 보고서에도 국가의 영역관리 책임에 대해 법적 의무가 아니라 마땅히 노력한다는 내용이 포함되었을 뿐이다. 그러나 이러한 미국의 태도는 변화하고 있는 것으로 보인다. 국가의 영역관리 책임은 우리나라가 북한의 해킹 공격에 대응할 때 유용한 근거가 될 수 있다. 만약 북한이 중국 또는 러시아 등 제3국의 영토 내에 거점을 마련하고 해킹 활동을 한다면, 우리나라는 국제관습법에 따른 영역관리 책임 또는 상당 주의 의무를 근거로 해당 국가에 조치 및 재발 방지를 요구할 수 있다.

제3장 주요국의 사이버안보 정책

제3장에서는 주요국의 사이버안보 정책을 살펴본다. 여기서 주요국은 우리나라가 입법에 참고할 수 있는 미국, EU, 일본으로 선정했고, 러시아, 중국, 이란, 북한 등은 조사 대상에 포함하지 않는다. 또한 주요국의 '정책'은 '전략'과 '법률'로 나누어 검토한다. 보는 시각 또는 분야에 따라 '정책'과 '전략'의 위상 및 그에 따른 상호 포함관계가 다를 수 있다. 그러나 이 연구에서 미국, EU, 일본, 우리나라의 국가실행을 조사한 결과, 정책이 '전략'과 '법률'의 형식으로 구분된다는 사실을 발견했고, 이에 따라 제3장의 목차를 구성했다. 이 연구에서 조사된 결과 중에서 명칭에 전략이 아니라 정책이라는 단어가 사용된 문서의 유일한 예는 EU가 2022년 발표한 「EU 사이버 방어 정책」으로, 앞서 발표된 2013년 「EU 사이버안보 전략」 및 2020년 「EU 사이버안보 전략」과 대비된다. 그러나 「EU 사이버 방어 정책」 문서에 밝히듯, 이 정책은 2020년 「EU 사이버안보 전략」에 따른 것이다. 미국에서 추진하는 사이버안보 전략에 따른 이행계획에 가깝다. '정책'이 '전략'과 '법률'의 형식으로 나뉘는 것은 우리나라도 마찬가지이다. 사이버안보 '정책'이라는 용어를 제목으로 발표된 문서는 검색되지 않는다. 다만 2019년 「국가 사이버안보 전략」, 2024년 「국가 사이버안보 전략」, 그리고 이 전략에 따른 「국가 사이버안보 기본계획」이 있을 뿐이다. 따라서 제3장에서는 주요국의 '정책'을 '전략'과 '법률'로 나누어 살펴본다.

주요국의 사이버안보 정책 각각을 분석하기에 앞서, 관련 정보를 전체적으로 볼 수 있는 국내외 자료를 소개한다. 국내 자료로는 '국가 전략 정보포털'이 있다. 국회가 국가적 차원의 핵심 의제를 발굴하고 미래 비전을 제시할 수 있도록 국회도서관이 제공하는 자료이다. 국가 전략 포털은 국가 전략에 관한 정보

를 정치, 경제, 사회, 기술, 환경, 자원이라는 여섯 가지 주제로 나누어 제공하는데, 사이버안보는 기술 분야에 속한다.[120]

국외 자료로는 세 가지가 있다. 첫째, 세계경제포럼(WEF: World Economic Forum)의 '2024년 글로벌 사이버안보 전망(Global Cybersecurity Outlook 2024)'이 있다. 이 자료는 사이버안보에 관한 WEF 연례 회의에 참석한 120명의 기업인에 대한 설문조사 결과를 반영한 것이 특징이다. 이 설문에서 90% 이상의 기업인은 사이버안보 관련 대기업과 중소기업 사이의 불균등 문제 해결을 시급한 과제로 꼽았다. 사이버사고 대비 보험 가입 등에서 대기업과 중소기업 사이에는 큰 격차가 발견된다.[121] WEF는 1971년 비영리 재단으로 설립된 국제 공공-민간 협력 기구이다. 특정 이익에 얽매이지 않고 독립적으로 운영하는 것을 지향하며, 정치, 비즈니스, 학계, 시민사회 및 기타 사회 지도자들을 참여시켜 글로벌, 지역 및 산업 의제를 형성하는 것을 목표로 한다.[122]

둘째, UN의 표준화 전문기구인 ITU의 '2024년 글로벌 사이버안보 지수(ITU Global Cybersecurity Index 2024)'가 있다.[123] 제목에 지수라는 단어가 포함된 것을 바탕으로 알 수 있듯이, 이 보고서는 전체적인 파악을 하는데 도움이 될 수 있다. 그러나 특정 국가의 구체적인 법률이나 제도에 관한 정보는 알기 어려운 한계가 있다.

ITU가 2015년부터 시작한 글로벌 사이버안보 지수(GCI: Global Cybersecurity Index) 사업은 각국이 개선이 필요한 분야를 파악하고 역량을 구축하도록 장려하는 것이 목표이다. 변화하는 위험에 각국이 더 잘 대응할 수 있도록 돕기 위해 GCI는 지속적으로 개정되었다. 2024년에 발표된 GCI는 제5판으로, 조사 대상 기간은 2023년부터 2024년까지이고 조사 대상 국가는 194개국이다. 총 83개 질문을 바탕으로 20개 세부 지표와 5개 중요 지표를 도

120) 국가전략정보포털(2024), 「서비스 소개」(검색일: 2024. 10. 20.).
121) WEF(2024), "Global Cybersecurity index 2024"(검색일: 2024. 10. 20.).
122) WEF 홈페이지(2024), "Our Mission"(검색일: 2024. 10. 20.).
123) ITU(2024), "Global Cybersecurity index 2024"(검색일: 2024. 10. 20.).

출했다.[124] ITU의 조사 결과는 다음과 같다. 각국은 2021년 이후 점점 더 많은 사이버안보 조치를 시행하는 추세를 보였고, 전 세계 평균 점수도 65.7/100점으로 상승했다. 다섯 가지 요소 중에서 가장 점수가 높은 요소는 법률이었고, 가장 약한 요소는 역량확충과 기술이었다.

표 3-1. ITU의 2024년 글로벌 사이버안보 지수에 따른 분류

대분류	설명	소분류	국가 수
법률	사이버안보 및 사이버범죄에 관한 법률 및 규정	개인정보보호 또는 침해 통지에 관한 규정 시행	177
		데이터 보호 규정 시행	151
		중요 인프라 규정 시행	104
기술	국가 및 전문기관을 통한 기술역량 구현	CIRT가 활성화된 국가	139
		지역 CIRT 협회에 가입한 국가	83
		사이버안보 표준을 채택하기 위한 제도적 틀이 있음.	110
조직	사이버안보를 시행하는 국가전략과 조직	국가 사이버안보 전략이 있는 국가	132
		사이버안보 담당 기관이 있는 국가	161
		아동 온라인 보호 전략 및 계획이 있는 국가	94
역량확충	사이버안보 역량확충을 위한 인식 제고 교육훈련 및 장려책	사이버안보 인식 제고 교육훈련 제도가 있는 국가	152
		국정과제에 사이버안보를 포함시킨 국가	153
		사이버안보 역량확충 장려책이 있는 국가	99
협력	기업, 국가 사이의 협력 관계	국내 또는 국제 사이버안보 민관협력에 참여(예정)국	108
		국제 사이버안보 협정 체결국	166

주: CIRT는 사이버사고 대응팀(Cyber Incident Response Team)을 의미함.
자료: ITU(2024), "Global Cybersecurity index 2024," p. 2(검색일: 2024. 10. 20.).

국가는 평가 점수에 따라 크게 다섯 그룹으로 나뉘는데, 95~100점에 해당하는 제1그룹은 모범이 되는 국가 그룹이고, 0~20점에 해당하는 제5그룹에 속한 국가는 도움이 필요하다고 평가된다. 국가 대부분을 차지하는 105개국은 제3그룹(55~85점)과 제4그룹(20~55점)에 속한다. 그런데 제1그룹에 속한 국가의 수가 무려 46개국에 달한다. 194개국을 5개 그룹에 분류한 결과임을

124) *Ibid.*, p. 1.

고려하더라도, 제1그룹에 속한 국가의 수는 많은 편으로 보인다. 제1그룹에 속한 국가의 대륙별 분포는 유럽(20개국), 아시아태평양(11개국), 중동(8개국), 미주(2개국), 아프리카(5개국)이다. 제1그룹에는 미국, 유럽 각국, 우리나라, 일본이 포함되어 있는데, 중국은 제1그룹이 아닌 제2그룹으로 분류되어 있다. 중국이 낮게 나온 분야는 역량 개발 조치이고 사이버보안 교육 및 인식 제고 노력 등을 평가한다. 일반 국민을 상대로 한 사이버 인식 개선 캠페인 실시 횟수 등이 고려 요소이다. 방글라데시, 케냐 등 개발도상국도 다수가 제1그룹에 속해 있는데, 중국이 제2그룹에 분류되어 있는 점이 ITU의 '2024년 글로벌 사이버안보 지수'에서 특징적이라 평가할 수 있다.

셋째, 국외 자료 중에서 주요국의 사이버안보 정책 각각에 관한 더 구체적인 정보를 확인할 수 있는 곳으로 UN 군축연구소(UNIDIR: United Nations Institute for Disarmament Research)의 '사이버 정책 포털(Cyber Policy Portal)'이 있다. 우리나라에 관한 정보가 가장 최근에 갱신된 시점이 2024년 5월일 정도로 지속하여 관리되고 있다. 제공하는 정보는 크게 네 가지 주제인데, 사이버안보 정책, 구조, 법적 틀, 협력이 그것이다. 이러한 네 가지 대분류는 다시 소분류로 나뉜다. 예컨대 사이버안보 정책은 다시 전략 문서와 이행의 틀로 나뉜다.[125] UNIDIR의 사이버 정책 포털이 제공하는 정보의 품질을 평가하기 위해 우리나라에 관한 정보를 살펴본다. 포털에서 제시하는 네 가지 주제 중에서 법적 틀을 예로 들면, 소분류로는 우리 국회가 제정한 법률만 제공된다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」, 「개인정보보호법」, 「전자정부법」, 「정보통신기반보호법」까지 총 네 가지 법률이 제시되어 있다. 대체로 정보와 정보시스템이라는 사이버안보를 구성하는 두 가지 큰 요소를 염두에 둔 법률 정보가 수록된 것으로 평가할 수 있다. 하지만 최근에는 클라우드컴퓨팅 서비스가 확산하면서, 사이버안보를 이유로 어떤 국가들은 클라우드컴퓨팅 서버를 자국 영역 내에 두도록 하는 이른바 서버 현지화

125) UN 군축연구소 사이버 정책 포털(2024)(검색일: 2024. 10. 20.).

요구를 하기도 한다. 따라서 변화하는 기술 환경과 규제 환경에 맞추어, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(약칭: 클라우드컴퓨팅법)」도 포함될 필요가 있다고 생각된다. 사이버안보에 관련되는 법률의 범위가 어디까지인지 명확하게 확정하기 어려운 측면을 드러내는 사례이다.

표 3-2. UN 군축연구소가 운영하는 사이버 정책 포털이 제공하는 정보의 분류

대분류	소분류
사이버안보 정책(Cybersecurity Policy)	전략 문서(Strategy Documents)
	이행의 틀(Implementation Framework)
구조(Structures)	책임기관(National Centre or Responsible Agency)
	책임자(Key Position)
	담당기관(Dedicated Agencies and Departments)
	국가 대응팀(National CERT or CSIRT)
법적 틀(Legal Framework)	입법(Legislation)
협력(Cooperation)	UN 활동(UN Processes)
	양자 및 다자 협력(Bilateral and Multilateral Cooperation)
	기타 활동(Select Activities)
	회원으로 가입한 현황(Membership)

주: CERT는 컴퓨터 비상 대응팀(Computer Emergency Response Team)을, CSIRT는 컴퓨터 보안사고 대응팀(Computer Security Incident Response Team)을 의미함.
자료: UN 군축연구소 사이버 정책 포털(2024)(검색일: 2024. 10. 20.).

따라서 이 연구에서는 하나의 자료에 바탕을 두기보다는 한국 인터넷진흥원 등 국내외 기관의 보고서 및 사이버안보 전략에 관한 주요국 정부의 공식 문서와 관련 국내법 등을 다양하게 참고하여 국가별로 정리할 수밖에 없다. 더불어 앞서 제2장에서는 사이버공격과 사이버 무력공격이라는 국제법상 용어를 엄밀히 구분했으나, 주요국의 사이버안보 정책에 관한 제3장에서는 각국 전략 문서의 원문 표현을 존중하여 사이버공격이라는 용어를 사용한다.

1. 미국

가. 전략

1) 2023년 「국가 사이버안보 전략」

미국 백악관은 2023년 3월 1일 「국가 사이버안보 전략(National Cybersecurity Strategy)」을 발표했다. 이 전략은 서론과 다섯 가지 접근방법(pillar, 기둥)에 대한 설명, 이행까지 총 일곱 부분으로 구성되어 있는 35장 분량의 문서이다.[126]

미국 최초의 사이버안보 전략은 2003년에 발표된 「안전한 사이버공간을 위한 국가 전략(National Strategy to Secure Cyberspace)」이다. 이 전략은 민관협력 체계 구축과 사이버사고 대응을 위한 미국 연방 차원의 대응계획 수립에 이바지한 것으로 평가된다. 당시는 조지 W. 부시 대통령이 재임하던 때였다. 미국은 2000년대부터 다양한 정책문서에서 사이버안보를 강조했고, 특히 2001년 9.11 테러 직후 백악관에 사이버안보 담당 보좌관이라는 직제도 설치했다. 이후 2018년에는 「2018 국가 사이버 전략(National Cyber Strategy)」이 발표되었다. 주요 내용은 미국의 사이버공격 대응 능력 강화, 사이버 위협에 대한 정보 수집 및 분석 능력 향상을 위한 민간 협력 강화, 인프라와 중요시스템 보호 역량 강화, 사이버공격에 대한 규제와 법적 대응 강화를 위한 국제협력 추진이다.[127]

2023년 「국가 사이버안보 전략」의 목표는 안전한 디지털 생태계의 혜택을 모든 미국인이 누릴 수 있도록 보장하는 것이다.[128] 이를 위해 사이버공간을 민주적 가치를 반영하는 방식으로 재구성하겠다고 밝혔다. 방어 가능하고(defensible), 회복성이 뛰어나며(resilient), 가치에 맞는(values-aligned)

126) The White House(2023), "National Cybersecurity Strategy"(검색일: 2024. 10. 20.).
127) 김소정(2023), pp. 1~2.
128) The White House 홈페이지(2023a), "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy"(검색일: 2024. 10. 20.).

디지털 생태계 형성이 비전으로 제시되었다. 이러한 비전을 실현하려면 사이버 공간에서의 역할, 책임, 자원을 할당하는 방식에 크게 두 가지 근본적인 변화가 필요하다고 언급했다. 첫째, 공공 및 민간 부문에서 가장 크고 가장 유능하며 가장 유리한 위치에 있는 기관이 사이버 위험을 완화할 책임을 더 많이 부담하도록 보장하겠다고 밝혔다. 사이버안보에 대한 부담을 개인, 중소기업, 지방 정부에 지우던 것을 바꾸어, 모두의 위험을 줄일 수 있는 가장 유능하고 최적의 위치에 있는 조직이 부담하도록 한다. 둘째, 사이버안보에 대한 장기적인 투자를 촉진하는 인센티브를 강화해 나가는 것이다. 현재의 긴급한 위협으로부터의 방어와 균형을 유지하도록 한다.

표 3-3. 미국 「국가 사이버안보 전략」의 다섯 가지 접근방법

	제목	주요 내용
1	중요 인프라 방어	사이버안보 최소 요건의 적용을 확대하여 중요 인프라 복원력 확보
2	위협 행위자 저지	국가 권력 수단 모두 동원 및 민간 부문 참여
3	시장의 복원력 형성	소프트웨어 상품 및 서비스에 대한 책임 전환
4	회복성 있는 미래에 투자	전략적 투자와 조율된 협력으로 차세대 기술과 인프라 혁신 선도
5	국제협력	책임 있게 행동하지 않는 국가 등에 대해 다른 국가와 공동 대응

자료: The White House(2023), "National CyberSecurity Strategy"(검색일: 2024. 10. 20.).

2023년 「국가 사이버안보 전략」은 5가지 접근방법을 중심으로 협업 구축 및 강화를 목표로 한다. 다섯 가지 접근방법은 (ⅰ) 중요 인프라 방어, (ⅱ) 위협 행위자 저지, (ⅲ) 시장의 복원력 형성, (ⅳ) 회복성 있는 미래에 투자, (ⅴ) 국제 협력이다. 주요 내용을 중심으로 살펴보면 다음과 같다.

첫째, 중요 인프라 방어와 관련한 사이버안보 최소 요건의 적용을 확대하여 중요 인프라 복원력을 확보한다.[129] 인프라의 사이버안보와 관련하여 우리나라는 「주요정보통신기반보호법」이라는 통합된 근거가 있지만, 미국은 에너

129) *Ibid.*

지, 금융, 의료 등 영역별로 나누어 자발적 인프라 보안 활동을 시행했다. 미국 주요 인프라의 상당 부분은 민간이 소유 또는 운영하고 있고, 미국정부는 국토안보부를 통해 간접적으로 관리했다. 그러나 2021년 5월 7일 발생한 콜로니얼 파이프라인 해킹 공격(Colonial Pipeline ransomware attack)[130]으로 민간 부문의 자발적 보안 체계로는 사이버안보 위협에 효과적으로 대응할 수 없다는 사실이 드러났다. 정부의 직접 개입과 보안 요구사항의 강제적 적용 필요성이 제기되었고, 2023년 국가 사이버안보 전략은 주요 인프라 보호의 체계를 변경하기 위한 시작점이 되었다.[131]

둘째, 사이버 위협 행위자 저지에 국가 권력 수단을 모두 동원하고, 이러한 활동에 민간 부문을 참여시킨다.[132] 사이버 위협 행위자가 불법적으로 취득한 암호화폐를 압수하는 등, 이용할 수 있는 국가 권력 수단을 모두 동원하여 사이버 위협 활동의 수익성이 낮아져 더 이상 효과적이지 않도록 만들겠다는 내용이다. 사이버 분야의 혁신 속도가 빨라 민간 부문의 역량이 정부 기관보다 더 뛰어난 경우가 있으므로, 민간 부문과 권한을 가진 연방 정부 기관 사이의 협력은 사이버 위협행위에 대한 효과적인 대응에 중요하다. 따라서 민간 부문이 하나 이상의 비영리 단체를 만들어 참여하도록 장려한다.[133]

셋째, 시장의 복원력 형성을 위해, 소프트웨어 상품 및 서비스에 대한 책임 전환 등으로 디지털 생태계 내부 위험을 감소시킨다.[134] 소프트웨어 상품 및 서비스 공급자가 안전하지 않은 기본 구성이나 알려진 취약점이 있는 상품 또는 서비스를 공급하고, 입증되지 않았거나 알려지지 않은 타사 소프트웨어를

130) 콜로니얼 파이프라인은 미국 동부 지역에서 유류를 공급하는 회사이다. 1962년에 설립되었다. 본사는 미국 조지아주 알파레타(Alpharetta)에 있다. Hart Energy 홈페이지(2024), "Colonial Pipeline Co."(검색일: 2024. 12. 9.).
131) 김소정(2023), p. 3.
132) The White House 홈페이지(2023a), "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy"(검색일: 2024. 10. 20.).
133) The White House(2023), "National Cybersecurity Strategy"(검색일: 2024. 10. 20.).
134) The White House 홈페이지(2023a), "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy"(검색일: 2024. 10. 20.).

통합하는 경우가 적지 않다고 본다. 소프트웨어 생산업체는 시장 지위를 활용하여 계약에 의한 책임을 피할 수 있으므로 안전한 설계 원칙을 따르거나 발매 전 시험 평가를 할 유인이 더 줄어든다. 이에 미국정부는 의회 및 민간 부문과 협력하여 소프트웨어 상품 및 서비스에 대한 책임을 확립하는 법안을 마련하려 한다.[135] 즉 미국정부는 최종 사용자가 소프트웨어의 취약점과 고의적인 악용에 대한 책임을 지는 오늘날의 현실이 문제가 있다고 인식하고, 책임을 최종 사용자에서 기업 등으로 전환하는 방안을 추진한다. 이에 대해 일부 기업은 기업의 책임이 명확해지고 규제가 간소화되고 통일되면 이 분야에 대한 투자 부담도 줄어들 것으로 기대하며 환영의 뜻을 나타냈다. 반면 다른 기업은 정부의 이러한 조치가 위험을 줄이는 데 도움은 되지 않으면서 기업 활동의 효율성은 낮추는 등 의도하지 않은 결과를 초래할 수 있다고 우려했다. 책임의 전환에는 입법이 필요하므로 미국 의회에서도 주목하는 부분이다.[136]

2) 2024년 「국가 사이버안보 전략 이행계획」

2024년 5월 7일 미국 백악관은 「국가 사이버안보 전략 이행계획(National Cybersecurity Strategy Implementation Plan)」을 발표했다.[137] 제목에서 알 수 있는 것처럼 「국가 사이버안보 전략」에 대한 이행계획이다. 또한 정식 명칭은 「국가 사이버안보 전략 이행계획 제2판(version 2)」인데, 제2판인 이유는 약 1년 전인 2023년 7월 13일에 「국가 사이버안보 전략 이행계획」이 발표되었기 때문이다.[138]

먼저 2023년 7월 13일 발표된 「국가 사이버안보 전략 이행계획」 제1판에서

135) The White House(2023), "National Cybersecurity Strategy"(검색일: 2024. 10. 20.).
136) Congressional Research Service(2023a), "The National Cybersecurity Strategy-Going Where No Strategy Has Gone Before"(검색일: 2024. 11. 1.).
137) The White House 홈페이지(2024), "Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan"(검색일: 2024. 11. 1.).
138) The White House 홈페이지(2023b), "FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan"(검색일: 2024. 11. 1.).

는 전략에 따른 책임기관과 협력 주체, 완료 시기를 정했다. 우선 사이버 위협 저지 활동 조직을 위한 플랫폼 확대는 미국 법무부가 담당하고 완료 기한은 회계연도 기준 2025년 1/4분기이다. 저지 활동의 속도와 규모 증대는 미국 연방수사국이 담당하고 완료 기한은 회계연도 기준 2024년 2/4분기이다. 다음으로 안전하고 신뢰할 수 있는 ICT 네트워크 및 서비스 개발 촉진은 국무부가 담당하고 완료 기한은 회계연도 기준 2024년 2/4분기이다. 국무부는 안전한 ICT 생태계를 위한 정책 및 규제를 국제적 차원에서 채택하기 위해 동맹국과의 협력을 추진한다. 끝으로 약속을 이행하지 못하는 국가에 책임을 추궁하는 방안은 국무부가 담당하고 완료 기한은 회계연도 기준 2025년 4/4분기이다.[139]

한편 2024년 5월 7일 발표된 「국가 사이버안보 전략 이행계획 제2판」은 이행계획 제1판에서 31개의 새로운 계획과 6개 담당 기관이 추가되었다. 이행계획 제1판에 따른 36개 계획 중 33개(92%)가 회계연도 기준 2024년 2/4분기까지 완료되었다. 나머지 3개는 진행 중이다.[140]

3) 「CISA 전략계획 2023~2025」

미국 사이버안보 및 기반시설 안보국(CISA: Cybersecurity and Infrastructure Security Agency)은 미국의 가상 및 물리적 기반시설에 대한 위험을 감소시켜 안전하고 복원력 있는 기반시설을 유지하는 것을 목적으로 하는 조직이다.[141]

2022년 9월 1일 CISA은 「CISA 전략계획 2023~2025(CISA Cybersecurity Strategic Plan FY 2024-2026)」를 발표했다. 「CISA 전략계획 2023~2025」의 가장 큰 특징으로는 미국의 핵심 네트워크에 대한 침해가 발생하기 전에 능동적으로(proactively) 위협을 완화한다는 내용이 포함된 점을 들 수 있다. 구체적으로 네트워크 모니터링, 위협 분석, 사이버 위협 수색(cyber threat hunting)에서

139) 천곤웅, 김성훈(2024), p. 9, pp. 25~27.
140) The White House 홈페이지(2024), "Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan"(검색일: 2024. 11. 1.).
141) CISA 홈페이지(2024a), "About CISA"(검색일: 2024. 8. 5.).

노력의 효과를 측정하여 탐지와 조치에 걸리는 시간을 줄이는 것을 제시하고 있다.[142]

나. 법률

사이버안보에 관한 미국의 법률은 UN 군축연구소 사이버 정책 포털에서 「2015년 사이버안보법」, 「2018년 사이버안보 및 기반시설 안보국 법」 등 총 9건이 검색된다.[143] 이 중 「2015년 사이버안보 정보공유법」은 「2015년 사이버안보법」에 하나의 장(title)으로 통합된 내용이다. 또 「1984년 컴퓨터 사기와 남용법(Computer Fraud and Abuse Act of 1984)」, 감청 금지와 전자통신 프라이버시 보호에 관한 「1986년 전자통신 프라이버시 법(Electronic Communications Privacy Act of 1986)」 등도 9건에 포함되어 있다. 그러나 이러한 법률은 사이버안보법이라기보다는 사이버보안법에 가깝다.

미국에서 사이버보안법이 아닌, 국가안보법이라고 평가할 수 있는 법률이 제정된 시기는 2001년 9월 11일에 발생한 9.11 테러 이후이다.[144] 「2002년 국토안보법(Homeland Security Act of 2002)」 제1장은 국토안보부를 신설하여 미국 내 테러 방지 등 국토 안보 사무를 담당하도록 한다는 내용이고, 제2장은 정보 분석과 기반시설 보호에 관한 내용인데 여기에는 사이버안보에 관한 내용이 일부 포함되어 있다.[145] 이후 2014년에는 12월 12일에 「2014년 국가 사이버안보 보호법」이, 그리고 12월 15일에 「2014년 사이버안보 강화법」이 각각 미국 의회를 통과했다.[146] 미국에는 이러한 의회 제정법뿐 아니라 대통령이 제정하는 법률인 행정명령도 있으나, 의회 제정법만으로도 그 수가 적지 않다.

142) CISA(2022), "Strategic Plan 2023-2025"(검색일: 2024. 8. 5.).
143) UN 군축연구소 사이버 정책 포털(2024)(검색일: 2024. 8. 19.).
144) 박상돈(2022), pp. 45~46.
145) 미국 의회 홈페이지(2024a), "H.R.5005 - Homeland Security Act of 2002"(검색일: 2024. 11. 5.).
146) 박상돈(2022), pp. 46~47.

그러므로 이 연구에서는 의회 제정법에 집중하여 살펴본다. 행정부가 바뀌면 행정명령은 쉽게 폐지될 수 있지만, 의회 제정법은 폐지가 상대적으로 어려운 점을 고려한 결과이다.

1) 「2014년 국가 사이버안보 보호법」

2014년 12월 18일에 제정된 「2014년 국가 사이버안보 보호법(National Cybersecurity Protection Act of 2014)」의 의의는 사이버안보 및 통신 통합센터(NCCIC: National Cybersecurity and Communication Integration Center)를 명시적으로 규정하여, 센터 설치의 법적 근거를 마련한 최초의 법률이라는 점이다. 이 법률 제3조는 「2002년 국토안보법」을 제2장에 NCCIC 센터에 관한 제3절을 추가하여 개정한다고 규정함으로써 NCCIC를 명시했다.[147] NCCIC는 국토안보부 국가보호 및 프로그램 국(NPPD: National Protection and Programs Directorate)의 한 부서로 설치되었다. NPPD는 2007년에 인프라 보호국 등 국토안보부 내 기존 부서를 통합한 조직의 본부로 설립되었다.[148]

NCCIC는 「2014년 국가 사이버안보 보호법」이 제정되기에 훨씬 앞서 설치되어 운영되고 있었다. 미국 국토안보국은 NCCIC가 기존 사이버사고 대응 조직을 통합하여 운영할 필요성을 강조한 국가안보 통신자문위원회(National Security Telecommunications Advisory Committee), 미국 회계감사원(GAO: Government Accountability Office), 기업과 정부 간 작업반 등의 권고에 따라 2009년에 설치되었다고 설명한다.[149] 그러나 이러한 위원회 권고를 포함하여, 미국 대통령의 각종 행정명령 등 NCCIC의 설치 근거로 설명되는 문서는 사이버 위협에 대한 통합 대응을 요청하는 내용을 담고 있을 뿐이

147) 미국 의회 홈페이지(2024b), "S.2519 - National Cybersecurity Protection Act of 2014"(검색일: 2024. 11. 5.).
148) 미국 회계감사국 홈페이지(2015), "National Protection and Programs Directorate"(검색일: 2024. 11. 25.).
149) 미국 국토안보부 홈페이지(2009), "New National Cybersecurity Center Opened"(검색일: 2024. 11. 25.).

었다. 따라서 NCCIC가 2014년에 최초로 설치된 것이 아니고 그 이전에도 설치되어 활동했지만, 설치 근거가 법적으로 명확하게 마련된 것은 「2014년 국가 사이버안보 보호법」에 의해서이다.

2) 「2014년 사이버안보 강화법」

2014년 12월 18일에 제정된 「2014년 사이버안보 강화법(Cybersecurity Enhancement Act of 2014)」은 사이버안보 분야에 관한 공공기관과 민간 주체 사이의 협력에 관한 법률이다.[150] 주요 내용은 미국 국립표준기술연구소(NIST: National Institute of Standards and Technology)에 관한 법률에 일부 내용을 추가하는 것이다(제101조(사이버안보 분야에 관한 공공기관과 민간 주체 사이의 협력)). 추가된 내용은 "핵심 인프라에 대한 사이버 위험을 비용 효율적으로 줄이기 위해 자발성과 합의에 기반한 업계 주도의 표준, 지침, 모범 사례, 방법론, 절차 및 프로세스의 개발을 지속하여 촉진하고 지원한다"라는 것이다.

즉 「2014년 사이버안보 강화법」은 공공기관과 민간 주체 사이의 협력을 다루는데, 이를 NIST의 임무로 추가한다는 것이 핵심적인 내용이다. 그리고 이를 위해 연구개발(제2장), 교육훈련(제3장), 인식 제고 및 준비 태세 확립(제4장), 사이버안보 기술표준 발전(제5장)에 관한 내용을 담았다. 하지만 추가적인 규제 권한을 부여하지 않고(제2조), 추가적인 기금의 사용을 허용하는 것이 아님을 명시적으로 규정했다(제3조).

이 법률에서 말하는 핵심 인프라(critical infrastructure)는 2001년 10월 25일 제정된 「2001년 미국 애국법(USA PATRIOT Act of 2001)」의 정의와 같다. 이에 따르면 핵심 인프라는 "무력해지거나 파괴되는 경우 안보, 국가 경제 안보, 국가 공중 보건이나 안전, 또는 위 사항들의 결합에 치명적인 영향을 미칠

150) 미국 의회 홈페이지(2024c), "S.1353 - Cybersecurity Enhancement Act of 2014," 온라인 자료 (검색일: 2024. 11. 5.).

정도로 미국의 사활적(vital) 물리 또는 가상 시스템과 자산"으로 정의된다.[151]

3) 「2015년 사이버안보법」

2015년 12월 18일에 제정된 「2015년 사이버안보법(Cybersecurity Act of 2015)」은 사이버안보에 관한 여러 법안을 「2016년도 통합 세출 예산법(Consolidated Appropriations Act, 2016)」의 일부(Division N)로 통합하여 의회를 통과했다. 이 법률은 사이버안보 정보 공유(제1장), 국가 사이버안보 발전(제2장), 연방 사이버안보 인력평가(제3장), 기타 사이버안보 사항(제4장)으로 구성되어 있다. 그런데 각 장의 제목은 당시 미국 의회에 제안되어 계류 중이던 법률안의 제목과 같다.[152] 이의 원인은 이 법률이 같은 시기에 제출된 여러 법률안을 통합하여 제정된 배경에서 찾을 수 있다.[153]

「2015년 사이버안보법」 제101조는 제1장의 제목을 「2015년 사이버안보 정보 공유법(Cybersecurity Information Sharing Act (CISA) of 2015)」으로 인용할 수 있다고 규정했다. 제1장의 주요 내용은 (i) 사적 주체(private entity)가 사이버 위협에 대응하기 위해 자체 정보시스템에서 방어 조치를 모니터링하고 구현할 수 있도록 허가하고, (ii) 사적 주체가 연방 정부와 주 정부 및 다른 민간 기업 등과 사이버 위협 지표에 관한 정보를 자발적으로 공유하도록 장려하기 위한 보호 조치로 통신 비밀에 관한 여러 법률에 따른 책임으로부터의 면책을 규정했다.[154]

여기서 제1장에 따라 공유할 수 있는 정보의 범위는 공유 주체가 연방 주체인지 비연방 주체(non-federal entity)인지에 따라 차이가 있다. 비연방 주체는 사이버 위협 지표와 방어 조치에 관한 정보만 공유할 수 있다. 반면 연방 주체는

151) 「2001년 미국 애국법(USA PATRIOT Act of 2001)」 제1016(e)조.
152) 미국 의회 홈페이지(2024d), "H.R.2029 - Consolidated Appropriations Act, 2016"(검색일: 2024. 11. 5.).
153) 박상돈(2022), pp. 48~49.
154) Harvard Law School Forum on Corporate Governance 홈페이지(2024), "Federal Guidance on the Cybersecurity Information Sharing Act of 2015"(검색일: 2024. 11. 5.).

이러한 정보 외에도 이 법률이 허용하는 정보 이용에 관한 정보, 사이버보안 위협에 관련된 정보도 공유할 수 있다.[155]

한편 제1장 제102조(정의)는 다양한 용어의 뜻을 정의했다. 사이버 위협 지표(cyber threat indicator)는 보안 취약점, 보안 취약점을 악용하는 방법, 보안 취약점이 관련된 기술 정보를 수집할 목적으로 전송되는 것으로 보이는 비정상적인 통신 패턴을 포함한 악의적인 정찰 등을 설명하거나 식별하는 데 필요한 정보를 뜻한다. 또한 방어 조치(defensive measure)는 알려진 또는 의심되는 사이버보안 위협 또는 보안 취약성을 탐지, 예방, 또는 완화하는 정보시스템 또는 정보시스템에 저장, 처리, 또는 전송되는 정보에 적용되는 조치, 장치, 절차, 서명, 기법, 또는 기타 조치를 뜻한다. 그러나 방어 조치를 운영하는 민간 주체 또는 동의를 제공할 권한이 있고 해당 민간 주체에 동의를 제공한 다른 단체 또는 연방 주체가 소유하지 않은 정보시스템 또는 해당 정보시스템에 저장, 처리 또는 전송되는 정보를 파괴하거나, 사용할 수 없게 만들거나, 무단 액세스를 제공하거나, 실질적으로 해를 끼치는 조치는 포함되지 않는다.[156]

끝으로 제1장의 제106조(법적 책임으로부터의 보호)는 제104조(사이버보안 위협에 대한 탐지, 분석, 완화, 방지에 대한 승인)에 따른 정보시스템 및 정보 모니터링에 관련해서는 어떤 사기업에 대해서도, 어떠한 소송도 법원에 제기되거나 유지될 수 없으며, 이러한 소송은 즉시 기각되어야 한다고 명시한다.[157]

다음으로 제2장은 제201조에 따르면 「2015년 국가 사이버안보 보호 발전법(National Cybersecurity Protection Advancement Act of 2015)」으로 인용할 수 있다. 제2장의 주요 내용은 정보공유 구조와 절차, 관련 분석 조직, 대응 틀에 관해 「2002년 국토안보법」을 일부 개정하는 것, 그리고 국토부 장관이 데이터센터의 사이버안보 위험 감소에 관한 보고서 및 미국 항구의 사이버

155) 양천수, 지유미(2018), p. 169.
156) 미국 의회 홈페이지(2024d), "H.R.2029 - Consolidated Appropriations Act, 2016"(검색일: 2024. 11. 5.).
157) *Ibid.*

안보 취약성에 관한 보고서를 각각 작성하여 이 법률의 시행일로부터 1년 이내에 미국 의회의 관련 위원회에 제출해야 한다는 것이다.[158]

4) 「2018년 사이버안보 및 기반시설 안보국 법」

2018년 11월 16일에 제정된 「2018년 사이버안보 및 기반시설 안보국 법(Cybersecurity and Infrastructure Security Agency Act of 2018)」은 국토안보부 내의 기존 조직인 NPPD를 사이버안보 및 기반시설 안보국(CISA: Cybersecurity and Infrastructure Security Agency)으로 재지정하는 것이 주요 내용이다.[159]

구체적으로 제2202조는 NPPD가 CISA로 재정비되며, 다른 법률에서 NPPD를 규정한 것도 CISA를 규정한 것으로 간주한다고 명시한다. NPPD와 CISA 모두 국토안보부 내의 조직인 점에서는 같다. 그러나 조직의 명칭(National Protection and Programs Directorate, 국토안보부의 국가보호 및 프로그램 국)에서 알 수 있는 것처럼, 국가안보라는 일반적인 목표를 가진 조직이 아니라 사이버안보와 기반시설 안보라는 더 구체적인 임무를 명시한 조직으로 정비한 것이다. 그러므로 「2018년 사이버안보 및 기반시설 안보국 법」에 따라 NPPD가 CISA로 전환된 것이라고 말할 수 있다.

CISA를 「2018년 사이버안보 및 기반시설 안보국 법」에 따라 신설한 조치는 사이버안보와 기반시설 안보가 미국정부의 정책에서 중점 분야로 격상된 것을 나타낸다. 이후 CISA는 사이버안보와 기반시설 안보에 대한 위험을 관리하기 위한 계획, 분석, 협업 담당 조직인 국가 위험 관리 센터(NRMC: National Risk Management Center)를 설치했다.[160]

---

158) *Ibid.*

159) 미국 의회 홈페이지(2024e), "H.R.3359 - An act to amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes"(검색일: 2024. 11. 5.).

160) Congressional Research Service(2019), "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress"(검색일: 2024. 11. 6.).

NRMC와 별개로, CISA의 조직 내에는 사이버보안, 기반시설 보안, 응급통신, 통합 운영, 이해관계자 참여를 담당하는 각각의 부서가 설치되어 있다.[161] CISA의 임무는 국가의 주요 기반시설을 물리적 위협과 사이버 위협으로부터 보호하는 것이기 때문이다. 응급통신 담당 부서의 임무는 응급통신 능력 향상을 위한 훈련, 조정, 지침 등을 제공하는 것이다. 이해관계자 참여 담당 부서의 임무는 민간 주체인 이해관계자의 참여, 협력, 그리고 조정을 임무로 한다. 이것은 미국 기반시설 상당 부분의 소유 또는 운영 주체가 민간이라는 사실에서 비롯된다.[162]

한편 2018년 12월 20일에는 중소기업의 사이버 위협 대응 능력 향상을 위해서 「미국 국립표준기술연구소 중소기업 사이버안보법(NIST Small Business Cybersecurity Act)」도 제정되었다. 이 법률의 주요 내용은 NIST가 사이버보안 위험 식별, 평가, 관리, 감소를 위한 지침을 제공하고 관련 홈페이지(Small Business Cybersecurity Corner)를 운영하도록 한 것이다.[163] NIST는 상무부 산하기관이다.

5) 「2019년 안전하고 신뢰할 수 있는 통신네트워크법」

2020년 3월 12일에 제정된 「2019년 안전하고 신뢰할 수 있는 통신네트워크법(Secure and Trusted Communications Networks Act of 2019)」의 제정 목적은 미국의 연방 보조금이 국가안보 위험(national security risks)을 초래하는 통신 장비 또는 서비스를 구매하는 데 사용되는 것을 금지하고, 국가안보 위험을 초래하는 통신 장비 또는 서비스의 교체 및 기타 목적을 위한 환급 제도의 근거를 마련하기 위해 제정되었다. 구체적으로 제2조는 국가안보에 위험을

161) CISA 홈페이지(2024b), "Divisions & Offices"(검색일: 2024. 11. 6.).
162) 한국과학기술정보연구원 홈페이지(2024), 「미 국토안보부(DHS), 사이버보안 및 기반보호를 위한 전문기관(CISA) 설립」(검색일: 2024. 11. 6.).
163) NIST 홈페이지(2024), "Cybersecurity: Challenges and Opportunities for Small Businesses, Field Hearing"(검색일: 2024. 11. 4.).

초래하는 통신 장비로서 이 법률의 적용 대상이 되는 '대상 통신 장비 및 서비스 목록(covered communications equipment or services list)'을 작성할 책무를 연방통신위원회(FCC: Federal Communications Commission)에 부여한다. 또한 제4조는 안전하고 신뢰할 수 있는 통신 네트워크 환급 제도를 FCC가 마련하여 통신 장비 및 서비스의 교체 비용을 지원하도록 규정한다.[164]

「안전하고 신뢰할 수 있는 통신네트워크법」에 대하여 총 19억 달러(한화 약 2조 6,500억 원)의 자금이 2020년 12월 27일에 제정된 「2021년 통합 세출법(Consolidated Appropriations Act)」에 따라 배정되었다. 이 중에서 통신 장비 및 서비스의 교체 비용 환급에 18억 9,500만 달러(한화 약 2조 6,000억 원)가 배정되었다. 「2019년 안전하고 신뢰할 수 있는 통신네트워크법」에 따른 환급금 수혜자에는 초고속 광대역 통신망과 같은 고급 통신 서비스를 공급하는 고객 수 2백만 명 이하의 소규모 통신 서비스 제공자가 포함된다. 이에 더하여 「2021년 통합 세출법(Consolidated Appropriations Act)」은 최종 사용자에게 시설 기반 광대역 서비스를 공급하는 고객 수 1,000만 명 미만의 통신 서비스 제공자, 학교, 도서관, 의료 서비스 제공업체 또는 이들의 컨소시엄을 포함하도록 규정하여 수혜 자격을 확대했고, 환급 순위도 소규모 공급자, 교육 및 의료 기관, 나머지 신청자로 규정했다.[165]

'대상 통신 장비 및 서비스'의 정의는 이 법에 없다. 이에 대해 이 법 제2조 (c)항은 「2019 회계연도 존 S. 매케인 국방수권법(John S. McCain National Defense Authorization Act for Fiscal Year 2019)」의 정의를 따른다고 규정한다.[166] 이에 따르면 화웨이 테크놀로지스 컴퍼니, ZTE 코퍼레이션 및 기타 세 개 중국 기업에서 생산한 통신 장비로 정의된다. 2021년 3월 FCC는 화

164) 미국 의회 홈페이지(2024f), "H.R.4998 - Secure and Trusted Communications Networks Act of 2019"(검색일: 2024. 11. 5.).
165) Congressional Research Service(2023b), "Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions"(검색일: 2024. 11. 6.).
166) 미국 의회 홈페이지(2024f), "H.R.4998 - Secure and Trusted Communications Networks Act of 2019"(검색일: 2024. 11. 5.).

