일감법학 | 제60호
2025년 4월 241-268쪽
건국대학교 법학연구소

Ilkam Law Review
Vol.60, Apr., 2025. pp.241-268
The Institute of Legal Studies, Konkuk Univ.

국제연합 사이버범죄협약의 주요 내용과 가입 방안에 관한 고찰

A Study on the Adoption and Accession of the UN Convention on Cybercrime

정 완*
Choung, Wan

목 차

최근 급속한 기술발전과 디지털화의 확산으로 사이버범죄가 폭발적으로 증가하고 있으며, 이는 국경을 초월한 국제문제로 부상하고 있다. 이러한 상황에서 유엔의 사이버범죄협약 채택은 국제사회가 사이버범죄에 공동으로 대응하기 위한 법제도를 마련하는데 중요한 계기가 될 전망이다.

국제연합의 사이버범죄협약 채택은 여러 국가와 이해관계자 간의 복잡한 협상을 통해 이루어졌으며, 각국의 법체계와 문화적 차이를 반영한 조정의 산물이다. 협약은 사이버범죄의 정의와 유형, 국가협력 메커니즘, 법집행과 사법절차의 조화 등을 포함하여, 글로벌차원에서 통일된 법적 대응을 가능케 한다.

협약은 사이버범죄의 범위를 명확히 하고, 사이버공격, 데이터절도, 온라인사기, 디지털 증거수집과 같은 중요문제에 대한 구체적 규정을 두고 있으며, 또한 회원국간 정보공유와 기술지원을 촉진하여 사이버범죄에 대한 보다 효과적인 대응을 가능하게 한다. 이를 통해 각국은 자국의 법적・기술적 역량을 강화할 수 있을 것으로 기대된다.

https://doi.org/10.35148/ilsilr.2025..60.241
투고일: 2025. 3. 16. / 심사완료일: 2025. 4. 15. / 게재확정일: 2025. 4. 16.

* 경희대학교 법학전문대학원 교수
Professor, Kyung Hee University Law School

협약의 채택은 국제사회에 다방면으로 영향을 미치고 있다. 협약은 사이버범죄에 대한 국제대응을 강화함으로써 글로벌안보와 경제안정을 증진시킬 것으로 예상되며, 특히 중소국가나 개발도상국들은 협약을 통해 강력한 사이버보안체계를 구축하는 기회를 갖게 됨으로써 국제사회의 사이버안보 강화에 크게 기여할 것이다. 협약채택 후에도 그 실행과정에서 각국의 법체계와 실행능력 차이로 인해 발생할 수 있는 문제점, 국가주권 침해우려 및 개인정보보호와의 균형유지 등이 주요쟁점으로 부상할 것이므로 이러한 과제를 해결하기 위하여 국제사회의 지속적 협력과 조정이 필요하다.

국제연합 사이버범죄협약은 사이버범죄에 대한 국제적 대응의 중요한 이정표로서, 글로벌안보와 경제안정에 긍정적 영향을 미칠 것으로 평가되며, 협약의 성공적 이행과 지속적 발전을 위해서는 국제사회의 협력과 조정이 필수적이다. 이러한 측면에서 협약의 내용과 의미를 상세히 분석하고 전망함으로써, 향후 사이버범죄 대응전략수립에 기여하고자 한다.

[주제어] 국제연합 사이버범죄협약, 사이버범죄, 사이버보안, 글로벌안보, 국제협약 가입방안

Ⅰ. 서언

193개국이 가입한 세계 최대 국제기구인 국제연합이 사이버범죄방지협약(United Nations Convention against Cybercrime)을 채택하여 2025년 중반부터 회원국의 서명을 받을 준비를 하고 있다. 동 협약작성을 위해 설치한 UN임시위원회가 3년간 작업 끝에 회원국간 협상쟁점 합의를 통해 협약전문을 완성하여 2024년 8월 9일 UN총회에 제출한 이 협약은 2026년 말까지 회원국들의 가입을 위해 개방되며, 40개 회원국이 비준하면 그로부터 90일 후에 발효될 예정이다. 발효된 이후에 가입한 국가는 가입 후 30일이 지나면 발효된다.[1)]