웨이, ZTE 및 기타 3개 중국 기업의 상품을 포함한 대상 장비 및 서비스 목록을 발표했고, 환급 프로그램은 화웨이와 ZTE 장비에 적용했다.[167] 또한 이 법 제4조 제(e)항은 장비 및 서비스 교체 비용을 환급받은 자는 지출 보고서를 FCC에 제출해야 하고, FCC는 불시에 현장 조사를 실시하여 신청서대로 장비가 대체되었는지 확인해야 한다고 규정한다.[168]

FCC는 승인된 신청에 자금을 지원하기에 예산이 충분하지 않으면 이를 의회에 통보해야 한다. 2022년 2월 4일 FCC는 총 56억 달러(한화 약 7조 8,000억 원)에 달하는 181건의 신청서를 접수했다고 의회에 통보했다. 그런데 이어 2022년 6월 1일에는 자금 수요가 책정된 예산을 초과했다고 의회에 통보했다. FCC 위원장은 2022년 7월 15일 의회에 보낸 서한에서 소규모 제공업체의 FCC 승인 신청에 대해 지급할 28억 8,000만 달러(한화 약 4조 원)가 부족하고, 모든 적격 신청에 대해 지급할 30억 8,000만 달러(한화 약 4조 3,000억 원)가 부족하다고 보고했다.

한편 업계도 자금 조달을 가장 큰 어려움으로 들었고, 충분한 자금이 제공되지 않으면 통신 네트워크의 작동이 중단될 수도 있다고 우려했다. 더불어 반도체 부족, 필요한 부동산의 임대 계약, 인력 부족, 날씨 등 다른 요소에 의해 장비 교체가 지연될 가능성에도 우려를 표시했다.[169]

6) 「2020년 사물인터넷 사이버안보 개선법」

2020년 12월 4일에 제정된 「2020년 사물인터넷 사이버안보 개선법(IoT Cybersecurity Improvement Act of 2020)」은 연방 정부가 소유하고 관리하는 사물인터넷(IoT: Internet of Things) 기기에 대한 최소한의 보안 기준

167) Congressional Research Service(2023b), "Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions"(검색일: 2024. 11. 6.).
168) 미국 의회 홈페이지(2024f), "H.R.4998 - Secure and Trusted Communications Networks Act of 2019"(검색일: 2024. 11. 5.).
169) Congressional Research Service(2023b), "Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions"(검색일: 2024. 11. 6.).

수립을 목적으로 한다.[170]

이 법률이 제정된 배경은 2016년 10월 미국 동부의 인터넷이 미라이 봇넷(Mirai Botnet)의 공격으로 마비된 경험에서 찾을 수 있다. 미라이라는 명칭의 악성 프로그램이 비밀번호 관리가 상대적으로 부실했던 인터넷 공유기, CCTV 등 IoT 기기를 감염시킨 후에, 특정 인터넷 제공업체의 서버에 동시 접속하여 과도한 전송량을 발생시키는 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격을 감행했다.[171]

이 법의 주요 내용은 IoT 기기 관련 표준 및 지침을 NIST가 개발·게시하고, 이러한 표준 및 지침에 일치하는 연방 정부 기관에 적용될 정책과 원칙을 예산관리국(OMB: Office of Management and Budget)이 발표하도록 한 것이다. NIST는 5년마다 표준 및 지침을 검토하여 필요시 수정해야 하며, 이러한 보안 표준 및 지침을 따르지 않는 협력업체와의 계약 및 구매는 금지된다.[172]

이 법률이 기술표준을 담당하는 NIST가 관련 표준과 지침을 마련하도록 한 점은 의의로 평가할 수 있다. 그러나 모든 IoT 기기가 아니라 연방 정부가 소유하고 관리하는 IoT 기기만을 규율 대상으로 하는 점에서 한계도 명확하다.[173]

한편 연방 정부가 소유하고 관리하는 IoT 기기가 아닌 민간의 IoT 기기에는 연방통신위원회(FCC: Federal Communications Commission)의 「IoT 사이버보안 표지」 규정이 적용되며, 2024년 8월 29일부터 시행되었다. 사이버보안 표지 프로그램에는 미국정부 인증 표지(U.S. Cyber Trust Mark)와 소비자를 제품에 대한 특정 정보로 안내하는 QR 코드가 포함된다.[174]

---

170) 미국 의회 홈페이지(2024g), "H.R.1668 - IoT Cybersecurity Improvement Act of 2020"(검색일: 2024. 11. 5.).
171) 한국인터넷진흥원(2020a), 「인터넷 법제동향 제157호」, p. 12.
172) 한국인터넷진흥원(2020b), 「인터넷 법제동향 제159호」, p. 57.
173) 한국인터넷진흥원(2020a), 「인터넷 법제동향 제157호」, p. 14.
174) 미국 관보 홈페이지(2024), "Cybersecurity Labeling for Internet of Things"(검색일: 2024. 12. 11.).

7) 「2022년 핵심 기반시설 사이버사고 보고법」

2022년 3월 15일 제정된 「2022년 핵심 기반시설 사이버사고 보고법(CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act)」은 핵심 인프라 부문의 주체(entity)에게 사이버사고가 발생했을 때 일정 시간 내에 정부 기관에 보고할 법적 의무를 부과하는 것이 특징이다.

사이버사고가 발생했다고 합리적으로 믿게 된(reasonably believe) 후 72시간 이내에 이를 정부 기관에 보고해야만 하는(shall report) 법적 의무를 적용 대상 주체(covered entity)에 부과한다.[175] 특히 사이버사고 중에서도 랜섬웨어(ransomware) 공격의 결과로 대가(ransom)를 지급했을 때 적용 대상 주체는 그 때부터 24시간 이내에 이를 정부 기관에 보고해야만 하는 법적 의무를 진다.[176]

랜섬웨어 피해도 사이버사고의 한 유형에 포함되지만, 별도로 더 엄격하게 규정했다. 그 이유는 범죄자에게 전달된 자금이 추가 공격이나 다른 범죄에 빠르게 사용될 수 있는 점, 거래의 특성상 시간이 지날수록 추적이 어려워지는 점, 빠른 보고를 통해 법 집행기관이 신속하게 개입하면 자금 회수 또는 자금 추적의 가능성이 증가하는 점 등을 고려했기 때문으로 풀이된다.

「2022년 핵심 기반시설 사이버사고 보고법」에서 핵심은 적용 대상 주체라고 할 수 있는데, 이는 대통령 정책 지침(PPD-21: Presidential Policy Directive 21)에 정의된 핵심 인프라 부문의 주체(entity)로서 CISA 국장이 마련하는 최종 규칙(final rule)을 충족하는 주체로 정의된다.[177] PPD-21은 미국 오바마 전 대통령이 2013년 서명한 정책문서인데 16개 분야를 핵심 인프라 분야로 지정했다. 지정된 16개 분야는 화학, 상업시설, 통신, 주요 제조업, 댐, 국방산업기지, 비상 서비스, 에너지, 금융, 식품/농업, 정부 시설, 의료와 보건, IT,

---

175) 미국 의회 홈페이지(2024h), "H.R.2471 - Consolidated Appropriations Act, 2022," Section 2242(Required Reporting of Certain Cyber Incidents) (a)(1)(A)(검색일: 2024. 11. 25.).
176) *Ibid.*, Section 2242(Required Reporting of Certain Cyber Incidents) (a)(2)(A)(검색일: 2024. 11. 25.).
177) *Ibid.*, Section 2240(Definition) (5)(검색일: 2024. 11. 25.).

원자력 시설, 교통, 수처리와 상하수도이다.[178] 그러므로 민간 병원, 민간 통신 회사, 민간 IT 서비스회사의 소유자나 운영자는 이 법의 적용 대상 주체가 될 가능성이 있다. 그러나 CISA 국장의 최종 규칙은 2024년 3월 27일부터 6월 3일까지 국민으로부터 의견을 접수받았을 뿐, 아직 마련되지 않았다.[179]

다. 특징

미국의 사이버안보 전략과 법령의 특징은 다음과 같이 정리할 수 있다. 먼저 미국의 2023년 「국가 사이버안보 전략」은 사이버안보 최소 요건의 적용을 확대하여 중요 인프라 복원력을 확보한다. 이것은 2021년 발생한 콜로니얼 파이프라인 해킹 공격으로 민간 부문의 자발적 보안 체계는 사이버안보 위협에 효과적인 대응책일 수 없다는 점이 드러났다고 보아, 정부의 직접 개입과 보안 요구사항의 강제적 적용 필요성이 제기된 결과물이다. 중요 인프라의 상당수를 민간이 소유 또는 운영하는 미국은 「2003년 안전한 사이버공간을 위한 국가 전략」에서부터 민관협력 체계 구축과 사이버사고 대응을 위한 미국 연방 차원의 대응계획을 수립했다. 또한 미국은 2024년 「국가 사이버안보 전략 이행계획」에 따라 안전한 ICT 생태계를 위한 정책 및 규제를 국제적 차원에서 채택하기 위해 동맹국과의 협력을 추진했다. 특히 미국의 「CISA 전략계획 2023~2025」에는 미국의 핵심 네트워크에 대한 침해가 발생하기 전에 능동적으로 위협을 완화한다는 내용이 포함되었다. 구체적 방법으로 네트워크 모니터링, 위협 분석, 사이버 위협 수색 등이 제시되었다.

---

178) CISA 홈페이지(2024c), "Presidential Policy Directive(PPD) 21: Critical Infrastructure Security and Resilience," Section 2240(Definition) (5)(검색일: 2024. 11. 25.).

179) CISA 홈페이지(2024d), "CISA Marks Important Milestone in Addressing Cyber Incidents; Seeks Input on CIRCIA Notice of Proposed Rulemaking," Section 2240(Definition) (5)(검색일: 2024. 11. 25.).

다음으로 미국 사이버안보 법률의 특징은 정부 내 전담 조직 설치, 새로운 사이버 위협 대응, 그리고 민간과의 공조 강화를 위한 근거법 제정으로 요약할 수 있다. 「2014년 국가 사이버안보 보호법」은 사이버 위협에 대한 통합 대응을 요청한 위원회 등의 권고로 이미 설치해 운영하던 사이버안보 전담 조직 NCCIC를 명시하는 법적 근거를 마련했다. NCCIC는 NPPD의 한 부서로 설치되었고, 이후 「2018년 사이버안보 및 기반시설 안보국 법」에 따라 NPPD가 CISA로 전환되었다. 「2014년 사이버안보 강화법」에서는 핵심 인프라에 대한 사이버 위협을 줄일 민간 주도의 표준 등의 개발을 촉진하고 지원했다. 특히 「2015년 사이버안보법」에서는 민간이 사이버 위협 지표에 관한 정보를 정부와 자발적으로 공유하도록 장려하기 위한 보호조치로서, 통신 비밀에 관한 여러 법률에 따른 책임으로부터의 면책을 규정했다. 또한 「2019년 안전하고 신뢰할 수 있는 통신네트워크법」에 따라 미국의 국가안보 위험을 초래하는 통신 장비 또는 서비스의 교체를 위한 환급 제도의 근거를 마련했고, 이후 예산이 배정되어 신청도 받는 등 시행되고 있다. 나아가 미국은 2016년 미국 동부의 인터넷이 미라이 봇넷의 공격으로 마비된 후, 「2020년 사물인터넷 사이버안보 개선법」을 제정하여 연방 정부가 소유하고 관리하는 IoT 기기에 대한 최소한의 보안 기준을 마련했다. 「2022년 핵심 기반시설 사이버사고 보고법」은 핵심 인프라 소유자 또는 운영자에게 사이버사고 발생과 랜섬웨어 피해에 대해 각각 72시간, 24시간 내 보고의무를 부과했는데, 적용 대상 주체에 관한 구체적인 기준은 하위 규정이 확정되어야 알 수 있다.

2. EU

가. 전략

1) 2013년 「EU 사이버안보 전략」

2013년 EU 최초의 통합적인 사이버안보 전략으로 발표된 「EU 사이버안보 전략(EU Cybersecurity Strategy)」은 사이버보안 분야에서 EU의 비전 및 역할, 책임 및 필요한 조치를 규정했다. 이 전략은 「EU 디지털 어젠다」로 편입되어 그 일부를 형성했다. EU는 활기찬 디지털 사회를 위해서는 인터넷 신뢰와 보안이 필수적이라고 보았다.[180]

2013년 「EU 사이버안보 전략」은 5대 사이버보안 정책의 원칙으로 (ⅰ) 오프라인과 온라인에서 같은 핵심 가치 적용, (ⅱ) 표현의 자유, 개인정보 등 기본권 존중, (ⅲ) 인터넷 접근성 향상을 위한 사이버 보안성 확보, (ⅳ) 다수 이해관계자의 거버넌스 접근 지지, (ⅴ) 사이버 위협 해결을 위한 민간·공공 등 관련 부문 사이의 효율적 대응 등의 준수를 제시했다. 이를 위해 사이버 복구 능력 강화, 사이버 범죄 예방 및 억제, 사이버보안 능력 제고를 위한 산업 및 기술 자원 개발, 공동 보안 및 사이버 방어 정책 및 역량 개발, EU의 통일된 사이버공간 정책 수립 및 EU의 핵심 가치 실현을 위해 노력하기로 했다.[181]

사이버안보의 맥락에서 중앙 집중화된 EU의 감독은 해결책이 아니며, EU 각 회원국의 사이버사고 예방 및 대응도 중요함을 강조했다. 따라서 2013년 「EU 사이버안보 전략」은 EU와 회원국 각각의 차원에서 사이버안보를 담당할 기관을 정하고, 사이버안보를 네트워크 및 정보보안, 법 집행, 방위의 세 가지 분야(pillar, 기둥)로 나누어 다루었다.

첫째, 네트워크 및 정보보안 분야에는 EU 집행위원회(EU Commission),

180) NATO 사이버 방위센터 홈페이지(2024), "European Union"(검색일: 2024. 11. 6.).
181) 박민숙, 이효진(2020), p. 42.

EU 사이버안보청(ENISA: European Union Agency for Cybersecurity), EU 회원국의 컴퓨터비상대응팀 네트워크(CERT-EU), 회복성을 위한 유럽 공공-민간 파트너십이 참여했다. 법적 조치에 대한 표준을 설정하고 안전한 온라인 환경을 만들기 위한 인센티브 제공, 민간 부문과의 협업과 국제협력, 중요 ICT 인프라 보안 및 복원력 강화를 목표로 활동했다. 특히 네트워크 및 정보시스템에 관한 EU 차원의 지침을 제안했다.

둘째, 법 집행 분야에는 유럽 사이버 범죄 센터와 EUROPOL 등이 참여했다. 사이버 범죄에 관한 더 강력한 형사 제재를 도입하는 등 EU 회원국의 국내법을 강화함으로써 대규모 사이버공격에 대처하는 것을 목표로 하는 내용의 정보시스템 공격에 대한 지침을 채택했다.

셋째, 방위 분야에는 EU 군사 참모부, 유럽 방위청(EDA) 등이 참여했다. 방위 분야와 관련하여, 2013년 「EU 사이버안보 전략」은 "특별히 심각한 사이버 사고나 공격은 회원국이 EU 연대 조항(EU 기능조약 제222조)을 적용할 충분한 근거가 될 수 있다"라고 명시했다.[182]

2) 2020년 「EU 사이버안보 전략」

2020년 12월 16일 EU 집행위원회(EU Commission)는 「EU 사이버안보 전략(EU Cybersecurity Strategy)」을 발표했다. 이 전략의 목표는 사이버 위협에 대한 유럽의 집단적 복원력을 강화하고, 모든 시민과 기업이 안정적이고 신뢰할 수 있는 서비스와 디지털 도구의 혜택을 충분히 누릴 수 있도록 돕는 것이다. 이를 위해 사이버공간에서 국제규범과 표준에 대한 지도력을 강화하고, 전 세계 파트너들과 협력을 강화하여 법치주의, 인권, 기본적 자유, 민주적 가치에 기반한 글로벌하고 개방적이며 안정적이고 안전한 사이버공간을 촉진한다. 또한 디지털화와 상호 연결성으로 인해 증가하는 위협에 대응하기 위해 연합 전체의 높은 공통 수준의 사이버안보를 강화하고자 기존 「네트워크 및 정보

182) NATO 사이버 방위센터 홈페이지(2024), "European Union"(검색일: 2024. 11. 6.).

시스템(NIS: Network and Information Systems) 지침」을 개정한 NIS 2를 채택할 것을 제안했다.

「EU 사이버안보 전략」은 (ⅰ) 복원력, 기술적 주권 및 리더십, (ⅱ) 예방, 억제 및 대응을 위한 운영 역량구축, (ⅲ) 협력 강화를 통한 글로벌하고 개방적인 사이버공간 구축이라는 세 가지 영역으로 나누어 규제, 투자, 정책의 측면에서 구체적인 제안을 했다. 이러한 전략의 실현을 위해 EU는 향후 7년 동안 차기 장기 EU 예산을 투자하여, 특히 디지털 유럽 프로그램과 Horizon Europe, 유럽 회복 계획을 통해 사이버안보 전략을 지원하기로 합의했다. 공공과 민간을 합하여 총 45억 유로(한화 약 6조 7,000억 원)를 투자할 계획이다.[183]

3) 2022년 「EU 사이버 방어 정책」

2022년 11월 10일 EU 집행위원회는 「EU 사이버 방어 정책(EU Policy on Cyber Defence)」을 발표했다. 이 정책의 주요 내용은 (ⅰ) 국가 및 EU 사이버 방어 주체 사이의 조정 제도 강화, (ⅱ) EU 방위 생태계 보호, (ⅲ) 사이버 방어 역량에 대한 투자, (ⅳ) 공통 과제 해결을 위한 동반관계 구축이다. 「EU 사이버 방어 정책」이 발표된 배경은 2020년 「EU 사이버안보 전략」에서 EU 사이버 방어 정책 검토의 필요성이 강조된 것에서 찾을 수 있다. 또한 더 직접적인 배경은 러시아의 우크라이나 침략에 따라 악화하는 안보 환경을 해결하고 EU의 시민과 인프라를 보호하는 역량을 강화하기 위해서이다.[184]

183) EU 집행위원회 보도자료(2020. 12. 16.), "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient"(검색일: 2025. 2. 4.).
184) EU 집행위원회 보도자료(2022. 11. 10.), "Cyber Defence: EU boosts action against cyber threats"(검색일: 2024. 12. 10.).

나. 법률

1) 2016년 「네트워크 및 정보시스템 법」

2016년 8월 8일 EU의 사이버안보 분야 최초 법률인 「네트워크 및 정보시스템 법(NIS: Network and Information Systems Directive)」이 발효했다.[185] EU 스스로 이 법률을 NIS1으로, 2023년 개정 법률을 NIS2로 부르기도 한다. 국내 자료에서는 지침으로 옮기기도 한다.

EU 법의 두 가지 유형으로 지침(Directive)과 규정(Regulation)이 있고, 두 가지 모두 EU 회원국이 이에 반하는 국내법을 제정하거나 국내 정책을 추진할 수 없는 법적 효력이 있다는 공통점이 있다. 양자의 차이는 EU 규정은 EU 회원국의 국내법 체계에서 국내법과 같은 지위로서 직접 적용되지만 EU 지침은 이러한 효력이 없다는 점이다. 그런데 개인정보에 관한 EU 규정을 우리나라에서는 EU 개인정보보호법으로 번역하는 것이 일반적이다. 따라서 이 연구에서도 네트워크 및 정보시스템 지침(Directive)이라 하지 않고 법이라고 옮긴다.

2016년 「네트워크 및 정보시스템 법」의 주요 내용은 다음과 같다. 첫째, 디지털 서비스의 다양한 유형 중에서 에너지, 운송, 금융, 의료, 식수, 디지털 기반시설은 부속서 2에 따른 필수서비스(Essential Service)로, 온라인 시장, 온라인 검색엔진, 클라우드컴퓨팅 서비스는 부속서 3에 따른 디지털 서비스(Digital Service)로 정의되었다.[186] 둘째, 법률의 적용 대상자는 특정 분야에 종사하는지에 따라 정하여, 필수서비스 운영자(Operator of Essential Services)와 디지털 서비스 제공자(Digital Service Provider)로 나누었다.[187] 셋째, 필수서비스 또는 디지털 서비스 유형에 해당하는 서비스를 제공

185) EU 집행위원회 홈페이지(2024a), "Cybersecurity Policies"(검색일: 2024. 11. 6.).
186) EUR-Lex 홈페이지(2024a), "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union"(검색일: 2024. 11. 17.).
187) *Ibid.*

하는 기업이면 기업 규모와 무관하게, 중소기업이라고 하더라도 원칙적으로 이 법률이 적용되었다.[188]

이 법률 제14조(보안 요건과 사고 통지)는 필수서비스 운영자가 네트워크 및 정보시스템에 대한 위험을 관리할 적절한 기술적 또는 조직적 조치를 하고, 보안 사고가 발생하면 즉시 통지하도록 보장할 법적 의무가 EU 회원국에 있다고 규정한다.[189]

2) 2023년 「네트워크 및 정보시스템 법」

2023년 1월 16일 EU의 「네트워크 및 정보시스템 법」이 발효했다. 2024년 10월 18일부터 이 법은 2016년 「네트워크 및 정보시스템 법」을 대체했다.[190] 2023년 법률을 제정한 이유는 기존 2016년 법률의 성과에도 불구하고 EU 회원국 사이에, 그리고 각 산업 부문 사이에 복원력의 수준이 일정하지 않고, EU 내 사업체의 사이버 복원력 수준이 충분하지 않으며, 주요 위협에 대한 공통된 이해와 공동 위기 대응이 부족하다고 평가되었기 때문이다.[191]

2023년 법률의 주요 내용은 다음과 같다. 첫째, 디지털 서비스를 중요도가 높은 분야(Sectors of High Criticality)와 기타 중요 분야(Other Critical Sectors)로 나누었다. 기존 법률에서는 필수서비스(Essential Service)와 디지털 서비스(Digital Service)로 나누었는데, 2023년 법률에서는 기존 법률의 필수서비스에 공공행정(사법부, 의회, 중앙은행 미포함), 폐수, ICT 서비스 관리, 우주를 추가했다. 특히 클라우드컴퓨팅 서비스가 기존 법률에서는 필수서비스가 아닌 디지털 서비스에 포함되었으나 개정 법률에서는 중요도가 높은

188) 고은아 외(2023), pp. 20~22.
189) EUR-Lex 홈페이지(2024a), "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union"(검색일: 2024. 11. 17.).
190) EU 집행위원회 홈페이지(2024a), "Cybersecurity Policies"(검색일: 2024. 11. 6.).
191) EU 집행위원회 홈페이지(2024b), "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs"(검색일: 2024. 11. 24.).

분야로 격상되었다.[192]

둘째, 개정 법률은 적용 대상자를 필수 조직(Essential Entities)과 중요 조직(Important Entities)으로 나누었다.[193] 특정 분야에 해당하는지에 따라 일률적으로 지침의 적용 대상자를 정하기보다는, 위험에 따라 유연하게 적용함으로써 규제 효과를 유지하면서도 기업 부담을 줄이고자 한 것으로 평가할 수 있다.

셋째, 기존 법률에서는 중기업(Medium-sized Enterprise)에 대한 정의 및 기준이 없었으나,[194] 개정 법률에서는 법률이 중기업 이상의 기업에 적용된다고 명시하고 중기업의 정의에 관한 조항을 추가했다. 중기업은 직원 수 50~250명, 매출액 1,000만~5,000만 유로, 연간 대차대조표 총액 1,000만~4,300만 유로의 기업으로 정의된다.[195] 그 결과 기존 법률에서는 필수서비스 또는 디지털 서비스에 해당하는 서비스를 제공하는 기업이면 기업 규모와 무관하게, 소규모 기업이더라도 원칙적으로 적용 대상이었으나, 개정 법률에 따르면 소규모 기업은 적용 대상에서 제외된다.

3) 2019년 「사이버안보법」

2019년 6월 27일 EU의 「사이버안보법(EU Cybersecurity Act)」이 발효했다. 제69조(발효) 제1항에 따라 이 법이 관보에 게재된 날로부터 20일 후에 조항 대부분이 발효했다. 다만 제58조(국가 사이버보안 인증 당국), 제60조(적합성 평가 기관), 제61조(통지), 제63조(제소권), 제64조(사법 구제권), 제65조(벌칙)는 제69조(발효) 제2항에 따라 발효일로부터 2년 후인 2021년 6월 28일

192) EUR-Lex 홈페이지(2024b), "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA)"(검색일: 2024. 11. 17.).
193) *Ibid.*
194) EUR-Lex 홈페이지(2024a), "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union"(검색일: 2024. 11. 17.).
195) 고은아 외(2023), pp. 20~22.

부터 적용되었다.[196]

「사이버안보법」의 주요 내용은 두 가지다. 첫째, ENISA에 영구적 권한을 부여하여 기관을 강화하고, 재정 및 인적 자원을 보강하며, EU가 높은 수준의 공통된 사이버안보를 달성하도록 지원하는 역할을 전반적으로 향상하는 것이다. 둘째, EU 역내 시장에서 공통된 사이버보안 인증 접근 방식을 보장하고 궁극적으로는 IoT와 같은 광범위한 디지털 상품 및 서비스의 사이버보안을 개선하기 위해 EU 전역에 적용되는 EU 사이버보안 인증 제도(European cybersecurity certification framework)를 구축한다.[197]

EU 사이버보안 인증 제도는 EU 디지털 단일 시장을 강화하고 소비자에게 보안에 관한 더 많은 정보를 제공하기 위한 자발적인 성격의 제도이다.[198] ICT 상품에 대한 EUCC 인증에 관한 법이 2024년 1월 제정되어 2월 27일부터 시행됐다. 또한 클라우드컴퓨팅 서비스에 대한 EUCS 인증 제도의 초안을 마련하여 의견 수렴 절차를 거치고 있고, 5G 통신에 대한 EU5G 인증은 개발을 위한 두 단계 중 첫 번째 단계를 마쳤다. 인공지능(AI: Artificial Intelligence)에 대한 인증 제도는 준비 단계에 있다.[199] 특히 2024년 1월 31일 ICT 상품에 대한 EUCC 인증 시행을 위한 법을 제정했고 2024년 2월 27일부터 시행했다. 제50조에 규정된 일부 조항은 2025년 2월 27일부터 적용된다.[200] 이 법에서 말하는 기준은 ISO/IEC 15408이라는 국제 표준화 기구의 표준을 따른다.[201]

---

196) EUR-Lex 홈페이지(2021), "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)" (검색일: 2024. 12. 11.).

197) EU 집행위원회 홈페이지(2019), "The Cybersecurity Act strengthens Europe's cybersecurity" (검색일: 2024. 12. 11.).

198) ENISA 홈페이지(2024a), "What is EU Cybersecurity Certification?"(검색일: 2024. 12. 11.).

199) ENISA 홈페이지(2024b), "Developing Certification Schemes"(검색일: 2024. 12. 11.).

200) ENISA 홈페이지(2024c), "EUCC Certification Scheme"(검색일: 2024. 12. 11.).

201) EUR-Lex 홈페이지(2024d), Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European

4) 2023년 「사이버안보법(개정안)」

2023년 4월 18일 EU 집행위원회는 「사이버안보법(개정안)」을 제안했다. 2019년에 제정된 기존 「사이버안보법」에 대한 개정 제안이다. 주요 내용은 '관리형 보안 서비스(managed security services)'에 대한 유럽 인증 제도를 채택하는 것이다.[202] 「EU 사이버안보법(개정안)」 주해(recital) 제2항은 관리형 보안 서비스에 대해 고객의 사이버보안 위험관리와 관련된 활동을 수행하거나 지원하는 서비스라고 설명한다.[203] 관리형 보안 서비스에는 사고 대응, 침투 테스트, 보안 감사 및 컨설팅과 같은 분야를 포함하는 관리형 보안 서비스에 대한 인증 제도가 포함된다.[204] 관리형 보안 서비스는 개정안에서 신설된 내용으로, 시행 중인 2019년 「사이버안보법」에는 없는 내용이다.

5) 2024년 「사이버복원력법」

2024년 12월 10일 EU의 「사이버복원력법(Cyber Resilience Act)」이 발효되었다. 이 법률에 규정된 주요 의무는 2027년 12월 11일부터 적용된다. 이 법률은 2020년 「EU 사이버안보 전략」에 따라 제정되었으며 2023년 「네트워크 및 정보시스템 법」을 보완한다. 「사이버복원력법」이 제정된 목적은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품의 사이버보안 표준을 강화하여, 제조업체와 소매업체가 제품 수명주기 전반에 걸쳐 사이버안보를 보장하는 것이다. 이러한 목적을 위해 「사이버복원력법」은 다른 장치나 네트워크에 직간접적으로 연결된 모든 상품의 계획, 설계, 개발 및 유지관리 단계에 의무적 사이버보안 요구사항을 도입했다. 다만 특정 오픈소스 소프트웨어 또는 기존 법률

Common Criteria-based cybersecurity certification scheme(EUCC)," 제2조(정의) 제1항 (검색일: 2024. 12. 11.).

202) EU 집행위원회 홈페이지(2023a), "Proposed Regulation on 'managed security services' amendment"(검색일: 2024. 11. 7.).

203) EUR-Lex 홈페이지(2023), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services"(검색일: 2024. 12. 11.).

204) EU 집행위원회 홈페이지(2023b), "The EU Cybersecurity Act' amendment"(검색일: 2024. 11. 7.).

의 규제를 받는 의료기기, 항공기, 자동차 등의 서비스 상품은 적용 대상에서 제외했다.[205]

디지털 요소가 있는 상품은 「사이버복원력법」 제6항에 규정된 분류 기준에 따라 중요 상품(critical product)과 핵심 상품(highly critical product)으로 나뉜다.[206] 구체적인 상품의 목록은 EU 집행위원회가 제안하기로 했다.[207] 중요 상품은 등급 Ⅰ과 Ⅱ로 나뉘는데, 등급 Ⅱ가 더 높은 위험성을 내포한다. 등급 Ⅰ에는 소프트웨어, 브라우저, 네트워크 관리 시스템, VPN 등이, 등급 Ⅱ에는 방화벽, 라우터, 인터넷 연결용 모뎀 등이 속한다. 제조업체의 의무는 사이버보안 위험 평가, 기술문서 작성, 적합성 평가 수행, EU 적합성 선언서 작성, 취약점 관리, 사고 보고 등이다.[208]

제조업자는 이 법 부속서 1(필수적 사이버 요건) 제1항에 규정된 필수 요구사항에 따라 상품이 설계, 개발 및 생산되었는지 확인하고, 상품 관련 사이버보안 위험을 평가하여 제조 단계에 고려하며, 기술문서를 작성한다. 적합성평가 절차를 수행하고 지속적인 적합성 유지하며 취약점을 인지하면 시장감시 당국과 사용자에게 알려야 한다. 상품이 필수 요구사항을 충족하지 않으면, 제조업자는 시정 조치를 취해야 한다.[209]

수입업자와 유통업자는 디지털 요소가 있는 상품을 시장에 판매하기 전에 CE(Conformité Européenne) 표지(CE marking)를 부착할 법적 의무가 있다. CE 표지는 디지털 요소가 있는 상품이 「사이버복원력법」의 요구사항을

---

205) EU 집행위원회 홈페이지(2024c), "EU Cyber Resilience Act"(검색일: 2024. 11. 7.).
206) 제3조(정의) 제3항 및 제4항, 제6조(디지털 요소가 있는 상품) 제2항 및 제5항, EUR-Lex 홈페이지(2024c), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"(검색일: 2024. 12. 11.).
207) 한국인터넷진흥원(2024), p. 31.
208) 한국인터넷진흥원(2022), pp. 23~26.
209) 제10조(제조업자의 의무) 및 제11조(제조업자의 보고의무). EUR-Lex 홈페이지(2024c), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"(검색일: 2024. 12. 11.).

준수함을 나타내는 표지이다. 나아가 수입업체 또는 유통업체는 요건을 갖춘 상품만 수입 및 유통할 수 있고, 심각한 보안 취약점이 있다고 판단하면 제조업체와 시장감시 당국에 알릴 법적 의무가 있다.[210]

필수적 사이버 요건(부속서 1)과 제조업자의 의무(제10조 및 제11조) 위반에 대해서는 최대 1,500만 유로(한화 약 225억 원) 또는 위반한 경제주체가 회사인 때에는 전년도 세계 연간 매출액의 2.5% 중 더 높은 금액의 과징금이 부과된다. 이 법에 규정된 다른 의무 위반에 대해서는 최대 1,000만 유로(한화 약 150억 원) 또는 위반한 경제주체가 회사인 때에는 전년도 세계 연간 매출액의 2% 중 더 높은 금액에 해당하는 과징금이 부과된다.[211]

한편 「사이버복원력법」은 초안이 2002년 9월 제안된 후, 과도한 부담과 적용 범위의 모호함에 대한 우려가 EU 회원국으로부터 제기되었다. 그 결과 최종적으로는 EU 회원국이 합의한 수정안이 발효되었다. 원본 상품과 동일한 개발 및 생산 과정을 거쳐 제조된 예비 부품을 제조업체가 사용하는 때는 예외로 인정하여 적용 범위에서 제외한다는 규정을 신설했다.[212]

6) 2024년 「사이버 연대법」

2025년 2월 4일 EU의 「사이버 연대법(Cyber Solidarity Act)」이 발효되었다. 2023년 4월 19일 EU 집행이사회가 제안했고, 2024년 12월 19일 EU 의회(European Parliament)와 EU 이사회(EU Council)가 서명했으며, 2025년 1월 15일 관보에 게재되었다.[213]

---

210) 제13조(수입업자의 의무) 제2항, 제14조(유통업자의 의무) 제2항. EUR-Lex 홈페이지(2024c), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"(검색일: 2024. 12. 11.).

211) 제53조(벌칙). EUR-Lex 홈페이지(2024c), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"(검색일: 2024. 12. 11.).

212) 한국인터넷진흥원(2023), p. 15, p. 18.

213) EUR-Lex 홈페이지(2025), "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and

이 법의 제정 목적은 유럽 사이버보안 (ⅰ) 경보 시스템, (ⅱ) 비상 시스템, (ⅲ) 검토 시스템을 구축하는 것이다. 첫째, 경보 시스템은 EU 회원국 사이의 사이버 허브 네트워크로 구성된다. AI 및 고급 데이터 분석과 같은 최첨단 도구와 기반시설을 활용하여 사이버 위협 및 사고를 신속하게 감지한다. 둘째, 비상 시스템은 대비 조치, EU 사이버보안 보호구역 창설, 상호 지원 보장의 세 영역으로 구성된다. 대비 조치는 보건, 에너지 등의 분야에서 운영되는 기관의 잠재적 취약성을 파악하기 위한 대비 테스트를 포함한다. EU 사이버보안 보호구역은 회원국이나 연합 기관, 단체, 기관의 요청에 따라 배치될 수 있는 민간 서비스 제공자('신뢰할 수 있는 공급자')의 사고 대응 서비스로 구성된다. 대규모 사이버보안 사고 해결에 EU 사이버보안 보호구역이 도움이 될 수 있다. 상호 지원 보장은 중대 또는 대규모 사이버보안 사고로 피해를 당한 EU 회원국에 기술 지원을 제공하는 EU 회원국에 재정지원을 한다는 내용이다. 셋째, 검토 시스템은 중대 또는 대규모 사이버보안 사고를 검토하고 평가한다. 이를 바탕으로 개선을 위한 권고안을 제출한다.[214]

다. 특징

EU의 사이버안보 전략은 기본권 존중을 강조한다. 또한 시기별로 약간의 변화를 보인다. 2013년 「EU 사이버안보 전략」에서는 안전하면서도 개방적인 사이버공간을 강조했다. 한편 2020년 「EU 사이버안보 전략」에서는 복원력과 기술 주권을 강조했다. 각각의 전략에 따라 「네트워크 및 정보시스템 법」이 제정되고 개정되었다. 2013년 전략에 없던 예산 계획이 2020년 전략에는 마련되었다. 전략이 점차 구체화하고 있다고 평가할 수 있다.

---

capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)"(검색일: 2025. 2. 6.).

214) EU 집행위원회 보도자료(2024), "Commission welcomes political agreement on Cyber Solidarity Act"(검색일: 2024. 11. 7.).

EU 사이버안보 법률의 특징은 EU 조직과 EU 법의 특성을 고려하여, 사안별로 그에 맞는 EU 지침과 EU 규정으로 제정되고 있다. 디지털 서비스 공급자가 적절한 보안 조치를 했는데도 보안 사고가 발생하면 즉시 통지할 의무는 EU가 직접 규율하지 않고 EU 회원국에 맡긴다. 「네트워크 및 정보시스템 법」은 EU 지침으로 제정한 것이다. 반면 사고 대응 등을 수행하는 관리형 보안 서비스에 대한 인증 제도를 규정한 「사이버안보법」과 디지털 구성 요소가 포함된 소프트웨어 또는 하드웨어 상품의 사이버보안 준수 표지 부착을 규정한 「사이버복원력법」은 EU 회원국의 법체계에 직접 적용되는 EU 규정이다.

또한 시행 과정에서 과도한 부담이 되는 부분, 또는 EU 역내에서 불일치가 있는 부분에 개선이 이루어진 점도 EU 사이버안보 법률의 특징이다. 2016년 「EU 네트워크 및 정보시스템 법」에는 적용 대상 기업의 규모에 관한 규정이 없었으나, 2023년 「EU 네트워크 및 정보시스템 법」에서는 중기업 이상의 기업에 적용됨을 명확히 하여 소기업이 부담을 덜게 되었다. EU 회원국마다 사이버보안 인증 제도가 여전히 불일치하여 시장의 파편화 현상이 발생하자 이를 바로잡고자 2023년 「EU 사이버안보법(개정안)」이 제안되었다.

끝으로 EU 사이버안보 법률은 직접적인 수입 제한 조치보다는 인증 제도 또는 표시 제도와 같은 간접적인 조치를 사용한다. EU는 2019년 「사이버안보법」을 제정하여 다양한 사이버보안 인증 제도를 마련하고 있다. 이에 따라 2024년에는 ICT 상품에 대한 EUCC 인증 시행법이 제정되었다. 클라우드컴퓨팅 서비스, 5G 통신, AI에 대한 인증도 준비하고 있다. 또한 2024년 「사이버복원력법」은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품에 보안 요건을 준수한다는 CE 표지를 부착할 법적 의무를 수입업자 또는 유통업자에게 부과했다.

3. 일본

가. 전략

1) 「사이버보안 전략」

일본 「사이버보안 전략(サイバーセキュリティ戦略)」은 2024년 현재까지 2013년, 2015년, 2018년, 2021년 등 총 네 건의 문서가 책정된 바 있다.[215] 2013년 6월에 책정된 「사이버보안 전략」은 사이버공간을 둘러싼 위험이 확산해 글로벌 수준의 문제가 된 배경에서, 「정보보안 전략(国民を守る情報セキュリティ戦略)」(2010년 5월 책정)을 대체해 더 포괄적인 대응 전략을 마련하기 위해 '정보보안'에서 '사이버보안'으로 정책 용어를 변경한 데에 의의가 있다.[216] 「사이버보안 기본법」에 근거해 각의 결정[217] 방식으로 책정되는 「사이버보안 전략」은 2015년 문서가 처음으로, '자유, 공정, 안전한 사이버공간의 창출·발전'이라는 일본의 사이버보안에 대한 가치관을 국제사회에 공표한 문서로 평가된다.[218]

가장 최근에 책정된 문서는 2021년 「사이버보안 전략」으로, 2021년 이후 3년간, 즉 2024년까지 일본의 관련 정책이 지향해야 할 방향성을 제시한다. 주요 내용은 다음과 같다.

먼저 일본 사이버보안 전략의 목적은 「사이버보안 기본법」 제1조에 명시된 바와 같이 (ⅰ) 경제사회의 활력 향상 및 지속적 발전(이하 경제사회), (ⅱ) 국민

215) 일본은 가타카나인 사이버시큐리티(サイバーセキュリティ)란 용어를 활용하고 있다. 본 절에서는 2022년 「국가안보전략」에 명시된 사이버안보(サイバー安全保障)와 차별성을 두고자 사이버시큐리티를 사이버보안으로 통칭한다. 사이버안보(サイバー安全保障)란 용어의 정의는 「국가안보전략」에 별도로 명시되지는 않았으나, 기밀성, 완전성, 가용성의 확보를 의미하는 사이버보안 외에 국가나 중요 인프라 등의 안보를 염두에 둔 능동적인 사이버 방어 관련 조치를 포함하는 포괄적인 개념을 의미하는 것으로 간주된다는 의견이 있다. 三角育生(2023), pp. 2~3.