사이버범죄는 기본적으로 국경을 갖지 않은 국제범죄이므로 효율적 범죄단속을 위해서는 국가간 합의 즉, 국제조약체결이 필수지만 각국의 정치적 이해와 법제도가 일치하지 않아 이제까지 조약은 거의 체결되지 못하다가, 유일하게 탄생된 조약이 유럽에서 2001년 채택되고 2004년부터 발효된 '유럽사이버범죄방지협약'(일명 부다

1) 유엔총회(General Assembly)는 2024년 12월 24일 화요일 사이버범죄에 대항하기 위한 국제협력을 강화하고 사회를 디지털위협으로부터 보호하는 것을 목표로 하는 획기적 글로벌조약인 유엔사이버범죄협약을 채택했다. 이 협약은 2025년 중반경 베트남 하노이에서 개최되는 공식행사에서 서명을 위해 개방될 예정이며, 40번째 서명국이 비준한 90일 후에 발효된다. UN News, "UN General Assembly adopts milestone cybercrime treaty", 2024. 12. 24, <https://news.un.org/en/story/2024/12/1158521>, 검색일: 2025. 3. 16. 참조.

페스트협약)이었다. 유럽사이버범죄협약은 유럽 회원국뿐 아니라 비유럽국가도 가입할 수 있도록 개방되어 미국, 일본, 캐나다, 호주 등 비유럽국가도 가입한 상태이며 우리나라도 늦었지만 가입절차가 현재 거의 마무리되고 있는 상황이다. 유럽사이버범죄협약은 유럽중심조약이라 세계적 규범력을 갖지 못한 조약이지만 준세계적 규범력을 가진 국제사이버범죄조약이 처음 탄생된 의미를 가졌다.[2)]

그런데 이번에 유럽지역을 벗어나 유엔총회에서 채택된 UN사이버범죄협약은 유엔회원국이 시민사회, 학계 및 민간부문의 의견을 수렴하여 수년간 노력한 결과 체결이 가능했고 UNODC[3)]가 그 사무국 역할을 했다. 이 협약은 20년만에 체결된 최초의 다자간 범죄방지조약이자 급속도로 증가하는 사이버범죄의 방지를 위해 만들어진 최초의 유엔사이버범죄협약이라는 의미를 가진다.[4)]

UN사이버범죄협약의 내용은 유럽협약과 비슷한 구성을 취하여 실체적 금지규정과 절차적 협력규정으로 나누어볼 수 있고, 협약상 금지된 사이버범죄의 유형으로 제2장 범죄화 챕터에서 불법접속, 불법가로채기(감청), 전자데이터방해, 정보통신기술시스템방해, 장치오용, 정보통신기술시스템관련위조, 정보통신기술시스템관련 도난과 사기, 온라인아동 성적학대 또는 아동 성적착취 자료와 관련된 범죄, 아동성범죄를 저지를 목적으로 하는 권유 또는 미행, 사적 이미지의 동의없는 배포, 범죄수익세탁, 법인책임 등을 규정하고 있다. 이는 해킹, 인터넷사기, 저작권침해, 아동성범죄 등을 규정한 유럽사이버범죄협약과 일견 유사하지만 부분적으로 차이가 있다. 절차협력규정으로는 전자데이터의 신속보존, 실시간 데이터수집, 콘텐츠차단, 전자데이터의 수색과 압수, 증인보호, 피해자지원, 24/7 네트워크, 공동수사, 몰수 등이 규정되

2) 유럽사이버범죄협약에 관한 상세한 내용은 이영준, “유럽의회(Council of Europe)의 사이버범죄방지를 위한 국제협약(案) 소고”, 형사정책연구 제46권, 한국형사법무정책연구원, 2001, 5-30쪽 참조. UN협약과 유럽협약의 비교에 관하여는 Dig Watch, “Comparative analysis: the Budapest Convention vs the UN Convention Against Cybercrime”, 2024. 10. 22, <https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime>, 검색일: 2025. 3. 16; UN협약 초안과 유럽협약의 비교에 관하여는 진우경/권헌영, “UN 사이버범죄협약의 초안과 국내법의 비교에 관한 연구”, 치안정책연구 제37권 제4호, 경찰대학 치안정책연구소, 2023, 117-120쪽 등 참조.

3) 유엔마약범죄사무소(United Nations Office on Drugs and Crime, UNODC)는 약물규제와 마약범죄예방을 목적으로 1997년 설립된 유엔기관이다.

4) 유럽사이버범죄협약 체결에 적극적 역할을 했던 미국, 일본 등과 달리 아무런 역할도 하지 않고 가입조차 소극적이었던 우리나라는 이번에 국제연합이 채택한 사이버범죄조약 성안과정에는 적극 참여하였다는 기사가 있다. 법률신문, “UN사이버범죄방지협약 성안, 이젠 국내법 마련할 차례”, 2024. 8. 14, <https://www.lawtimes.co.kr/opinion/200508>, 검색일: 2025. 3. 16. 기사 참조.

어 있는데 이 역시 유럽협약의 절차규정과 일견 유사하다. 최종협약안이 완성되기 전 조약초안에는 더많은 유형의 사이버범죄가 규정되어 있었으나 후술하는 바와 같이 회원국간 활발한 토론과 논쟁과정에서 많은 규정이 삭제되었다.[5)]

우리나라가 이 협약에 가입하기 위해서는 국내법을 협약의 기준에 맞도록 개정해야 하므로 이 개정작업을 통해 사이버범죄법제도를 보완하고 국제적 대응을 위한 국제공조시스템을 정비하는 기회로 삼아야 할 것이다.[6)]

Ⅱ. 사이버범죄의 정의와 현황

1. 사이버범죄의 정의

사이버범죄란 디지털기기와 네트워크를 이용하여 불법적인 행위를 수행하는 범죄를 의미한다. 이는 전통적 범죄가 디지털환경으로 확장된 형태이기도 하며, 새로운 형태의 범죄행위를 포함하기도 한다.

사이버범죄는 기술적 관점과 법적 관점 및 사회적 관점으로 나누어 정의할 수 있다. 기술적 관점의 사이버범죄는 주로 컴퓨터시스템, 네트워크, 인터넷을 이용하여 수행되는 불법행위를 포괄한다.[7)] 이러한 범죄는 데이터의 불법접속, 변조, 파괴를 포함하며, 컴퓨터바이러스, 웜, 트로이목마 등의 악성소프트웨어를 활용하기도 한다. 법적 관점에서의 사이버범죄는 다양한 국가에서 달리 정의될 수 있지만, 일반적으로

5) 예컨대 협약초안에 규정되었던 개인정보침해, 저작권침해, 사이버스토킹, 자살조장 및 강요, 성착취, 극단주의 관련범죄, 집단살해 관련범죄, 마약 관련범죄, 무기밀매 관련범죄, 사법방해 등 규정이 논의과정에서 삭제되었다.

6) 협약은 가입희망국가에 대해 사이버범죄수사에 필수적인 보관데이터 보전, 트래픽데이터 보전, 제출명령, 트래픽데이터 실시간수집 등 제도를 마련할 것을 요구하고 있다. 법률신문, “UN사이버범죄 방지협약 성안, 이젠 국내법 마련할 차례”, 2024. 8. 14, <https://www.lawtimes.co.kr/opinion/200508>, 검색일: 2025. 3. 16. 참조.

7) 사이버범죄의 통일된 정의나 법적 정의는 없다. 많은 논문 중에 사이버문제행동을 지칭하는 10개의 용어, 즉 사이버(디지털) - 범죄, 성범죄, 인권침해, 폭력, 불링, 언어폭력, 명예훼손, 성폭력, 일탈(행동), 비행의 개념적 정의를 제시하고 특히 사이버폭력과 사이버범죄와 사이버인권침해, 사이버폭력과 사이버불링, 사이버일탈(행동)과 사이버비행의 차이도 아울러 비교한 논문으로 송도언/전성은/강영신, “사이버 문제행동에 관한 문헌 연구 - 개념적 정의를 중심으로 -”, 현대사회과학연구 제25권, 전남대학교 사회과학연구소, 2021, 1-27쪽 참조.

개인정보도용, 금융사기, 온라인괴롭힘, 사이버테러리즘, 지식재산권 침해 등이 포함된다. 법적 정의는 각국의 법체계와 문화적 배경에 따라 차이가 있을 수 있다. 사회적 관점에서의 사이버범죄는 개인이나 집단의 사회적 신뢰를 저해하고 공공의 안전을 위협하는 행위를 포함한다. 예컨대, 사이버스토킹이나 명예훼손은 피해자의 정신적·사회적 안정에 심각한 영향을 미친다.