216) 최숙현(2023), p. 2; 2013년 전략은 정보보안 정책회의에서 결정된 문서이다. 三角育生(2020), p. 30.

217) 각의결정(閣議決定)이란 내각총리대신와 그 외 국무대신으로 구성된 합의체인 내각의 회의(각의)에서 내각의 의사(권한사항)를 결정하는 것을 의미한다. 법률안 및 정령은 모두 각의결정 방식으로 정해지며, 중요한 정책 또한 각의결정으로 정해지는 경우가 많다.

218) 三角育生(2021), p. 39.

이 안심하고 안전하게 생활할 수 있는 사회 실현(이하 안전·안심), (iii) 국제사회의 평화 및 안전의 확보와 일본 안보에 대한 기여이다. 이를 바탕으로 한 전략 문서는 인재 육성 등 횡단적 시책을 함께 제시하고 있다.

표 3-4. 일본의 2021년 「사이버보안 전략」 구성

<table>
<tr><td colspan="3">기본이념
- 확보해야 하는 사이버공간은 '자유, 공정, 안전한 공간'
- 5대 기본원칙 견지: (ⅰ) 정보의 자유로운 유통 확보, (ⅱ) 법의 지배, (ⅲ) 개방성, (ⅳ) 자율성, (ⅴ) 다양한 주체와의 연계</td></tr>
<tr><td colspan="3">목표 달성을 위한 정책 방향성</td></tr>
<tr><td>목표: 경제사회의 활력 향상 및 지속적 발전
방향: 디지털 개혁을 바탕으로 한 디지털 전환과 사이버보안 동시 추진</td><td>목표: 국민이 안심하고 안전하게 생활할 수 있는 사회 실현
방향: 공적 공간화와 상호연계되는 사이버공간 전체를 고려한 안전·안심 확보</td><td>목표: 국제사회의 평화 및 안전의 확보와 일본 안보에 기여
방향: 안보 관점에서의 대응 강화</td></tr>
<tr><td>1. 경영층의 의식개선
2. 지역·중소기업의 디지털전환과 사이버시큐리티 지원
3. 공급망 등의 신뢰성 확보를 위한 기반 조성
4. 디지털/시큐리티 문해력(security literacy) 향상과 정착</td><td>1. 국가·사회를 지키기 위한 사이버시큐리티 환경 제공
2. 디지털청을 사령탑으로 하는 디지털 개편과 일관된 사이버시큐리티 확보
3. 정부기관 등 중요 인프라, 대학·교육연구기관 등의 대응 강화
6. 다양한 주체 간 정보공유·연계 및 도쿄올림픽 대응 활용
7. 대규모 사이버공격 사태 등에 대한 대응 태세 강화</td><td>1. 자유, 공정, 안전한 사이버공간의 확보
2. 일본의 방어력, 억제력, 상황 파악력 강화
3. 국제협력·연계</td></tr>
<tr><td colspan="3">횡단적 시책</td></tr>
<tr><td colspan="3">1. 연구개발의 추진 2. 인재확보·육성·활약 촉진 3. 산관학 협력 강화 및 기술보급 제고</td></tr>
<tr><td colspan="3">추진체제: 자유, 공정, 안전한 사이버공간을 확보하기 위한 일관된 정부 추진체제</td></tr>
</table>

자료: NISC(2021), p. 9.

일본 사이버보안 정책의 5대 기본원칙은 (ⅰ) 정보의 자유로운 유통 확보, (ⅱ) 법의 지배, (ⅲ) 개방성, (ⅳ) 자율성, (ⅴ) 다양한 주체와의 연계 등이다. 이는 2015, 2018년 전략과 동일한 것으로, 정보의 자유로운 유통의 확보 및 표현의

자유를 중시하는 미국, 유럽 등과 유사한 일본의 가치관을 엿볼 수 있다.[219] 아울러 일본 사이버보안 정책의 3대 방향성은 (ⅰ) 디지털 개혁을 바탕으로 한 디지털전환과 사이버보안의 동시 추진, (ⅱ) 공적 공간화 및 상호 연계되는 사이버공간 전체를 고려한 안전·안심 확보, (ⅲ) 안보 관점에서의 대응 강화 등이다. 일본 사이버보안 정책의 목적과 방향성에서 첫 번째로 강조되고 있는 분야가 디지털전환과 사이버보안의 동시 추진인 점이 주목된다. 민간 투자를 통해 상대적으로 취약한 일본의 디지털 경쟁력을 강화하고, 관련 인프라 마련에 주력하겠다는 것으로 평가된다. 추가로 2021년 「사이버보안 전략」은 사이버보안의 핵심 주체로 정부 기관과 중요 인프라 사업자 등에 더해 관련 서비스 사업자, 중요 기술을 보유한 주체를 포함하고, 향후 정부와 이들을 포함한 민간과의 협조체제를 강조하고 있다는 점에서 이전 전략과의 차별점을 찾을 수 있다.[220]

「사이버보안 전략」에 근거하여 일본 사이버보안 센터(NISC: National center of Incident readiness and Strategy for Cybersecurity)는 전년도 정책 실적 및 당해연도 계획 내용을 담은 연차보고서를 매년 발표한다.[221] 2023년 연차보고서에서는 (ⅰ) 정부 추진 체제의 일원화, (ⅱ) 중소기업의 보안 인프라 강화, (ⅲ) 일본의 독자적 사이버보안 정보·기술 모델 구축 등의 내용이 강조되었다는 평가이다.[222] 2024년 7월에 발표된 2024년 연차보고서에는 능동적인 사이버 방어 도입을 위한 법제도 조기 정비와 함께 정부 기관·중요 인프라 사업자·서비스업체의 책임을 강조하며 (ⅰ) 정부 기관 또는 중요 인프라의 평상시 대응 능력 향상, (ⅱ) 설치 단계부터 보안 개념 도입(Secure by Design)·보안 기본 탑재(Secure by Default) 원칙에 근거한 IoT 기기 및 소프트웨어 제품 관련 조치의 구체화, (ⅲ) 서방 주요국을 비롯한 관계국과의

219) 三角育生(2021), p. 39.
220) JCIC(2022), 「シリズ「日本のサイバーセキュリティ政策史」:誰も取りさない「サイバーセキュリティ戦略」実現に向けた政府の決意」, p. 3(검색일: 2024. 10. 11.).
221) NISC에 관한 설명은 다음 절에 소개된다.
222) 최숙현(2023), p. 11.

협조 등이 강조되었다.[223] 분야별로는 의료분야에서의 사이버보안 강화를 위한 대책이 두드러졌다.

2) 「국가안보전략」에 따른 능동적 사이버 방어 전략

2022년 12월 16일 당시 기시다 내각은 국가 외교와 방위의 기본지침을 기술하는 「국가안보전략」을 개정하였다(2013년 아베 2차 내각 제정).[224] 개정된 전략에는 '사이버안보(サイバー安全保障)' 개념이 새롭게 추가되고, 사이버안보 전략의 목표를 "사이버공간의 안전하고 안정된 이용, 특히 국가나 중요 인프라 등에 대한 안전 등을 확보하기 위해 사이버안보 분야에서의 대응 능력을 미국 등 주요국과 동등 이상으로 향상한다"로 설정하고 있다.

구체적인 방안으로는 첫째, 정부 기관의 시스템을 상시 평가해 위협 대책 및 시스템 취약성 등을 수시로 시정하기 위한 체계를 구축할 것을 제안하였다. 둘째, '능동적 사이버 방어(Active Cyber Defense)' 도입이 제시되었다. 능동적 사이버 방어는 '무력공격에 이르지는 않지만, 국가나 중요 인프라 등에 대한 안보상의 우려를 발생시키는 중대한 사이버공격의 우려가 있는 경우, 이를 미리 대비하고, 이러한 사이버공격이 발생했을 경우의 피해 확대를 방지'하는 것을 목적으로 한다. 이는 국가의 안보를 궁극적인 보호 법익으로 한다는 사이버안보 개념과 맥락을 같이한다. 이 개념이 등장하게 된 데에는 일본이 정부, 민간사업자 모두 사이버공격 방지 능력이 상대적으로 약해, 미국이 미일 안보 협력 강화 차원에서 도입을 강력히 주장했다는 배경이 있다.[225] 특히 이와 관련해 「국가안보전략」은 다음과 같은 체제 정비를 요청하였다. 첫째, 중요 인프라를 포함해 민간사업자 등이 사이버공격을 받았을 경우, 정부와 정보를 공유하고 정부의 민간사업자에 대한 대응책 조정 및 지원 등을 강화한다. 둘째, 국내 통신사업자의 통신정보를 활용해 악용이 의심되는 서버 등을 감지하는 조치를

223) サイバーセキュリティ戦略本部(2024a).
224) 国家安全保障会議(2022).
225) 「能動的サイバー防御、課題は」(2024. 9. 22.).

시행한다. 셋째, 국가 및 중요 인프라 등에 대한 사이버공격에 대해서는 공격받기 전에 공격자 서버 등을 침입, 무해화(無害化)할 수 있도록 정부에 필요한 권한을 부여한다. 또한 「국가안보전략」은 사이버안보 정책의 사령탑으로서 내각관방의 NISC 개편, 관련 법제도 정비 및 운용 강화를 촉구하였다.

2014년 「사이버보안 기본법」 제정 당시 전략 기반 산업에서 사이버보안은 민간사업자의 책임이라는 점이 강조되었다면,[226] 2022년 「국가안보전략」에서는 사이버안보 주체의 위험관리와 함께 국가 주도의 다층적이고 포괄적인 사이버 방어 체제 구축이 강조되고 있는 것으로 보인다.[227]

2024년 11월 현재 일본은 능동적인 사이버 방어 도입을 위한 법제도 정비를 위해, 2023년 1월에 내각관방에 설치된 사이버안보 체제 정비 준비실과 2024년 6월에 설치된 사이버안보 분야의 대응 능력 향상을 향한 전문가 회의를 통해 논의를 이어가고 있다.[228] 한편 자민당이 2024년 11월 이시바 내각에 제출한 사이버보안 정책의 방향성에 대한 제언 문서를 통해 향후 일본의 관련 정책의 추진 방향성을 엿볼 수 있다.[229] 이 문서는 크게 (ⅰ) 민관 협조, (ⅱ) 통신정보의 이용, (ⅲ) 침입·무해화 조치, (ⅳ) 횡단적 과제 등으로 구성되어 있으며, 항목별로 제안된 내용은 다음과 같다.

첫째, 민관 협조와 관련해서는 (ⅰ) 정부는 사이버공격 피해 예방에 필요한 정보제공, (ⅱ) 보안 클리어런스 제도의 활용 및 정부와 기간 인프라 사업자 등과 '정보공유 체제' 창설 (ⅲ) 기간 인프라 사업자 및 기밀 기술 보유자 등은 사이버공격을 받은 후 정부에 보고할 의무 부여, (ⅳ) 기간 인프라 사업자 중 특히 중요한 사람은 공격 가능성에 대한 정보를 정부에 보고할 의무 부여, (ⅴ) 기간 인프라 사업자는 정보시스템상 중요한 디지털 기기·서비스 등의 정부 등록을 의무

226) 김규판 외(2021), p. 110.
227) 柿沼重志, 榎本尚行(2024), p. 5; JCIC(2022), 「シリズ「日本のサイバーセキュリティ政策史」:誰も取りきない「サイバーセキュリティ戦略」実現に向けた政府の決意」, p. 7(검색일: 2024. 10. 11.).
228) 柿沼重志, 榎本尚行(2024).
229) 自由民主党(2024. 11. 7.), 「能動的サイバー防御、早期法制化を要望関係会議が石破総理に提言申し入れ」(검색일: 2024. 11. 8.).

화하고 정부는 해당 장비에 대한 리스크 평가 시행, (vi) 일본정부에 리스크 평가 결과에 따른 대응을 사업자에게 요청할 권한 부여 등의 내용이 포함되었다.

둘째, 통신정보의 이용 측면에서, 평상시 정부의 통신정보 수집·분석이 가능하도록 헌법 제21조 '통신의 비밀'과의 관계 정리 차원에서 (ⅰ) 공공의 복지 관점에서 '필요 최소한' 또는 개인의 동의 아래 통신정보[230]의 이용, (ⅱ) 일본정부의 통신정보 이용 활동을 감독하는, 독립성과 전문성이 확보된 기관 설치, (ⅲ) 통신정보의 이용은 국가의 책임임을 명확히 하고, 이를 위한 근거 규정 마련[231] 등을 들었다.

셋째, 침입·무해화 조치와 관련해서는 (ⅰ) 피해 사실을 인지한 즉시 조치할 수 있는 권한 정비, (ⅱ) 추진체계는 내각관방을 사령탑으로 방위성, 자위대, 경찰을 포함, (ⅲ) 안보 대상은 통신·전력 등 인프라와 국민의 생명·안전에 관련된 기간 인프라 포함 등의 내용이 포함되었다. 한편 일본정부가 주체가 되어 실시한 침입·무해화 조치의 대상이 해외에 있는 경우 주권 침해 등 외교 분쟁으로 확대될 위험이 있어 해당 조치의 적정성을 확보하는 제도적 검토의 필요성이 제기되었다.[232]

마지막으로 횡단적 과제로는 (ⅰ) 사이버보안 전략본부의 기능 강화(현재 5개 부처 장관에서 각 부처 장관 참여로 확대 등), (ⅱ) 사이버보안 정책 및 운용을 담당하는 장관 신설 및 관련 예산, 체제, 권한 강화 등의 내용이 포함되었다.

사이버안보 정책의 사령탑으로서 일본정부의 조정 역할 및 권한이 강화될 것으로 전망되는 가운데, 자민당의 권고사항이 이시바 내각에서 얼마나 반영되는지, 그리고 정부의 통신정보 이용에 대한 사회적 이해를 어떻게 구하는지의 과정을 지켜볼 필요가 있다.

---

230) 수집 정보 대상은 IP 주소, 송신 일시 등의 정보로 메일, 첨부파일 제목, 본문 등 본질적인 내용은 대상에서 제외하는 방안이 검토되고 있음. 「能動的サイバー防御、課題は」(2024. 9. 22.).

231) 2018년 NTT그룹은 만화 등을 무료로 읽을 수 있는 "해적판 사이트"의 접속을 차단한 바 있는데, 이 과정에서 사용자의 통신 기록 확인이 수반되어 민간 소송에 휘말린 사례가 있어 사업자의 리스크, 부담 등에 대한 회피책이 충분히 검토되어야 한다는 의견이 있음. 위의 자료.

232) 위의 자료.

나. 법률

UN 군축연구소 사이버 정책 포털에서 사이버안보에 관한 일본의 법률은 「사이버보안 기본법」과 「부정 접속 금지법」 등 두 건이 검색된다. 다만 사이버안보의 특성상 관련된 법률은 다양한 분야에서 발견된다.[233] 이에 본 절은 「사이버보안 기본법」, 「부정 접속 금지법」과 함께 「경제안보 추진법」 중 「기간(基幹) 인프라 역할의 안정적인 제공 확보에 관한 제도」, 「중요 경제안보 정보보호 및 활용에 관한 법률」 등 앞 절에서 소개된 법률을 중심으로 살펴본다.

1) 2014년 「사이버보안 기본법」

「사이버보안 기본법(サイバーセキュリティ基本法)」은 2014년에 제정되고 2015년 1월에 시행되었다.[234] 범정부 차원에서 사이버보안 정책을 체계적으로 추진할 목적으로 사이버보안의 정의(제2조), 기본 이념(제3조), 국가를 포함한 관계 주체의 책무(제4~9조), 사이버보안 전략 책정(제12조), 사이버보안 정책의 기본사항(제3장), 사이버보안 전략본부 신설(제4장) 등을 규정하고 있다. 민간사업자 등에 대한 구체적인 권리 및 의무는 동법에 규정되어 있지 않다.[235]

일본의 「사이버보안 기본법」은 2014년에 제정된 이후로 2016년과 2018년 두 차례 개정된 바 있다.[236] 2016년 개정은 2015년 일본 연금 기구의 정보 유출 사건을 계기로 국가가 실시하는 통신 조사 대상 범위를 중앙부처에서 특수법인, 독립행정법인(일본 연금 기구 포함)까지 확대한 것이 핵심이다. 2018년

---

233) 일례로 蔦大輔(2024)는 기본법, 보안사고 보고, 정보관리, 공급망 리스크 대책, 정보통신 네트워크, 통상·경제 안보, 제품 안전, 형사법 등 11개 분야별로 사이버보안과 관련된 일본의 법률 및 관련 지침, 행동계획 등을 소개한 바 있다. 여기에는 최근 주목받고 있는 의료기기의 사이버보안과 관련된 「의료품, 의료기기 등의 품질, 유효성 및 안전성 확보 등에 관한 법률(医療機器等の品質, 有効性及び安全性の確保等に関する法律), 약칭: 약기법(薬機法)」, 신용카드의 사이버보안과 관련된 「할부판매법(割賦販売法)」, 개인정보와 관련된 「개인정보보호법(個人情報保護法)」 등도 소개하고 있다.

234) e-gov 法令検索 홈페이지(2024), 「サイバーセキュリティ基本法」(검색일: 2024. 10. 11.).

235) 蔦大輔(2024), p. 34.

236) 「サイバーセキュリティ基本法」とは？背景や内容を分かりやすく解説」(2024. 1. 25., 검색일: 2024. 10. 11.).

개정은 2020년 도쿄올림픽 개최에 대비해 민관이 협의할 수 있는 사이버보안 협의회 창설(2019년 4월)의 법적 근거 마련이 핵심이다.

「사이버보안 기본법」의 핵심 내용은 다음과 같다. 첫째, 동법은 사이버보안을 정의하고 있는데(2조), 요약하면 안보 대상으로 데이터, 정보시스템, 정보통신 네트워크를 규정하고, 사이버공격에 대한 피해 방지를 위한 조치[237]뿐 아니라 정보 무단 반출 등 내부 부정, 재해로 인한 피해 방지 등을 위한 조치를 통해 보안 대상이 적절하게 유지, 관리되는 것을 의미한다.[238]

둘째, 사이버보안 정책의 기본 이념은 (ⅰ) 정보의 자유로운 유통 확보를 위해 민관이 협력하여 적극 대응, (ⅱ) 국민이 자발적으로 대응하고, 회복탄력성이 있는 강인한 체제 구축, (ⅲ) IT 네트워크 정비와 기술 활용에 의한 활발한 경제사회 구축, (ⅳ) 국제협조 시행, (ⅴ)「디지털 사회 형성 기본법」(2021년 9월 시행)[239] 존중, (ⅵ) 국민 권리보호 등으로 요약된다.

셋째, 동법에 근거하여 일본은 2015년 1월 9일 사이버보안 정책을 추진하는 조직으로서 내각에 내각관방 장관을 본부장으로 하는 '사이버보안 전략본부'를 신설하고, 동시에 내각관방에 사무국인 '사이버보안 센터(NISC: National center of Incident readiness and Strategy for Cybersecurity)'를 신설하였다. 사이버보안 전략본부는 기존에 사이버보안 정책의 사령탑 역할을 담당하던 정보보안 정책회의(情報セキュリティ政策会議, 의장: 내각관방 장관)의 기능을 강화하고, 정부 기관 사이의 정보공유, 신속한 대응, 제휴 등을 도모하기 위해 새로운 사이버보안 정책의 사령탑으로서 설치되었다.[240]

---

237) 일례로 시스템 조달, 설계 및 운용과 관련된 사건(incident)에 대한 대응을 포함한다. サイバーセキュリティ戦略本部(2024a).

238) 사이버보안이란 전자적 방식 등에 의해 기록되거나 발신되어 전송되거나 수신되는 정보의 유출, 소실(滅失), 훼손 방지, 그 외 해당 "정보"의 안전 관리에 필요한 조치 및 "정보시스템," "정보통신 네트워크"의 안전성 및 신뢰성 확보를 위해 필요한 조치(전자적 기록 매체를 통해 전자계산기에 대한 부정한 활동으로 인한 피해를 방지하기 위한 조치 포함)를 강구하여 그 상태가 적절하게 유지, 관리되고 있는 것을 의미한다. 蔦大輔(2024), p. 34; NISC (2023), p. 9.

239) e-gov 法令検索 홈페이지(2024),「デジタル社会形成基本法」(검색일: 2024. 10. 11.).

240) 三角育生(2023), pp. 3~4.

표 3-5. 일본 사이버보안 추진체계

<table>
<tr><td colspan="3">내각총리대신</td></tr>
<tr><td colspan="3">사이버보안 전략본부
본부장: 내각관방장관
부본부장: 사이버보안전략본부에 관련한 사무를 담당하는 국무대신
본부원: 국가공안위원회위원장, 총무대신, 경제산업대신, 디지털대신, 외무대신, 방위대신 외 내각총리대신 지정 전문가</td></tr>
<tr><td>[긴밀연대] 국가안전보장회의</td><td>[긴밀연계] 디지털청</td><td>[연대] 사이버보안협의회
다양한 민관 주체가 서로 연계해 조기 단계에서 사이버보안 확보를 위한 정보의 신속 공유 등</td></tr>
<tr><td colspan="3">[사무국] 내각관방 사이버보안센터(NISC)
정부관계기관 정보보안 횡적감시 대응조절 팀(GSOC)
정보보안 긴급지원팀(CYMAT)</td></tr>
<tr><td>[협력] 주요인프라소관청
금융청(금융), 총무성(지방공공단체, 정보통신), 후생노동성(의료), 경제산업성(전력, 가스, 화학, 신용, 석유), 국토교통성(철도, 항공, 수도, 물류, 항만, 공항)</td><td>[협력] 관료본부원 6성청
경찰청(사이버 범죄단속), 디지털청(디지털사회형성), 총무성(통신/네트워크정책), 외무성(외교안전보장), 경제산업성(정보정책), 방위성(국가방위)</td><td>[협력] 그 외 관계성청 등
문부과학성 등</td></tr>
<tr><td colspan="3">주요인프라사업자, 정부기관, 기업, 개인</td></tr>
</table>

자료: NISC(2024); 최숙현(2023), pp. 8~9.

「사이버보안 기본법」에 근거한 정책에는 타 국가가 관여된 사이버공격 혹은 중요 인프라에 대한 사이버공격, 즉 국가안보와 관련된 사이버공격에 대한 대응이 포함된다. 이 경우 사이버보안 전략본부는 국가안전보장회의(NSC)에 관련 정보를 제공하는 등 NSC와 긴밀한 협력을 도모하는 방식으로 대응해 왔다. 다만 이러한 국가안보 차원에서의 대응 방식에 대해 일본 내에서는 경찰청, 외무성, 방위성 등 관계 기관 사이의 사이버보안 확보를 위한 체제 정비의 필요성[241] 및 NISC 사령탑의 권한을 명확화하는 차원에서 NISC와 관련 정부 기관 등의 역할, 책임 범위를 명확하게 정리할 필요성이 제기된 바 있다.[242] 이러한

241) *Ibid.*, pp. 4~5.
242) 2022년 베이징 올림픽 당시 중국이 출전 선수를 대상으로 다운로드를 의무화한 스마트폰용 건강 관

맥락에서 일본은 「국가안보전략(2022년 개정)」에 근거해 사이버안보 정책을 종합적으로 조정할 수 있는 NISC 대체 조직을 신설하는 안을 검토하고 있다.

2) 2022년 「부정 접속 금지법」

「부정 접속 행위의 금지 등에 관한 법률」(이하 부정접속금지법)은 1999년 제정되어 2022년 개정된 후 같은 해 6월 27일 시행되었다.[243] 부정 접속 행위나 그 행위로 이어지는 식별 부호의 부정적인 취득·보관 행위, 부정 접속 행위를 조장하는 행위, 식별 부호의 입력을 요구하는 행위를 금지하는 법률이다. 여기에서 식별 부호란 정보 기기, 서비스에 접속할 때 사용하는 ID, 패스워드를 일컫는다. 「부정 접속 금지법」은 사이버보안에 관한 형사법으로 언급되며, 부정 접속 행위는 3년 이하의 징역 또는 100만 엔 이하의 벌금, 부정 접속 행위로 이어지는 행위에 대해서는 1년 이하 징역 또는 50만 엔 이하의 벌금이 부과된다.

3) 2022년 「경제안보추진법」

「경제시책의 일체화에 의한 안전보장 확보 추진에 관한 법률」(이하 "경제안보추진법")은 2022년 5월 18일 제정되었다.[244] 동법은 (ⅰ) 중요물자의 안정적인 공급 확보에 관한 제도, (ⅱ) 기간 인프라 역할의 안정적인 제공 확보에 관한 제도, (ⅲ) 첨단 중요기술의 개발지원에 관한 제도, (ⅳ) 특허출원의 비공개에 관한 제도 등 크게 네 가지 내용을 담고 있다.

리 앱에 대해 캐나다 연구소에서 참가 선수의 개인정보를 수집하고 악용할 가능성이 있음을 시사하는 보고서를 공표한 바 있다. 이에 미국 CISA는 올림픽 개막식 약 30분 전 렌털 스마트폰을 사용하도록 주의 권고를 발표한 바 있다. 한편 일본은 올림픽위원회 소관 부처인 문부과학성이 NISC가 주의 권고를 내는 것에 반대하는 등 조정에 난항을 겪어 주의 권고 발표가 늦어진 사례가 있었다. 「サイバー安保強化へ遠い米英の背中データでみる日本の守り」(2024. 12. 16., 검색일: 2024. 12. 17.).

243) e-gov 法令検索 홈페이지(2024), 「不正アクセス行為の禁止等に関する法律」(검색일: 2024. 10. 11.).

244) e-gov 法令検索 홈페이지(2024), 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」(검색일: 2024. 10. 11.).

표 3-6. 기간 인프라 역할의 안정적인 제공 확보에 관한 제도

항목		주요 내용
심사대상	대상업종 (15종)	금융, 신용카드, 전기, 가스, 석유, 수도, 철도, 화물자동차운송, 외항화물, 항공, 공항, 전기통신, 기간방송, 우편, 항만운송('24. 5. 17. 공포)
	대상 사업자	설비 기능 저하로 국가·국민의 안전이 침해될 우려가 큰 경우에 해당되는 성령(省令) 지정 기간에 해당되는 자 ※ 총무성 소관 업종의 대상 사업자 예시: (1) 전기통신사업: KDDI, 오키나와셀룰러, 소프트뱅크, NTT도코모, 동일본전신전화, 서일본전신전화, NTT커뮤니케이션스, 라쿠텐, NTT리미티드재팬, **LINE야후** (2) 방송사업(지상기간방송): 일본방송협회, TBS, TV아사히, TV도쿄, 후지TV, 일본TV방송망 (3) 우편사업: 일본우편
사전신고 심사		대상설비: 설비, 기기류, 프로그램, 클라우드 시스템 심사기간: 원칙적으로 30일(최대 4개월 연장가능)
정부권한		주무대신이 대상사업자에 대해 정보·자료의 제출을 요구하고 출입검사 실시 가능 주무대신은 도입 등의 계획의 변경 등에 대해 권고 가능(불이행시 도입 등 중지명령 가능) 사전심사를 받지 않고 중요설비의 도입 등을 실행했을 경우 형사죄(2년 이하의 징역)에 해당

주: 대상사업자는 소관부처의 성령으로 지정요건을 정하며, 소관부처에서 대상 사업자를 지정함.
자료: KPMG(2023. 11. 21.), 「経済安全保障推進法 (基幹インフラ制度) に対応するセキュリティ施策とは」(검색일: 2024. 10. 7.); 総務省, 「経済安全保障推進法」(검색일: 2024. 10. 7.).

일본정부는 「사이버보안 전략」과 「경제안보추진법」을 상호 보완적 관계로 활용하며, 사이버보안 전략으로 대처할 수 없는 분야를 경제안보 체제로 대응한다는 인식을 보인다.[245] 이에 대해 본 연구에서는 사이버 위협에 대응하는 규정이 포함된 「기간 인프라 역할의 안정적인 제공 확보에 관한 제도(基幹インフラ役務の安定的な提供の確保に関する制度)」(이하 '기간 인프라 방호제도')를 살펴본다.

사이버안보 관점에서 공급망 리스크는 (ⅰ) 제품 생산 과정에서 악의적인 기능이 포함될 우려, (ⅱ) 전체 공급망에서 상대적으로 취약한 단계가 리스크에 노출될 우려 등 크게 두 가지로 구분된다.[246] 이에 기간 인프라 방호제도가 제품

245) JCIC(2022), 「シリズ「日本のサイバーセキュリティ政策史」:誰も取りさない「サイバーセキュリティ戦略」実現に向けた政府の決意」, p. 3(검색일: 2024. 10. 11.).
246) 蔦大輔(2024), p. 37.

생산 과정에서 악의적인 기능이 포함될 우려에 대응하는 차원에서 2024년 5월 17일부터 운영되고 있다. 구체적으로 동 제도는 기간 인프라의 중요 설비가 해외로부터 기간 인프라의 안정적인 제공을 방해하는 수단으로 활용되는 것을 방지할 목적으로 국가가 기간 인프라 사업(특정 사회기반 사업)과 사업자(특정 사회기반 사업자)를 지정하고, 국가가 정한 중요 설비(특정 중요 설비)를 도입할 때 또는 특정 중요 설비의 유지·관리 등을 위탁할 때 국가(사업 소관 장관)에 사전 신고를 하여 심사받도록 하는 제도를 일컫는다(표 3-6 참고).[247] 여기에서 기간 인프라는 국민 생활 및 경제활동의 기반이 되는 역할을 하며, 그 안정적인 제공에 지장이 생겼을 경우 국가, 국민의 안전을 해치는 사태를 일으킬 우려가 있는 것으로 정의되며 금융, 신용카드, 전기, 가스, 전기통신 등 15개 업종이 포함된다. 아울러 대상 사업자는 소관 부처에서 특정 사회 기반 사업자 지정 기준(성령)에 따라 지정한다. 일례로 2024년에 발표된 총무성령에 따르면 전기통신사업의 대상 사업자에는 라인 야후가 포함되었다. 일본정부는 대상 사업자에 대해 정보·자료 제출을 요구할 수 있으며, 관련 설비 도입의 계획 변경에 대한 권고, 그리고 불이행 시 중지 명령이 가능하다.

한편 「사이버보안 기본법」에도 중요 사회기반 인프라(이하 '중요 인프라')의 개념이 포함되어 있는데, 이는 국민 생활 및 경제활동의 기반이며, 그 기능이 정지되거나 저하되었을 때 국민 생활 또는 경제활동에 큰 영향을 미칠 우려가 있는 사업으로 정의된다. 「경제안보추진법」에서 규정하는 기간 인프라와 「사이버보안 기본법」에서 규정하는 중요 인프라는 크게 다음과 같은 차이점이 있다. 첫째, 기간 인프라는 국가 및 국민의 안전을 해치는 사태를 일으킬 우려가 있는 것에 초점을 두는 것과 달리 중요 인프라는 국민 생활 및 경제활동에 큰 영향이 있는 것에 방점을 두고 있다.[248] 둘째, 기간 인프라와 중요 인프라 분야에 차이가 있음에 유의할 필요가 있다. 2024년에 개정된 「중요 인프라의 사이

247) 総務省, 「基幹インフラ役務の安定的な提供の確保に関する制度」(검색일: 2024. 10. 19.).
248) 三角育生(2024), p. 14.

버보안에 관한 행동계획」에 의하면 중요 인프라는 정보통신, 금융, 항공, 공항, 철도, 전력, 가스, 정부·행정서비스, 의료, 수도, 물류, 화학, 신용카드, 석유, 항만 등 15개 산업을 포함한다.[249] 대부분의 산업이 기간 인프라 산업과 중복되는 한편 의료, 정부·행정서비스, 물류 중 창고업, 정보통신 중 케이블TV 등은 2024년 11월 현재 기간 인프라 대상에 미포함되어 있다. 셋째, 「경제안보 추진법」은 규율 대상을 지정하는 의무제도인 반면 「사이버보안 기본법」은 민간사업자와 정부 간 합의에 근거하는 임의의 제도라는 점에서 차이점을 찾을 수 있다.[250]

4) 2024년 「중요 경제안보 정보보호 및 활용에 관한 법률」

일본은 경제안보와 관련해서 추가적으로 보안 적격성 평가(이른바 '클리어런스') 법률로서 「중요 경제안보 정보보호 및 활용에 관한 법률(重要経済安保情報の保護及び活用に関する法律)」을 2024년 5월 10일에 제정하였다.[251] 정부가 보유하고 있는 중요 경제안보 정보에 접근하고 활용할 수 있는 자격을 부여하는 제도이다. 여기에서 중요 경제기반 보호 정보란 (ⅰ) 중요한 인프라나 물자(프로그램 포함)의 공급망에 관한 정보 중 일본의 안보와 관련되며, 특정 방위비밀이나 특정 비밀로 지정되어 있지 않은 정보, (ⅱ) (ⅰ)과 관련된 미공개 정보, (ⅲ) (ⅱ)까지의 요건을 만족하는 정보로 누설될 경우 일본의 안보에 지장을 줄 우려가 있어 은폐할 필요가 있는 정보를 일컫는다.[252] 법률에서는 중요 경제기반에 관한 정보를 (ⅰ) 외부로부터 중요 경제기반을 보호하기 위한 조치·계획·연구, (ⅱ) 중요 경제기반의 취약성, 혁신기술을 비롯한 중요 경제기반에 관한 안보 관련 중요한 정보, (ⅲ) (ⅰ)의 조치에 관해 수집된 외국 정부·국제기관으로부터의 정보, (ⅳ) (ⅱ)과 관련된 정보로 정의하고 있다(제2조). 중요 경제기반에 관한

249) サイバーセキュリティ戦略本部(2024a), pp. 47~52.
250) 三角育生(2024), p. 14.
251) e-gov 法令検索 홈페이지(2024), 「重要経済安保情報の保護及び活用に関する法律」(검색일: 2024. 10. 11.).
252) 備酒 求(2024. 6. 14.), 「重要経済安保情報の保護及び活用に関する法律」(검색일: 2024. 10. 11.).

정보의 예로는 사이버 위협 및 대책에 관한 정보, 규제·제도 관련 정보(심사 등에 관한 검토·분석 등), 산업·기술 전략, 공급망의 취약성과 같은 조사·분석·연구 관련 정보, 국제공동연구개발과 같은 국제협력 관련 정보 등이 포함된다.[253]

최근 첨단기술 분야에서 이중 용도(dual use)가 있는 기술 혁신이 진행되는 상황에서, 일본정부는 본 제도를 통해 국가 간 안보에 관한 정보 제휴 기반을 강화하고,[254] 민간기업이 기밀 기술이 포함된 국제 공동연구 및 공공 조달 입찰에 참가하는 환경이 개선되는 것을 기대 효과로 언급하고 있다.[255] 이 법을 근거로 2024년 10월 현재 일본은 기밀정보의 대상 범위(분야 혹은 기준), 적격성 평가 방법, 조사 결과의 목적 이외의 이용을 금지하는 담보책 등 구체적인 운용 기준을 설정하기 위한 준비위원회를 설치하였으며, 2024년 6월 26일 제1차 회의가 개최되었다.

다. 특징

일본의 사이버안보와 관련된 전략 및 법·제도의 특징은 다음과 같이 요약된다. 첫째, 자유, 공정, 안전한 사이버공간으로 대변되는 「사이버보안 전략」의 기본 이념과 5대 기본원칙에서 나타나는 것과 같이, 일본은 정보의 자유로운 유통의 확보 및 표현의 자유를 중시하는 미국을 비롯한 서방권과 유사한 가치관을 추구하는 점이 확인된다.

둘째, 2022년 「국가안보전략」에서 '사이버안보' 개념과 '능동적인 사이버 방어' 도입 방안이 제시됨에 따라 국가안보의 중요성이 보다 강조되고 있는 것

253) 위의 자료.

254) AUKUS와 같은 안보 관련 기밀정보를 공유하기 위한 다자간 협의체에 가입하기 위한 요건에는 보안클리어런스(SC: Security Clearance) 제도의 정비가 있다. 일본은 「특정 비밀보호법」을 근거로 한 군사분야 보안클리어런드 제도는 있었지만 경제안보 분야에서는 SC제도가 부재했다. 위의 자료.

255) 「機密扱う資格制度、年内に運用基準策定有識者が初会合」(2024. 6. 26., 검색일: 2024. 9. 4.); 외국에서 실시된 우주 관련 사업의 참여요건 중 SC의 취득이 규정되어 있어 참여하지 못한 사례가 있었다. 위의 자료.

으로 확인된다. 특히 일본의 능동적인 사이버 방어는 미국의 '능동 방어' 전략과 유사하다는 점에 주목할 필요가 있다. 관련해서 최숙현(2023)은 일본이 미·일 동맹을 통해 미국의 사이버안보 이슈를 수동적으로 수용하고 제도화하고 있음을 언급한 바 있다.

셋째, 2022년 「국가안보전략」에서는 능동적 사이버 방어 도입 차원에서, 사이버공격을 받았을 경우 정보공유 등 민관 공조 체제를 강화할 것을 촉구하고 있다. 다만 여기에서 언급된 정보공유가 미국, EU와 같이 의무로 규정될지, 민간사업자 등의 자발적인 참여로 이루어지는 임의의 제도로 도입될지 향후 추이를 지켜볼 필요가 있다. 추가로 일본은, 예를 들어 EU가 「사이버복원력법」을 통해 도입한 CE 마크와 같은 인증 제도를 아직 도입하지 않은 상태이다. 이에 대해 일본 경제산업성은 2024년 8월 「IoT 제품에 대한 보안 적합성 평가제도」 구축 방침을 발표한 바 있는데, 의무제도가 아닌 임의의 제도라는 점에서 EU의 제도와 차별화된다.[256]

넷째, 일본은 2014년 제정된 「사이버보안 기본법」에 근거해 사이버보안 정책을 추진하는 사이버보안 전략본부와 사무국인 사이버보안 센터를 주축으로 한 일원화된 추진체계를 갖추고 있다. 2022년 「국가안보전략」 발표 이후 일본은 사이버안보 정책을 종합적으로 조정하는 사령탑으로서 정부의 기능 및 권한을 강화하는 방향으로의 추진체계 개편안을 논의하고 있다.

다섯째, 일본은 「사이버보안 전략」과 「경제안보추진법」을 상호 보완하여 운용하려는 것으로 보인다. 대표적인 예로는 국가가 지정한 특정 사회 기반 사업자에게 특정 중요 설비 도입 및 유지·관리 등을 위탁할 때 사전심사를 받게 하는 「기간 인프라 방호제도」를 들 수 있다. 이 제도에서 정부는 관련 설비 도입의 계획 변경에 대한 권고, 그리고 불이행 시 중지 명령의 권한을 갖는다.

256) 小野寺大毅(2024. 10. 3.), 「外交·安全保障　第18回 : IoT製品へのサイバー脅威を防ぐ適合性評価制度とは? : 安全保障の維持・強化に貢献する経産省の新制度」(검색일: 2024. 11. 27.).

4. 한국

가. 전략

1) 2019년 「국가 사이버안보 전략」

2019년에 발표된 우리나라의 「국가 사이버안보 전략」은 2017년 5월 10일부터 2022년 5월 9일까지가 임기였던 문재인 정부 시기에 작성된 것이다. 비전은 자유롭고 안전한 사이버공간을 구현하여 국가안보와 경제 발전을 뒷받침하고 국제 평화에 기여하는 것이라고 정했다. 이러한 비전에 따라 세 가지 목표로 (ⅰ) 국가 주요 기능의 안정적 수행, (ⅱ) 사이버공격에 빈틈없는 대응, (ⅲ) 튼튼한 사이버안보 기반 구축을 설정했다. 세 가지 기본원칙은 (ⅰ) 국민 기본권과 사이버안보의 조화, (ⅱ) 법치주의 기반 안보 활동 전개, (ⅲ) 참여와 협력의 수행 체계 구축으로 정했다.[257]

우리나라의 「국가 사이버안보 전략」은 여섯 가지 전략과제와 전략과제마다 이에 따른 몇 가지 세부 과제를 제시했다. 첫 번째 전략과제는 국가 핵심 인프라 안전성 제고인데, 여기에는 국가 정보통신망 보안 강화가 포함되어 있다. 장비의 보안 취약점 점검과 백업 설비 확충 등 망 자체의 보안 강화 대책뿐 아니라, 암호체계 및 기밀 보호시스템 고도화와 같이 국가기밀이 유출·훼손되지 않고 안전하게 보호될 수 있도록 하는 대책도 포함된 것이 주목된다. 또한 모바일, 클라우드 등 최신 ICT 기술 기반 업무환경이 사이버 위협의 표적이 되지 않도록 보안 기술·시스템을 적시에 개발 및 적용한다는 내용이 포함된 점도 특징적이다.

257) 한국인터넷진흥원 홈페이지(2019), 「대한민국 정부 최초 「국가 사이버안보 전략」 발간」(검색일: 2024. 8. 4.).

표 3-7. 2019년 「국가 사이버안보 전략」의 전략과제

1. 국가 핵심 인프라 안전성 제고	2. 사이버공격 대응역량 고도화
1) 국가 정보통신망 보안 강화	1) 사이버공격 억지력 확보
2) 주요 기반시설 보안환경 개선	2) 대규모 공격 대비태세 강화
3) 차세대 보안 인프라 개발	3) 포괄적·능동적 수단 강구
-	4) 사이버 범죄 대응역량 제고
3. 신뢰와 협력 기반 거버넌스 정립	4. 사이버보안 산업 성장기반 구축
1) 민·관·군 협력 체계 활성화	1) 사이버보안 투자 확대
2) 범국가 정보공유체계 구축 및 활성화	2) 보안 인력·기술 경쟁력 강화
3) 사이버안보 법적기반 강화	3) 보안기업 성장환경 조성
-	4) 공정경쟁 원칙 확립
5. 사이버보안 문화 정착	6. 사이버안보 국제협력 선도
1) 사이버보안 인식 제고 및 실천 강화	1) 양·다자 간 협력체계 내실화
2) 기본권과 사이버안보의 균형	2) 국제협력 리더십 확보

자료: 청와대 국가안보실(20019), 「국가사이버안보전략」.