2. 사이버범죄의 현황

오늘날 디지털기술의 발전과 인터넷사용의 보편화로 인해 사이버범죄는 급격히 증가하고 있다.[8] 세계적으로 인터넷사용자수가 증가하면서 사이버범죄의 표적이 될 가능성도 높아지고 있다. 특히, 팬데믹상황에서 온라인활동이 증가하면서 사이버범죄도 이에 비례하여 증가하였다.

사이버범죄의 유형은 크게 금융범죄와 정보도용 및 사이버테러리즘과 사이버전쟁 등으로 나누어볼 수 있는데, 금융범죄는 피싱, 랜섬웨어, 크립토재킹[9] 등 금융관련 사이버범죄가 가장 흔한 유형이다. 이러한 범죄는 주로 개인의 금융정보를 탈취하거나 시스템을 감염시켜 금전을 요구하는 형태로 나타난다. 정보도용은 개인정보나 기업기밀정보를 불법적으로 획득하는 행위로서 기업과 개인에게 막대한 피해를 준다. 이는 데이터브리치[10] 사건으로 이어질 수 있으며, 피해규모는 수백만 달러에 이를 수 있다. 사이버테러리즘 및 사이버전쟁 즉, 국가주요기반의 해킹과 사이버테러리즘

8) 일반적인 사이버범죄 현황에 대하여는 조기영, "사이버범죄의 현황과 대책", 동북아법연구 제13권 제3호, 전북대학교 동북아법연구소, 2020, 441-466쪽 참조.

9) 최근 급상승한 암호화폐의 인기로 암호화폐 채굴 악성코드인 크립토재킹 위협이 증가하고 있다. 특히 웹기반 크립토재킹은 피해자가 웹사이트에 접속만 해도 피해자의 PC자원을 사용해 암호화폐를 채굴할 수 있으며, 간단히 채굴스크립트만 추가하면 되기 때문에 공격이 쉽고 성능열화와 고장의 원인이 된다. 크립토재킹은 피해자가 피해상황을 인지하기 어렵기 때문에 크립토재킹을 효율적으로 탐지하고 차단할 수 있는 연구가 필요하다. 이에 관하여는 임은지/이은영/이일구, "머신러닝을 활용한 행위 및 스크립트 유사도 기반 크립토재킹 탐지 프레임워크", 정보보호학회논문지 제31권 제6호, 한국정보보호학회, 2021, 1105-1114쪽 참조.

10) 데이터유출을 뜻하는 데이터브리치 사건이 증가하고 있다. 2014년경 미국에서 발생한 사건이 유명한데, 대형 저가유통점인 타깃(Target)의 고객정보가 무더기로 새 나갔고, 타깃과 제휴된 씨티은행 카드와 JP모건 체이스은행 카드도 같이 피해를 봤다. 미국과 캐나다에 1,921개 점포를 갖고 연간 730억 달러 매출을 올리는 타깃 사태의 파괴력은 컸으며, 정보유출 피해자가 1억 1천만 명에 달하였다. 데일리시큐, "美 Target사, 4천만개 신용카드 정보 해킹당해", 2013. 12. 22, <https://www.dailysecu.com/news/articleView.html?idxno=5897>, 검색일: 2025. 3. 16. 참조.

은 국가안보에 중대한 위협을 가한다. 이는 주로 정치적・군사적 목적을 위해 수행되며, 국가간 긴장을 고조시킬 수 있다.

사이버범죄는 국경을 초월하여 발생하기 때문에 국제협력과 대응이 필수적이다. 인터폴, 유로폴 등 국제기구는 정보공유와 협력수사를 통해 사이버범죄에 대응하고 있으며, UN과 같은 국제기구는 사이버범죄방지를 위한 조약(Treaty)[11]과 규범을 제정하고 있다. 또한 인공지능, 사물인터넷(IoT), 블록체인 등 신기술은 새로운 기회를 제공하는 동시에 새로운 사이버위협을 야기하고 있다.[12] 아울러, 사이버범죄는 사회적 신뢰를 저해하고, 경제적 손실을 초래하며, 개인의 사생활과 안전을 위협한다. 이에 대응하기 위해 정부와 민간부문은 사이버보안을 강화하고, 교육과 인식을 높이며 피해자지원프로그램을 운영하고 있다.