두 번째 전략과제인 사이버공격 대응 역량 고도화에는 사이버공격 억지력 확보와 포괄적 및 능동적 수단 강구가 포함되어 있어 주목된다. 다만 사이버공격 원인 분석과 공격자 규명을 위한 실질적 역량을 확보한다는 내용 외에는, 억지력을 확보할 수 있는 구체적인 대책은 보이지 않는다. 포괄적 및 능동적 수단 강구라는 전략과제에 속한 세부 과제 중에도 능동적 수단을 어떻게 마련할 수 있는지 더 구체적인 내용은 포함되어 있지 않다. 사이버전에서 국가안보와 국익을 보호할 수 있도록 다양한 전략·전술 개발, 전력 체계 보강 및 핵심기술을 확보한다는 세부 전략이 간접적으로나마 능동적 수단과 관련이 있다고 생각된다. 한편 중대한 사이버안보 위협 발생 시 국제규범에 따라 취할 수 있는 모든 대응 수단을 검토하고 구체적 방안을 마련한다는 세부 전략이 있다. 따라서 우리나라가 이 전략에 따라 능동적 수단을 쓰기 위해서는 국제규범에 따라 능동적 수단을 취할 수 있다는 해석이 도출될 수 있어야 할 것으로 보인다.

2) 2024년 「국가 사이버안보 전략」

2024년 2월 1일 대통령실은 「국가 사이버안보 전략」을 발표했다. 이 전략은 2022년 5월 출범한 윤석열 정부가 마련한 것이다. 비전은 '사이버공간에서 자유·인권·법치의 가치를 수호하면서 국제적 역할과 책임을 다하는 글로벌 중추 국가'로 설정되었다. 이러한 비전에 따라 3대 전략과 5대 전략과제가 제시되었다. 3대 전략은 공세적 사이버 방어와 대응, 국제적 지도력 확장, 건실한 사이버 복원력이고, 5대 전략과제는 (ⅰ) 공세적 사이버 방어 활동 강화, (ⅱ) 글로벌 공조 체계 구축, (ⅲ) 국가 핵심 인프라 사이버 복원력 강화, (ⅳ) 신(新)기술 경쟁 우위 확보, (ⅴ) 업무 수행 기반 강화이다.[258]

대통령실이 직접 밝힌 국가 사이버안보 전략의 주요 특징은 다음 네 가지이다. 첫째, 북한의 사이버 위협에 중점을 두었다. 우리나라의 기반시설에 대한 사이버 위협은 물론, 핵과 미사일 개발 자금을 확보하기 위한 가상자산 탈취, 허위 정보 유포 등 북한의 사이버 위협에 대처하기 위한 정책과 대응 방안이 제시되었다. 둘째, 기존의 방어 중심 대응에서 벗어나 사이버 위협을 선제적으로 식별하고 대응하는 공세적이고 포괄적인 접근과 이를 위한 대응 역량구축 방안이 포함됐다. 셋째, 전 세계적 사이버 협력의 중요성을 강조했다. 넷째, 신속한 대응체계 마련에 주력했다.

우리나라의 2024년 「국가 사이버안보 전략」에서 확인되는 가장 큰 특징은 공세적 사이버 방어 및 대응이라고 평가할 수 있다. 명시적으로 "방어 위주의 기존 전략만으로는 고도화하는 사이버 위협 대응에 한계가 있으므로 공격징후를 사전에 포착하고 이에 대한 선제 대응을 취하여 위협을 제거·완화"하겠다는 목표를 천명한 것이다.

더 구체적으로 정보기관과 군은 공격 근원지를 능동적으로 탐지·분석하여 사전징후를 포착하고 관련 정보를 유관 부처와 신속 공유하여, 예상되는 공격

258) 대한민국 대통령실(2024. 2. 1.), 「국가안보실, 윤석열 정부의 '국가 사이버안보 전략' 수립」(검색일: 2024. 8. 4.).

에 대비하는 등 공세적이고 선제적으로 대응한다는 내용이 명시되어 있다. 또한 "과학적 증거를 바탕으로 우리나라에 대한 사이버공격의 배후 세력을 규명하고 악의적 행동에 상응하는 책임을 부과하도록 한다"라는 내용도 포함되어 있는데, 억지력 강화에 유의미한 대책이 될 수 있다고 평가할 수 있다.

결국 우리나라가 2024년 발표한 「국가 사이버안보 전략」은 기존 2019년 「국가 사이버안보 전략」에서 언급한 능동적 대응을 선제 대응으로 한 차원 더 강화했고, 억지력을 형성하는 방안도 더 구체화하는 등 진일보한 측면이 있다고 평가할 수 있다.

이와 관련하여 공세적 전략을 뒷받침하기 위한 논리적, 이론적 논리 보강이 필요하다는 주장도 제기된다. 공세적 전략이 과도하게 공격적인 전략이라는 오해를 초래할 수도 있다는 우려이다. 우리나라의 공세적 전략의 지향점과 논리적 근거를 구체화하기 위해 미국이 2023년 「국가 사이버안보 전략」과 「국방 사이버 전략」에서 명시한 지속적 개입(Persistent Engagement)과 전진 방어(Defend Forward) 개념을 참고할 수 있다는 견해도 제시된다.[259]

3) 2024년 「국가 사이버안보 기본계획」

2024년 9월 1일 대통령실은 「국가 사이버안보 기본계획」을 발표했다. 이것은 같은 해 2월 1일 대통령실이 발표한 「국가 사이버안보 전략」의 후속 조치이다. 국가정보원, 외교부, 국방부, 과학기술정보통신부, 검찰, 경찰 등 14개 정부 부처 합동으로 수립했다. 기본계획은 5대 전략과제를 중심으로, 14개 부처가 실행할 93개 개별과제와 7개 공동과제 등 총 100대 실천 과제를 담았다. 특히 선제적·능동적 사이버 방어 활동을 통해, 국가안보와 국익을 저해하는 사이버 활동과 위협 행위자에 대한 위협 억지력을 확보하는 등 공세적 사이버 방어 활동을 펼치기로 했다. 또한 국가·공공기관 망 분리 체계는 데이터 등급을 기밀·민감·공개로 나눈 뒤 등급에 따라 규제를 차등 적용하는 '다중계층 보안'으

259) 김소정(2024), p. 7.

로 전환하기로 했다. 정보통신기반시설, 사회기반시설 등 국가 핵심 인프라와 대다수 국민이 사용하는 중요정보통신시스템의 사이버 복원력을 높여 국가 핵심 인프라 사이버 복원력도 강화하기로 했다.[260]

나. 법령

우리나라의 법률 중에는 사이버안보라는 용어가 명칭에 포함된 것이 없다. 법률안으로는 「사이버안보 기본법(안)」과 「국가사이버안보법(안)」이 각각 2020년과 2021년에 국회에서 제안되었으나 회기 만료로 폐기되었다.[261] 다만 대통령령 중에서는 명칭에 '사이버안보'라는 용어가 포함된 것으로 「사이버안보 업무규정」이 있다.

우리나라의 사이버안보 관련 법률로 UN 군축연구소의 사이버 정책 포털은 「전자정부법」, 「정보통신기반 보호법」, 「정보통신망법」, 「개인정보보호법」을 소개한다.[262] 여기에 더하여 이 연구에서는 「국가전략기술육성법」도 추가로 간략히 살펴본다.

1) 2024년 「사이버안보 업무규정」

대통령령인 「사이버안보 업무규정」은 2020년에 제정되었는데, 현행 규정은 2024년에 개정된 것이다. 여기에는 '정보통신망'과 '사이버공격·위협'에 대한 정의 규정이 있다. 이에 따르면 '정보통신망'이란 "「전기통신사업법」 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용 기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보

260) 「국가사이버안보 기본계획 발표..양자암호 개발·망 분리 개선·사이버보안 R&D 확대」(2024. 9. 1.),
261) 대한민국 국회 의안정보시스템(2020), 「[2101220] 사이버안보 기본법안(조태용의원 등 27인)」; 대한민국 국회 의안정보시스템(2021a), 「국가사이버안보법안(김병기의원 등 13인)」(모든 자료의 검색일: 2024. 8. 19.).
262) UN 군축연구소 사이버 정책 포털(2024)(검색일: 2024. 8. 19.).

통신체제"로 정의된다. 그리고 '사이버공격·위협'은 "해킹, 컴퓨터바이러스, 서비스거부(DDoS: Distributed Denial of Service), 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협"으로 정의된다.[263]

이러한 「사이버안보 업무규정」은 2024년 3월 5일에 개정되어 같은 날부터 시행되었다.[264] 제10조 사이버보안 교육의 개정 규정은 2025년 1월 1일부터 시행되었다.[265] 개정된 부분은 여러 곳이지만, 이 연구의 목적에 비추어 가장 관련성이 높은 부분은 클라우드컴퓨팅 서비스를 사이버공격에 대한 예방 조치 등의 규정에 추가한 것이다.

표 3-8. 사이버안보 업무규정에서 클라우드컴퓨팅 서비스 추가

「사이버안보 업무규정」(시행 2021. 1. 1. 대통령령 제31356호, 2024. 3. 5., 일부개정)	「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정)
제9조(사이버공격·위협 예방 조치 등)	제9조(사이버보안 예방 조치 등)
② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 "정보보호시스템등"이라 한다)의 도입·운영에 관한 보안대책을 수립할 수 있다.	② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 "정보보호시스템등"이라 한다)의 도입·운영 **및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스(이하 이 조에서 "클라우드컴퓨팅서비스"라 한다)의 이용**에 관한 보안대책을 수립할 수 있다.

주: 제2항 이외의 나머지 항은 생략했음. 밑줄 및 굵은 글씨는 저자가 추가.
자료: 「사이버안보 업무규정」(시행 2021. 1. 1. 대통령령 제31356호, 2024. 3. 5., 일부개정) 및 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정).

즉 기존에는 국가정보원장이 중앙행정기관 등의 정보보호 시스템, 암호장치, 암호모듈 및 보안 기능이 있는 정보통신기기(정보보호 시스템 등)의 도입·

263) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정) 제2조(정의).
264) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5., 일부개정) 제2조(정의).
265) 「사이버안보 업무규정」(시행 2025. 1. 1. 대통령령 제34287호, 2024. 3. 5., 일부개정) 부칙 제1조(시행일).

운영에 관한 보안대책을 수립했었다. 그러나 시행 예정인 대통령령에서는 중앙행정기관 등이 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조 제3호에 따른 클라우드컴퓨팅 서비스를 도입·운영하는 때에도 국가정보원장이 보안대책을 수립하도록 했다. 사이버안보에서 클라우드컴퓨팅의 부상이 갖는 의미를 엿볼 수 있게 하는 대목이라 평가할 수 있다.

2) 「전자정부법」

「전자정부법」의 목적은 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진 방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민 삶의 질을 향상하는 것이다. 그리고 이 법에서 말하는 전자정부는 행정기관과 공공기관의 업무를 전자화하여 효율적으로 수행하는 정부이다.[266] 사이버안보와 관계가 깊은 부분은 제5장(전자정부 운영 기반의 강화)이다. 여기에는 정보 자원의 효율적 관리 기반 조성(제2절)과 정보시스템의 안정성·신뢰성 제고(제3절)가 포함되어 있다.

먼저 정보 자원에 관한 가장 핵심적인 내용은 정보 자원 통합관리라 할 수 있다.[267] 이에 따라 정부 통합 데이터센터인 국가정보자원관리원이 설립되어 운영되고 있다. 정부 통합 데이터센터로는 세계 최초 사례로 소개된다.[268] 이러한 규정의 본질은 국가가 자국 영역 내에 데이터가 있도록 요구하는, 이른바 '데이터 현지화'이다. 민간사업자가 행정기관 또는 공공기관의 데이터를 저장하고 공급하는 사업을 하고자 하더라도, 데이터의 위치가 한국 내에 있어야 하는 것은 물론 더 나아가 통합관리되어야 하는 것이다.

이에 미국은 2017년 3월 공개한 2017년 미국 무역 장벽(NTE: National Trade Estimate Report on Foreign Trade Barriers) 보고서에서부터 데이터 현지화를 요구하는 우리나라의 조치에 대해 문제를 제기하기 시작했다.[269]

---

266) 「전자정부법」(시행 2023. 5. 16. 법률 제19030호, 2022. 11. 15., 일부개정) 제1조(목적) 및 제2조(정의).
267) 「전자정부법」(시행 2023. 5. 16. 법률 제19030호, 2022. 11. 15., 일부개정) 제54조(정보자원 통합관리).
268) 국가정보자원관리원 홈페이지, 「인사말」(검색일: 2024. 10. 21.).

행정기관과 공공기관에 획일적으로 적용되던 기존 규정을 개선하고자 우리나라 국정원은 이른바 다층 보안 체계(MLS: Multi-Level Security)를 2024년 9월 9일 발표했다.[270] 중요도를 기준으로 정보를 C등급(Classified, 기밀정보), S등급(Sensitive, 민감정보), O등급(Open, 공개정보)으로 분류하여 차등화된 보안정책을 운영하겠다는 내용이다. 2024년까지는 기반을 마련하고 2025년부터 시행한다.[271] C등급에 대해선 기관이 내부에 구축한 '프라이빗 클라우드'를 사용하고, S등급은 민관협력(PPP: Public Private Partnership)형 공공 클라우드를 사용한다. PPP형 공공 클라우드 방식의 예는 국가정보자원관리원 대구센터처럼 정부 통제에 따라 민간이 별도의 기반시설을 구축·운영하는 방식이다. O등급만 민간 클라우드에 전면 개방될 전망이다.[272]

표 3-9. 한국의 공공 데이터 분류 체계

등급	분류 기준
C등급(Classified, 기밀정보)	국방, 외교, 안보, 수사 등 기밀정보와 국민의 생명, 안전, 생활과 직결된 정보
S등급(Sensitive, 민감정보)	개인 또는 국가이익을 침해할 수 있는 비공개 정보
O등급(Open, 공개정보)	가명 처리 정보와 C등급과 S등급 이외 모든 정보

자료: 「다중계층보안(MLS) 핵심 '데이터 중요도 분류', 미국과 영국은」(2024. 10. 22.).

우리나라가 도입하려는 MLS에서 데이터는 3단계로 분류되는데, 국방, 외교, 안보, 수사 등 기밀정보와 국민의 생명, 안전, 생활과 직결된 정보를 가장 높은 C등급으로 분류하고, 개인 또는 국가이익을 침해할 수 있는 비공개 정보를 그 다음 S등급으로, 이외 모든 정보와 가명 처리 정보를 O등급으로 분류한다.[273]

269) USTR(2017), "National Trade Estimate Report", p. 280(검색일: 2025. 2. 6.).
270) 국가정보원(2024. 9. 9.), 「국정원, 「CSK 2024」에서 주요 사이버안보 정책방향 공개」(검색일: 2024. 10. 21.).
271) 「국정원 'MLS' 적용 발표…공공 클라우드 시장 위축 우려」(2024. 9. 13.).
272) 「국정원, 공공클라우드 규제 신설…민간사업자 진입 '그림의 떡'」(2024. 9. 4.).
273) 「다중계층보안(MLS) 핵심 '데이터 중요도 분류', 미국과 영국은」(2024. 10. 22.).

표 3-10. 미국의 공공 데이터 분류 체계

조직 자산에 미치는 영향 등급	정보의 미승인 공개가 조직 운영 및 자산, 또는 개인에 미칠 부정적 영향
높은(High) 등급	심각한 또는 재난적(severe or catastrophic)
중간(Moderate) 등급	중대한(serious) 영향
낮은(Low) 등급	제한적(limited) 영향

자료: US DOC, Technology Administration, National Institute of Standards and Technology(2004), "Standards for Security Categorization of Federal Information and Information Systems," p. 6(검색일: 2024. 10. 23).

이와 달리 미국은 정보의 미승인 공개가 조직 운영 및 자산, 또는 개인에 미칠 부정적 영향의 심각성에 따라 등급을 세 단계로 분류했다. 심각한 또는 재난적(severe or catastrophic) 영향에 대해서는 높은(High) 등급을, 중대한(serious) 영향에 대해서는 중간(Moderate) 등급을, 제한적(limited) 영향에 대해서는 낮은(Low) 등급을 각각 부여했다.[274]

영국도 2024년 8월 갱신한 '정부 비밀 분류 정책(Government Security Classifications Policy)'에서 일급비밀(top secret), 비밀(secret), 대외비(official)의 3단계로 구분했다.[275] 일급비밀(top secret)은 보안이 고도로 보장된 전용 물리적 기반시설과 보안 네트워크를 사용하고 영국 또는 동맹국의 국가안보를 직접적으로 지원하는 특별히 민감한 정보 자산(exceptionally sensitive information asset)에 부여되는 등급이다. 비밀(secret)은 전용 물리적 기반시설과 보안 네트워크를 사용하고 강화된 보안 통제가 요구되는 대단히 민감한 정보(very sensitive information)로서, 정보 침해로 인해 개인의 생명이 위협받거나, 영국의 안보 또는 국제 관계, 재정적 안보 또는 안정성이

274) US DOC, Technology Administration, National Institute of Standards and Technology(2004), "Standards for Security Categorization of Federal Information and Information Systems," p. 6(검색일: 2024. 10. 23).

275) 이 연구에서 영국의 "top secret", "secret", "official"이라는 등급 명칭은 각각 "일급비밀", "비밀", "대외비"로 번역한다. 이것은 영국 비밀 분류체계의 변경이 2014년 4월 2일 발효함에 따라 한국과 영국 양국은 2009년 체결한 「영국 정부와 대한민국 정부 간의 군사비밀정보의 보호에 관한 협정」을 2019년 개정했는데, 여기서 secret, official(official-sensitive)을 각각 군사 Ⅱ급 비밀, 군사 대외비로 번역한 것을 고려한 번역이다. 참고로 우리나라의 군사 Ⅲ급 비밀에 대응하는 등급은 영국에는 없는 등급(No UK equivalent)이다. 외교부 홈페이지(2019), 「(조약 제2410호) 한-영국 군사비밀정보보호협정 개정 교환각서」(검색일: 2024. 10. 23.).

심각하게 손상되거나(seriously damage), 심각하고 조직적인 범죄를 조사하는 능력이 방해받을 수 있는 정보에 부여되는 등급이다. 대외비(official)는 공공부문에서 생성, 처리, 전송 또는 수신되는 정보의 대부분을 차지하는 정보로서, 침해되더라도 중간 정도의 피해(moderate damage) 이상을 일으키지 않는 정보이다.[276]

표 3-11. 영국의 공공 데이터 분류 체계

등급	분류 기준
일급비밀(top secret)	영국 또는 동맹국의 국가안보를 직접 지원하는 특별히 민감한 정보 자산(exceptionally sensitive information asset)
비밀(secret)	전용 물리적 기반시설과 보안 네트워크를 사용하는 대단히 민감한 정보(very sensitive information)
대외비(official)	공공부문에서 생성, 처리, 전송 또는 수신되는 정보의 대부분을 차지하는 정보로서, 침해되더라도 중간 정도의 피해(moderate damage) 이상을 일으키지 않는 정보

자료: Government of the United Kingdom 홈페이지(2024), "Government Security Classifications Policy"(검색일: 2024. 10. 23.).

미국과 영국 모두 다소 정성적인 평가에 따른 분류 기준이라 할 수 있다. 반면 우리나라가 전환을 추진 중인 MLS에 따른 분류는 가명 처리 정보, 비공개 정보 등 객관적인 기준이 포함되어 있으므로, 미국 또는 영국의 분류 체계에 비해 기준이 더 명확한 발전된 분류 체계라고 평가할 수 있다.

다만 MLS 도입 과정에서 기관별 상황에 맞게 데이터를 분류하는 방향으로 추진하게 되면, 책임 회피를 위해 C등급이나 S등급으로 분류되는 데이터가 많을 것이라는 우려도 있다. 미국은 2015년을 기준으로 미국 연방 정부 기관은 정보시스템의 88%가 중간과 낮은 등급의 데이터를 처리하는 것으로 분류했다. 영국도 2013년 발표에 따르면 데이터의 90%를 대외비(official) 등급으로 분류했다.[277] 미국과 영국 모두 높은 등급으로 분류되는 정보의 비중이 15%를

276) Government of the United Kingdom 홈페이지(2024), "Government Security Classifications Policy"(검색일: 2024. 10. 23.).
277) 「다중계층보안(MLS) 핵심 '데이터 중요도 분류', 미국과 영국은」(2024. 10. 22.).

넘지 않은 것이다. 제도 개선의 취지에 맞게 등급 분류가 적절하게 이루어져야 할 것이다.

다음으로 정보시스템에 관한 가장 핵심적인 내용은 정보통신망 등의 보안대책 수립·시행이라 할 수 있다.[278] 이에 규정에 따라 중앙행정기관, 주요 정보통신기반시설 관리기관, 광역시·도, 광역시·도 교육청은 정보 보호시스템 도입 후 국가정보원에 보안 적합성 검증을 신청하여야 하고, 검증 과정에서 발견된 취약점을 제거하여 운용하여야 한다.[279]

이러한 우리나라의 보안 적합성 검증 제도와 관련해서도 미국은 개선이 필요하다고 2017년부터 매년 주장하고 있다.[280] 2024년 3월 공개한 2024년 무역장벽보고서에서도 미국은 AES(Advanced Encryption Standard)라는 암호화 알고리즘이 세계적으로 널리 사용되는데도, 한국정부가 자국이 개발한 ARIA, SEED 암호만을 허용한다고 비판했다. 그리고 이러한 조치는 시장접근을 사실상 제한하는 조치라고 지적했다.[281]

이에 우리나라 국정원은 행정기관과 공공기관이 사용하는 암호모듈에 대한 안전성을 검증하는 '암호모듈검증 제도(KCMVP: Korea Cryptographic Module Validation Program)'에서 SEED 등 국내 개발 암호뿐 아니라 국제표준암호(AES)를 도입하는 방안에 대해 업계 및 전문가와의 논의를 거쳐 개선안을 발표했다. 우리나라는 암호모듈검증 제도를 2005년부터 시행했다.[282] 우리나라가 국내 개발 암호만 인정했던 이유가 오로지 국내 산업 보호에만 있다고 보기는 어렵다. 로이터 등 외국 주요 언론이 외국 보안업체가 전산시스템에 접근할 수 있는 우회 통로를 외국 정보당국에 제공했다는 의혹을 제기한

278) 「전자정부법」(시행 2023. 5. 16. 법률 제19030호, 2022. 11. 15., 일부개정) 제56조(정보통신망 등의 보안대책 수립·시행).
279) 국가정보원 홈페이지, 「보안적합성 검증」(검색일: 2024. 10. 21.).
280) USTR(2017), "National Trade Estimate Report," p. 285(검색일: 2025. 2. 6.).
281) USTR(2024), "National Trade Estimate Report," p. 241(검색일: 2024. 10. 21.).
282) 국가정보원(2024. 9. 9.), 「국정원, 「CSK 2024」에서 주요 사이버안보 정책방향 공개」(검색일: 2024. 10. 21.).

사례가 없지 않았으므로, 국내에서 개발하지 않은 암호모듈을 우리 정부가 전적으로 신뢰하기 어려운 측면도 있었기 때문이다.[283] 암호모듈검증 제도 개선안에 따르면, 국제표준암호(AES)도 허용하되, 시행은 산업계와 시험기관의 준비기간을 고려하여 2026년 1월부터 한다.[284]

3) 「정보통신기반 보호법」

2001년에 제정되고 2024년에 개정된 「정보통신기반 보호법」의 목적은 전자적 침해행위에 대비하여 주요 정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 주요 정보통신기반시설을 안정적으로 운용하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것이다.[285]

「정보통신기반 보호법」에서 말하는 '정보통신기반시설'은 "국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 정의 규정에 따른 정보통신망"이다.[286] 즉 '정보통신기반시설'에는 정보통신망뿐 아니라, 국방, 치안, 금융, 운송, 에너지 등 기간시설에 관련된 전자적 제어 및 관리 시스템도 포함된다.

「정보통신기반 보호법」은 주요 정보통신기반시설의 보호 체계(제2장), 주요 정보통신기반시설의 지정 및 취약점 분석(제3장), 주요 정보통신기반시설의 보호 및 침해사고의 대응(제4장), 기술지원 및 민간 협력(제6장), 벌칙(제7장)에 관한 규정을 두고 있다.

먼저 주요 정보통신기반시설의 보호 체계와 관련해서는 정보통신기반 보호위원회를 국무총리 소속으로 하여, 주요 정보통신기반시설의 보호에 관한 사항을 심의한다.[287]

---

283) 「RSA, 암호화SW에 '백도어' 심고 '뒷돈' 챙겨」(2023. 12. 22.).
284) 「공공업무에도 챗GPT 활용…AI·클라우드·데이터 경제 창출 기대」(2024. 9. 11.).
285) 「정보통신기반 보호법」(시행 2025. 1. 24. 법률 제20068호, 2024. 1. 23., 일부개정) 제1조(목적).
286) 「정보통신기반 보호법」(시행 2025. 1. 24. 법률 제20068호, 2024. 1. 23., 일부개정) 제2조(정의).
287) 「정보통신기반 보호법」(시행 2025. 1. 24. 법률 제20068호, 2024. 1. 23., 일부개정) 제3조(정보통

다음으로 중앙행정기관의 장은 소관 분야의 정보통신기반시설 중에서 보호가 필요하다고 인정하는 정보통신기반시설을 주요 정보통신기반시설로 지정할 수 있다.[288] 그리고 주요 정보통신기반시설을 관리하는 기관(관리기관)의 장은 정기적으로 소관 주요 정보통신기반시설의 취약점을 분석·평가해야 한다.[289] 지정 여부 심사는 지정 후 6월 이내, 이후에는 매년 시행한다.[290]

또한 주요 정보통신기반시설의 보호 및 침해사고의 대응 시 관계 중앙행정기관의 장이 해당 관리기관의 장에게 주요 정보통신기반시설의 보호에 필요한 조치를 명령할 수 있다.[291] 관리기관의 장은 침해사고가 발생하여 소관 주요 정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관, 또는 인터넷진흥원에 그 사실을 통지해야 한다.[292]

끝으로 벌칙은 주요 정보통신기반시설을 교란·마비 또는 파괴한 자를 10년 이하의 징역 또는 1억 원 이하의 벌금에 처한다.[293] 주요 정보통신기반시설의 교란, 마비 또는 파괴가 초래할 중대한 영향을 고려할 때, 처벌 기준이 상향 조정될 필요가 있다.

4) 「정보통신망법」

「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」은 법률의 명칭과 목적에 관한 규정에서 알 수 있는 것과 같이, 정보통신서비스를

신기반보호위원회).

288) 「정보통신기반 보호법」(시행 2022. 9. 11. 법률 제18870호, 2022. 6. 10., 일부개정) 제8조(주요 정보통신기반시설의 지정 등).

289) 「정보통신기반 보호법」(시행 2022. 9. 11. 법률 제18870호, 2022. 6. 10., 일부개정) 제9조(취약점의 분석·평가).

290) 「정보통신기반 보호법시행령」(시행 2023. 3. 7. 대통령령 제33321호, 2023. 3. 7., 타법개정) 제17조(취약점 분석·평가의 시기).

291) 「정보통신기반 보호법시행령」(시행 2023. 3. 7. 대통령령 제33321호, 2023. 3. 7., 타법개정) 제11조(보호조치 명령 등).

292) 「정보통신기반 보호법시행령」(시행 2023. 3. 7. 대통령령 제33321호, 2023. 3. 7., 타법개정) 제13조(침해사고의 통지).

293) 「정보통신기반 보호법시행령」(시행 2023. 3. 7. 대통령령 제33321호, 2023. 3. 7., 타법개정) 제28조(벌칙).

이용하는 자를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하는 것이 일차적인 목적이다.[294] 주요 내용도 정보통신망에서의 이용자 보호 등(제5장)과 정보통신망의 안정성 확보 등(제6장)이다.

이런 측면에서 「정보통신망법」은 「정보통신기반 보호법」과 차이가 있다. 우선 「정보통신망법」은 정보통신망의 안정성 확보와 더불어 정보통신망에서의 이용자 보호도 이와 대등한 목적이라 할 수 있다. 그러나 「정보통신기반 보호법」은 궁극적으로는 이용자 보호도 목적이라 할 수 있겠지만, 주된 목적은 '정보통신기반시설'의 보호에 있다. 또한 「정보통신망법」은 정보통신망에 적용되는 측면에서, 정보통신망을 포함하여 국가안보·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리 시스템에도 적용되는 「정보통신기반 보호법」에 비해 적용 대상이 되는 물적 범위가 더 좁다.

타법과의 관계에 관한 규정에서 「정보통신망법」은 정보통신망 이용촉진 및 정보보호 등에 관해서는 다른 법률에서 특별히 규정된 때 외에는 이 법으로 정하는 바에 따른다고 규정한다.[295] 그러므로 정보통신망 이용촉진 및 정보보호의 문제에 대해서는 「정보통신망법」이 우선한다고 볼 수 있다. 다만 다른 법률에서 특별히 규정하였을 때는 다른 법률의 그 규정이 우선 적용될 것이다. 구체적인 사건에서는 판단이 쉽지 않을 것이고, 법원의 판결로 명확해질 수밖에 없을 것이다.

사이버안보와 관계가 있는 「정보통신망법」의 주요 내용을 간략히 살펴본다. 먼저 정보통신망에서의 이용자 보호 등(제5장)과 관련이 있는 내용이다. 정보통신서비스 공급자가 공급하는 정보통신서비스를 이용하는 자(이용자)는 사생활 침해 또는 명예훼손 등으로 타인의 권리를 침해하는 정보를 정보통신망에 유통하지 않을 의무를 진다. 또한 정보통신서비스 공급자는 자신이 운영·관리하는 정보통신망에 타인의 권리를 침해하는 정보가 유통되지 않도록 노력해야

294) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제1조(목적).
295) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제6조(다른 법률과의 관계).

한다.[296] 사람을 비방할 목적으로 정보통신망을 통하여 다른 사람의 명예를 훼손한 자는 공공연하게 사실을 드러내어 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처한다. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만 원 이하의 벌금에 처한다.[297]

다음으로 정보통신망의 안정성 확보 등(제6장)과 관련이 있는 내용이다. 정보통신서비스 공급자, 정보통신망 연결기기 등을 제조 또는 수입하는 자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 해야 한다. 또한 과학기술정보통신부장관은 보호조치의 구체적 내용을 정한 정보보호 조치에 관한 지침(정보보호 지침)을 정하여 고시하고 이를 지키도록 정보통신서비스 공급자, 정보통신망 연결기기 등을 제조 또는 수입하는 자에게 권고할 수 있다.[298] 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하는 자에 대하여 기준에 적합한지에 관하여 인증을 할 수 있다.[299] 끝으로 정보통신서비스 공급자는 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고해야 한다.[300] 이 규정은 2009년 개정 때 신설된 것이다.[301] 우리 법에서의 '즉시'는 시행령에 따르면 24시간 이내를 뜻한다.

끝으로 「정보통신망법」은 정보통신망 연결기기 등이 인증 시험 대행 기관의

296) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제44조(정보통신망에서의 권리보호).
297) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제70조(벌칙).
298) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제45조(정보통신망의 안정성 확보 등).
299) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제47조(정보보호 관리체계의 인증).
300) 「정보통신망법」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정) 제48조의3(침해사고의 신고 등).
301) 「정보통신망법」(시행 2009. 7. 23. 법률 제9637호, 2009. 4. 22., 일부개정) 제48조의3 (침해사고의 신고 등).

시험 결과 인증 기준에 적합한 경우 과학기술정보통신부장관이 정보보호 인증을 할 수 있다고 규정한다. 인증 및 취소 업무를 한국인터넷진흥원에 위탁할 수 있다는 규정에 따라,[302] 한국인터넷진흥원이 해당 업무를 수행 중이다.[303]

5) 「개인정보보호법」

「개인정보보호법」은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.[304] 헌법재판소가 2005년 결정에서 개인정보자기결정권을 헌법상 독자적 권리로 인정한 이후, 우리나라에서 개인정보에 관한 문제는 헌법상 기본권 차원의 논의로 다루어지게 되었다.[305]

우리나라 「개인정보보호법」은 개인정보를 개인의 자유와 권리를 보호하는 측면에서 다루므로 정보통신기반시설 보호에 주안점을 두는 「정보통신기반 보호법」, 그리고 정보통신망에서의 이용자 보호와 정보통신망의 안정성 확보에 주안점을 두는 「정보통신망법」과 차이가 있다. 특히 「개인정보보호법」은 온라인 오프라인을 가리지 않고 모든 영역에서의 개인정보 보호를 다룬다. 반면 「정보통신망법」은 정보통신서비스 공급자와 이용자 모두를 규율하며, 이용자 보호는 정보통신망에서의 권리보호에 주안점이 있다. 다시 말해 정보통신망, 즉 온라인에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 유통하는 것을 규제한다.

사이버안보와 관계가 있는 「개인정보보호법」의 주요 내용을 간략히 살펴본다. 이 법에서 국가안보는 한 차례 언급되는데, 적용의 일부 제외에 관한 규정에서이다. 국가안보와 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보에 대해서는 제3장(개인정보의 처리)부터 제8장(개인정보 단체소송)까지

302) 「정보통신망법 시행령」(시행 2024. 8. 14. 대통령령 제34821호, 2024. 8. 13., 일부개정) 제48조의6(정보통신망 연결 기기 등에 관한 인증) 제1항 및 제6항.
303) 한국인터넷진흥원 홈페이지(2024), 「정보통신망연결기기 보안인증(IoT)」(검색일: 2024. 12. 11.).
304) 「개인정보 보호법」(시행 2024. 3. 15. 법률 제19234호, 2023. 3. 14., 일부개정) 제1조(목적).
305) 전상현(2019), 고학수, 임용 편저, p. 63.

를 적용하지 않는다는 내용이다. 국가안보 관련 예외와 더불어 「개인정보보호법」에서 인정되는 또 다른 예외로는 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보가 있다.[306]

그러나 국가안보가 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보라고 하더라도 적용되는 규정이 있다. 적용의 일부 제외에 관한 규정에서 제3장(개인정보의 처리)부터 제8장(개인정보 단체소송)까지는 적용되지 않는다고 했으므로, 제1장(총칙)에 속한 규정은 적용되는 것이다. 여기에는 목적, 정의, 개인정보 보호 원칙, 정보주체의 권리, 국가 등의 책무, 다른 법률과의 관계가 포함되는데, 이 중에서도 특히 제3조(개인정보의 처리), 제4조(정보주체의 권리), 제5조(국가 등의 책무)가 의미가 있다.

사이버안보와 개인정보보호 사이의 관계는 대립하는 성격도 있지만, 보완적인 성격도 동시에 가지고 있다. 사이버안보를 보호하기 위해서는 개인정보를 정보 주체의 의사와 무관하게 처리해야 하는 불가피한 상황도 있을 것이므로, 이때는 대립적인 관계라고 볼 수 있다. 하지만 사이버안보가 지켜지지 않으면 개인정보 보호도 기대하기 어렵다는 측면에서는 서로 보완적인 성격도 있다. 사이버안보와 개인정보 보호라는 두 가치의 조화로운 추구를 위해서는 사이버안보 담당 기관의 자율적 통제와 관련 절차를 외부에서 적절히 통제하기 위한 법적인 근거를 발전시켜 나갈 필요가 있다.[307]

6) 「산업기술보호법」

국가로부터 연구개발비를 지원받아 개발한 국가핵심기술을 보유한 기업·연구기관·전문기관·대학 등 대상기관이 해당 국가핵심기술을 외국기업 등에 매각 또는 이전 등의 방법으로 수출할 때는 산업통상자원부 장관의 승인을 얻어야

306) 「개인정보 보호법」(시행 2024. 3. 15. 법률 제19234호, 2023. 3. 14., 일부개정) 제58조(적용의 일부 제외).
307) 최경진(2015), pp. 219~220.

한다. 이것은 「산업기술의 유출방지 및 보호에 관한 법률(약칭: 산업기술보호법)」에 따른 의무이다.[308] 「산업기술보호법」은 '국가핵심기술'을 "국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출되면 국가의 안보 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술"이라고 정의하고, 별도의 지정 절차를 규정한다.[309]

이러한 국가핵심기술 수출심사의 신속처리절차를 마련하기 위해 산업통상자원부는 2023년 7월 26일 「산업기술보호지침」을 개정하여 시행했다. 국내기관이 100% 지분을 보유한 해외기관(자회사)과 공동 연구 개발을 할 때는 연간 사전 포괄심사와 사후 보고를 도입하는 것 등이 주요 내용이다.[310]

다만 개정된 「산업기술보호지침」은 국가핵심기술 수출의 방법에 "클라우드서비스 또는 이와 유사한 서비스에 저장된 국가핵심기술에 대한 외국기업 등의 접근권한 부여·열람·사용 등의 허용"을 포함했고, 이때에도 산업통상자원부장관에게 승인을 신청해야 한다고 규정한다.[311] 따라서 기술 정보를 클라우드서비스에 저장하고 해외 자회사에서 사용하고자 하는 기업 등은 승인 신청 과정에서 유무형의 비용이 들 수 있다. 그런데 한편으로는 클라우드서비스 공급업체 또는 서버가 위치한 국가의 당국 등이 우리의 국가핵심기술을 열람하는 것을 막을 필요가 있다. 이와 관련하여 국가핵심기술의 저장 위치를 국내로 한정하는 안, 저장 위치에 관한 정보를 이용자에게 제공하는 안, 외국 정부 당국이 수사 과정에서 영장 집행 등을 할 때도 우리 기업에 직접 연락을 하도록 하는 방안 등을 제안하는 견해도 있다.[312]

이와 관련하여 미국의 거대 기술기업이자 클라우드서비스 공급자이기도 한

---

308) 「산업기술의 유출방지 및 보호에 관한 법률(약칭: 산업기술보호법)」(시행 2024. 8. 21. 법률 제20319호, 2024. 2. 20., 타법개정) 제11조(국가핵심기술의 수출 등).
309) 「산업기술보호법」 제2조(정의) 및 제9조(국가핵심기술의 지정·변경 및 해제 등).
310) 산업통상자원부(2023. 7. 25.), 「의약품 해외 인·허가 등 포괄·신속 수출심사 도입으로 국가 핵심기술 수출 애로 해소」(검색일: 2024. 10. 22.).
311) 「산업기술보호지침」(시행 2023. 7. 26. 산업통상자원부고시 제2023-151호, 2023. 7. 26., 폐지제정) 제17조(수출승인 신청 대상).
312) 「"국가핵심기술은 韓영토에만 저장"…클라우드 활용기준 바뀌나?」(2023. 11. 22., 검색일: 2024. 10. 22.).

애플(apple)의 데이터 보안 방식을 참고할 수 있을 것으로 보인다. 애플은 자사의 클라우드서비스(iCloud)에 적용되는 데이터 보안 규칙을 표준과 고급으로 구분하는데, 고급 데이터 보호는 이용자 외에는 애플을 포함한 다른 누구도 암호화된 데이터에 접근할 수 없는 방식이다. 클라우드 서버가 아니라, 이용자의 기기와 같이 신뢰할 수 있는 기기에만 암호 데이터를 저장하는 방식으로 이른바 '종단 간 암호화(End-to-end Encryption)'이다.[313]

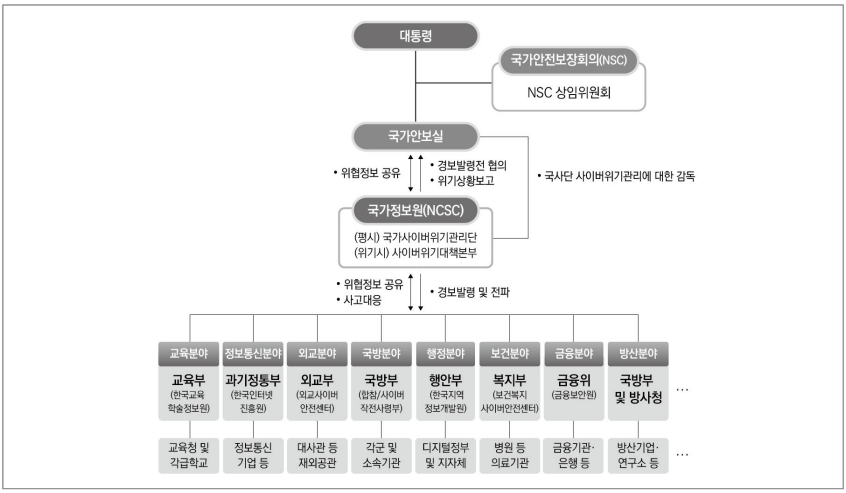
다. 특징

우리나라 사이버안보 전략과 법령의 특징은 다음과 같다. 먼저 우리나라의 2024년 「국가 사이버안보 전략」은 2019년 「국가 사이버안보 전략」에 자유라는 가치를 비전에 추가하여 민주적 가치 지향을 명백히 밝혔고, 기존의 방어 위주 전략에서 공세적 방어를 표방하는 것으로 수정되었다. 2019년의 자유롭고 안전한 사이버공간 구현이라는 비전이 자유·인권·법치 가치 수호 및 글로벌 중추 국가 지향으로 바뀌었다. 주요 목표 역시 사이버공격에 대한 대응과 국가 주요 기능의 안정적 수행을 강조했으나, 공세적 사이버 방어와 대응 그리고 건실한 사이버 복원력으로 강조점이 이동했다. 북한의 사이버 위협에 대한 대응을 강조한 점도 변화된 부분이다. 2024년 2월 발표된 「국가 사이버안보 전략」은 같은 해 9월 발표된 「2024년 국가 사이버안보 기본계획」으로 구체화했다. 2024년 전략 부분에서 가장 눈에 띄는 것은 방어 위주의 기존 전략만으로는 고도화하는 사이버 위협 대응에 한계가 있으므로, 공격징후를 사전에 포착하고 선제 대응을 취하여 위협을 제거·완화하겠다는 목표를 천명한 점이다. 이를 구체화하여, 2024년 기본계획에는 정보기관과 군은 공격 근원지를 능동적으로 탐지·분석하여 사전징후를 포착하고 관련 정보를 유관 부처와 신속하게 공유하여, 예상되는 공격에 대비하는 등 공세적이고 선제적으로 대응한다는 계획이 수립되었다.

313) Apple 홈페이지, "iCloud data security overview"(검색일: 2024. 10. 22.).

다음으로 우리나라의 사이버안보 법률의 특징은 사이버안보에 관한 단일한 법률이 없다는 것이다. 이 점에 대해 과거부터 학계와 연구계의 전문가로부터 우려가 제기되었으나, 통합 법률의 제정은 이루어지지 못했다. 이와 관련하여, 사이버안보 관련 규정이 여러 법률에 흩어져 있어 책임의 한계가 불분명하고 법 적용 과정에서 적용 우선순위 결정 또는 중복 적용에 따른 처리를 둘러싼 혼란 등을 우려하는 시각이 있다. 통합된 근거 법률의 부재는 필연적으로 통합된 관리 조직의 출현을 어렵게 만든다는 지적도 있다.[314] 관계 기관의 역할이 법률에 적절한 수준으로 정해져 있지 않은 채 대통령훈령인 「국가사이버안전관리규정」에 상당 부분을 의존하는 것 역시 관계 부처 기관의 집행력을 미약하게 하고 특히 민간 부문에 대한 대국민 효력을 발휘하는 데 한계를 발생시킨다는 시각도 있다.[315]

그림 3-1. 국가 사이버안보 수행 체계



자료: 국가정보원, 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 금융위원회, 외교부(2024), 『2024 국가정보보호백서』, p. 11(검색일: 2024. 12. 9.).

314) 현대호(2007), p. 66.
315) 박상돈, 김소정(2013), p. 92.

우리나라에는 사이버안보에 관한 통합된 법률이 없을 뿐, 우리나라의 국가 사이버안보 수행 체계는 마련되어 있다. 2015년 4월 국가안보실 내에 사이버안보 비서관을 둔 것이다.[316] 이후 담당 비서관의 명칭 변경은 있지만, 현재 우리나라의 사이버안보 업무에서 최상위 사령탑 역할은 국가안보실이 담당하고 있다. 정부는 국가안보실의 관리 감독하에 민·관 합동 통합 대응조직인 국가사이버위기 관리단을 국가정보원에 설치함으로써, 국가 차원의 일원화된 대응체계를 갖추었다.[317] 다만 민간 분야 정보보호 정책·제도의 총괄과 조정은 과학기술정보통신부가 담당한다. 행정안전부·지식경제부·방송통신위원회에 나뉘어 있던 정보보호 업무가 과학기술정보통신부로 2013년 3월 이관되었다.[318] 그러므로 공공 분야 그리고 국가 전체 차원에서의 대응은 국가정보원이 담당한다고 할 수 있다. 그러나 이러한 우리나라 사이버 대응체계는 사이버 침해사고가 공공과 민간을 구분하지 않고 발생하는 현실을 반영하지 못한다는 문제의식에서 지난 21대 국회 시기인 2021년 12월 과학기술정보통신부에 사이버보안 본부를 설치하여 공공과 민간의 사이버 침해를 체계적으로 대응하려는 법률안이 발의되기도 했다.[319]

한편 우리나라는 비록 통합된 기본법은 없지만, 변화하는 상황에 신속하게 대응하는 점이 돋보인다. 대통령령인 「사이버안보 업무규정」을 2024년 3월 5일에 개정하여 클라우드컴퓨팅 서비스를 도입·운영하는 때에도 보안대책을 수립하도록 했다. 「사이버안보 업무규정」은 클라우드컴퓨팅 서비스를 직접 정의하지 않고 「클라우드컴퓨팅법」의 정의를 따름을 명시한다.[320] 클라우드컴퓨팅 서비스라는 새로운 유형의 사이버안보 도전에 대응할 때, 이미 제정된

316) 「국가안보실 직제」(시행 2015. 4. 3. 대통령령 제26182호, 2015. 4. 3., 일부개정). 제5조(비서관).
317) 국가정보원, 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 금융위원회, 외교부(2024), 『2024 국가정보보호백서』, p. 11.
318) 위의 자료, p. 31.
319) 대한민국 국회 의안정보시스템(2021b), 「[2113670] 사이버보안 기본법안(윤영찬 의원 등 12인)」(검색일: 2024. 8. 19.).
320) 「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024.3.5. 일부개정). 제9조(사이버보안 예방 조치 등) 제2항.

「클라우드컴퓨팅법」이 도움이 되었음을 엿볼 수 있는 부분이다. 최근 AI를 이용한 다양한 사이버공격 역시 사이버안보에 대한 중대한 위협으로 부상하고 있으므로, 이에 대한 대비도 필요하다. 2025년 1월 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」이 제정되었으므로,[321] 사이버안보 분야에도 도움이 될 토대를 마련한 것으로 평가할 수 있다.

5. 소결

제3장에서는 주요국의 사이버안보 정책을 살펴보았다. 미국, EU, 일본, 우리나라의 사이버안보 전략과 법률을 조사하고 분석한 후, 각국의 특징을 도출했다.

미국의 2023년 「국가 사이버안보 전략」의 주요 내용은 사이버안보 최소 요건의 적용을 확대하여 중요 인프라 복원력을 확보한다는 것이다. 중요 인프라의 상당수를 민간이 소유 또는 운영하는 미국은 「2003년 안전한 사이버공간을 위한 국가 전략」에서부터 민관협력 체계 구축과 사이버사고 대응을 위한 미국 연방 차원의 대응계획을 수립했다. 특히 미국의 「CISA 전략계획 2023~2025」에는 미국의 핵심 네트워크에 대한 침해가 발생하기 전에 능동적으로 위협을 무력화시킨다는 내용이 포함되었다. 구체적으로 네트워크 모니터링, 위협 분석, 사이버 위협 수색 등이 제시되었다.

미국 사이버안보 법률의 특징은 정부 내 전담 조직 설치와 민간과의 공조 강화를 위한 근거법 제정으로 요약할 수 있다. 「2018년 사이버안보 및 기반시설 안보국 법」은 국가안보라는 일반적인 목표를 가진 국토안보부 내의 기존 조직을 사이버안보와 기반시설 안보라는 더 구체적인 임무를 수행하는 국토안보부

321) 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」(시행 2026. 1. 22. 법률 제20676호, 2025. 1. 21., 제정).

내의 새 조직인 CISA로 전환했다. 「2020년 사물인터넷 사이버안보 개선법」을 제정하여 우선 연방 정부가 소유하고 관리하는 IoT 기기에 대한 최소한의 보안 기준을 마련했다. 「2022년 핵심 기반시설 사이버사고 보고법」은 핵심 인프라 소유자 또는 운영자에게 사이버사고 발생과 랜섬웨어 피해에 대해 각각 72시간, 24시간 내 보고의무를 부과했다.

EU의 사이버안보 전략은 기본권 존중을 강조한다. 2013년 「EU 사이버안보 전략」에서 안전하면서도 개방적인 사이버공간을 강조했다. 그러나 2020년 「EU 사이버안보 전략」에서는 복원력과 기술 주권을 강조했다. 각각의 전략에 따라 「네트워크 및 정보시스템 법」이 제정 및 개정되었다. 2013년 전략에 없던 예산 계획이 2020년 전략에는 마련되는 등, 전략이 점차 구체화하고 있다.

EU 사이버안보 법률의 특징은 직접적인 수입 제한 조치보다는 인증 제도 또는 표시 제도와 같은 간접적인 조치를 사용하는 점이다. 2019년 「사이버안보법」을 제정하여 다양한 사이버보안 인증 제도를 마련하고 있다. 이에 따라 2024년에는 ICT 상품에 대한 EUCC 인증 시행법이 제정되었다. 클라우드컴퓨팅 서비스, 5G 통신, AI에 대한 인증도 준비하고 있다. 또한 2024년 「사이버 복원력법」은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품에 보안 요건을 준수한다는 CE 표지를 부착할 법적 의무를 수입업자 또는 유통업자에게 부과한다.

일본의 「사이버보안 전략」의 자유, 공정, 안전한 사이버공간이라는 기본이념은 미국 및 EU 등 서방권과 유사하다. 2022년 「국가안전보장전략」에서는 사이버안보 개념이 처음 도입되었는데, 여기서 제안된 '능동적인 사이버 방어' 역시 미국의 능동 방어 전략과 비슷하다. 또한 사이버안보 정책을 종합적으로 조정하는 사령탑으로서 정부의 기능 및 권한을 강화하는 방향으로의 제도 개정이 논의되고 있다.

일본의 「경제안보추진법」에 따른 기간 인프라 방호제도는 국가가 지정한 특정사회기반사업자가 특정 중요 설비 도입 및 유지·관리 등을 위탁할 때 사전

심사를 받도록 요구한다. 정부는 관련 설비 도입에 대한 중지 명령권을 갖는다. 일본에는 미국의 CIRCIA 또는 EU의 개정 법률과 같이 민간사업자에게 보안 사고 보고의무를 부여하는 법률이 없고, EU가 「사이버 복원력 법」을 통해 도입한 CE 마크와 같은 인증 제도도 아직 도입하지 않았다. IoT 보안 적합성 평가 제도 정비 계획은 2024년에 발표했다.

우리나라의 2024년 「국가 사이버안보 전략」의 특징은 자유·인권·법치 수호라는 민주적 가치를 표방한 점과 "방어 위주의 기존 전략만으로는 고도화하는 사이버 위협 대응에 한계가 있으므로 공격징후를 사전에 포착하고 이에 대한 선제 대응을 취하여 위협을 제거·완화"하겠다는 공세적 사이버 방어와 대응 전략을 도입한 점이다. 이 전략은 「2024년 국가 사이버안보 기본계획」으로 구체화했다. 정보기관과 군은 공격 근원지를 능동적으로 탐지·분석하여 사전징후를 포착하고 관련 정보를 유관 부처와 신속하게 공유하여, 예상되는 공격에 대비하는 등 공세적이고 선제적으로 대응한다는 계획이다.

우리나라의 사이버안보 법률을 주요국과 비교할 때 두드러진 차이점은 사이버안보에 관한 통합된 법률이 없다는 것이다. 물론 사이버안보에 관한 통합된 법률이 없을 뿐, 국가안보실에 사이버안보 비서관이 있고 그 관리 감독 아래 민·관 합동 통합 대응조직인 국가 사이버위기 관리단이 설치되어 있다. 그러나 아무리 통합 조직이 있더라도 근거 규정이 여러 법률에 흩어져 있다면, 적용 과정에서 우선순위 결정 또는 중복 적용 처리를 둘러싼 혼란이 발생할 수 있다며 우려하는 시각도 있다. 한편 통합된 사이버안보 법률이 없어도 우리나라가 변화하는 사이버안보 상황에 신속하게 대응하는 점은 돋보인다. 예컨대 2024년에 「사이버안보 업무규정」을 개정하면서 클라우드컴퓨팅 서비스도 적용 대상에 추가했는데, 이미 제정되어 있던 「클라우드컴퓨팅법」이 도움이 되었다. 마찬가지로 2025년 1월 제정된 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」도 사이버안보에 도움이 될 것으로 기대된다.

제4장 사이버안보 조치와 국제통상법

1. 사이버안보 조치에 적용될 수 있는 통상협정

사이버안보 조치는 사이버안보를 목적으로 정부가 채택 또는 시행하는 등의 조치이다. 사이버안보 조치는 상품 및 서비스 무역, 투자 등 국제 통상에 영향을 미칠 가능성이 있다. 이는 사이버안보 조치만의 문제가 아니므로, 오늘날 각국이 취하는 다양한 조치는 국제 통상에 영향을 미칠 의도가 없다고 하더라도 사실상 영향을 미치지 않는 사례를 찾기가 오히려 더 어렵다.

사이버안보 조치는 동종의 상품 또는 서비스에 대해 특정 국가의 상품을 대상으로 하는 경우가 대부분일 것이므로, 그 조치가 FTA 협정 또는 WTO 협정의 안보 예외 조항이 허용한 예외 조치로 인정되지 않는 한, WTO 협정 또는 FTA 협정의 최혜국 대우 또는 내국민 대우 의무에 위반된다는 판단이 내려질 가능성이 크다.

일단 WTO 협정 또는 FTA 협정에 따른 의무 위반이라는 점이 인정되면, 이러한 위반을 정당화할 수 있는 예외에 해당하는지 검토가 필요하다. WTO 협정에서 GATT를 예로 들면, 제20조의 일반적 예외와 제21조의 국가안보상 예외가 여기에 해당한다. 다만 실제 사건에서는 FTA 협정이 WTO 협정에 대비되는 특별법의 지위에 있을 것이므로 FTA 분쟁해결절차에 따라 설치된 분쟁해결 패널에서는 FTA 협정을 적용하여 검토할 것이다. 그러나 FTA 협정 본문 또는 예외 규정이 일부 다양하다 하더라도 그 의미를 판단한 판정례가 희소하다. 따라서 당분간은 국가안보에 관한 WTO 분쟁 패널 및 상소기구의 판정례가 여전히 의미가 있다.

가. 디지털 통상협정

이 연구에서 디지털 통상협정(DTA: Digital Trade Agreement)은 명칭을 불문하고, FTA와는 구별되는 독립된 디지털경제 협정 또는 기존 FTA의 전자상거래에 관한 장을 디지털경제에 관한 장으로 대체하는 내용의 디지털경제 협정(DEA: Digital Economic Agreement)을 뜻한다. 전자의 예로는 뉴질랜드, 칠레, 싱가포르 디지털 경제동반자협정과 미국·일본 디지털 통상협정이 있다. 후자의 예로는 싱가포르·호주 디지털경제 협정과 한·싱가포르 디지털 동반자협정이 있다. 전자상거래에 관한 장(chapter)이 포함된 기존의 FTA는 이 연구에서는 DTA와 구별되는 형태로 보아 따로 살펴본다.[322]

1) 싱가포르·호주 디지털경제 협정

2020년 발효한 싱가포르·호주 디지털경제 협정(DEA: Digital Economy Agreement)은 싱가포르·호주 FTA의 전자상거래에 관한 장(제14장)을 디지털경제(Digital Economy)에 관한 장(제14장)으로 대체하는 것을 핵심 내용으로 한다. 2003년에 발효한 싱가포르·호주 FTA는 전자상거래에 관한 장이 최초로 포함된 FTA였다.[323]

이 협정의 제14장은 디지털경제(Digital Economy)에 관한 장이다. 싱가포르·호주 DEA에서 사이버보안에 관한 제34조는 사이버보안이 디지털경제를 뒷받침한다는 이상을 양국이 공유하고, 정부 기관(government agencies)의 역량 강화와 당사국 협력 및 인력 개발이 중요함을 인식한다고 규정한다.[324]

---

322) 우리 정부도 전자상거래 관련 2개 조항만 있는 기존 한-EU FTA에 대한 개선 협상을 개시하면서, "디지털 통상협정 협상"으로 표현했다. 전자상거래 규정이 있는 FTA를 좁은 의미의 디지털 통상협정에서 제외한 예로 볼 수 있다. 산업통상자원부 보도자료(2024. 9. 10.), 「한-유럽연합(EU) 디지털통상협정 협상 가속화」(검색일: 2024. 11. 23.).

323) 호주 외교통상부 홈페이지(2024), "Australia-Singapore Digital Economy Agreement"(검색일: 2024. 11. 23.).

324) 싱가포르·호주 FTA 제34조(사이버보안).

인식한다는 문언의 조항은 다른 조항과 결합하여 적용되는 등의 특별한 사정이 없으면, 그 자체로는 일반적으로 법적인 구속력이 없는 조항으로 평가할 수 있다. 또한 규정된 내용은 사이버안보라기 보다는 사이버보안에 가깝다.

2) 디지털 경제동반자협정

2020년 서명되고 2021년 발효한 디지털 경제동반자협정(DEPA: Digital Economic Partnership Agreement)의 당사국은 뉴질랜드, 칠레, 싱가포르이다. DEPA의 사이버보안 협력 조항은 두 개 항으로 구성되어 있다. 제1항은 당사국들은 글로벌 번영을 달성하기 위해 안전한 디지털 무역을 촉진하고 사이버보안이 디지털경제를 뒷받침한다는 공통된 이상(vision)을 가지고 있다는 내용이다.

제2항은 (i) 컴퓨터 보안 사고 대응을 담당하는 국가기관의 역량구축, (ii) 기존 협력 메커니즘을 사용하여 당사국의 전자 네트워크에 영향을 미치는 악성 침입 또는 악성코드 유포를 식별하고 완화하기 위한 협력, (iii) 자격, 다양성, 그리고 평등에 대한 상호 인정 관련 계획을 포함한 사이버보안 분야의 인력 개발의 중요성을 당사국이 인식한다는 내용이다.[325] 이 조항 자체로는 법적인 구속력은 없다. 내용도 사이버안보라기보다는 사이버보안에 관한 것으로 평가할 수 있다.

3) 한·싱가포르 디지털 동반자협정

한·싱가포르 디지털 동반자협정(KSDPA: Korea-Singapore Digital Partnership Agreement)의 핵심 내용은 한·싱 FTA의 전자상거래에 관한 장(제14장)을 한·싱가포르 디지털 동반자협정의 부속서 1로 대체하여 디지털경제에 관한 장(제14장)으로 개정하는 것이다.[326]

---

325) DEPA 제5.1조(사이버보안 협력).
326) 산업통상자원부(2023. 1. 13.), 「1.14일 「한-싱가포르 디지털동반자협정」 발효」(검색일: 2024. 11. 22.).

KSDPA 제14.22조(사이버보안 협력)의 내용은 대체로 DEPA와 비슷하다. 문언에서 차이가 있는 부분은 DEPA의 "평등 향상"이라는 문언이 KSDPA에서는 "청년층 연수 및 육성"으로 수정된 부분뿐이다.[327]

KSDPA는 우리나라가 당사국이므로 국문본도 정본인 협정인데, 협정문 국문본에서 이 조의 제목은 '사이버안보'가 아닌 '사이버보안'이다. 사이버안보와 완전히 무관하다고 볼 수는 없지만, 사이버안보에 관한 조항이라기보다는 사이버보안에 관한 규정에 가깝다.

4) 미국·일본 디지털 통상협정

미국·일본 디지털 통상협정(United States-Japan Digital Trade Agreement)은 2019년 10월 7일 서명되고 2020년 1월 1일 발효했다. 미국·일본 디지털 통상협정에서 사이버보안에 관한 제19조는 두 개 항으로 구성된다. 제1항의 제1문은 당사국은 사이버보안에 대한 위협이 디지털 무역에 대한 신뢰를 약화한다는 사실을 인식하고 있다는 내용이다. 싱가포르·호주 FTA, DEPA, 그리고 KSDPA에서 사이버보안이 디지털경제를 뒷받침한다는 공통된 이상을 가지고 있다고 규정한 것에 비해, 사이버보안에 대한 '위협'을 언급하고 이러한 위협이 디지털 무역에 대한 신뢰 약화라는 해악을 초래할 것임을 인식한다고 규정했으므로 조금 더 적극적으로 규정한 차이가 있다.[328] 그러나 여전히 제1항 제1문은 그 자체로는 원칙적으로 법적 구속력이 없는 규정으로 평가된다.

그러나 제1항의 제2문은 이에 따라 당사국은 특정 사항을 위해 "노력해야만 한다(shall endeavor)"라고 규정함으로써 노력해야 할 법적 의무를 부여했다. 노력 의무는 과정에서의 법적 부담이라는 측면에서 결과 발생 또는 보장 의무와 구별되지만, 노력 의무도 엄연히 법적 의무이다. 노력해야 할 특정 사항은 (ⅰ) 컴퓨터 보안 사고 대응을 담당하는 각 당사국 권한 있는 당국(competent

327) 한·싱가포르 디지털 동반자협정 제5.1조(사이버보안 협력).
328) 미국·일본 디지털통상협정 제19조(사이버보안) 제1항 제1문.

authorities)의 역량을 구축하고, (ii) 전자 네트워크에 영향을 미치는 악성 침입 또는 악성코드 유포를 식별하고 완화하기 위해 협력하기 위한 기존 협력 메커니즘을 강화하고, 이러한 메커니즘을 사용하여 사이버보안 사고에 신속하게 대처하고 인식을 위한 정보와 모범사례를 공유하는 것이다. DEPA 및 KSDPA와 비교할 때, 미국·일본 디지털 통상협정에는 인식을 위한 정보(information for awareness)와 모범 사례(best practice) 공유가 포함된 점이 특징이다.

제2항 제1문은 사이버보안 위협의 진화하는 특성을 고려할 때, 당사국은 이러한 위협 대처에 지시적 규제(prescriptive regulation)보다 위험 기반 접근 방식(risk-based approach)이 더 효과적일 수 있음을 인식한다는 내용이다.[329] 제1항 제1문과 마찬가지로 제2항 제1문에서도 일정한 내용을 인식한다고 규정돼 있으므로 법적 구속력이 없는 내용이다. 그런데 DEPA 및 KSDPA와 비교할 때, 위험 기반 접근 방식을 언급하며 강조한 점이 주목된다.

여기서 지시적 규제는 다른 말로 감독적 규제라고도 번역할 수 있다. 지시적 규제의 특징으로는 모든 상황에 같은 규제가 적용되고 규제의 내용은 세부적이고 구체적이라는 점을 들 수 있다. 반면 위험 기반 접근 방식은 원칙만 정하고 위험 수준에 따라 다르게 규율하는 유연성이 높은 규제 방식이라고 정리할 수 있다. 위험 기반 방식이 더 효과적일 수 있다고 규정하면서, 서두에 "사이버보안 위협의 진화하는 특성을 고려"할 때라는 언급이 있는 것도 이러한 이해와 맥락이 일치한다.

그런데 제2항 제2문은 제1항 제2문과 마찬가지로 특정 사항을 위해 노력할 법적 의무를 당사국에 부과한다. 구체적으로 각 당사국은 사이버보안 위험을 식별하고 보호하며 사이버보안 사고를 감지, 대응 및 복구하기 위해 합의 기반 표준 및 위험관리 모범사례에 의존하는 위험 기반 접근 방식을 자국 영토 내 기업에 적용하고 이를 장려하기 위해 노력해야 한다.

미국·일본 디지털 통상협정의 관련 규정도 사이버안보에 관한 조항이라기

329) 미국·일본 디지털통상협정 제19조(사이버보안) 제2항 제1문.

보다는 사이버보안에 관한 규정에 가깝다. 다만 역량구축과 협력 강화를 위해 노력할 법적 의무를 규정한 부분은 다른 디지털 통상협정에서 찾아보기 어려운 미국·일본 디지털 통상협정의 특징이다.

나. FTA

1) RCEP

역내포괄적경제동반자협정(RCEP: Regional Comprehensive Economic Partnership) 제12.13조(사이버보안)의 내용은 앞서 살펴본 디지털 통상협정과 비교하면 더욱 간략하다. 당사국들은 (ⅰ) 모범 관행의 교환을 통하는 것을 포함하여, 컴퓨터 보안 사고 대응을 담당하는 권한 있는 당국(competent authorities)의 역량구축, (ⅱ) 사이버보안과 관련된 사안에서 협력하기 위한 기존의 협력 메커니즘 사용의 중요성을 인정했다.[330]

협력의 중요성을 인정한다고 규정하여 법적 구속력이 없는 점과 두 가지 세부 내용을 고려할 때, RCEP 제12.13조의 규범 수준은 DEPA 및 KSDPA와 비슷하고 미국·일본 디지털 통상협정보다 낮다고 평가할 수 있다.

2) CPTPP

포괄적·점진적 환태평양경제동반자협정(CPTPP: Comprehensive and Progressive Agreement for Trans-Pacific Partnership) 제14.16조(사이버보안 사안에 관한 협력)도 다음 두 가지 사항의 중요성을 인정한다고 언급하면서, 두 가지 사항으로는 (ⅰ) 컴퓨터 보안 사고 대응을 담당하는 국가기관(national entities)의 역량구축, (ⅱ) 기존 협력 메커니즘을 사용하여 당사국의 전자 네트워크에 영향을 미치는 악성 침입 또는 악성코드 유포를 식별하고 완화하기 위한 협력을 규정한다.[331] CPTPP 제14.16조의 규범 수준도 RCEP

330) RCEP 제12.13조(사이버보안).

제12.13조, DEPA, 그리고 KSDPA와 비슷하고, 미국·일본 디지털통상협정보다는 낮다.

3) USMCA

미국·멕시코·캐나다 협정(USMCA: United States-Mexico-Canada Agreement) 제19.15조(사이버보안)의 문언은 미국·일본 디지털 통상협정과 대체로 같다. 유일하게 차이가 있는 부분은 미국·일본 디지털 통상협정에서 "권한 있는 당국(competent authorities)", "컴퓨터 보안(computer security)", "영역(territory)"이라는 용어를 사용했는데, USMCA에서는 "책임 있는 국가기관(national entities)", "사이버보안(cybersecurity)", "관할권(jurisdiction)"이라는 용어로 바꾸어 사용한 것뿐이다.[332] 그러므로 미국·일본 디지털 통상협정과 비슷한 수준으로 평가할 수 있다. 결국 USMCA의 관련 규정은 사이버안보가 아닌 사이버보안에 관한 규정으로 볼 수 있다는 한계가 있고, 미국·일본 디지털 통상협정과 같이 역량구축과 협력 강화를 위해 노력할 법적 의무를 규정한 점은 긍정적으로 평가할 수 있다.

다. WTO

1) GATT

사이버안보를 이유로 상품의 수입을 제한하는 조치에 적용될 수 있는 GATT의 규정은 조치의 구체적인 내용에 따라 최혜국 대우, 내국민 대우, 시장접근 등 다양할 것이다. 자국에서 생산되는 상품이 없는 국가라도 특정 국가로부터의 상품 수입에 대해서만 사이버안보를 이유로 제한하고 또 다른 국가로부터의 상품 수입에 대해서는 수입을 제한하지 않는다면, 내국민 대우 의무 위반은

331) CPTPP 제14.16조(사이버안보 사안에 관한 협력).
332) USMCA 제19.15조(사이버보안).

문제가 되지 않겠지만 이때에도 최혜국 대우 의무 위반은 문제가 될 수 있다. 그러므로 아래에서는 최혜국 대우 의무에 집중하여 살펴본다.

최혜국 대우 의무에 관한 GATT 1994 제1조 제1항은 (i) 국내 상품과 동종의 수입 상품에, (ii) 불리하지 않은 대우를, (iii) 즉시 그리고 무조건 부여해야 한다는 세 가지 요건이 충족되어야 한다고 규정한다. 사이버안보 조치의 맥락에서는 안보 우려가 제기된 상품에 대한 직접적이고 즉각적인 수입 제한 조치가 대개 이루어질 것이므로, 요건 (ii)와 (iii)은 문제가 될 여지는 크지 않다. 다만 안보 우려가 제기된 상품이 그렇지 않은 다른 상품과 비교할 때 동종 상품인지가 유일한 쟁점으로 부상할 것이다.

일본 주세 사건에서 상소기구는 동종성(likeness)이 이것을 규정한 WTO 협정의 개별 규정뿐 아니라 이 규정이 적용되는 맥락과 상황에 따라 확장하기도 하고 수축할 수도 있는 개념이라고 설명했다.[333] 물론 이러한 언급은 내국민 대우 의무에 관한 GATT 제3조 제2항을 판단하는 과정에서 이루어진 것이지만, 언급된 내용은 내국민 대우로만 의미가 제한되지는 않는다.

결국 동종성은 사안별로 결정되어야 할 개념으로서 절대적 정의가 불가능하다고 본 것이다. 또한 동종성 결정 과정에서 패널 또는 상소기구의 개별적 판단이 불가피한데, 상소기구는 판단이 사안에 따라 개별적으로 내려지더라도 이것이 자의적인(arbitrary) 판단으로 볼 수 없는 재량적인(discretionary) 판단이라고 보았다. 재량적 판단임을 명확히 했으므로, 기준이 모호하다는 반론도 일정 부분 차단할 수 있다.[334]

EC-석면 사건에서 상소기구는 특정 상품의 위험성이 충분히 크면 최종 소비자는 해당 제품을 구매하지 않을 수도 있고, 이러한 측면이 제조업체의 의사결정에 영향을 미칠 것이라는 점은 의심의 여지가 없다고 보았다. 그리고 특정 석면 섬유가 암을 유발하는 물질이라는 점은 1977년 이후 국제적으로 널리 알려

333) Appellate Body Report(1996), *Japan – Alcoholic Beverages II*, p. 21.
334) 권현호(2013), p. 111.

졌다는 것을 인정했다.[335]

요컨대 특정 상품이 개인정보 보호 기능이 취약하여 개인정보가 유출될 위험이 클 수 있다. 나아가 특정 상품이 해킹에 대한 방호벽이 취약하여 그 자체가 서버로 악용되어 국가 핵심 기간망에 대한 분산 서비스 거부 공격을 하여 국가안보에 위협이 되는 경우도 있을 수 있다. 이 경우 특정 상품을 소유한 개인은 관리 책임 등에 따른 민·형사상 책임을 일정 정도까지 부담할 위험까지 있다. 그리고 이러한 위험성이 시장에 널리 알려진다면, 최종 소비자의 상품 선택에 영향을 미칠 것이다. 이때는 어느 국가의 정부가 특정 국가로부터 수입되는 보안이 취약한 상품에 대해 수입 규제 조치를 하더라도, 보안이 취약하지 않은 다른 상품과 동종 상품이라는 상대국 정부의 주장이 받아들여지지 않을 가능성도 있다.

2) GATS

사이버안보를 이유로 서비스 공급을 제한하는 조치에 적용될 수 있는 GATS의 규정은 조치의 구체적인 내용에 따라 최혜국 대우, 내국민 대우, 시장접근 등 다양할 수 있다. 이러한 구체적인 규정의 측면에서 GATS가 GATT와 차이가 있는 부분은, 최혜국 대우 의무는 일반적 의무이지만, 시장접근과 내국민 대우 의무는 구체적 약속의 대상이므로 서비스 양허표에 기재한 제한을 받는다는 것이다. 그러나 WTO가 인터넷 확산 초기인 1995년에 발효한 점을 고려하면, WTO에 가입하면서 사이버안보를 이유로 서비스 양허표에 제한 사항을 기재한 사례는 많지 않을 것이다. 따라서 대부분은 안보예외에 관한 GATS 본문의 예외 규정의 적용을 받을 수 있을 것인지가 쟁점으로 부상할 것으로 보인다.

우선 최혜국 대우 의무와 관련, 협정의 대상이 되는 모든 조치에 관하여 회원국은 다른 어떤 국가의 동종 서비스 또는 서비스 공급자에 부여하는 대우보다 불리하지 않은 대우를 다른 회원국 서비스 또는 서비스 공급자에게 부여해야

335) Appellate Body Report(2001), *EC - Asbestos*, paras. 122, 135.

한다고 규정한다.[336] 동종(like) 서비스 또는 서비스 공급자 여부의 문제는 앞서 다룬 GATT에서의 동종 상품에 관한 쟁점과 크게 다르지 않다. 상품 또는 서비스 그 자체의 특성뿐 아니라 소비자의 인식 등도 고려되며, 사안마다 판단하는 것이 WTO 분쟁 사례에서 일관되게 확인된 원칙이다.

다음으로 시장접근 및 내국민 대우 제한에 대해서는 서비스 양허표에 기재된 내용의 해석이 주로 문제가 된다. 예컨대 스포츠를 제외한 기타 레크리에이션 서비스에 도박 서비스가 포함된다고 해석해야 하는지는 사이버와 직접 관련이 없는 전통적인 쟁점이라 할 수 있다.

사이버와 관련해서 제기되는 문제의 대부분은 WTO가 출범한 1995년 당시가 인터넷 확산 초기였다는 시대적 한계에서 비롯된다. 달리 말하면 서비스 양허표를 기재할 때 WTO 회원국은 오늘날과 같은 디지털 사회를 예상할 수 없었다. 예컨대 서비스 양허표의 시청각 서비스(Audiovisual Service) 항목에 기재한 "녹음 배포 서비스(Sound recording distribution service)"의 범위가 물리적인 형태 없이 전자적인 수단으로 이루어지는 서비스까지 확장되는지 의문이 제기될 수 있다. 이 의문은 2007년 분쟁이 개시된 중국 - 저작물 유통 분쟁 사건에서 쟁점으로 부상했고, 패널은 조약법에 관한 협약 제32조(해석의 보충적 수단)를 근거로 녹음 배포 서비스의 범위가 물리적인 형태 없이 전자적인 수단으로 이루어지는 서비스까지 확장된다고 결론 내렸다. 상소기구도 이러한 패널의 판단에 오류가 없다고 결론 내렸다.[337]

또한 GATS가 인터넷으로 공급되는 서비스를 규정한 서비스 공급 유형 중에서 어떤 유형(모드, mode)으로 보아야 하는지에 관한 의문이 제기될 수도 있다. 서비스 공급 유형에 대해 GATS는 (ⅰ) 국경 간 공급, (ⅱ) 해외 소비, (ⅲ) 상업적 주재를 통한 공급, (ⅳ) 자연인의 주재를 통한 공급으로 나눈다. 인터넷으로 공급되는 서비스는 특히 유형 1과 유형 2중에서 어느 것인지가 문제이다.

---

336) GATS 제2조(최혜국 대우).
337) Appellate Body Report(2009), *China - Publications and Audiovisual Products*, para. 411.

한 국가의 서비스 수요자가 서비스 공급자가 있는 상대방 국가에 전자적으로 방문하여 서비스를 소비한 것으로 볼 수 있는 측면도 있으므로, 의문이 제기될 수 있다.[338]

소비자가 상대국을 방문하여 소비하는 유형(모드 2)이 외국 서비스 공급자가 국경을 넘어 상대국 국내시장에 서비스를 공급하는 유형(모드 1)에 비해 국가 규제의 필요성이 낮다고 보아, 시장접근 또는 내국민 대우에 대한 양허표에서 모드 2에 대한 제한 사항을 모드 1에 비해 더 적게 기재했다면, 분쟁이 발생했을 때 서비스 공급자의 모국은 해당 사건의 서비스 공급이 해외 소비의 유형으로 이루어졌다고 주장할 것이므로 이런 점에서는 의미가 있다.[339]

이와 관련하여 2003년에 분쟁이 개시된 미국 - 도박 서비스 사건에서 패널은 쟁점에 관해 판단하기에 앞서, GATS 제1조(범위 및 정의) 제2항에 규정된 서비스 공급의 유형 중의 하나인 '국경 간 공급(cross-border supply)'이라는 용어의 정의 문제를 결정했다. 패널에 따르면, 국경 간 공급은 원격 공급과 구별된다. 원격 공급은 서비스 공급자가 국내에 있는 때에도 해당할 수 있다고 설명했다. 국경 간 공급은 원격 공급이지만, 모든 원격 공급이 국경 간 공급은 아니라고 보았다.[340] 서비스 공급자와 서비스 소비자의 물리적 위치가 중요한 판단 기준이 됨을 알 수 있다.

중국 - 저작물 유통 분쟁 사건은 과거에 만들어진 규범을 명시적인 개정 없이 오늘날의 현실에 맞게 해석함으로써 묵시적으로 개정하는, 규범의 '변천'으로 평가할 수 있는 측면이 있다. 반면 미국 - 도박 서비스 사건에서 제시된 기준은 서비스 공급자와 서비스 소비자의 물리적 위치가 여전히 중요하다고 보는 측면이 있다. 사이버공간의 별도 영역성을 인정하는 서방 주요국의 관행에 비

338) Munin(2010), p. 8.
339) Wunch-Vincent(2006), p. 325.
340) Panel Report(2004), *US -Gambling*, para. 6.32. 다만 이 사건에서 해당 서비스 분야에 대한 미국의 서비스 양허표 기재는 모드 1과 모드 2에 대해 모두 "제한 사항 없음(None)"이었으므로, 구별의 실익이 크지 않았다.

추어 보면, 통상 분야와 사이버 분야의 규범 사이에 차이가 발견되는 부분으로 평가할 수 있다.

3) TBT

무역에 대한 기술장벽에 관한 협정(TBT: Technical Barriers to Trade)은 기술규정, 표준, 적합성 판정 절차를 적용 대상으로 한다.[341] 여기서 기술규정(technical regulation)은 적용할 수 있는 행정규정을 포함하여 상품의 특성 또는 관련 제조공정방법(PPM: process and production method)을 규정하고 있으며 그 준수가 강제적인(compliance is mandatory) 문서이다.[342] 표준(standard)은 규칙, 지침 또는 상품 특성 또는 관련 PPM의 공통적이고 반복적인 사용을 위한 규정으로서, 인정된 기관에 의하여 승인되고 그 준수가 강제적이지 않은 문서이다.[343] 적합성 평가 절차(Conformity assessment procedures)는 기술규정 또는 표준의 관련 요건이 충족되었는지를 결정하기 위하여 직접적 또는 간접적으로 사용되는 모든 절차이다.[344]

기술규정과 적합성 판정 절차와 관련하여, TBT 협정은 WTO 회원국으로부터 수입되는 상품은 수입국인 WTO 회원국을 원산지로 하는 동종 상품 또는 다른 국가로부터 수입되는 동종 상품에 비해 불리하지 않은 대우를 받아야 한다는 최혜국 대우 의무와 내국민 대우 의무를 규정한다.[345]

표준에 대해서 TBT 협정은 WTO 회원국의 중앙정부 표준기관이 TBT 협정 부속서 3에 규정된 표준의 준비, 채택, 그리고 적용에 관한 모범 관행 규약을 준수하도록 보장할 법적 의무를 규정한다. WTO 회원국에는 모범 관행 규약을 수용하고 준수하는 다른 WTO 회원국의 중앙정부 표준기관이 TBT 협정을 준수하고 있는 것으로 인정할 법적 의무를 부과한다.[346]

---

341) TBT 협정 제1.6조.
342) TBT 협정 부속서 1 제1항.
343) TBT 협정 부속서 1 제2항.
344) TBT 협정 부속서 1 제3항.
345) TBT 협정 제2.1조, 제5.1.1조.

그러므로 사이버안보 조치와 관련해서도 이러한 TBT 협정이 규정한 의무가 안보상 예외에 의해 면제되지 않는 한, 원칙적으로 적용된다. TBT 협정에는 안보상 예외 규정이 없지만, GATT의 안보상 예외 규정이 적용된다.

한편 기술규정은 준수가 강제적인 문서이고, 표준은 준수가 강제적이지 않은 문서라는 구별 기준은 명확해 보인다. 그러나 판정례를 보면, 어떤 조치가 기술규정이고 표준인지 판단이 쉽지 않다. 2008년에 발생한 미국-돌고래 사건(US - Tuna II)에서 문제가 된 조치는 참치 가공품 등의 상품을 포함한 참치의 수입, 판촉, 판매와 관련하여 '돌고래 안전 라벨'의 부착에 적용되는 미국의 연방 법률, 규정, 판례였다.[347] 이 라벨이 없는 참치도 미국으로의 수입과 미국 국내시장에서의 판매가 금지되지 않았다. 다만 이 라벨 외에는 돌고래 또는 해양포유류를 언급하는 다른 어떤 표시도 할 수 없었다. 이러한 미국의 조치는 참치의 원산지에 따른 차별 없이 적용되었다.[348]

미국정부가 요구하는 이러한 돌고래 안전 라벨에 대해 미국-돌고래 사건의 패널은 구속력이 있고 배타적인 방식(binding and exclusive manner)으로 규율하므로 기술규정이라고 판단했다. 그 이유로 (i) 참치 상품에 돌고래 등의 용어를 언급하기 위한 조건을 규정한 점과 (ii) 조건을 준수하지 않은 채 라벨을 상품에 부착하는 행위는 단속 등 집행을 위한 조치의 대상이 되는 점을 제시했다.[349] 상소기구도 (i) 미국의 조치가 참치 상품의 돌고래 안전을 언급하기 위한 단일하고 법적으로 강제적인(single and legally mandated) 요건을 규정한 점과 (ii) 위반에 대한 집행 제도 역시 마련되어 있는 점을 근거로, TBT 협정 부속서 제1.1조의 의미 내에서의 기술규정에 해당한다고 결론 내렸다.[350]

한편 패널은 제소국인 멕시코가 미국 원산지의 참치 상품과 다른 국가가 원산지인 참치 상품이 동종 상품이라는 점을 입증했다고 결론 내렸다. 패널은

346) TBT 협정 제4조(표준의 준비, 채택 그리고 적용).
347) Panel Report(2011), *US - Tuna II(Mexico)*, para. 2.1.
348) 김민정(2012), p. 121.
349) Panel Report(2011), *US - Tuna II(Mexico)*, paras. 7.126-128.
350) Appellate Body Report(2015), *US - Tuna II(Mexico)*, paras. 190-195, 199.