사이버범죄는 현대사회에서 점점 더 복잡하고 다차원적 문제로 진화하고 있다. 이에 효과적으로 대응하기 위해서는 법적・기술적・사회적 관점에서의 통합적 접근이 필요하다. 사이버범죄의 정의와 현황을 정확히 이해하는 것은 이러한 통합적 접근을 가능하게 하는 기초가 될 것이다. 각국은 사이버범죄에 대한 법제도를 강화하고 국제협력을 통해 글로벌차원의 해결책을 모색해야 한다.

Ⅲ. 국제연합 사이버범죄협약의 채택과정

유엔회원국들은 2021년 5월부터 사이버범죄대응을 위한 국제조약을 협상해 왔다.[13] 이 조약이 채택되면 사이버문제에 관한 최초의 구속력있는 유엔문서가 되며, 사이버범죄를 예방하고 조사하며 범죄자를 기소하는데 있어 국제협력을 촉진하는 중요한 글로벌 법제도가 될 것이다. 그러나 조약의 범위가 명확하지 않거나 충분한 보호조치

11) UN사이트에 가보면 협약(Convention)을 간혹 조약(Treaty)이라고 부르기도 하므로 굳이 양 표현을 다른 것으로 인식할 필요는 없는 것 같다. UN News, “UN General Assembly adopts milestone cybercrime treaty”, 2024. 12. 24, <https://news.un.org/en/story/2024/12/1158521>, 검색일: 2025. 3. 16. 참조.

12) 예컨대, IoT 장치의 보안취약점은 대규모 봇넷공격에 악용될 수 있으며, AI를 활용한 공격은 점점 더 정교해지고 있다. 인공지능시대의 사이버범죄 현황과 대책에 관하여는 윤지영, “생성형 AI 시대의 사이버범죄와 형사법적 대응”, 법학연구 제34권 제1호, 연세대학교 법학연구원, 2024, 373-399쪽 참조.

13) 2017년부터 러시아 주도로 시작된 사이버범죄협약 논의와 러시아가 작성한 초안에 대한 검토는 박재성, “사이버범죄 국제조약의 동향 - 부다페스트협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로 -”, 저스티스 제185호, 한국법학원, 2021, 266-280쪽 참조.

가 없다면, 인권을 위험에 빠뜨릴 수 있고, 억압적인 정부가 이를 남용하여 온라인상의 자유로운 발언을 범죄화할 위험이 있다. 또한, 인권침해적 조사와 법집행기관의 개인정보 무제한접근을 정당화하여 디지털권리를 위협할 수도 있다.

사이버범죄에 대한 보편적 정의는 없으나 일반적으로 사이버의존범죄(cyber-dependent crime)와 사이버지원범죄(cyber-enabled crime)로 나뉜다. 사이버의존범죄는 정보통신기술(ICT)을 통해 저지를 수 있는 범죄로, 랜섬웨어 사례가 대표적이다. 사이버지원범죄는 전통범죄가 ICT를 통해 변화된 형태로, 온라인뱅킹사기, 신원도용, 아동성착취 등이 포함된다. 이러한 범죄들은 기술발전과 함께 급속도로 진화해 왔다.

지난 20년간 새로운 기술과 위협행위자가 급속도로 증가했고, 이에 대응하기 위한 국가적·국제적 노력도 다양하게 이루어졌다. 사이버범죄 피해자는 개인과 커뮤니티에서부터 기업과 정부까지 다양한 범위에 걸쳐 있으며, 사이버사기, 강탈, 괴롭힘 등 범죄가 증가하고 있다.[14]

2019년 12월 유엔은 범죄목적으로 정보통신기술을 사용하는 것을 막기 위한 포괄적 국제협약개발을 목표로 하는 임시위원회(AHC)를 설립했다. 협상은 2022년초부터 시작되었으며, 협상 로드맵에 따라 비엔나와 뉴욕에서 총 6회의 협상세션이 열렸다. 각 회의에서는 협약의 각 챕터 즉, 범죄화, 절차적 수단, 법집행기관의 역할, 국제협력, 기술지원, 예방조치 및 이행에 관한 여러 부분을 다루었다. 회원국들은 합의를 목표로 협상하였고,[15] 합의에 도달하지 못할 경우 3분의 2 다수결원칙을 적용하였다.