돌고래 안전 라벨을 부착한 참치 상품에 대한 소비자의 선호가 있다는 점이 제출된 자료에 의해 뒷받침되고, 이러한 사정은 상품의 동종성 판단에 관계가 있을 수 있다고 보았다. 그러나 패널은 이 사건에서 멕시코 원산지의 참치와 미국 또는 제3국 원산지의 참치 사이의 동종성을 분석했을 뿐, 돌고래 안전 라벨을 부착한 참치와 그렇지 않은 참치 사이의 동종성을 분석한 것이 아니라고 지적했다. 돌고래 안전 라벨 부착 여부를 기준으로 한 분석은 멕시코 원산지의 참치 상품은 미국 원산지의 참치 상품과 달리 돌고래 안전 라벨을 부착하기 위한 기준을 충족하지 못할 것이라는 추정에 바탕을 두는 것인데, 이를 뒷받침할 자료가 없다고 패널은 설명했다.[351]

한편 표준에 관한 TBT 협정 위반 역시 미국-돌고래 사건에서 쟁점으로 부상했다. 멕시코는 미국의 돌고래 안전 라벨이 관련 국제표준에 기초하지 않았으므로 TBT 협정 제2.4조를 위반했다고 주장했다.[352] 멕시코는 이러한 주장에 대한 근거로 (i) 관련 국제표준으로서 국제 돌고래 보존 프로그램 협정(AIDCP: Agreement on International Dolphin Conservation Program)에 따른 표준이 있고, (ii) 미국이 해당 국제표준을 자국의 규정에 대한 기초로 사용하지 않았으며, (iii) 이러한 국제표준은 미국이 추구하는 정당한 목적 달성에 비효율적이거나 부적절한 수단이 아니라고 주장했다.[353]

패널도 멕시코가 제시한 세 가지 조건이 충족되었는지 검토했다. 첫째, '관련(relevant) 국제표준'인지와 관련하여, 먼저 TBT 협정 제2.4조의 의미에서 '국제표준'이라 함은 (i) 표준이고, (ii) 국제 표준화 또는 표준 조직(international standardizing/standards organization)에서 채택한 것이며, (iii) 일반에 공개된 것이어야 한다는 세 가지 요소로 구성된다고 설명했

351) Panel Report(2011), *US - Tuna II(Mexico)*, para. 7.625.
352) TBT 협정 제2.4조. 주요 내용은 기술규정이 요구되고 관련 국제표준이 존재하거나 그 완성이 임박한 경우, WTO 회원국은 그 국제표준이 정당한 목적 달성에 비효과적이거나 부적절한 수단인 경우를 제외하고는, 이러한 국제표준을 자국 기술규정의 기초로 사용하여야(shall) 한다는 것이다.
353) Panel Report(2011), *US - Tuna II(Mexico)*, paras. 7.249-251.

다.[354] 제기된 주장과 제출된 증거를 바탕으로 패널은 AIDCP가 국제표준에 해당한다고 결론 내렸다. 다음으로 '관련성'에 대해 패널은 미국의 라벨링 제도와 AIDCP는 어획 방법에 관한 규제 유형을 둔 점에서 관련이 있다고 보았다. 따라서 AIDCP라는 관련 국제법이 존재한다는 점을 인정했다.[355]

둘째, 패널은 AIDCP를 미국이 자국의 규정에 대한 기초로 사용하지 않았는지 검토했다. 미국 법원이 호가스 판결(Hogarth ruling)에서 AIDCP 표준 채택을 명시적으로 거부한 점 등을 근거로 미국의 돌고래 안전 라벨링 규정은 관련 국제표준에 근거하지 않았다고 결론 내렸다.[356] 셋째, 패널은 AIDCP가 미국이 추구하는 정당한 목적 달성에 비효율적이거나 부적절한 수단인지 검토했다.

이러한 WTO 판정례에서의 교훈은 사이버보안 인증 라벨링 등 사이버안보 조치의 채택을 고려하거나 시행 중인 국가, 또는 이러한 조치가 WTO 협정에 위반된다고 주장하는 상대국 모두에 시사점이 될 수 있다.

2. 안보 예외 규정

가. WTO 안보 예외 규정

GATT와 GATS에서의 안보 예외 규정을 각각 살펴본다. TBT에는 안보 예외 규정이 없다. WTO 설립협정 부속서 1은 GATT와 부속서 1A의 다른 협정의 규정이 상충하면 다른 협정의 규정이 우선한다고 명시한다. 그러므로 TBT 협정에 안보 예외 규정이 없더라도, GATT의 안보 예외 규정이 적용될 수 있다.

---

354) *Ibid.*, para. 7.664.
355) *Ibid.*, paras. 7.702-703, 7.707.
356) *Ibid.*, *US - Tuna II(Mexico)*, paras. 7.714-715.

1) GATT 안보 예외 규정

GATT 제21조는 안보상 예외를 규정한다. 사이버공간은 다른 분야에 비해 민군 겸용의 성격이 강하고 전시와 평시의 구분과도 다소 거리가 있는 특성이 있으므로 (b)항과 가장 관계가 깊다. 그러므로 나머지 (a)항과 (c)항은 간략히 정리한 후, (b)항에 집중하여 살펴본다.

먼저 (a)항의 내용은 GATT 협정의 어떤 부분도 당사국이 중대한 안보 이익이라고 인정하는 정보를 제공하도록 요구하는 것으로 해석되지 않는다는 것이다. 다음으로 (c)항은 국제 평화와 안전의 유지를 위하여 WTO 협정 당사국이 UN 헌장에 의한 의무에 따라 취하는 조치에 관한 것이다. UN 안보리 결정이 있는 때에는 근거로 활용될 관련성이 높다. 이러한 두 경우가 아닌 나머지는 대부분 (b)항의 적용 대상일 수밖에 없다.

GATT 제21조 (b)항은 두문(頭門)과 그 아래 제(ⅰ)호부터 제(iii)호까지로 구성되어 있다. 두문의 내용은 WTO 회원국이 자국의 안전보장상 중대한 이익을 보호하는 데 필요하다고 판단하는 각호의 조치를 하는 것을 방해하도록 해석될 수 없다는 내용이다. 그리고 각호는 핵 물질에 관련된 조치, 전쟁 물자 또는 군사시설 보급용 기타 물품, 전시 또는 기타 국제 관계에서 비상 상황에서 취하는 조치를 규정한다. GATT 제21조를 심리할 때 패널 또는 상소기구는 각 목의 요건을 먼저 심사한 다음 두문의 요건을 심사하는 순서로 판단한다. 이 순서에 따라 제(ⅰ)호부터 제(iii)호까지를 먼저 살펴본다.

표 4-1. GATT 제21조(안보상 예외)

Article XXI (Security Exceptions)	제21조(안전보장을 위한 예외)
Nothing in this Agreement shall be construed	본 협정의 어떠한 규정도 다음과 같이 해석되어서는 아니된다.
(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests	(b) 체약국이 자국의 안전보장상 중대한 이익을 보호하기 위하여 필요하다고 인정되는 다음의 어느 조치를 취하는 것을 방해하는 것.
(i) relating to fissionable materials or the materials from which they are derived;	(i) 핵분열성물질 또는 이로부터 유출된 물질에 관한 조치
(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;	(ii) 무기, 탄약 및 전쟁 기재의 거래 및 군사시설에 공급하기 위하여 직접 또는 간접으로 행하여지는 기타의 물품 및 원료의 거래에 관한 조치
(iii) taken in time of war or other emergency in international relations; or	(iii) 전시 또는 기타 국제 관계에 있어서의 긴급 시에 취하는 조치
(c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.	(c) 체약국이 국제평화와 안전의 유지를 위하여 국제연합 헌장에 의한 의무에 따라 조치를 취하는 것을 방해하는 것.

주: 굵은 글씨 표시와 음영 표시는 저자가 추가한 것임. (a)항 생략.
자료: GATT 협정문 및 외교부 번역본.

첫째, (i)호는 핵분열성물질 또는 이로부터 유출된 물질에 관한 조치를 규정한다. 다른 호에 비해 대상 물질 등 요건의 의미가 명확하여 논란이 없다. 둘째, (ii)호는 무기, 탄약 및 전쟁 기재의 거래 및 군사시설에 공급하기 위하여 직접 또는 간접으로 행하여지는 기타의 상품 또는 원료의 거래에 관한 조치를 규정한다. 컴퓨터 등 군사와 민간 분야 양쪽에서 사용될 수 있는 이중 용도(dual-use) 상품에 적용될 수 있다. 그러나 적용 대상 상품의 범위에 관한 규정이 없다. 그러므로 이중 용도 상품에 대한 수출통제는 실무적으로 각 WTO 회원국의 재량에 맡겨져 있다.[357] 최근 반도체, AI 상품 등 이중 용도에 관한 관

심이 높아지고 있어, (ii)호의 활용이 늘어날 것으로 전망된다. 특히 (ii)호는 (iii)호와 달리 국제 관계에서의 비상 상황이 요구되지도 않는다. 다만 "군사시설에 공급하기 위하여"라는 요건에서 "군사시설(a military establishment)"이라는 문언으로 표현되어 있으므로, 장기적인 군사 계획을 위해 공급하는 때에는 (ii)호를 원용하는 것이 인정되지 않을 것으로 보는 견해가 있다.

또한 (ii)호에서 가장 중요한 요건은 "공급하기 위하여(for the purpose of supplying)"라는 목적 심사(purpose test)이다. 목적 심사에는 주관적 인식과 객관적 증거가 모두 필요하다. 주관적 인식은 자국의 조치가 (ii)호에 근거했다고 주장하는 국가가 해당 조치를 할 때, 해당 상품이 군사시설에 공급되기 위한 목적으로 거래된다는 상황에 대한 주관적 인식(subjective awareness)이 있었다는 점을 증명해야 한다는 것을 뜻한다. 객관적 증거는 대상 상품이 군사시설 등에 직접 또는 간접적으로 공급된다는 사실에 관한 증거를 신뢰할 만한 정보 출처로부터 확보해야 한다는 것을 뜻한다.[358]

셋째, (iii)호는 전시 또는 기타 국제 관계에서 긴급할 때 취하는 조치를 규정한다. 그러므로 (i) 국제 관계상 비상 상황에 해당하는지, (ii) 비상 상황 중에 취한 조치인지가 주요 쟁점이 된다. 먼저 (i) 국제 관계상 비상 상황에 해당하는지에 관한 쟁점은 결국 "국제 관계에 있어서 전시 기타 비상 상황(other emergency in international relations)"이라는 요건에 대한 해석 문제이다. '비상 상황'에 대해 Russia-Traffic in Transit 사건 패널은 이 요건을 "무력 충돌, 잠재적 무력 충돌, 긴장 또는 위기 고조, 국가를 집어삼키거나 둘러싸고 있는 일반적인 불안정 상황"이라고 해석했다.[359] 그리고 이러한 상황은 해당 회원국의 국방 또는 군사적 이익, 법 및 공공질서의 유지와 같은 특정 유형의

357) Matsushita *et al.*(2017), p. 550.
358) Svetlicinii and Su(2024), p. 12, p. 18.
359) Panel Report(2019), Russia-Traffic in Transit, para. 7.111. 원문은 "a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state"이다.

이익을 발생시킨다고 보았다.[360] Saudi Arabia - IPRs 사건 패널도 이 사건에서 비상 상황이 존재했다고 판단했다. 패널이 설명한 판단의 이유는 다음과 같다. 2017년 6월 5일 사우디아라비아는 카타르와의 외교 및 영사 관계와 모든 경제 및 통상 관계를 종료했다. 또한 사우디아라비아는 카타르가 중동지역 안보 우려를 해소하기 위한 리야드 협정을 준수하지 않고 테러 단체와 극단주의자를 지원하여 타국의 내정에 간섭한다고 반복해서 주장했으나, 카타르가 이를 부인하는 등 이러한 관계 종료가 발생한 맥락은 국가안보와 명시적으로 관련되어 있다고 보기에 충분하다고 패널은 보았다.[361] 나아가 US-Origin Marking 사건 패널은 "국제 관계에 있어서 기타 비상 상황(other emergency in international relations)"의 범위에 무력 충돌이 발생하지 않은 상황도 포함될 수 있는 것으로 더 넓게 해석할 수 있다는 태도를 보였다.[362] 이와 관련하여 '조치'와 '비상 상황' 사이의 관계가 너무 멀거나 무관(so remote from, or unrelated to)하지 않아야 한다는 내용의 이른바 '최소 타당성 요건'도 충족되어야 한다고 보았다.[363]

다음으로 비상 상황 중에 취한 조치인지도 (iii)호와 관련한 쟁점이다. GATT 제21조의 문언은 기타 비상 상황 "때(in the time)"이므로, 예방적으로 취할 수 있도록 허용된 것이 아니라 기타 비상 상황이 있는 때에 비로소 조치할 수 있다. 안보 예외 주장이 받아들여진 Russia-Traffic in Transit 사건과 Saudi Arabia – IPRs 사건에서는 모두 비상 상황 "때(in the time)"에 조치해야 한다는 요건이 충족되었다.

지금까지 각호의 내용과 요건을 살펴보았다. 아래에서는 두문의 내용과 요건을 살펴본다. 두문은 WTO 회원국이 자국의 안전보장상 중대한 이익을 보호

360) *Ibid.*, para. 7.76. 원문은 "such situations give rise to particular types of interests for the Member in question, i.e. defence or military interests, or maintenance of law and public order interests"이다.
361) Panel Report(2020), Saudi Arabia - IPRs, paras. 7.245, 7.258, 7.263.
362) Panel Report(2022), US-Origin Marking (Hong Kong, China), para. 7.311.
363) Panel Report(2019), Russia-Traffic in Transit, paras. 7.138-7.139.

하는 데 필요하다고 판단하는 각호의 조치를 하는 것을 방해하도록 이 협정이 해석될 수 없다고 규정한다. 따라서 (i) 두문 요건의 충족 여부 판단이 조치한 국가의 전적인 자기 판단의 대상인지, (ii) 필수적 안보 이익이 인정되는지가 주요 쟁점이 된다.

첫째, (i) 두문 요건의 충족 여부 판단이 조치한 국가의 전적인 자기 판단 사항인지가 쟁점이다. GATT 제21조 (b)항 두문이 이 협정의 어느 규정도 "자국의 필수적인 안보 이익의 보호를 위하여 필요하다고 '당사국이 판단하는(it considers)' 조치를 방해하지 않는다"라고 규정한다. 미국은 안보 예외 규정의 성격이 자기 판단(self-judging) 규정이므로 패널의 판단이 제한된다고 주장했다. 그러나 4건의 사건 모두에서 패널은 각국 재량이 인정되지만, 신의칙(in good faith)의 제한을 받는다고 판단했다.[364]

그런데 두문의 이른바 자기 판단 규정이 두문에 부속된 세 개의 호에도 적용된다고 보아야 할 것인지도 논란이 있었다. 두문에 부속된 세 개의 호에도 자기 판단 규정이 적용된다고 보면, 부속된 세 항에 규정된 각 사유의 존재와 관련성 등에 대한 패널의 판단이 제한되기 때문이다. 네 건의 사건 모두에서 패널은 두문에 규정된 자기 판단에 관한 내용이 각호까지 적용되는 것은 아니라고 판단했다. 조약의 해석은 조약문의 문맥 및 조약의 대상과 목적에 비추어 그 조약의 문언에 부여되는 통상적 의미에 따라, 또 신의칙에 따라 성실하게 해석되어야 한다는 조약법 협약에 따른 조약해석 원칙을 적용한 결과인 것은 공통된다. 그러나 문언 자체로 명확하다고 본 패널, 대상과 목적을 고려한 패널, 협상국의 의도를 고려한 패널 등 구체적인 이유에는 다소 차이가 있다.[365]

둘째, 두문에 규정된 '필수적 안보 이익'이라는 요건에 관한 쟁점이 있다. Russia-Traffic in Transit 사건의 패널은 '필수적 안보 이익'은 '안보 이익'보다는 좁은 개념으로, 국가의 본질적 기능에 관련된 것이라고 설명했다. 무엇이

364) 이동은(2024), pp. 111~112.
365) 박주현(2024), p. 15.

자국의 필수적 안보 이익인지 판단할 재량이 조치국에 있지만, 이러한 판단에도 신의칙이 적용된다. 그러므로 조치국은 해당 조치가 진실성을 입증할 수 있을 만큼 충분히 명시(articulation)해야 한다.[366]

표 4-2. 안보 예외 규정을 다룬 패널의 주요 판정

구분	Russia – Traffic in Transit	Saudi Arabia – IPRs	US – Steel and Aluminium Products	US – Origin Marking
조치국의 자기 판단	×	×	×	×
국제 관계상 비상 상황	○ (무력 충돌 등 국제 관계 위기)	○ (외교관계 중단)	× (공급과잉은 국제 관계 비상 상황 ×)	× (미중통상 정상지속)
비상 상황 중의 조치	○	○	–	–
필수적 안보이익	○(무력충돌 상황)	○(테러 방지)	–	–
필요한 조치	○	○(적대국 국민 교류 금지), ×(저작권법 미집행)	–	–

주: "–"는 자료 없음을 뜻함. 비상 상황이 아니라고 판단한 패널이 다른 쟁점을 더 나아가 판단하지 않은 결과임.
자료: 박주현(2024), p. 20, [표 1] 안보예외조항 관련 패널 보고서 주요 내용; Panel Report(2022), US – Steel and Aluminium Products, para. 7.149. 및 Panel Report(2022), US – Origin Marking, paras. 7.360-361.

GATT 제21조를 다룬 사건은 1995년 WTO 출범 이후 현재까지 Russia-Traffic in Transit 사건, Saudi Arabia – IPRs 사건, US-Steel and Aluminium Products 사건, US-Origin Marking Requirement 사건 등 총 네 건이 있다. 주요 쟁점별 판정 내용을 정리하면 표와 같다. 미국의 첨단 반도체 수출통제 조치에 대해 중국이 2022년 12월 제기한 미국 - 반도체 사건 분쟁은 2023년 9월 협의요청서 수정본을 제출하는 등 진행 중이다.[367]

366) Panel Report(2019), *Russia - Traffic in Transit*, paras. 7.130-7.131, 7.134.
367) WTO 홈페이지(2024), "DS615: United States - Measures on Certain Semiconductor and other Products, and Related Services and Technologies"(검색일: 2024. 11. 21.).

2) GATS 안보 예외 규정

GATS 제14조의2는 안보상 예외를 규정한다. (a)항은 공개하면 WTO 협정 당사국의 안전보장상 중대한 이익에 반한다고 인정하는 정보의 제공을 요구하는 것으로 GATS 협정이 해석되지 않는다는 내용이다. GATT 제21조 (a)항과 같다.

표 4-3. GATS 제14조의2(안보상 예외)

Article XIV bis (Security Exceptions)	제14조의2(안보상 예외)
Nothing in this Agreement shall be construed	본 협정의 어떠한 규정도 다음과 같이 해석되어서는 아니된다.
(b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:	(b) 자기 나라의 중대한 안보 이익을 보호하기 위해 필요하다고 회원국이 간주하는 다음과 같은 조치를 취하는 것을 금지하는 것으로 해석될 수 없으며.
(i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;	(i) 군사시설에 공급할 목적으로 직접 또는 간접적으로 행하여지는 서비스 공급과 관련된 조치
(ii) relating to fissionable and fusionable materials or the materials from which they are derived;	(ii) 핵분열과 핵융합물질 혹은 이들의 원료가 되는 물질과 관련된 조치
(iii) taken in time of war or other emergency in international relations; or	(iii) 전시 또는 기타 국제 관계에 있어서의 긴급시에 취하는 조치
(c) to prevent any Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security..	(c) 국제평화와 안전을 유지하기 위하여 국제연합헌장상의 의무를 준수하기 위하여 회원국이 조치를 취하는 것을 금지하는 것으로 해석될 수 없다.

주: 굵은 글씨 표시와 음영 표시는 저자가 추가한 것임. (a)항 생략.
자료: GATS 협정문 및 외교부 번역본.

GATS 제14조의2 (b)항 두문과 (ii)호와 (iii)호 그리고 (c)항은 GATT 제21조와 문언이 같다. 단지 GATT (i)호와 (ii)호가 GATS에서는 (ii)호와 (i)호로 순서가 바뀌어 있는 차이가 있을 뿐, (c)항의 문헌도 GATS와 GATT가 같다. 결국 GATS 제14조의2에서 가장 중점을 두고 살펴볼 분야는 GATT와 문언이 다른

(b)항 (ⅰ)호이다. 내용은 "군사시설에 공급할 목적으로 직접 또는 간접적으로 행하여지는 서비스 공급과 관련된 조치"이고, 이중 용도 서비스와 관련이 있는 규정이다. 최근 AI 서비스 또는 AI 개발 및 응용을 위한 서비스에 대해 수출통제 조치를 해야 한다는 주장이 미국 내에서 제기되고 있어 앞으로 중요성이 커질 것으로 예상되는 규정이다.

그러나 이중 용도 상품의 공급이 아니라 서비스의 공급이라는 차이만 있을 뿐 본질적으로 GATT와 같은 규정으로 평가할 수 있다. 따라서 예상되는 쟁점도 같다. '군사시설(military establishment)'의 의미와 관련하여 텐트와 같은 임시 시설 또는 해외의 군사시설도 인정이 되는지 의문이 제기된다.[368] '공급할 목적으로'라는 요건에서 유래하는 목적 심사에 관한 쟁점도 GATT와 같으므로 여기서 반복하지 않는다.

일부 용어의 모호성에도 불구하고, "중대한 안보 이익을 보호하기 위해 필요"한 조치여야 한다는 필요성 요건은 지금까지의 판정례에서는 높은 심사 기준을 적용했다고 평가할 수 있다. 안보 예외를 다루어 판정을 내린 WTO 사건 네 건 중 두 건에서 필요성이 인정되었는데, 한 사건은 무력 충돌 상황이었고 다른 사건은 국교 중단 상황이었다. 따라서 무력 충돌 상황까지는 아니고 국교 중단 상황도 아닌 다른 상황에서 안보 조치를 할 때 예외로 인정될 가능성은 크지 않으리라고 전망된다. 그러나 이렇듯 무력 충돌에 준하는 상황이 되어야 예외적 상황이 인정되는 WTO 협정의 엄격한 안보 예외 규정과 WTO 판정례의 기준은 핵심 인프라에 대한 사이버공격, 온라인 정보 조작, 산업스파이 행위 등 오늘날 사이버공간에서 발생하는 다양한 위협에 WTO 회원국이 정당하게 대응할 수 있는 여지를 지나치게 좁힌다는 비판도 제기된다.[369] 사회 변화에 맞게 그 사회의 법도 바뀌듯, WTO 협정 또는 이에 대한 해석도 개정되거나 변천이 필요할 것으로 보인다.

368) Munin(2010), p. 384.
369) Meltzer(2019), p. 32.

나. FTA 안보 예외 규정

1) 한·미 FTA와 CPTPP 및 USMCA

한·미 FTA의 안보 예외 규정은 각주가 있는 점을 제외하면 CPTPP 및 USMCA와 같다.[370] 이 FTA들은 두 개 항으로 구성되어 있다. 첫 번째 항은 공개하면 자국의 필수적 안보 이익(essential security interest)에 반한다고 "당사국이 결정하는(it determines)" 정보를 당사국이 공급하거나 이에 대한 접근을 허용하도록 요구하는 것으로 이 협정이 해석되지 않는다는 내용이다. RCEP의 안보 예외 규정에서 첫 번째 항의 내용과 같다.

두 번째 항은 당사국이 국제 평화 또는 안보의 유지 또는 회복에 대한 자국의 의무를 이행하기 위하여, 또는 자국의 필수적 안보 이익의 보호를 위하여 필요하다고 판단하는 조치를 적용하지 못하도록 배제하는 것으로 이 협정이 해석되지 않는다는 내용이다. RCEP의 안보 예외 규정에서 세 번째 및 네 번째 항의 내용과 같다.

결국 한·미 FTA는 CPTPP 및 USMCA와 더불어 안보 예외에 관한 규정에서 두 가지 항을 규정함으로써, 하위에 세부 제한 규정을 둔 RCEP의 안보 예외 규정에 비해 더 완화된 규정을 둔 것으로 평가된다. RCEP 안보 예외 규정은 GATT 및 GATS와 문언이 같다.[371] 위에서 살펴본 것처럼, GATT와 GATS는 안보상 필요한 조치를 하더라도 군사시설에 직간접적으로 공급하는 이중 용도 상품, 핵분열 물질 관련 조치, 국제 관계의 긴급상황에서 취해지는 조치 등 추가적인 제한이 있기 때문이다.

한편 한·중 FTA는 GATT 제21조와 GATS 제14조의2에 필요한 변경을 가하여 이 협정에 통합되어 그 일부가 된다고 규정한다.[372] 비록 필요한 변경을

370) 한·미 FTA 제23.2조(필수적 안보), CPTPP Article 29.2(Security Exceptions), USMCA Article 32.2(Essential Security).
371) RCEP 제17.13조(안보 예외).
372) 한·중 FTA 제21.2조(필수적 안보).

가한다는 문언이 추가되어 있지만, 다른 특별한 사정이 없으면 GATT와 GATS의 안보 예외 규정이 적용될 것으로 보인다. 상대 국가에 따라 FTA 규범의 수준을 다르게 정한 것은 다자조약인 WTO와 다른 FTA의 본질을 생각할 때, 당연한 결과라 볼 수 있다.

다만 디지털 산업은 여러 국가의 시장을 마치 하나의 세계시장인 것처럼 아우를 수 있는 특성이 있으므로, 이 점을 고려하여 우리나라가 체결한 FTA 사이의 정합성에 대한 정비가 필요하다는 지적도 있다. 비단 디지털 산업뿐 아니라, 반도체와 같은 첨단산업도 여러 국가에서 연구개발, 원료 조달, 생산 등이 이루어지는 등 글로벌 공급망의 문제가 있으므로, 상대방 국가별로 국가안보를 주장할 요건을 다르게 규정하는 것이 바람직하지 않다는 견해이다.[373]

2) 한·미 FTA 각주의 의미

한·미 FTA에는 CPTPP와 USMCA와 달리 각주가 추가되어 있다. 당사국이 제11장(투자) 또는 제22장(제도 규정 및 분쟁 해결)에 따라 개시된 중재절차에서 제23.2조를 원용하는 경우, 그 사안을 심리하는 중재판정부 또는 패널은 그 예외가 적용됨을 판정한다는 내용이다. 이러한 문언은 흔하지는 않지만 전례가 없지는 않다. 미국·페루 FTA와 미국·콜롬비아 FTA에도 같은 규정이 있지만, 미국·칠레 FTA에는 없는 등 미국이 체결한 FTA 중에서도 혼재되어 있다.[374] 미국·페루 FTA를 언급한 기존 연구에서는 이러한 규정에 대해, 중재판정부의 관할권을 제한한 것이지만 협정 당사국이 합의로 한 것이므로 적법성에 의문이 없다고 평가했다.[375] 그러므로 한·미 FTA의 각주에 대해서도 특별한 논란 없이 같은 판단이 내려질 것으로 예상된다.

그런데 한·미 FTA의 이 각주는 제22장(제도 규정 및 분쟁 해결)에 따라 개시된 중재절차에 대해서만 이 각주가 적용된다고 규정한 것이 아니라, 제11장(투

373) 이재민(2023), pp. 239~240.
374) 장성길(2021), p. 16.
375) Schill and Briese(2009), p. 91.

자)에 대해서도 이 각주가 적용된다고 명시했다. 국가 사이의 분쟁은 제22장이 적용되고 국가와 투자자 사이의 투자분쟁은 제11장이 적용된다.

국가와 투자자 사이의 투자분쟁에서 투자자는 FTA 협정의 당사자가 아닌 제3자이다. FTA의 당사국이 제3자인 투자자에게 투자유치국을 상대로 국제투자중재를 제기할 수 있도록 중재합의에 대한 청약(offer)을 사전에 FTA 협정문에 규정한 것이다. 이후 실제로 분쟁이 발생하여 투자자가 중재신청서를 중재기관 등에 접수하면, 투자자는 투자유치국이 한 청약을 수락(accept)한 것이 되어 중재합의가 성립하는 것이다. 이러한 구조는 FTA 협정의 한쪽 당사국이 제3자인 외국인 투자자에게 권리를 부여하는 규정이다. 제3자에 의무를 부과하는 것은 제3자의 동의가 필요하지만, 권리 부여는 상대방의 동의가 없더라도 허용되거나 동의가 추정된다고 해석하는 것이 일반적이다.

그러나 한·미 FTA의 각주는 일단 부여한 권리를 이후에 일방적으로 박탈하는 내용이다. 외국인 투자자로서는 합리적 기대가 침해되었다고 생각할 수 있다. 외국인 투자자가 투자유치국에 투자할 때, FTA에 이러한 규정이 있다는 사실을 알았거나 알 수 있었다고 지적할 수도 있겠으나, 문제는 투자유치국이 주장하는 필수적 안보 예외가 진정한 권리행사가 아니라 위장된 무역 장벽이라고 외국인 투자자가 반발할 때 발생한다. 이때는 투자유치국의 필수적 안보 예외 주장이 신의성실하게 주장된 것인지 중재판정부가 판단할 수밖에 없다.

만약 투자유치국이 자국의 해석을 내세워 중재절차에 응하지 않고, 투자유치국이 출석하지 않은 채 중재절차가 진행되어 판정이 내려진다면 외국인 투자자는 투자유치국의 영역 밖에서 중재판정을 집행하게 될 것이다. 설혹 중재판정부가 투자유치국의 FTA 해석에 동의하여 관할권 부존재 결정을 내려 투자자 패소 판정을 내리더라도, 투자자로서는 이 각주의 해석에 대한 중재판정의 판단에 대해 중재판정 취소 절차를 개시할 위험도 있다. 근본적인 절차 규칙으로부터의 중대한 이탈이라는 사유에 해당할 가능성을 완전히 배제하기 어렵다. 결국 제11장에도 각주를 적용하는 문제에 대해서는 최근 판정례에 대한 광범

위한 조사와 분석이 필요할 것으로 보인다.

한편 한·미 FTA의 이러한 각주는 2004년 미국 모델 BIT에도 같은 문언과 형식으로 포함되어 있다.[376] 그러나 2004년 미국 모델 BIT가 영향을 미친 2005년 미·우루과이 BIT 제18조와 2008년 미·르완다 BIT 제18조에는 이러한 각주가 포함되어 있지 않다.[377] 그리고 문언과 형식이 다르지만, 유사한 사례로는 2006년 6월 29일 서명된 싱가포르·인도 포괄적 경제협력협정을 들 수 있다.[378] 이 협정은 각주가 아니라 별도의 부속서에 이러한 내용을 더 자세히 규정했다.

한편 한·미 FTA의 각주와 같은 문언이 미국이 체결한 BIT에 상당수 포함되어 있다는 사실은 미국 투자자가 외국 정부를 상대로 제기한 국제투자분쟁에서 이러한 각주의 의미를 다룬 판정례가 내려졌을 가능성이 있음을 의미한다.

2024년 6월 27일 중재판정이 내려진 Seda v. Colombia 사건에서는 투자유치국이 안보 예외에 따른 조치라고 주장만 하면 중재판정부가 더 이상 심리할 수 없는지 여부가 다루어졌다.[379] 이 사건에 적용된 투자협정은 미국·콜롬비아 투자증진협정(TPA: Trade Promotion Agreement)이었는데, 한·미 FTA의 그 각주와 같은 내용과 형식의 각주가 있다.[380] 이 사건에서 투자자의 모국인 미국은 제3국 의견서를 중재판정부에 제출했다. 미국은 필수적 안보 이익에 관한 예외라는 주장이 제기된 사건에 대해서는 중재판정부가 관할권을 갖지 않는다는 견해를 밝혔다. 이에 대해 미국은 필수적 안보 이익에 관한 예외라는 항변을 제기할 권리를 투자유치국은 명시적으로든 묵시적으로든 포기할 수 없는데, FTA에 이를 허용하는 근거 규정이 없는 것이 그 이유라고 설명

376) 2004 U.S. Model Bilateral Investment Treaty Article. 18(2).
377) 장성길(2021), p. 16.
378) 싱가포르·인도 CECA 제6장(투자) 제6.12조(안보 예외) 및 부속서 5(안보예외에 관한 사법심사불능, Non-justiciability of Security Exceptions).
379) "Analysis: Tribunal in Seda v. Colombia finds that state invoked essential security interests exception in good faith, precluding any finding of wrongfulness"(2024. 8. 22.).
380) 미국·콜롬비아 TPA 제22장(예외) 제22.2조(필수적 안보이익).

했다.[381] 그러나 중재판정부는 ICSID 협약과 ICISD 중재규칙에 따라 중재판정부의 관할권을 결정할 권한이 중재판정부에 있으며, 따라서 조약법 협약에 따른 이 사건 투자협정의 해석 등을 근거로, 투자유치국이 필수적 안보 이익에 관한 규정을 신의성실(good faith)하게 제기했는지 심리할 수 있는 권한이 중재판정부에 있다고 결정했다.[382] 심리 결과 중재판정부는 투자유치국이 신의성실하게 필수적 안보 이익에 관한 규정을 주장했다고 결론 내렸다.[383]

이렇듯 최근에 내려진 ICSID 중재판정에서 한·미 FTA의 각주와 같은 문언과 형식의 필수적 안보 이익에 관한 예외 규정에 대해, 투자유치국이 제한 없는 재량을 갖는 것은 아니며 신의성실 원칙에 따른 판단은 중재판정부가 할 수 있다는 판정이 내려졌다. 그러므로 우리나라도 한·미 FTA에 필수적 안보 이익에 관하여 중재판정부가 판단할 수 없다는 내용의 각주가 있다고 하여, 무제한의 재량이 있다고 여기는 일은 없어야 할 것이다. 이 사건에서 중재판정부가 신의성실 원칙을 충족한다고 판단한 구체적 근거가 무엇이었는지 후속 연구에서 더 자세히 분석한다면, 우리나라가 관련 정책을 펼칠 때 참고가 될 수 있을 것이다. 더불어 이 사건에서는 미국정부가 자국 국적의 투자자에게 불리한 주장이 될 것인데도, 안보 이익 예외 규정을 판단할 권한이 중재판정부에 없다는 제3국 의견서를 제출했다. 이 사건처럼 투자협정의 당사국은 투자유치국도 될 수 있고 투자자의 모국도 될 수 있다. 그러므로 앞으로 체결하거나 개정하는 투자협정에서는 신의성실 원칙을 적용한 판단이 가능하다는 점을 명시하여, 중재판정부마다 다른 판단이 내려지는 등의 불필요한 혼란을 방지할 필요가 있다. 이에 그치지 않고 안보 예외 규정을 더 정교화하고 합리화하는 노력이 꾸준히 필요하다. 불필요한 논란으로 초래될 유·무형의 비용을 줄이기 위해서이다. 여기에

381) Seda v. Colombia (Monte Glenn Adcock, Stephen John Bobeck, Justin Tate Caruso and others v. Republic of Colombia). ICSID Case No. ARB/19/6. Award dated 27 June 2024, paras. 607-608.
382) *Ibid.*, para. 756.
383) *Ibid.*, para. 801.

는 이러한 안보 예외 규정만 믿은 나머지, 정부가 안보를 강화하면서 투자자 보호 등 다른 가치도 조화롭게 추구할 방법이 있는데도 방법을 찾으려 노력하지 않게 되는 폐해도 포함된다.

안보상 이유로 한 조치에 대해 중재판정부가 신의성실하게 이루어졌는지 심사하더라도, 이것이 우리 안보에 심각한 위해를 가할 가능성은 거의 없다. 안보상 이유로 위장하여 다른 이유를 위해 조치하지 않는 한, 신의성실하게 조치하면 될 일이다. 설혹 투자분쟁에서 중재판정부가 판단을 그르치더라도 취소 절차가 있으며, 끝내 바로잡을 수 없게 되더라도 금전 배상의 문제가 남을 뿐이다. 안보 조치를 할 수 없는 것은 아니므로, 투자협정에 신의성실 원칙에 따른 판단이 가능하다는 내용을 명시하더라도 그 자체가 안보에 위협이 된다고 볼 수는 없다.

3. 소결

제4장에서는 사이버안보 조치에 대한 국제통상법 적용 가능성을 살펴보았다. 디지털 통상협정에서 발견되는 대부분의 규정은 사이버안보가 아닌 사이버보안에 관한 규정이었고, 협력의 중요성을 인정한다는 내용으로 법적 구속력이 없었다. 다만 미국·일본 디지털 통상협정은 역량구축과 협력 강화를 위해 노력할 법적 의무를 규정했다. 그러나 미국·일본 디지털 통상협정의 규정도 사이버안보에 관한 규정이라기보다는 사이버보안에 관한 규정으로 평가할 수 있다.

RCEP, CPTPP의 규정도 사이버안보가 아닌 사이버보안에 관한 규정이었고, 협력의 중요성을 인정한다는 내용으로 법적 구속력이 없는 것이었다. USMCA의 규정은 용어가 일부 다를 뿐, 미국·일본 디지털 통상협정의 내용과 같다.

WTO GATT와 GATS는 국내 상품 또는 다른 국가로부터 수입되는 동종의

상품과 서비스에 비해 불리한 대우를 수입 상품에 부여하지 않아야 한다는 내국민 대우 의무와 최혜국 대우 의무를 규정한다. 동종성에 대해 WTO 패널과 상소기구는 사안별로 결정되어야 할 개념으로서 절대적 정의가 불가능하다고 본다. 상품 또는 서비스 그 자체의 특성뿐 아니라 소비자의 인식 등도 고려되는데, 특히 EC-석면 사건에서 상소기구는 특정 상품의 위험성이 충분히 크면 최종 소비자는 해당 제품을 구매하지 않을 수도 있고, 이러한 측면이 제조업체의 의사결정에 영향을 미칠 것이라는 점은 의심의 여지가 없다고 보았다. 특정 상품이 개인정보 보호 기능 또는 해킹에 대한 방호벽이 취약하여 소유한 개인의 정보가 유출되는 것은 물론 특정 상품 자체가 서버로 악용되어 국가 핵심 기간망에 대한 분산 서비스 거부 공격을 하여 국가안보에 위협이 되는 때도 있을 수 있다. 이 경우 최종 소비자의 상품 선택에 영향을 미칠 것이고, 보안이 취약하지 않은 다른 상품과 동종 상품이라는 상대국 정부의 주장이 받아들여지지 않을 가능성도 있다.

한편 WTO TBT 협정도 사이버안보 조치가 기술규정, 표준, 또는 적합성 판정과 관계가 있는 한 적용된다. 기술규정과 적합성 판정 절차에서, 수입 상품을 동종 상품인 수입국 국내 상품 또는 다른 국가로부터 수입되는 상품에 비해 불리하게 대우하지 않을 내국민 대우 의무와 최혜국 대우 의무가 적용된다. 표준과 관련해서도 TBT 협정은 WTO 회원국의 중앙정부 표준기관이 TBT 협정 부속서 3에 규정된 표준의 준비, 채택, 그리고 적용에 관한 모범 관행 규약을 준수하도록 보장할 법적 의무를 규정한다. 그러므로 사이버안보 조치와 관련해서도 이러한 TBT 협정이 규정한 의무가 안보상 예외에 의해 면제되지 않는 한, 원칙적으로 적용된다. TBT 협정에는 안보상 예외 규정이 없지만, GATT의 안보상 예외 규정이 적용된다. 한편 기술규정은 준수가 강제적인 문서이고, 표준은 준수가 강제적이지 않은 문서이다. 그러나 WTO 판정례는 강제성 판단이 단순하지 않음을 보여준다. 미국-돌고래 사건에서 참치 상품은 돌고래 안전 라벨의 부착 없이 미국으로 수입될 수 있었다. 그러나 패널과 상소기구는 미국

의 법령 등이 참치 상품에 돌고래 등의 용어를 언급하기 위한 조건을 규정한 점과 조건 미준수에도 라벨을 부착하면 단속 등 집행 조치의 대상이 되는 점을 바탕으로, 돌고래 안전 라벨 제도는 강제성 있는 기술규정이라고 판단했다. 이러한 WTO 판정례에서의 교훈은 사이버보안 인증 라벨링 등 사이버안보 조치의 채택을 고려하거나 시행 중인 국가, 또는 이러한 조치가 WTO 협정에 위반된다고 주장하는 상대국 모두에 시사점이 될 수 있다.

동종 상품에 대한 조치가 아니라거나 강제성이 없는 조치라는 등의 이유를 제시하더라도, 결국 사이버안보 조치가 WTO GATT, GATS, TBT 협정 등에 원칙적으로 위반된다는 판단을 피할 가능성은 지금까지의 WTO 판정례를 바탕으로 보면 높지 않다. 그러므로 사이버안보 조치가 안보 예외로서 인정될 수 있는지 살펴보아야 한다.

전시 또는 국제 관계에서 긴급상황에서 조치하는 것이 아닌, 평시에 취하는 사이버안보 조치는 상품 조치에 대해서는 GATT 제21조 (b)항 (ii)호가, 서비스 조치에 대해서는 GATS 제14조의2 (b)항 (i)호가 적용된다. 두 규정의 내용은 군사시설에 공급하기 위해 간접적으로 행하는 조치에 관한 것으로 같으며, 이중 용도 상품 또는 서비스와 관계가 깊다. 그리고 사이버보안 조치의 대상이 되는 상품 또는 서비스 역시 이중 용도인 경우가 흔하다.

그런데 지금까지 국가안보 예외 규정을 다룬 WTO 판정례는 모두 전시 또는 국제 관계에서 긴급상황에 관한 GATT 제21조 (b)항 (iii)호가 적용된 사건이었다. 따라서 (ii)호에 따라 예외로 인정될 수 있을 것인지는 이를 정면으로 다룬 판정례 없이 조문의 해석과 학설을 참고할 수밖에 없다.

먼저 (ii)호에 규정된 "군사시설에 공급하기 위하여"라는 요건에서 가장 중요한 부분은 '위하여'로 표시된 목적이고, 여기에는 조치 당시 목적을 인식했다는 주관적 증거와 실제로 군사시설 등에 간접적이나마 공급한다는 증거를 신뢰할 만한 출처로부터 확보해야 한다고 보는 견해가 있다. 그밖에는 '군사시설'이라는 문언을 근거로 장기적인 군사 계획을 위해 공급하는 때에는 (ii)호를 원용

하는 것이 인정되지 않을 것으로 보는 견해가 있다. 천막과 같은 임시 시설 또는 해외의 군사시설도 인정이 되는지 의문이 제기된다는 견해도 있다.