협상과정에서 회원국들은 쟁점을 논의하기 위해 비공식 작업그룹을 구성했다. 2023년 6월 의장은 협약초안을 발표하였고 회원국들은 이를 8월부터 논의했다. 시민사회와 민간부문은 성명, 협의, 부대행사 등을 통해 조약형성에 중요한 역할을 해왔다. 시민사회단체들은 초안이 인권과 기본적 자유를 위협하지 않도록 최소 요구사항을 명시한 긴급공동성명서를 발표했다.

---

14) 예컨대, 로맨스 사기(Romance scam)로 인해 지난 5년간 개인 피해자는 최소 13억 달러의 손실을 보았고, 2022년 코스타리카 정부는 랜섬웨어 공격으로 비상사태를 선포해야 했다. 한국경제, "美 '로맨스 스캠' 1년새 138% 급증…1조7천억원 규모", 2023. 4. 19, <https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=AKR20230419004300009>, 검색일: 2025. 3. 16; 한겨레, "코스타리카, 잇단 랜섬웨어 공격에 비상사태 선포", 2022. 5. 13, <https://www.hani.co.kr/arti/international/international_general/1042757.html>, 검색일: 2025. 3. 16. 등 참조.

15) UN사이버범죄협약에 관한 주요 타임라인에 관하여는 Electronic Frontier Foundation, "UN Cybercrime Draft Treaty Timeline", <https://www.eff.org/deeplinks/2023/04/un-cybercrime-treaty-timeline>, 검색일: 2025. 3. 16. 참조.

조약협상과정에서 몇 가지 우려사항이 제기되었다. 첫째, 사이버범죄로 이해되는 범위를 넘어서는 범죄의 범위가 문제로 지적되었다. 모호하게 작성된 조항은 차별이나 박해로 이어질 수 있는 것으로 해석될 수 있으며, 반대의견을 억누르고 인권옹호자를 범죄자로 만드는데 악용될 수도 있다. 둘째, 법집행기관의 정보공유권한이 과도하게 확대될 위험이 있어 사전에 사법적 승인 및 투명성 조치가 부족한 상황에서 기소 또는 인도로 이어질 수 있다. 셋째, 보안연구자, 고발자, 활동가, 언론인을 위한 보호조치가 미흡하다는 점도 문제로 지적되었다.

2024년 8월 회원국들은 3년간의 협상 끝에 뉴욕에서 사이버범죄에 대항하는 새로운 조약을 채택했다. 협상 마지막날, 이란은 초안의 몇몇 조항에 반대의견을 제기했으나, 3분의 2 다수결에 크게 못 미쳤다. 협약발효를 위해서는 40개국의 서명이 필요하며, 인권언급 등 긍정적 측면이 있지만, 세계적 감시위협이 될 우려가 남아 있다.

협약은 정부에 많은 협력적 집행권한을 부여하지만, 감시와 탄압, 박해에 대한 잠재적 오용을 막기 위해 보다 좁은 범위로 다룰 필요가 있다. 대안적이고 권리를 존중하는 접근방식이 요구되는 상황이며, 협약 시행과정에서 회원국들이 주의를 기울여 지켜볼 필요가 있다.

협약은 2025년 중반 베트남 하노이에서 열리는 서명식에서 서명을 위해 개방되며, 그 후 2026년 12월 31일까지 뉴욕 유엔본부에서 개최되며, 40번째 비준, 수락, 승인 또는 가입이 기탁된 후 발효된다. 유엔형사사법조약에 대한 과거 선례에 따라, 총회의 결정대로 베트남은 새로운 조약에 주목하여 고위공무원이 참석하여 자국을 대신하여 협약에 서명하도록 장려하기 위해 공식서명식을 개최할 예정이며 관련정보가 신속히 제공될 예정이다.[16] 각국은 새로운 조약에 서명한 후, 조약을 비준하기 위한 국내절차를 거쳐 공식적으로 당사국이 되며, 이는 가입, 수락 또는 승인을 통해서도 이루어질 수 있다. 조약발효 후에는 당사국 회의가 주기적으로 소집되어 당사국간 역량과 협력을 통하여 협약목적을 달성하고 이행을 촉진한다.[17]

---

16) 관련 내용은 United Nations, “United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes”, <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>, 검색일: 2025. 3. 16. 참조.