다음으로 (b)항 두문에 규정된 '자국의 안전보장상 중대한 이익을 보호하기 위하여 필요하다고 인정되는 조치를 취하는 것을 방해하지 않는다'와 관련해서 대표적인 쟁점은 당사국의 전적인 자기 판단이 허용되는지였다. (ii)호가 아닌 (iii)호를 다뤘던 WTO 판정례 네 건에서 (b)항 두문의 이 요건이 심리되었는데, 당사국이 자국의 필수적 안보 이익의 보호를 위해 필요한 조치라고 '신의성실하게 판단했는지'는 패널과 상소기구가 판단할 수 있다는 일관된 판정이 네 사건 모두에서 내려졌다. 여기서 또 다른 중요 쟁점은 '필요'한 조치인지이다. 안보 예외를 다루어 판정을 내린 WTO 사건 네 건 중 두 건에서 필요성이 인정되었는데, 한 사건은 무력 충돌 상황이었고 다른 사건은 국교 중단 상황이었다. 오늘날 사이버공간에서 발생하는 다양한 위협에 WTO 회원국이 정당하게 대응할 수 있는 여지를 지나치게 좁힌다는 비판도 제기된다.

끝으로 FTA 안보 예외 규정은 RCEP은 WTO와 같다. CPTPP와 USMCA의 필수적 안보에 관한 규정의 문언은 완벽하게 서로 같다. 한·미 FTA도 각주가 있는 점을 제외하면 본문은 이 두 FTA와 같다. CPTPP, USMCA, 한·미 FTA의 안보 예외 규정 본문에는 두 개의 항만 있고, 두 번째 항의 하위에 호가 없다. 군사시설에 직간접적으로 공급하는 이중 용도 상품, 핵분열 물질 관련 조치, 국제 관계의 긴급상황에서 취해지는 조치 등 추가적인 제한 규정이 없다.

한편 한·미 FTA의 안보 예외 규정은 각주에서, 당사국이 제11장(투자) 또는 제22장(제도 규정 및 분쟁 해결)에 따라 개시된 중재절차에서 제23.2조를 원용하는 경우, 그 사안을 심리하는 중재판정부 또는 패널은 그 예외가 적용됨을 판정한다고 규정한다. 이 문언의 의미에 따라 신의성실 원칙의 적용조차도 배제되는지 의문이 제기될 수 있다. 이러한 각주는 미국이 체결한 FTA, BIT, TPA의 일부에 포함되어 있다. 중재판정부의 관할권을 제한하는 내용이지만, 협정 당사국이 합의로 규정한 것이므로 적법성에 의문이 없다고 평가하는 견해가

있다. 다른 한편으로는 국가 사이의 분쟁에서는 적법하겠으나, 투자협정의 당사자가 아닌 제3자 투자자와 투자유치국 사이의 분쟁에서는 적법성에 의문을 제기하는 시각도 있다.

이 각주와 관련, 2024년 6월 27일 판정이 내려진 Seda v. Colombia 사건에서 중재판정부는 이 각주의 규정에도 불구하고 투자유치국이 필수적 안보 이익에 관한 규정을 신의성실(good faith)하게 제기했는지 심리할 수 있는 권한이 중재판정부에 있다고 결정했다. 그러므로 우리 정부로서는 한·미 FTA에 이 각주에 있다고 하여 무제한의 재량이 있다고 여기는 일은 없어야 할 것이다. 우리 기업 등 투자자로서는 문제가 된 투자협정에 이 각주가 있다는 이유로 대응을 미리 포기하는 일도 없어야 할 것이다. 이와 관련하여 앞으로 체결하거나 개정하는 투자협정에서는 신의성실 원칙을 적용한 판단이 가능하다는 점을 명시하여, 중재판정부마다 다른 판단이 내려지는 등의 불필요한 혼란을 방지할 필요가 있다. 투자협정에 신의성실 원칙에 따른 판단이 가능하다는 내용을 명시하더라도 그 자체가 안보에 위협이 된다고 볼 수는 없다.

제5장 결론

1. 연구 내용 요약

사이버안보는 군사안보, 에너지 안보, 경제안보와 같은 국가안보의 하위 개념이다. 사이버안보는 사이버공격 또는 위협을 방어하여, 사이버공간이 적절히 기능하게 함으로써 국가와 국민의 안전이 보장되는 상태이다. 사이버공간은 '정보시스템'과 여기에 저장된 '정보'로 구성된다.

사이버안보 규범에 관한 국제적 논의에서는 미국을 중심으로 한 서방 자유민주 국가와 러시아와 중국을 중심으로 한 상하이협력기구 회원국 사이의 견해 대립이 계속되었다. 그러나 UN 차원에서는 정부 전문가 그룹(UNGGE)이 2004년부터 활동했다. 제3차 보고서는 사이버공간에 국제법이 적용된다는 원칙을 처음 확인했고, 국가의 영역관리 책임을 노력 의무로 인정하는 등 제한적이나마 성과가 있었다. 그러나 사이버공격에 대한 자위권 허용 여부에 관한 견해 대립으로 제5차 보고서는 채택되지 못했다. 이에 러시아가 개방형작업그룹(OEWG) 설치를 제안했고, 제1차 OEWG가 2021년 보고서를 제출했으나, UNGGE 보고서의 결론을 재확인하는 내용에 머물렀다.

국제적 논의 과정에서 식별된 사이버안보 분야의 주요 쟁점은 (ⅰ) 사이버공간의 별도 영역성 인정 여부, (ⅱ) 사이버공간에 대한 국제법 적용 여부, (ⅲ) 사이버 무력공격에 대한 예방적 자위권 인정 여부, (ⅳ) 사이버공간 관련 상당 주의 의무 적용 여부이다. 미국 등 서방 국가는 사이버공간을 별도 영역으로 인정하는 태도를 보이는 것으로 평가할 수 있고, 현행 국제법이 사이버공간에 그대로 적용될 수 있다고 주장한다. 러시아와 중국 등 비서방 진영은 사이버공간이

별도 영역이 아니라는 태도를 보이는 것으로 평가할 수 있고, 시스템 등 물리적인 ICT 기반시설 또는 정보가 저장된 서버의 위치가 국내이면 국내법이, 외국이면 외국법이 적용될 뿐 국제법은 적용되지 않는다고 주장한다. 예방적 자위권 인정 여부에 대한 ICJ 판정례는 없다. UN 헌장을 근거로 인정되는지와 관련해서는 학설 대립이 있다. 비록 임박한 무력공격이 무엇을 의미하는지 논란은 있지만, 국제관습법을 근거로 예방적 자위권이 인정된다는 견해가 설득력이 있다. 그러므로 사이버 무력공격에 대한 예방적 자위권을 주장할 때는 UN 헌장보다는 국제관습법을 근거로 주장하는 것이 상대적으로 더 유리할 것이다.

주요국의 사이버안보 정책을 전략과 법률로 나누어 조사한 결과는 다음과 같다. 미국의 2023년 「국가 사이버안보 전략」에 따라 민간 시설에 대한 사이버안보 최소 요건이 권고되었다. 「CISA 전략계획 2023~2025」는 핵심 네트워크에 대한 침해가 발생하기 전에 능동적으로 위협을 무력화시킨다는 내용을 포함한다. 또한 「2022년 핵심 기반시설 사이버사고 보고법」은 핵심 인프라 소유자에게 사이버사고 발생과 랜섬웨어 피해에 대해 각각 72시간, 24시간 내 보고의무를 부과했다. 이러한 점에서 미국 사이버안보 정책의 특징으로는 능동적 방어 전략을 택한 점, 그리고 상당수 인프라를 민간이 소유 또는 운영하는 점을 고려하여 민간과의 공조를 강화한 점을 들 수 있다.

EU는 2013년 「EU 사이버안보 전략」에서 안전하면서도 개방적인 사이버공간을 강조했으나, 2020년 「EU 사이버안보 전략」에서는 복원력과 기술 주권을 강조했다. EU 사이버안보 법률은 직접적인 수입 제한 조치보다는 인증 제도 또는 표시 제도와 같은 간접적인 조치를 채택한 특징이 있다. 2019년에는 「사이버안보법」을 제정하여 다양한 사이버보안 인증 제도를 마련했다. 이에 따라 2024년에는 ICT 상품에 대한 EUCC 인증 시행법이 제정되었다. 클라우드컴퓨팅 서비스, 5G 통신, AI에 대한 인증도 준비 중이다. 또한 2024년 「사이버복원력법」은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품에 보안 요건 준수를 표시하는 CE 표지를 부착할 의무를 수입업자 또는 유통업자에게 부과한다.

표 5-1. 주요국의 사이버안보 정책 요약

구분	미국	EU	일본	한국
전략	2003년 「안전한 사이버공간을 위한 국가 전략」	2013년 「EU 사이버안보 전략」	2013년 「사이버보안 전략」	2019년 「국가 사이버안보 전략」
기본법	「2015년 사이버안보법」	2019년 「EU 사이버안보법」	2014년 「사이버보안 기본법」	없음
능동 방어 도입	「CISA 전략계획 2023~2025」	미도입	2022년 「국가안전보장전략」	2024년 「국가 사이버안보 전략」
침해 사고 통지 의무	「2022년 핵심 기반 시설 사이버사고 보고법」: 핵심 인프라 소유자·운영자는 사이버사고 발생, 랜섬웨어 피해를 각각 72시간, 24시간 내 보고	2016년 「네트워크 및 정보시스템 법」: 필수서비스 운영자가 보안 사고 발생 즉시 통지할 법적 의무가 EU 회원국에 있음.	검토 중	2009년 「정보통신망법」 및 「정보통신망법시행령」: 정보통신서비스 공급자는 침해사고 발생 즉시(24시간 내, 시행령) 방통위나 인터넷진흥원에 신고해야
인증	「2020년 사물인터넷 사이버안보 개선법」: 연방 정부 소유·관리 IoT 기기 대상(의무)	「사이버안보법」: ICT 상품에 대한 EUCC 인증(자율) 시행, 클라우드컴퓨팅·5G·AI 인증 준비 중	2024년 8월에 「IoT 제품에 대한 보안 적합성 평가제도」 구축 방침 발표: 2025년 3월 신청접수 예정(자율)	「정보통신망법」 제48조의6(정보통신망 연결 기기 등에 관한 인증): 자율
	IoT를 위한 FCC 규정(Cyber Trust Mark): 민간 IoT 대상(자율)	2024년 「사이버복원력법」: 다른 장치나 네트워크에 연결된 모든 상품에 CE 표지 부착(2027년 12월부터 적용, 의무)		

자료: 저자 요약.

일본에서 사이버안보 개념은 2022년 「국가안보전략」에서 처음 제시되었는데, 추진 방안인 '능동적인 사이버 방어'는 미국의 전략과 유사한 것으로 확인

된다. 2014년에 제정된 「사이버보안 기본법」은 총리실 산하 사이버시큐리티 전략본부를 중심으로 일원화된 사이버안보 추진 체제가 구축된 근거가 되었다. 「사이버보안 기본법」은 민간사업자 등에 대한 의무를 부과하지 않고 있는데, 이는 2022년에 제정된 「경제안보추진법」에서 다룬다. 구체적으로 「경제안보 추진법」을 근거로 한 「기간 인프라 방호제도」는 소관 부처에서 지정한 민간사업자를 대상으로 특정 중요 설비 도입 시 및 유지관리 등의 위탁 시 사전심사를 요구하며, 정부는 설비 도입 중지 명령권을 갖는다. 아울러 일본은 EU와 같은 의무적 제도는 아니지만 기업의 자발적 참여에 의한 인증 제도인 「IoT 제품에 대한 보안 적합성 평가제도」를 마련했다.

우리나라의 2024년 「국가 사이버안보 전략」은 자유·인권·법치 수호라는 민주적 가치를 표방한 점과 공세적 사이버 방어와 대응 전략을 도입한 점을 특징으로 볼 수 있다. 사이버안보 법률의 특징은 통합된 법률이 없이 관련 규정이 여러 법률에 흩어져 있다는 것이다. 이는 필연적으로 통합된 관리 조직의 출현을 어렵게 만든다. 한편 클라우드컴퓨팅 등 변화하는 사이버안보 상황에 신속하게 대응하는 점은 돋보인다.

사이버안보 조치에 대한 국제통상법 적용 가능성은 다음과 같다. 대부분의 디지털 통상협정에서 발견되는 규정은 사이버안보가 아닌 사이버보안에 관한 규정이었고, 중요성을 인정한다는 내용으로 법적 구속력이 없었다. RCEP, CPTPP의 규정도 사이버안보가 아닌 사이버보안에 관한 규정이었고, 중요성을 인정한다는 내용으로 법적 구속력이 없는 것이었다. 다만 미국·일본 디지털 통상협정은 역량구축과 협력 강화를 위해 노력할 법적 의무를 규정했다. 그러나 미국·일본 디지털 통상협정의 규정도 사이버보안에 관한 규정으로 평가된다. USMCA의 규정은 용어가 일부 다를 뿐, 미국·일본 디지털 통상협정의 내용과 같다.

WTO GATT와 GATS는 국내 상품 또는 다른 국가로부터 수입되는 동종의 상품과 서비스에 비해 불리한 대우를 수입 상품에 부여하지 않아야 한다는

내국민 대우 의무와 최혜국 대우 의무를 규정한다. 동종성에 대해 WTO 패널과 상소기구는 사안별로 결정되어야 할 개념으로서 절대적 정의가 불가능하다고 본다. 상품 또는 서비스 그 자체의 특성뿐 아니라 소비자의 인식 등도 고려되는데, EC-석면 사건에서 상소기구는 특정 상품의 위험성이 충분히 크면 최종 소비자는 해당 제품을 구매하지 않을 수도 있고, 이러한 측면이 제조업체의 의사결정에 영향을 미칠 것이라는 점은 의심의 여지가 없다고 보았다. 특정 상품이 개인정보 보호 기능 또는 해킹에 대한 방호벽이 취약하면 최종 소비자의 상품 선택에 영향을 미칠 것이고, 보안이 취약하지 않은 다른 상품과 동종 상품이라는 상대국 정부의 주장이 받아들여지지 않을 가능성도 있다.

한편 WTO TBT 협정에 따라 기술규정과 적합성 판정 절차에서 수입 상품을 동종 상품인 수입국 국내 상품 또는 다른 국가로부터 수입되는 상품에 비해 불리하게 대우하지 않을 내국민 대우 의무와 최혜국 대우 의무가 적용된다. 표준과 관련해서도 TBT 협정은 WTO 회원국의 중앙정부 표준기관이 표준의 준비, 채택, 그리고 적용에 관한 모범 관행 규약을 준수하도록 보장할 법적 의무를 규정한다. 그러므로 사이버안보 조치와 관련해서도 이러한 TBT 협정이 규정한 의무가 안보상 예외에 의해 면제되지 않는 한 원칙적으로 적용된다. TBT 협정에는 안보상 예외 규정이 없지만 GATT의 안보상 예외 규정이 적용된다. 한편 기술규정은 준수가 강제적인 문서이고 표준은 준수가 강제적이지 않은 문서이다. 그러나 WTO 판정례는 강제성 판단이 단순하지 않음을 보여준다. 미국-돌고래 사건에서 참치 상품은 돌고래 안전 라벨의 부착 없이 미국으로 수입될 수 있었다. 하지만 패널과 상소기구는 미국의 법령 등이 참치 상품에 돌고래 등의 용어를 언급하기 위한 조건을 규정한 점과 조건 미준수에도 라벨을 부착하면 단속 등 집행 조치의 대상이 되는 점을 바탕으로, 돌고래 안전 라벨 제도는 강제성 있는 기술규정이라고 판단했다. 이러한 WTO 판정례에서의 교훈은 사이버보안 인증 라벨링 등 사이버안보 조치의 채택을 고려하거나 시행 중인 국가 또는 이러한 조치가 WTO 협정에 위반된다고 주장하는 상대국 모두에 시사점

이 될 수 있다.

동종 상품에 대한 조치가 아니라거나 강제성이 없는 조치라는 등의 이유를 제시하더라도, 결국 사이버안보 조치가 WTO GATT, GATS, TBT 협정 등에 원칙적으로 위반된다는 판단을 피할 가능성은 지금까지의 WTO 판정례를 바탕으로 보면 높지 않다. 그러므로 사이버안보 조치가 안보 예외로서 인정될 수 있는지 살펴보아야 한다.

전시 또는 국제 관계에서 긴급상황에 조치하는 것이 아닌 평시에 취하는 사이버안보 조치는 상품 조치에 대해서는 GATT 제21조 (b)항 (ii)호가, 서비스 조치에 대해서는 GATS 제14조의2 (b)항 (i)호가 적용된다. 두 규정의 내용은 군사시설에 공급하기 위해 간접적으로 행하는 조치에 관한 것으로 같으며, 이중 용도 상품 또는 서비스와 관계가 깊다. 그리고 사이버보안 조치의 대상이 되는 상품 또는 서비스 역시 이중 용도인 경우가 흔하다.

그런데 지금까지 국가안보 예외 규정을 다룬 WTO 판정례는 모두 전시 또는 국제 관계에서 긴급상황에 관한 GATT 제21조 (b)항 (iii)호가 적용된 사건이었다. 따라서 (ii)호에 따라 예외로 인정될 수 있을 것인지는 이를 정면으로 다룬 판정례 없이 조문의 해석과 학설을 참고할 수밖에 없다.

먼저 (ii)호에 규정된 '군사시설에 공급하기 위하여'라는 요건에서 가장 중요한 부분은 '위하여'로 표시된 목적이고, 여기에는 조치 당시 목적을 인식했다는 주관적 증거와 실제로 군사시설 등에 간접적이나마 공급한다는 증거를 신뢰할 만한 출처로부터 확보해야 한다고 보는 견해가 있다. 그밖에는 '군사시설'이라는 문언을 근거로 장기적인 군사 계획을 위해 공급하는 때에는 (ii)호를 원용하는 것이 인정되지 않을 것으로 보는 견해가 있다. 천막과 같은 임시 시설 또는 해외의 군사시설도 인정이 되는지 의문이 제기된다는 견해도 있다.

다음으로 (b)항 두문에 규정된 '자국의 안전보장상 중대한 이익을 보호하기 위하여 필요하다고 인정되는 조치를 취하는 것을 방해하지 않는다'와 관련해서 대표적인 쟁점은 당사국의 전적인 자기 판단이 허용되는지였다. (ii)호가 아닌

(iii)호를 다뤘던 WTO 판정례 네 건에서 (b)항 두문의 이 요건이 심리되었는데, 당사국이 자국의 필수적 안보 이익의 보호를 위해 필요한 조치라고 '신의성실하게 판단했는지'는 패널과 상소기구가 판단할 수 있다는 일관된 판정이 네 사건 모두에서 내려졌다. 여기서 또 다른 중요 쟁점은 '필요'한 조치인지이다. 안보 예외를 다루어 판정을 내린 WTO 사건 네 건 중 두 건에서 필요성이 인정되었는데, 한 사건은 무력 충돌 상황이었고 다른 사건은 국교 중단 상황이었다. 오늘날 사이버공간에서 발생하는 다양한 위협에 WTO 회원국이 정당하게 대응할 수 있는 여지를 지나치게 좁힌다는 비판도 제기된다.

끝으로 FTA 안보 예외 규정을 살펴보면 한·미 FTA, CPTPP, USMCA가 같다. 한·미 FTA에 각주가 있는 점만 다르다. 이 FTA들의 안보 예외 규정 본문에는 두 개의 항만 있고, 두 번째 항의 하위에 세부 제한 규정이 없다. 군사시설에 직간접적으로 공급하는 이중 용도 상품, 핵분열 물질 관련 조치, 국제 관계의 긴급상황에서 취해지는 조치 등 세부 제한 규정이 있는 RCEP과 다르다.

한편 한·미 FTA의 안보 예외 규정은 각주에서, 당사국이 제11장(투자) 또는 제22장(제도 규정 및 분쟁 해결)에 따라 개시된 중재절차에서 제23.2조를 원용하는 경우, 그 사안을 심리하는 중재판정부 또는 패널은 그 예외가 적용됨을 판정한다고 규정한다. 이 문언의 의미에 따라 신의성실 원칙의 적용조차도 배제되는지 의문이 제기될 수 있다. 이러한 각주는 미국이 체결한 FTA, BIT, TPA의 일부에 포함되어 있다. 중재판정부의 관할권을 제한하는 내용이지만, 협정 당사국이 합의로 규정한 것이므로 적법성에 의문이 없다고 평가하는 견해가 있다. 다른 한편으로는 국가 사이의 분쟁에서는 적법하겠으나, 투자협정의 당사자가 아니라 제3자인 투자자와 투자유치국 사이의 분쟁에서는 적법성에 의문을 제기하는 시각도 있다.

이 각주와 관련하여, 2024년 6월 27일 판정이 내려진 Seda v. Colombia 사건에서 중재판정부는 이 각주의 규정에도 불구하고 투자유치국이 필수적 안보 이익에 관한 규정을 신의성실(good faith)하게 제기했는지 심리할 수 있는

권한이 중재판정부에 있다고 결정했다. 그러므로 우리 정부로서는 한·미 FTA에 이 각주가 있다고 하여 무제한의 재량이 있다고 여기는 일은 없어야 할 것이다. 우리 기업 등 투자자로서는 문제가 된 투자협정에 이 각주가 있다는 이유로 대응을 미리 포기하는 일도 없어야 할 것이다. 이와 관련하여 앞으로 체결하거나 개정하는 투자협정에서는 신의성실 원칙을 적용한 판단이 가능하다는 점을 명시하여, 중재판정부마다 다른 판단이 내려지는 등의 불필요한 혼란을 방지할 필요가 있다. 투자협정에 신의성실 원칙에 따른 판단이 가능하다는 내용을 명시하더라도 그 자체가 안보에 위협이 된다고 볼 수는 없다.

2. 정책적 시사점

가. 우리나라의 사이버안보 정책에 대한 시사점

첫째, 사이버 무력공격에 이르지 않으면 자위권을 행사할 수 없다. 사이버 부당 이용 또는 사이버공격 등은 타국에 대한 부당한 간섭 또는 타국의 주권 침해에 해당하겠지만, 규모와 효과의 측면에서 중대한 인명 살상 또는 국가 핵심 기반시설에 대한 심각한 피해 등을 초래하지 않는 한 사이버 무력공격에는 해당하지 않는다. 따라서 사이버 무력공격에 이르지 않은 사이버 부당 이용 또는 사이버공격에 대해서는 자위권을 행사할 수 없다. 어떤 국가가 자위권 행사라고 주장하면서 사이버 무력공격에 이르지 않은 상대국의 사이버 부당 이용 또는 사이버공격에 대해 사이버공격을 한다면 부당한 간섭 또는 타국의 주권 침해를 저지르는 행위가 된다.

둘째, 공세적 방어 전략은 신중하게 추진되어야 한다. 국가 핵심 기반시설에 심각한 피해가 발생하면 복구에 오랜 시간이 필요하므로, 침해가 발생하기 전

에 능동적으로 위협을 무력화시키는 것을 내용으로 하는 공세적 또는 능동적 방어의 필요성이 제기된다. 2022년 미국은 「CISA 전략계획 2023~2025」에서 능동적 사이버 방어를 발표했고, 같은 해 일본 역시 「국가안전보장전략」에 능동적 사이버 방어에 관한 내용을 포함했다. 우리나라도 2024년 「국가 사이버안보 전략」에서 공세적 사이버 방어 전략을 도입했다. 우리나라의 공세적 방어 전략은 공격 근원지를 능동적으로 탐지·분석하여 사전징후를 포착하고 관련 정보를 유관 부처와 신속 공유하여, 예상되는 공격에 대비하는 것을 내용으로 한다. 현재와 같이 대비 차원이라면 문제가 없다고 생각된다. 공세적 성격을 더욱 강화하여 공격 개시 전에 상대를 무력화해야 한다는 주장도 제기되는데, 이에 대해서는 신중할 필요가 있다. UN 헌장은 무력공격이 발생한 때 공격받은 국가는 UN 안보리가 조치하기 전까지만 자위권을 행사할 수 있다고 규정한다. 따라서 무력공격 발생 전에 공세적으로 미리 자위권을 행사하는 행위는 UN 헌장을 근거로 해서는 정당화할 수 없다. 다만 국제관습법에 따라 허용된다는 학설이 설득력이 있고 다수설로 보인다. 그러나 예방적 자위(anticipatory self-defense)의 하위 유형 중에서도 무력공격이 임박하지 않은 방지적 자위(preventive self-defense)는 여전히 금지되고, '임박한(imminent)' 무력공격을 대상으로 하는 선제적 자위(pre-emptive self-defense)가 허용된다는 견해다. 하지만 '최초 무력공격에 합리적으로 인접(reasonably proximate to the initial armed attack)'했다는 것을 뜻하는 임박성을 판단할 구체적 기준에 대한 논란이 있다.

셋째, 사이버공간에 대한 국가의 영역관리 책임 또는 상당 주의 의무라는 법리는 우리나라가 북한으로부터의 사이버 위협에 대응하는 데 유용하게 활용할 수 있을 것이다. 우리나라는 북한의 존재라는 특수성을 안고 있는 국가이다. 우리나라에 가해지는 사이버 위협의 궁극적인 출처는 상당한 비중이 북한에 의한 것으로 추정되거나 확인되었다.[384] 그런데 북한이 인터넷에 연결하기 위해서

384) 「이더리움 580억 탈취, 北 소행…"북한 어휘 '혈한 일' 발견"」(2024. 11. 21.).

는 위성 인터넷을 사용하지 않는 한 중국 또는 러시아를 통할 수밖에 없다. 나아가 북한은 중국, 동남아, 아프리카 등 제3국 거점을 마련하여 그곳에서 해킹 활동을 한다는 의혹도 제기된다. 이러한 상황에서 우리나라는 제3국에 영역관리 책임 또는 상당 주의 의무 준수를 요구할 수 있다. UN 헌장과 국제관습법에 따라 국제사회에서는 주권 존중의 원칙이 인정되고 이에서 내정간섭 금지 원칙도 유래된다. 그러나 동시에 자국 영역 내에서 발생하는 행위로 타국에 손해를 끼치지 않아야 한다는 영역관리 책임 또는 상당 주의 의무 역시 인정되기 때문이다. 북한은 인터넷이 널리 보급되지 않은 특성이 있으므로, 우리나라로서는 북한으로부터 해킹을 당하더라도 대칭적인 대응을 하기가 어렵다. 그렇다고 해서 북한으로부터의 해킹에 대해 무력적인 수단을 동원하기도 제반 여건상 마땅하지 않다. 이러한 상황에서 제3국에 영역관리 책임을 촉구하는 것은 일정한 효과를 기대할 수 있을 것으로 기대된다.

제3국에 영역관리 책임을 촉구한 것으로 추정되는 사례로는 소니 픽처스 사건을 들 수 있다. 2014년 12월 23일부터 24일까지 이틀 동안 북한의 인터넷 접속이 끊어졌다.[385] 로이터 신문은 이틀 만에 복구된 점은 국가가 지원한 해킹 공격에 의한 것은 아니라는 방증이라는 미국 인터넷 업체의 인터뷰를 게재했다. 또한 미국이 중국에 대해 중국 인터넷을 사용하는 북한의 서버 등을 폐쇄하고 중국 내에서 활동하는 북한 해커를 파악하여 추방하라고 요구했다고 보도했다. 그리고 미국이 이러한 요구를 한 이유는 미국기업 소니 픽처스에 대한 북한의 해킹 공격이 있었기 때문이라고 전했다. 당시 미국기업 소니 픽처스는 북한 체제를 풍자한 영화의 개봉을 준비했었다.[386]

넷째, 우리나라도 통합된 사이버안보법을 마련할 필요가 있다. 그래야만 일원화되고 체계적인 예방과 대응이 가능하며, 사이버공격을 효과적으로 막아낼

385) 「북한 인터넷이 끊기자 종북 댓글도 줄었다?」(2014. 12. 26.).
386) "North Korea's Internet links restored amid U.S. hacking dispute"(2014. 12. 23.), 온라인 기사(검색일: 2024. 11. 19.).

수 있을 것이기 때문이다.[387] 물론 우리나라는 국가안보실에 사이버안보 비서관을 두고 국가정보원을 사이버 위기관리 주관기관으로 정하여 국가 차원의 일원화된 대응체계를 갖추었다. 그러나 민간 분야 정보보호 정책·제도의 총괄과 조정은 과학기술정보통신부가 담당한다. 통합된 기본법이 있다면, 공공과 민간을 구분하지 않은 사이버 위협에 더욱 효과적으로 대응할 수 있을 것이다. 이미 미국 동부에서는 2016년에 인터넷 공유기와 CCTV가 대규모로 해킹되어 인터넷 공급업체 서버를 공격한, 이른바 미라이 봇넷(Mirai Botnet) 사건이 발생했다. 미국을 비롯한 주요국은 통합된 사이버안보 기본법 체계를 근거로 일원화된 추진체계를 갖추고 있다. 미국의 일원화된 추진체계는 공공 분야와 민간 분야를 아우른다. 일본 또한 2014년에 제정된 「사이버보안 기본법」을 근거로 사이버시큐리티 전략본부와 사무국인 사이버시큐리티 센터를 주축으로 일원화된 추진 체제를 구축한 것으로 확인된다. 더불어 일본은 안보 환경의 변화에 대응해 정부의 정책조정 기능을 강화하기 위한 개편안을 논의하고 있다.

나. 우리나라의 통상 정책에 대한 시사점

첫째, 주요국이 도입하는 사이버안보 조치를 지속해서 관찰하여 우리 수출기업이 받는 부정적 영향을 최소화해야 한다. 미국 FCC는 미국정부 인증표지(U.S. Cyber Trust Mark) 제도를 위해 2024년 8월 「사물인터넷을 위한 사이버보안 표지」 규정을 시행했다. EU도 2019년 「사이버안보법」을 제정하여 다양한 사이버보안 인증 제도를 마련하고 있다. 이에 따라 2024년에는 ICT 상품에 대한 EUCC 인증 시행법이 제정되었다. 클라우드컴퓨팅 서비스, 5G 통신, AI에 대한 인증도 준비하고 있다. 일본 역시 2024년 8월 「IoT 제품에 대한 보안 적합성 평가제도」를 마련할 방침을 발표했다. 이러한 제도는 모두 준수할 법적 의무가 없으므로, 표지가 없더라도 수입 또는 유통이 금지되지 않는다.

387) 이성엽(2022), p. 258.

그러나 상품이나 서비스에 대한 소비자의 인식에 이러한 표지 등이 영향을 미칠 수 있으므로, 심사 과정에 차별적인 요소는 없는지 우리 정부가 주시할 필요가 있다. 특히 EU가 2024년 제정한 「사이버복원력법」은 디지털 요소가 있는 소프트웨어 또는 하드웨어 상품에 보안 요건을 준수한다는 CE 표지를 부착할 법적 의무를 수입업자 또는 유통업자에게 부과했다. 법적 의무가 있는 만큼 우리 정부로서는 더 면밀히 대응할 필요가 있다.

둘째, 우리 기업이 미국 또는 EU 시장 등에서 제3국과 경쟁할 때 사이버안보 관련 표지 및 인증 등에서 유리한 위치에 설 수 있도록 우리 정부가 지원해야 한다. 당장은 미국 또는 EU 시장 등에서 사이버보안 관련 표지와 인증 등의 요건이 늘어가는 현상이 우리 수출 기업에 부담일 수 있다. 하지만 제3국의 상품이 이러한 요건을 충족하는 것이 쉽지 않은 때는, 경쟁 관계에서 우리 기업의 상품에 유리한 요소로 작용할 수 있다.[388]

셋째, 우리나라가 사이버보안 조치를 할 때는 통상규범에 저촉되지 않도록 정밀한 제도 설계와 운영이 필요하다. 예컨대 인터넷에 연결된 카메라(IP카메라)에 대한 우려가 높아지자, 우리 정부도 제품 설계 단계부터 높은 보안 수준의 비밀번호를 설정하는 기능을 탑재하도록 의무화하는 조치를 발표했다. 「전파법」에 근거한 적합성 평가이다.[389]

넷째, 국가가 통상협정의 국가안보 예외 규정을 주장할 때도 제한이 없는 것이 아니라, WTO 패널 또는 국제투자중재 판정부 등의 최소한 신의칙에 따른 심사가 이루어진다. 국가안보 예외 주장이 제기된 네 건의 WTO 사건에서 패널은 국가안보 예외 규정에 따라 필수적 안보에 필요한 조치인지 판단할 재량을 조치국이 갖는다는 점을 인정했지만, 이때도 신의칙의 제한을 받는다고 일관되게 판단했다. FTA에서도 마찬가지이다. 예컨대 한·미 FTA 안보 예외 규정은

388) 「LG전자, 최고 수준 차량 사이버보안 인증 레벨3 받아」(2024. 12. 3.).
389) 과학기술정보통신부(2024. 11. 14.), 「안전한 인터넷 프로토콜 카메라(IP카메라) 이용환경을 조성하여 사생활 침해 등 국민 불안 해소」(검색일: 2024. 12. 11.).

각주에서 당사국이 중재절차에서 국가안보 예외를 주장하면 중재판정부는 그 예외가 적용됨을 판정한다고 규정한다. 그런데 같은 문언이 포함된 미국·콜롬비아 BIT가 적용된 Seda v. Colombia 사건에서 중재판정부는 투자유치국이 필수적 안보 이익에 관한 규정을 신의성실(good faith)하게 제기했는지 심리할 권한이 중재판정부에 있다는 판정을 2024년 6월 27일 내렸다.

참고문헌

[국문자료]

고은아, 김홍빈, 김진규, 윤주연. 2023.「EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점」. *KISA Insight*, Vol. 4. 한국인터넷진흥원. (8월)

권현호. 2013.「WTO 법에서 '동종성'(likeness)의 개념과 한계」.『법학연구』, Vol. 54, No. 3, pp. 107~132. 부산대학교 법학연구소.

김규판, 이형근, 이보람, 이정은, 김승현. 2021.「미중 갈등시대 일본의 통상대응 전략」. 연구보고서 21-09. 대외경제정책연구원.

김대순. 2022.『국제법』(21판). 삼영사.

김민정. 2012.「〈미국-멕시코 참치분쟁 II〉에 대한 WTO판결 분석」.『국제경제법연구』, 10(2), pp. 117~166. 한국국제경제법학회.

김상배. 2015.「사이버 안보의 미중관계: 안보화 이론의 시각」.『한국정치학회보』, 49(1), pp. 71~97. 한국정치학회.

김소정. 2023.「2023 미국 사이버안보 전략 주요내용과 한국에의 시사점」. 이슈 브리프 512호. 국가안보전략연구원.

_____. 2024.「국가 사이버안보 전략 개정의 특징과 시사점」. 이슈 브리프 423호. 국가안보전략연구원.

박노형. 2014.「미국의 사이버안전에 관한 법 제정 동향과 시사점」.『법제연구』, Vol. 46. 한국법제연구원.

박노형, 김효권. 2021.「국제사이버법상 상당한 주의 의무에 관한 국가실행」.『국제법학회논총』, 66(4), pp. 61~95. 대한국제법학회.

박노형, 박주희. 2021.「제6차 UNGGE 보고서 채택과 국제사이버법의 발전」.『국제법학회논총』, 66(3), pp. 173~202. 대한국제법학회.

박노형, 정명현. 2014.「사이버전의 국제법적 분석을 위한 기본개념의 연구」.『국제법학회논총』, 59(2), pp. 65~93. 대한국제법학회.

_____. 2016.「제4차 정보안보에 관한 유엔정부전문가그룹 논의 분석과 국제사이버법의 발전 전망」.『국가전략』, 제22권 제3호 통권 77호, pp. 173~198. 세종연구소.

_____. 2018.「국제사이버법의 발전: 제5차 UNGGE활동을 중심으로」.『국제법학회논총』, 63(1), pp. 43~68. 대한국제법학회.
박민숙, 이효진. 2020.『중국의 사이버보안 정책 연구』. 연구자료. 20-13. 대외경제정책연구원.
박상돈. 2022.「미국 2015 사이버시큐리티법(Cybersecurity Act of 2015)의 의의와 시사점」.『미국헌법연구』, Vol. 28, No. 1, pp. 41~78. 미국헌법학회.
박상돈, 김소정. 2013.「사이버안보법 제정을 위한 국내 사이버안보 법률안 연구」.『융합보안』, Vol. 13, No. 6, 통권 52호, pp. 91~98. 한국융합보안학회.
박주현. 2024.「WTO 안보예외조항 연구: WTO 미-중 반도체 분쟁 및 분쟁해결기구(DSB)에 대한 시사점」.『通商法律』, 2024-02.
양천수, 지유미. 2018.「미국 사이버보안법의 최근 동향」.『법제연구』, Vol. 54, pp. 155~192. 한국법제연구원.
이동은. 2024.「이중용도 물품 수출통제에 관한 국제통상법적 고찰: GATT 제21조(b)(ii)의 해석 및 적용을 중심으로」.『통상법률』, 164, pp. 103~145. 법무부.
이성엽. 2022.「국가 사이버안보 법제와 거버넌스의 바람직한 정립 방향: 미국의 사례와 한국의 시사점을 중심으로」.『행정법연구』, 67, pp. 239~262. 행정법이론실무학회.
이재민. 2023.「'경제안보'의 법적 의미와 외연: 국제법적 측면을 중심으로」.『국제법학회논총』, 68(4), pp. 203~254. 대한국제법학회.
이재성, 최선미, 안춘모, 유영상. 2023.「주요국 사이버안보 정책 동향 및 시사점」. 전자통신연구원.
장성길. 2021.「국가안보 측면에서의 투자분쟁 검토 및 대응 방안 모색」.『통상법률』, 3, pp. 3~33. 법무부.
전상현. 2019.「기본권으로서의 개인정보자기결정권: 개인정보자기결정권의 헌법상 근거의 보호영역」. 고학수, 임 용 편저.『데이터오너십』. 박영사.
정준현. 2021.「헌법과 사이버안보」. 안종만, 안상준 편저.『사이버안보와 법』. 박영사.
천곤웅, 김성훈. 2024.「미국 Cybersecurity 전략 및 실행계획 분석과 시사점」.『KISA Insight』, Vol. 01. 한국인터넷진흥원. (1월)
청와대 국가안보실. 2019.『국가사이버안보전략』.
최경진. 2015.「사이버안보와 개인정보보호법령의 상관성」.『가천법학』, Vol. 8, No. 4, 통권 25호, pp. 201~222. 가천대학교 법학연구소.
최숙현. 2023.「기시다 정부의 사이버 안보 전략의 동향과 시사점」.『NISS 전략보고』, No. 244. 국가안보전략연구원. (12월)

현대호. 2007.「정보보안 관련법제의 문제점과 개선방안」. 한국법제연구원.
한국인터넷진흥원. 2020a.「미국 하원, 사물인터넷 사이버보안 개선 법안 가결」. 인터넷 법제동향 제157호. (10월)
_____. 2020b.「미국 정부, 사물인터넷(IoT) 사이버보안 개선법 제정」. 인터넷 법제동향 제159호. (12월)
_____. 2022.「EU집행위원회, 네트워크 연결 기기 등에 사이버보안 의무를 도입하는「사이버복원력법(안)」발표(2022. 9. 15.)」. 인터넷 법제동향 제180호. (9월)
_____. 2023.「유럽 이사회,「사이버복원력법(안)」수정안에 대한 회원국 간 공동합의 도출(2023. 7. 19.)」. 인터넷 법제동향 제190호. (7월)
_____. 2024.「유럽의회,「사이버복원력법(CRA)」(2024. 3. 12.) 및「AI법」최종승인(2024. 3. 13.)」. 인터넷 법제동향 제198호. (3월)

[일문자료]
三角育生. 2020.「我が国のサイバーセキュリティ戦略策定の背景」.『日本セキュリティ・マネジメント学会誌』, Vol. 34, No. 1, pp. 29~34. (5月)
_____. 2021.「サイバーセキュリティ基本法制定・改正の経緯」.『日本セキュリティ・マネジメント学会誌』, Vol. 34, No. 3, pp. 39~46. (1月)
_____. 2023.『我が国のサイバー/情報セキュリティ政策の変遷:組織·戦略編』. JCIC. (7月)
_____. 2024.『我が国のサイバー/情報セキュリティ政策の変遷 (重要インフラ編) ~今後の重要インフラに係るサイバーセキュリティ政策立案において考慮すべき観点~』. JCIC. (5月)
柿沼重志, 榎本尚行. 2024.『能動的サイバー防御に係る制度構築の方向性と課題』. 内閣委員会調査室. 参議院事務局 企画調整室 (調査情報担当室) 239号. (10月 17日)
国家安全保障会議. 2022.「国家安全保障戦略」. 国家安全保障会議決定. 閣議決定.
サイバーセキュリティ戦略本部. 2024a.『重要インフラのサイバーセキュリティに係る行動計画』. (3月 8日)
_____. 2024b.「サイバーセキュリティ 2024」. (7月 10日)
蔦大輔. 2024.『〈特集1〉サイバーセキュ…リティ法制の概観と課題』. ジュリスト No. 1599. (6月 25日)
総務省.「基幹インフラ役務の安定的な提供の確保に関する制度」. https://www.soumu.go.jp/menu_seisaku/kokumin/keizaianzenhosho/index_00001.

html(검색일: 2024. 10. 19.).
_____.「経済安全保障推進法」. https://www.soumu.go.jp/menu_seisaku/kokumin/keizaianzenhosho/index_00001.html(검색일: 2024. 10. 7.).
自由民主党. 2024.「能動的サイバー防御、早期法制化を要望関係会議が石破総理に提言申し入れ」. (11月 7日). https://www.jimin.jp/news/policy/209359.html(검색일: 2024. 11. 8.).
小野寺大毅. 2024.「外交・安全保障 第18回：IoT製品へのサイバー脅威を防ぐ適合性評価制度とは？：安全保障の維持・強化に貢献する経産省の新制度.」.『三菱総合研究所』. (10月 3日). https://www.mri.co.jp/knowledge/column/20241003.html(검색일: 2024. 11. 27.).
備酒 求. 2024.「重要経済安保情報の保護及び活用に関する法律」. (6月 14日). https://www.newton-consulting.co.jp/itilnavi/guideline/economic_security_act.html(검색일: 2024. 10. 11.).
e-gov 法令検索 홈페이지.「デジタル社会形成基本法」. https://laws.e-gov.go.jp/law/503AC0000000035(검색일: 2024. 10. 11.).
_____.「サイバーセキュリティ基本法」. https://laws.e-gov.go.jp/law/426AC1000000104(검색일: 2024. 10. 11.).
_____.「不正アクセス行為の禁止等に関する法律」. https://laws.e-gov.go.jp/law/411AC0000000128(검색일: 2024. 10. 11.).
_____.「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」. https://laws.e-gov.go.jp/law/504AC0000000043(검색일: 2024. 10. 11.).
_____.「重要経済安保情報の保護及び活用に関する法律」. https://laws.e-gov.go.jp/law/506AC0000000027/20250516_000000000000000(검색일: 2024. 10. 11.).
JCIC. 2022.「シリズ「日本のサイバーセキュリティ政策史」:誰も取りさない「サイバーセキュリティ戦略」実現に向けた政府の決意」. (7月). https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy.pdf(검색일: 2024. 10. 11.).
KPMG 홈페이지. 2023.「経済安全保障推進法（基幹インフラ制度）に対応するセキュリティ施策とは」. (11月 21日). https://kpmg.com/jp/ja/home/insights/2023/11/cyber-economic-security.html(검색일: 2024. 10. 7.).
NISC. 2021.「サイバーセキュ…リティ戦略の概要」. (9月 28日)
_____. 2023.「サイバーセキュリティ関係法令 Q&AハンドブックVer2.0」.
_____. 2024.「サイバーセキュリティ政策の推進体制」. (7日)

「機密扱う資格制度、年内に運用基準策定有識者が初会合」. 2024. 『日本経済新聞』. (6月 26日). https://www.nikkei.com/article/DGXZQOUA25APJ0V20C24A6000000/(검색일: 2024. 9. 4.).
「サイバー安保強化へ遠い米英の背中データでみる日本の守り」. 2024.『日本経済新聞』. (12月16日). https://www.nikkei.com/telling/DGXZTS00012680R01C24A1000000/(검색일: 2024. 12. 17.).
「サイバーセキュリティ基本法」とは？背景や内容を分かりやすく解説」. 2024. *JBS*. (1月 25日). https://www.jbsvc.co.jp/corporate/outline/(검색일: 2024. 10. 11.).
「能動的サイバー防御、課題は」. 2024.『朝日新聞』. (9月 22日)

[영문자료]

Delerue, Francois. 2020. *Cyber Operations and International Law.* Cambridge.
DeWeese, Geoffrey S. 2015. "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence." M. Maybaum, A. M. Osula, L. Lindström eds. *Architectures in Cyberspace.* NATO CCD COE Publications.
Dinstein, Yoram. 2011. *War, Aggression, and Self-defence.* Cambridge University Press.
Eenma, Helen. 2005. "The Concept of Anticipatory Self-Defense in International Law after the Bush Doctrine." *Acta Societatis Martensis*, Vol. 1, pp. 42-66.
Ishikawa, Tomoko and Yarik Kryvoi. 2003. "Introduction." Ishikawa, Tomoko and Yarik Kryvoi eds. *Public and Private Governance of Cybersecurity: Challenges and Potential.* Cambridge University Press.
Matsushita, Mitsuo, Thomas J. Schoenbaum, Petros C. Mavroidis, and Michael Hahn. 2017. *The World Trade Organization: Law, Practice, and Policy.* Oxford University Press.
Meltzer, Joshua P. 2019. "Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rule." Working Paper no. 132. Brookings Institution.
Munin, Nellie. 2010. *Legeal Guide to GATS.* Wolters Kluwer.
O'Meara, Chris. 2022. "Reconceptualising the right of self-defence against 'imminent' armed attacks." *Journal on the Use of Force and International Law*, 9(2), pp. 278-323.

Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

Schill, S.W. and R. Briese. 2009. ""If the State Considers": Self-Judging Clauses in International Dispute Settlement." *Max Planck Yearbook of United Nations Law*, 13, pp. 61-140.

Schmitt, Michael N. 2016. *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge University Press.

Shaw, Malcolm N. 2017. *International Law.* Cambridge University Press.

Svetlicinii, Alexandr and Xueji Su. 2024. "The Unsettled Governance of the Dual-Use Items under Article XXI(b)(ii) GATT: A New Battleground for WTO Security Exceptions." *World Trade Review*, pp. 1-26. (February)

Wunsch-Vincent, Sacha. 2006. "The Internet, Cross-Border Trade in Services, and the GATS:· Lessons from US-Gambling." *Journal on the Use of Force and International Law,* 9(2), pp. 278-323.

[보도자료]

과학기술정보통신부 보도자료. 2024.「안전한 인터넷 프로토콜 카메라(IP카메라) 이용환경을 조성하여 사생활 침해 등 국민 불안 해소」. (11월 4일). https://www.msit.go.kr/bbs/view.do;jsessionid=gmDC7FwxyzPCYJ6JWOlPE8YjhEya7HoxUYYzY4c4.AP_msit_1?sCode=user&mPid=238&mId=113&bbsSeqNo=94&nttSeqNo=3185117(검색일: 2024. 12. 11.).

국가정보원 보도자료. 2024.「국정원,「CSK 2024」에서 주요 사이버안보 정책방향 공개」. (9월 9일). https://www.nis.go.kr/CM/1_4/view.do?seq=315 (검색일: 2024. 10. 21.).

산업통상자원부 보도자료. 2023.「1.14일「한-싱가포르 디지털동반자협정」발효」. (1월 13일). https://www.motie.go.kr/kor/article/ATCL3f49a5a8c/166660/view?mno=&pageIndex=1&rowPageC=0&displayAuthor=&searchCategory=0&schClear=on&startDtD=&endDtD=&searchCondition=1&searchKeyword=%EC%8B%B1%EA%B0%80%ED%8F%AC%EB%A5%B4#(검색일: 2024. 11. 22.).

_____. 2023.「의약품 해외 인·허가 등 포괄·신속 수출심사 도입으로 국가 핵심기술 수출 애로 해소」. (7월 25일). https://www.motie.go.kr/kor/article/ATCL3f49a5a8c/167605/view(검색일: 2024. 10. 22.).

_____. 2024.「한-유럽연합(EU) 디지털통상협정 협상 가속화」. (9월 10일). https://www.motie.go.kr/kor/article/ATCL3f49a5a8c/169503/view#(검색일: 2024. 11. 23.).

EU 집행위원회 보도자료. 2020. "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient." (December 16). https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391(검색일: 2025. 2. 4.).

_____. 2022. "Cyber Defence: EU boosts action against cyber threats." (November 10). https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642(검색일: 2024. 12. 10.).

_____. 2024. "Commission welcomes political agreement on Cyber Solidarity Act." (March 6). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332(검색일: 2024. 11. 7.).

[신문기사]

「공공업무에도 챗GPT 활용…AI·클라우드·데이터 경제 창출 기대」. 2024.『전자신문』. (9월 11일)

「국가사이버안보 기본계획 발표..양자암호 개발·망 분리 개선·사이버보안 R&D 확대」. 2024.『전자신문』. (9월 1일)

「"국가핵심기술은 韓영토에만 저장"…클라우드 활용기준 바뀌나?」. 2023.『머니투데이』. (11월 22일)

「국정원, 공공클라우드 규제 신설…민간사업자 진입 '그림의 떡'」. 2024.『아이티데일리』. (9월 13일)

「국정원 'MLS' 적용 발표…공공 클라우드 시장 위축 우려」. 2024.『이데일리』. (9월 13일)

「다중계층보안(MLS) 핵심 '데이터 중요도 분류', 미국과 영국은」. 2024.『전자신문』. (10월 22일)

「美국방부, 사이버사령부 창설 공식 발표」. 2009.『연합뉴스』. (6월 24일)

「미래 안전사회 조성을 위한 보안개념 정리 필요성과 향후 과제」. 2024.『전자신문』. (8월 30일)

「美법원 "틱톡금지 합헌…내달 19일까지 미국內 사업권 팔아야"」. 2024.『연합뉴스』. (12월 7일)

「북한 인터넷이 끊기자 종북 댓글도 줄었다?」. 2014.『동아일보』. (12월 26일)

「이더리움 580억 탈취, 北 소행…“북한 어휘 ‘헐한 일’ 발견”[일문일답]」. 2024. 『뉴시스』. (11월 21일)
「틱톡, 강제매각법 美서 위헌소송 제기」. 2024. 『한국경제신문』. (5월 8일)
「LG전자, 최고 수준 차량 사이버보안 인증 레벨3 받아」. 2024. 『전자신문』. (12월 3일)
「RSA, 암호화SW에 ‘백도어’ 심고 ‘뒷돈’ 챙겨」. 2023. 『지디넷코리아』. (12월 22일)
“Analysis: Tribunal in Seda v. Colombia finds that state invoked essential security interests exception in good faith, precluding any finding of wrongfulness.” 2024. *IA reporter*. (August 22)
“FBI Accuses North Korea in Sony Hack.” 2014. *Time*. (December 19)
“North Korea’s Internet links restored amid U.S. hacking dispute.” 2014. *Reuters*. (December 23)
“US expected to propose barring Chinese software in autonomous vehicles.” 2024. *Reuters*. (August 6)

[온라인 자료]

국가사이버안보센터. 2024.「정부 합동 ‘국가 사이버안보 기본계획’ 발표」. https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=147016&pageIndex=1&searchCnd2=%EA%B3%B5%EC%A7%80%EC%82%AC%ED%95%AD(검색일: 2024. 9. 26.).
국가전략정보포털. 2024.「서비스 소개」. https://nsp.nanet.go.kr/introduce.do(검색일: 2024. 10. 20.).
국가정보원 홈페이지. 2024.「보안적합성 검증」. https://www.nis.go.kr:4016/AF/1_7_2_1.do(검색일: 2024. 10. 21.).
국가정보원, 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 금융위원회, 외교부. 2024.『2024 국가정보보호백서』. https://www.kisa.or.kr/20303/form?postSeq=12004&page=1#fnPostAttachDownload(검색일: 2024. 12. 9.).
국가정보자원관리원 홈페이지. 2024.「인사말」. https://www.nirs.go.kr/subN05/sub05_101_01.jsp(검색일: 2024. 10. 21.).
국립국어원 표준국어대사전 홈페이지. ‘안보’, ‘보안’. https://stdict.korean.go.kr(검색일: 2024. 10. 10.).
대한민국 국회 의안정보시스템. 2020.「[2101220] 사이버안보 기본법안(조태용의원 등 27인)」. https://likms.assembly.go.kr/bill/billDetail.do?billId

=PRC_S2C0I0T6E3Q0C1X7W4E3I0B7S5Z7Z9(검색일: 2024. 8. 19.).
_____. 2021a.「국가사이버안보법안(김병기의원 등 13인)」. https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P2I1J1H0N0V6U1T8K5N5C5E2H8A6B0(검색일: 2024. 8. 19.).
_____. 2021b.「[2113670] 사이버보안 기본법안(윤영찬의원 등 12인)」. https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T2B1W1I1M1F7U1Z8F2R2A4I5D8L6X9(검색일: 2024. 8. 19.).
대한민국 대통령실. 2024.「국가안보실, 윤석열 정부의 '국가 사이버안보 전략' 수립」. (2월 1일). https://www.president.go.kr/newsroom/press/gdXzwtKB(검색일: 2024. 8. 4.).
법제처 홈페이지. 2018.「사이버안보법제 고찰」. https://world.moleg.go.kr/web/wli/rsrchReprtReadPage.do;jsessionid=IBTs3XETu2Pmo1EoXEMKwV4D3a7eynHzylnywOeeeN77esfWUJjxBuvDK2dOzIX8.eduweb_servlet_engine7?1=1&searchPageRowCnt=10&A=A&AST_SEQ=70&CTS_SEQ=47857&searchType=all&searchNtnl=DE&searchNtnlCls=4&pageIndex=1&ETC=1(검색일: 2024. 10. 10.).
_____. 2024.「국제연합헌장 및 국제사법재판소규정」. https://www.law.go.kr/trtySc.do?menuId=1&subMenuId=25&tabMenuId=135&query=UN%20%ED%97%8C%EC%9E%A5#licTrty190(검색일: 2024. 11. 17.).
외교부 홈페이지. 2019.「(조약 제2410호) 한-영국 군사비밀정보보호협정 개정 교환각서」. https://treatyweb.mofa.go.kr/usr/treaty/selectTreatyInfomationDetail.do(검색일: 2024. 10. 23.).
중화인민공화국 중앙인민정부 홈페이지. 2019.「新时代的中国国防」. https://www.gov.cn/zhengce/2019-07/24/content_5414325.htm(검색일: 2024. 8. 15.).
한국과학기술정보연구원 홈페이지. 2024.「미 국토안보부(DHS), 사이버보안 및 기반보호를 위한 전문기관(CISA) 설립」. https://scienceon.kisti.re.kr/srch/selectPORSrchTrend.do?cn=GTB2018004808(검색일: 2024. 11. 6.).
한국인터넷진흥원 홈페이지. 2019.「대한민국 정부 최초「국가 사이버안보 전략」 발간」. https://www.kisa.or.kr/401/form?postSeq=2372&lang_type=KO&page=(검색일: 2024. 8. 4.).
_____. 2024.「정보통신망연결기기 보안인증(IoT)」. https://www.kisa.or.kr/1050608(검색일: 2024. 12. 11.).
미국 관보 홈페이지. 2024. "Cybersecurity Labeling for Internet of Things." https://www.federalregister.gov/documents/2024/07/30/2024-14148

/cybersecurity-labeling-for-internet-of-things(검색일: 2024. 12. 11.).
미국 국토안보부 홈페이지. 2009. "New National Cybersecurity Center Opened." https://www.dhs.gov/archive/news/2009/10/30/new-national-cybersecurity-center-opened(검색일: 2024. 11. 25.).
미국 사이버사령부 홈페이지. 2024. "U.S. Cyber Command CODE." https://www.cybercom.mil/Our-CODE//(검색일: 2024. 8. 15.).
미국 상무부 홈페이지. 2024. "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles." https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces(검색일: 2024. 8. 6.).
미국 의회 홈페이지. 2024a. "H.R.5005 - Homeland Security Act of 2002." https://www.congress.gov/bill/107th-congress/house-bill/5005/text(검색일: 2024. 11. 5.).
_____. 2024b. "S.2519 - National Cybersecurity Protection Act of 2014." https://www.congress.gov/bill/113th-congress/senate-bill/2519(검색일: 2024. 11. 5.).
_____. 2024c. "S.1353 - Cybersecurity Enhancement Act of 2014." https://www.congress.gov/bill/113th-congress/senate-bill/1353/text(검색일: 2024. 11. 5.).
_____. 2024d. "H.R.2029 - Consolidated Appropriations Act, 2016." https://www.congress.gov/bill/114th-congress/house-bill/2029(검색일: 2024. 11. 5.).
_____. 2024e. "H.R.3359 - An act to amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes." https://www.congress.gov/bill/115th-congress/house-bill/3359/text(검색일: 2024. 11. 5.).
_____. 2024f. "H.R.4998 - Secure and Trusted Communications Networks Act of 2019." https://www.congress.gov/bill/116th-congress/house-bill/4998/text(검색일: 2024. 11. 5.).
_____. 2024g. "H.R.1668 - IoT Cybersecurity Improvement Act of 2020." https://www.congress.gov/bill/116th-congress/house-bill/1668(검색일: 2024. 11. 5.).

_____. 2024h. “H.R.2471 - Consolidated Appropriations Act, 2022.” https://www.congress.gov/bill/117th-congress/house-bill/2471/text(검색일: 2024. 11. 25.).
미국 회계감사국 홈페이지. 2015. “National Protection and Programs Directorate.” https://www.gao.gov/products/gao-16-140t(검색일: 2024. 11. 25.).
호주 외교통상부 홈페이지. 2024. “Australia-Singapore Digital Economy Agreement.” https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement(검색일: 2024. 11. 23.).
Apple 홈페이지. 2024. “iCloud data security overview.” https://support.apple.com/en-us/102651(검색일: 2024. 10. 22.).
CISA. 2022. “Strategic Plan 2023-2025.” https://www.cisa.gov/sites/default/files/2025-01/StrategicPlan%2023-25%20508.pdf(검색일: 2024. 8. 5.).
CISA 홈페이지. 2024a. “About CISA.” https://www.cisa.gov/about(검색일: 2024. 8. 5.).
_____. 2024b. “Divisions & Offices.” https://www.cisa.gov/about/divisions-offices(검색일: 2024. 11. 6.).
_____. 2024c. “Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience.” https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and(검색일: 2024. 11. 25.).
_____. 2024d. “PCISA Marks Important Milestone in Addressing Cyber Incidents; Seeks Input on CIRCIA Notice of Proposed Rulemaking.” https://www.cisa.gov/news-events/news/cisa-marks-important-milestone-addressing-cyber-incidents-seeks-input-circia-notice-proposed(검색일: 2024. 11. 25.).
Congressional Research Service. 2019. “Critical Infrastructure: Emerging Trends and Policy Considerations for Congress.” https://crsreports.congress.gov/product/pdf/R/R45809(검색일: 2024. 11. 6.).
_____. 2023a. “The National Cybersecurity Strategy-Going Where No Strategy Has Gone Before.” https://crsreports.congress.gov/product/pdf/IN/IN12123(검색일: 2024. 11. 1.).
_____. 2023b. “Secure and Trusted Communications Networks Reimbursement

Program: Frequently Asked Questions." https://www.congress.gov/crs-product/IN11663(검색일: 2024. 11. 6.).
ENISA 홈페이지. 2024a. "What is EU Cybersecurity Certification?" https://certification.enisa.europa.eu/index_en(검색일: 2024. 12. 11.).
_____. 2024b. "Developing Certification Schemes." https://certification.enisa.europa.eu/about-eu-certification/developing-certification-schemes_en(검색일: 2024. 12. 11.).
_____. 2024c. "EUCC Certification Scheme." https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en(검색일: 2024. 12. 11.).
EU 집행위원회 홈페이지. 2019. "The Cybersecurity Act strengthens Europe's cybersecurity." https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity(검색일: 2024. 12. 11.).
_____. 2023a. "Proposed Regulation on 'managed security services' amendment." https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-managed-security-services-amendment(검색일: 2024. 11. 7.).
_____. 2023b. "The EU Cybersecurity Act." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act(검색일: 2024. 11. 7.).
_____. 2024a. "Cybersecurity Policies." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies(검색일: 2024. 11. 6.).
_____. 2024b. "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs." https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs(검색일: 2024. 11. 24.).
_____. 2024c. "EU Cyber Resilience Act." https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act(검색일: 2024. 11. 7.).
EUR-Lex 홈페이지. 2021. "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)." https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881(검색일: 2024. 12. 11.).

_____. 2023. “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services.” https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52023PC0208(검색일: 2024. 12. 11.).
_____. 2024a. “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.” https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148(검색일: 2024. 11. 17.).
_____. 2024b. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).” https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1732417248582(검색일: 2024. 11. 17.).
_____. 2024c. “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.” https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52022PC0454(검색일: 2024. 12. 11.).
_____. 2024d. “Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme(EUCC).” https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R0482(검색일: 2024. 12. 11.).
_____. 2025. “Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).” https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng(검색일: 2025. 2. 6.).
Government of the United Kingdom 홈페이지. 2024. “Government Security

Classifications Policy." https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022(검색일: 2024. 10. 23.).
Hart Energy 홈페이지. 2024. "Colonial Pipeline Co." https://www.hartenergy.com/companies/colonial-pipeline-co(검색일: 2024. 12. 9.).
Harvard Law School Forum on Corporate Governance 홈페이지. 2024. "Federal Guidance on the Cybersecurity Information Sharing Act of 2015." https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/(검색일: 2024. 11. 5.).
ITU. 2024. "Global Cybersecurity index 2024." https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf(검색일: 2024. 10. 20.).
ITU 홈페이지. 2024. "Definition of cybersecurity." https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx(검색일: 2024. 7. 23.).
NATO 사이버 방위센터 홈페이지. 2024. "European Union." https://ccdcoe.org/organisations/eu/(검색일: 2024. 11. 6.).
NIST 홈페이지. 2024. "Cybersecurity: Challenges and Opportunities for Small Businesses, Field Hearing." https://www.nist.gov/speech-testimony/cybersecurity-challenges-and-opportunities-small-businesses-field-hearing(검색일: 2024. 11. 4.).
OEWG 홈페이지. 2024. "Open-Ended Working Group on Information and Communication Technologies." https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021(검색일: 2024. 8. 15.).
The White House. 2023. "National Cybersecurity Strategy." https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf(검색일: 2024. 10. 20.).
The White House 홈페이지. 2023a. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/(검색일: 2024. 10. 20.).

_____. 2023b. FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan." https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/(검색일: 2024. 11. 1.).

_____. 2024. "Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan." https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/(검색일: 2024. 11. 1.).

Tikk-Ringas, Eneken. 2012. "Developments in the Field of information and telecommunication in the context of international security: Work of the UN first Committee, 1998~2012." Cyber Policy Process Brief. ICT for Peace Foundation. https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf(검색일: 2024. 10. 15.).

UN 군축연구소 사이버 정책 포털. 2024. https://cyberpolicyportal.org/(검색일: 2024. 10. 20.).

UN 홈페이지. 2024a. "The Role of Science and Technology in the context of International Security and Disarmament." https://disarmament.unoda.org/topics/scienceandtechnology/(검색일: 2024. 10. 15.).

_____. 2024b. "Growth in United Nations membership." https://www.un.org/en/about-us/growth-in-un-membership(검색일: 2024. 11. 17.).

UN 디지털도서관 홈페이지. 2024. "Developments in the field of information and telecommunications in the context of international security: resolution/adopted by the General Assembly." https://digitallibrary.un.org/record/285350?ln=en(검색일: 2024. 10. 15.).

US DOC, Technology Administration, and National Institute of Standards and Technology. 2004. "Standards for Security Categorization of Federal Information and Information Systems." https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf(검색일: 2024. 10. 23.).

USTR. 2017. "National Trade Estimate Report." https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2017/2017-national-trade-estimate(검색일: 2025. 2. 6.).

_____. 2024. "National Trade Estimate Report." https://ustr.gov/sites/de

fault/files/2024%20NTE%20Report_1.pdf(검색일: 2024. 10. 21.).
WEF. 2024. "Global Cybersecurity index 2024." https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf?_gl=1*7vqy09*_up*MQ..&gclid=EAIaIQobChMIv47fjY2ciQMV6Ah7Bx33XirbEAAYASAAEgLmGvD_BwE(검색일: 2024. 10. 20.).
WEF 홈페이지. 2024. "Our Mission." https://www.weforum.org/about/world-economic-forum/(검색일: 2024. 10. 20.).
WTO 홈페이지. 2024. "DS615: United States - Measures on Certain Semiconductor and other Products, and Related Services and Technologies." https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds615_e.htm(검색일: 2024. 11. 21.).

[UN 문서]

United Nations General Assembly. 1990a. "UN Doc. A/45/560. Scientific and Technological Developments and Their Impact on International Security." (October 17). https://documents.un.org/doc/undoc/gen/n90/265/75/pdf/n9026575.pdf(검색일: 2024. 10. 15.).
_____. 1990b. "UN Doc. A/RES/45/60. Resolution Adopted by the General Assembly." https://documents.un.org/doc/resolution/gen/n90/359/03/pdf/n9035903.pdf(검색일: 2024. 10. 15.).
_____. 1998. "UN Doc. A/RES/54/49. Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General." (September 30). https://documents.un.org/doc/undoc/gen/n98/284/58/pdf/n9828458.pdf(검색일: 2024. 10. 15.).
_____. 1999. "UN Doc. A/RES/53/70. Developments in the field of information and telecommunications in the context of international security." (January 4). file:///C:/Users/DB400TDA/Downloads/A_RES_53_70-EN.pdf(검색일: 2024. 8. 15.).
_____. 2010. "UN Doc. A/65/201. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." (July 30). https://documents.un.org/doc/undoc/gen/n10/469/57/pdf/n1046957.pdf(검색일: 2024. 8. 15.).

_____. 2013. "UN Doc. A/68/98. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." (July 24). https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf(검색일: 2024. 8. 15.).
_____. 2015a. "UN Doc. A/70/174. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." (July 22). https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf(검색일: 2024. 8. 15.).
_____. 2015b. "UN Doc. A/69/723. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." (January 13). https://documents.un.org/doc/undoc/gen/n15/014/02/pdf/n1501402.pdf (검색일: 2024. 10. 17.).
_____. 2018. "UN Doc. A/RES/73/27. Developments in the field of information and telecommunications in the context of international security." (January 2). https://documents.un.org/doc/undoc/gen/n18/418/04/pdf/n1841804.pdf(검색일: 2024. 8. 15.).
_____. 2019. "UN Doc. A/RES/74/28. Advancing responsible State behaviour in cyberspace in the context of international security." (December 18). https://documents.un.org/doc/undoc/gen/n19/410/00/pdf/n1941000.pdf(검색일: 2024. 8. 15.).
_____. 2020. "UN Doc. A/RES/75/32. Advancing responsible State behaviour in cyberspace in the context of international security." (December 16). https://documents.un.org/doc/undoc/gen/n20/353/99/pdf/n2035399.pdf(검색일: 2024. 8. 15.).
_____. 2021a. "UN Doc. A/76/135. Developments in the field of information and telecommunications in the context of international security." (July 14). https://documents.un.org/doc/undoc/gen/n21/075/86/pdf/n2107586.pdf(검색일: 2024. 8. 15.).
_____. 2021b. "UN Doc. A/AC.290/2021/CRP.2. Final Substantive Report of the Open-ended working group on developments in the field

of information and telecommunications in the context of international security." (March 10). https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf(검색일: 2024. 8. 15.).

_____. 2021c. "UN Doc. A/75/240. Developments in the field of information and telecommunications in the context of international security." (January 4). https://documents.un.org/doc/undoc/gen/n21/000/25/pdf/n2100025.pdf(검색일: 2024. 8. 15.).

[WTO 판정문]

Appellate Body Report. *Japan - Alcoholic Beverages II*. WT/DS8/AB/R; WT/DS10/AB/R; WT/DS11/AB/R. 4 October 1996.

_____. *EC - Asbestos.* WT/DS135/AB/R. 12 March 2001.

_____. *China - Publications and Audiovisual Products.* WT/DS363/AB/R. 21 December 2009.

_____. *US - Tuna II (Mexico)*. WT/DS381/AB/RW. 20 November 2015.

Panel Report. *US - Gambling*. WT/DS285/R. 10 November 2004.

_____. *US - Tuna II (Mexico)*. WT/DS381/R. 15 September 2011.

_____. *Russia - Traffic in Transit*. WT/DS512/R. 5 April 2019.

_____. *Saudi Arabia - IPRs*. WT/DS567/R. 16 June 2020.

_____. *US - Origin Marking (Hong Kong, China).* WT/DS597/R. 21 December 2022.

_____. *US - Steel and Aluminium Products* (China). WT/DS544/R. 9 December 2022.

[국제투자중재 판정문]

Seda v. Colombia (Monte Glenn Adcock, Stephen John Bobeck, Justin Tate Caruso and others v. Republic of Colombia). ICSID Case No. ARB/19/6. Award dated 27 June 2024.

[ICJ 등 국제재판소 판결문]

Armed Activities on the Territory of the Congo (Democratic Republic

of the Congo v. Uganda), Judgment, ICJ Reports 2005.
Certain Norwegian Loans (France v Norway), Merits, ICJ Reports 1957, Separate Opinion of Judge Sir Hersch Lauterpacht.
Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania). Judgment, ICJ Reports 1949.
Island of Palmas Case (United States v. Netherlands), Permanent Court of Arbitration, Arbitral Award, 2 RIAA 829 (4 April 1928).
Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986.
Pulp Mills on the River Uruguay (Argentina v. Uruguay), Merits, Judgment, ICJ Reports 2010.
Trail Smelter Case (United States of America v. Canada), Reports of International Arbitral Awards, vol. 3 (1941).

[법령 및 규정]

「개인정보 보호법」(시행 2024. 3. 15. 법률 제19234호, 2023. 3. 14., 일부개정).
「경제안보를 위한 공급망 안정화 지원 기본법(약칭: 공급망안정화법)」(시행 2024. 6. 27. 법률 제19828호, 2023. 12. 26., 제정).
「국가사이버안전관리규정」(시행 2013. 9. 2. 대통령훈령 제316호, 2013. 9. 2., 일부개정).
「국가보안법」(시행 2024. 1. 1. 법률 제17646호, 2020. 12. 15., 전부개정) 제4조(직무) 제1항.
「국가사이버안전관리규정」(시행 2005. 1. 31. 대통령훈령 제141호, 2005. 1. 31., 제정).
「국가안보실 직제」 (시행 2015. 4. 3. 대통령령 제26182호, 2015. 4. 3., 일부개정).
「국방 사이버보안 위험관리 지시」(시행 2024. 4. 12. 국방부기타 제15호, 2024. 4. 12., 제정) 제2조(정의).
「사이버안보 업무규정」(시행 2025. 1. 1. 대통령령 제34287호, 2024. 3. 5. 일부개정).
「사이버안보 업무규정」(시행 2024. 3. 5. 대통령령 제34287호, 2024. 3. 5. 일부개정).
「사이버안보 업무규정」(시행 2021. 1. 1. 대통령령 제31356호, 2024. 3. 5., 일부개정)
「산업기술보호지침」(시행 2023. 7. 26. 산업통상자원부고시 제2023-151호, 2023. 7. 26., 폐지제정).
「산업기술의 유출방지 및 보호에 관한 법률(약칭: 산업기술보호법)」(시행 2024. 8. 21. 법률 제20319호, 2024. 2. 20., 타법개정).

인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」(시행 2026. 1. 22. 법률 제20676호, 2025. 1. 21., 제정).
「전자정부법」(시행 2023. 5. 16. 법률 제19030호, 2022. 11. 15., 일부개정).
「정보통신기반 보호법」(시행 2025. 1. 24. 법률 제20068호, 2024. 1. 23., 일부개정).
「정보통신기반 보호법시행령」(시행 2023. 3. 7. 대통령령 제33321호, 2023. 3. 7., 타법개정).
「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」(시행 2024. 8. 14. 법률 제20260호, 2024. 2. 13., 일부개정).
「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(약칭: 정보통신망법 시행령)」(시행 2024. 8. 14. 대통령령 제34821호, 2024. 8. 13., 일부개정).
「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」(시행 2009. 7. 23. 법률 제9637호, 2009. 4. 22., 일부개정).
「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 (약칭: 클라우드컴퓨팅법)」(시행 2023. 1. 12. 법률 제18738호, 2022. 1. 11., 일부개정).
「2001년 미국 애국법(USA PATRIOT Act of 2001. Pub. L. No. 107-56, 115 Stat. 272(2001)」.
「2015년 사이버안보법(Cybersecurity Act of 2015). section 102(Definitions)」.

[협정 및 국제조약]

「국제연합헌장」(발효일 1991. 9. 18. 다자조약, 제1059호, 1991. 9. 24.).
디지털 경제동반자협정(DEPA: Digital Economic Partnership Agreement).
무역에 대한 기술장벽에 관한 협정(TBT: Technical Barriers to Trade).
미국·멕시코·캐나다 협정(USMCA: United States-Mexico-Canada Agreement).
미국·일본 디지털통상협정(USJDTA: United States-Japan Digital Trade Agreement)
미국·콜롬비아 투자증진협정(TPA: Trade Promotion Agreement).
서비스 무역에 관한 일반협정(GATS: General Agreement on Trade in Services).
싱가포르·인도 포괄적 경제협력협정(CECA: Comprehensive Economic Cooperation Agreement).
싱가포르·호주 디지털경제 협정(DEA: Digital Economy Agreement).
싱가포르·호주 FTA(SAFTA: Singapore-Australia Free Trade Agreement).
역내 포괄적 경제 동반자 협정(RCEP: Regional Comprehensive Economic Partnership).
포괄적·점진적 환태평양경제동반자협정(CPTPP: Comprehensive and Progressive

Agreement for Trans-Pacific Partnership).
한·싱가포르 디지털 동반자협정(KSDPA: Korea-Singapore Digital Partnership Agreement).
한·미 FTA.
한·중 FTA.
GATT 협정문 및 외교부 번역본.
2004년 미국 모델 BIT(U.S. Model Bilateral Investment Treaty of 2004).

Executive Summary

Cybersecurity Policies of Major Nations and Implications for South Korea

Jun Hyun Eom and Boram Lee

Cybersecurity can be defined as a state where national and citizen safety is guaranteed by defending against cyber attacks or threats, thereby ensuring proper functioning of cyberspace. Cyberspace is composed of 'information systems' and the 'information' stored within them.

International discussions on cybersecurity norms have continued, showing a standoff between Western liberal democratic countries led by the United States versus Russia and China. The United States and other Western nations recognize cyberspace as a separate domain and argue that international law can be directly applied to it. Non-Western countries like Russia and China contend that cyberspace is not a separate domain, and that domestic laws of the location of systems or information should apply.

The United States adopted an active defense strategy and strengthened collaboration with the private sector, considering that a significant portion of infrastructure is owned or operated privately.

The EU implemented various voluntary certification systems and mandated labeling. Japan's active cyber defense strategy is similar to the United States', and it established a voluntary conformity assessment system for IoT products. South Korea also adopted an offensive cyber defense strategy in 2024. However, unlike major countries, we do not have a unified cybersecurity law.

The potential application of international trade law to cybersecurity measures is as follows. Even when arguing that cybersecurity measures do not apply to like products, such actions will likely be found by the panel as violations of WTO agreements. All WTO precedents addressing national security exceptions relate to wartime or emergency situations in international relations. There is a view that for measures during peacetime to be recognized under national security exceptions, there must be subjective evidence of understanding the purpose at the time of the measure and evidence of indirect supply to military facilities. Panels can assess whether parties have made good faith judgments about measures necessary to protect their essential security interests. A similar conclusion was reached in the international investment arbitration case of Seda v. Colombia.

Implications for South Korea's cybersecurity policy are as follows. First, self-defense cannot be exercised for cyber misuse or cyber attacks that do not reach the level of armed cyber attacks. Second, offensive defense strategies must be pursued cautiously. While there is a view that preemptive self-defense targeting imminent armed attacks is permitted under international customary law, there are controversies regarding specific criteria for determining imminence.

Third, the legal principle of state responsibility for domain management or due diligence in cyberspace can be usefully applied in responding to cyber threats from North South Korea. Fourth, there is a need to establish a unified cybersecurity law.

Implications for South Korea's trade policy are as follows. First, South Korea Government must continuously observe cybersecurity measures introduced by major countries to minimize negative impacts on our export companies. Second, the government should support our companies to gain a competitive advantage regarding cybersecurity labels and certifications when competing with third countries in markets like the United States or EU. Third, when implementing cybersecurity measures, precise institutional design and operation are necessary to avoid conflicting with trade norms. Fourth, even when a country claims national security exceptions in trade agreements, review will be conducted in accordance with the principle of good faith.

〈책임〉

엄준현

고려대학교 국제경제법 석사
대외경제정책연구원 무역통상안보실 신통상전략팀 전문연구원
(現, E-mail: jheom@kiep.go.kr)

저서 및 논문

『클라우드 서비스 해외투자 동향과 국내 규제 분석』(공저, 2022)
『수출규제의 경제적 함의와 글로벌 공급망에 미치는 영향에 관한 연구』(공저, 2023) 외

〈공동〉

이보람

이화여자대학교 중어중문학과, 동아시아연계학과 학사
이화여자대학교 국제대학원 국제통상학 석사
대외경제정책연구원 세계지역연구1센터 일본동아시아팀 전문연구원
(現, E-mail: brlee@kiep.go.kr)

저서 및 논문

『일본의 '사회적 과제 해결형' 4차 산업혁명에 관한 연구』(공저, 2020)
『미·중 갈등시대 일본의 통상 대응 전략』(공저, 2021) 외

KIEP 연구자료 발간자료 목록

■ 2024년

24-01 핵심광물협정의 주요 내용과 정책 시사점 / 오수현

24-02 주요국의 사이버안보 정책과 한국에 대한 시사점 / 엄준현·이보람

24-03 인도적 지원이 개발도상국 경제성장에 미치는 영향 분석: 2015년 네팔 지진을 중심으로 / 정원혁·이예림

24-04 중국 첨단 반도체 혁신 역량 분석 연구: 고대역 메모리 및 3세대 반도체를 중심으로 / 백서인·자오야리

24-05 홍해 위기가 우리 경제에 미친 영향과 물류 회랑 다변화에의 시사점 / 강문수·이지은

24-06 주요 선진국 과학기술 분야 규제 혁신 전략 분석 연구 / 최용찬

■ 2023년

23-01 외국인 직접투자가 베트남의 성별 임금 격차에 미치는 영향과 시사점 / 김제국

23-02 클라우드 서비스 해외투자 동향과 국내 규제 분석 / 이규엽·엄준현

23-03 동지중해 천연가스 개발 현황과 한국의 협력 방안 / 유광호·이지은

23-04 동남아·대양주 유권자들의 보호무역주의 성향 연구와 시사점: 필리핀, 태국, 호주, 뉴질랜드를 중심으로 / 김남석

23-05 WTO 서비스 국내규제 규범의 분석과 시사점 / 김준동·고준성·강준구

23-06 디지털 정책과 규제 변화 분석: Digital Policy Alert 통계를 중심으로 / 김지현

23-07 국내 전략산업 투자유치 인센티브 개편 방향 / 김준동·이성봉·김혁황

23-08 중국 태양광·BESS 산업의 글로벌 시장 독점화와 주요국 대응 / 김주혜

23-09 중국 하이난(海南) 자유무역항의 무역·투자자유화 성과와 시사점 / 김홍원·이한나

23-10 동티모르의 아세안 가입 지원 및 개발협력 확대 방안 / 정재완·이재호

23-11 산업보조금의 글로벌 확산 현황과 시사점 / 금혜윤

23-12 중국 전기차 배터리 기업의 해외 진출 사례 연구 및 시사점 / 최재희

KIEP 설립 이후 현재까지의 모든 발간자료 원문은 홈페이지(http://www.kiep.go.kr)에 수록되어 있습니다.

KIEP 발간자료회원제 안내

■ 본 연구원에서는 본원의 연구성과에 관심 있는 전문가, 기업 및 일반에 보다 개방적이고 효율적으로 연구 내용을 전달하기 위하여 「발간자료회원제」를 실시하고 있습니다.

■ 발간자료회원으로 가입하시면 본 연구원에서 발간하는 모든 보고서를 대폭 할인된 가격으로 신속하게 구입하실 수 있습니다.

■ 회원 종류 및 연회비

회원종류	배포자료	연간회비		
S	외부배포 발간물 일체	기관회원	개인회원	연구자회원*
		30만원	20만원	10만원
A	East Asian Economic Review	8만원		4만원

* 연구자 회원: 교수, 연구원, 학생, 전문가풀 회원

■ 가입방법

홈페이지, 우편, FAX를 이용하여 가입신청서 송부(수시접수)
30147 세종특별자치시 시청대로 370 세종국책연구단지 경제정책동
대외경제정책연구원 연구조정실 학술정보팀
연회비 납부 문의전화: 044) 414-1179 / FAX: 044) 414-1144
E-mail: kieppub@kiep.go.kr

■ 회원특전 및 유효기간

· S기관회원의 특전: 본 연구원 해외사무소(美 KEI) 발간자료 등 제공
· 자료가 출판되는 즉시 우편으로 회원에게 보급됩니다.
· 모든 회원은 회원가입기간에 가격인상과 관계없이 신청하신 종류의 자료를 받아보실 수 있습니다.
· 본 연구원이 주최하는 국제세미나 및 정책토론회에 무료로 참여하실 수 있습니다.
· 연회원기간은 가입일로부터 다음해 가입월까지입니다.

KIEP 발간자료회원제 가입신청서

기관명 (성명)	(한글)	(한문)
	(영문: 약호 포함)	
대표자		
발간물 수령주소	우편번호	
담당자 연락처	전화 FAX	E-mail :
회원소개 (간략히)		
사업자 등록번호	종목	

회원분류 (해당란에 ✓ 표시를 하여 주십시오)

	S 발간물일체	A 계간지
기 관 회 원 □ 개 인 회 원 □ 연 구 자 회 원 □		

* 회원번호 * 갱신통보사항

(* 는 기재하지 마십시오)

특기사항

Policy References 24-02

Cybersecurity Policies of Major Nations and Implications for South Korea

Jun Hyun Eom and Boram Lee

주요국의 사이버안보 조치도 통상협정에 위반될 가능성이 있다. 통상협정의 안보 예외 조항에 '조치국의 안보에 필수적인 조치'인지 판단할 주체로 조치국이 명시되어 있더라도, 주장된 목적과 실제 조치 사이의 관계가 믿을 만한지 신의칙에 따라 심사를 할 수 있다는 것이 통상분쟁 판정례의 일관된 결론이다. 나아가 '당사국이 안보 예외 주장을 제기하면 안보 예외를 적용해야 한다는 각주가 있더라도 마찬가지'라는 판정이 2024년 6월 27일 Seda v. Colombia 사건에서 내려졌다. 한·미 FTA에도 동일한 각주가 있으므로 참고가 될 수 있다.

9 788932 225142 94320

ISBN 978-89-322-2514-2
978-89-322-2064-2(세트)

정가 10,000원

KIEP 대외경제정책연구원
Korea Institute for International Economic Policy

30147 세종특별자치시 시청대로 370 세종국책연구단지 경제정책동
T.044-414-1114 F.044-414-1001 · www.kiep.go.kr