17) 최종 협상쟁점에 대하여는 The Record Recorded Future News, Alexander Martin, “Final negotiations on UN cybercrime treaty underway in New York”, 2023. 8. 23, <https://therecord.media/un-cybercrime-treaty-negotiations-new-york>, 검색일: 2025. 3. 16. 참조.

Ⅳ. 국제연합 사이버범죄협약의 주요 내용

1. 협약상 사이버범죄의 유형

협약[18] 제2장은 '범죄화(Criminalization)'라는 타이틀로 사이버범죄의 여러 가지 유형을 나열하여 당사국[19] 법률에 규정하도록 하고 있다.[20]

의도적으로 정보통신기술시스템의 전체 또는 일부에 대한 권리없이(without right)[21] 접속하는 불법접속(Illegal access),[22] 의도적으로 권리없이 정보통신기술시스템에서 비공개 전자데이터 전송을 기술적 수단으로 가로채는 불법가로채기(Illegal interception),[23] 의도적으로 권리없이 저질러진 전자데이터의 손상, 삭제, 악화, 변경 또는 억제 등 전자데이터 방해(Interference with electronic data), 의도적으로 권리없이 저질러진 전자데이터의 입력, 전송, 손상, 삭제, 악화, 변경 또는 억제를 통해 정보통신기술시스템의 기능을 심각하게 방해하는 정보통신기술시스템 방해(Interference with an information and communications technology system), 이상의 범죄를 목적으로 설계 또는 개조된 프로그램을 포함한 장치 또는 정보통신기술시스템에 접근할 수 있는 비밀번호, 액세스증명, 전자서명 또는 유사한 데이터를 취득, 생산, 판매, 사용을 위한 조달, 수입, 배포 기타 방식으로 제공하는 장치오용(Misuse of devices), 의도적으로 권리없이 전자데이터를 입력, 변경, 삭제 또는 억제하여 가짜데이터를 생성하고, 합법적 목적상 진짜인 것처럼 간주되거나 조치되도록 의도하는 정보통신기술시스템관련 위조(Information and communications technology system-related forgery), 의도적으로 권리없이 전자데이터의 입력, 변경, 삭제 또는 억제, 정보통신기술시스템의 작동에

18) 이하에서 서술하는 협약의 내용은 "Resolution adopted by the General Assembly on 24 December 2024"의 내용 중 Annex로 첨부된 협약 최종원문을 직접 번역하여 정리한 것이다. 협약을 번역하여 정리함에 있어서 영어원문이 중복수식어가 많고 반복되는 용어가 많아 매우 어색하다는 판단하에 반복과 중복을 줄이고 의역을 하였다.

19) 협약에 가입한 회원국을 지칭하여 이하에서 당사국이라고 표현한다.

20) Chapter II Criminalization.

21) 우리 법률은 '권한없이'라고 표현하는데, 협약은 '권리없이(without right)'라는 표현을 사용한다.

22) 불법접속(Illegal access)을 불법접근으로 번역한 글이 많은데 네트워크를 통해 정보시스템에 접속한다는 표현이 맞지 접근한다는 표현은 어색한 것 같아 불법접속으로 번역하였다.

23) 불법가로채기(Illegal interception)를 불법감청으로 번역한 글이 많은데, 음성정보의 경우 적합한 용어지만 그 외의 정보에 대하여는 감청이라는 용어보다 가로채기가 더 넓은 의미를 담은 용어로 보여 어색하지만 가로채기라는 용어를 사용한다.

대한 간섭, 정보통신기술시스템을 통해 사실적 상황에 대한 사기로 사람이 하지 않을 일을 하거나 하지 않게 하여 자신 또는 타인을 위해 권리없이 금전 기타 재산의 이득을 얻으려는 사기적 또는 부정직한 의도로 타인에게 재산손실을 초래하는 정보통신기술시스템 관련 도난 또는 사기(Information and communications technology system-related theft or fraud), 의도적으로 권리없이 정보통신기술시스템을 통해 아동성학대 또는 아동성착취 자료를 제작, 제공, 판매, 배포, 전송, 방송, 전시, 출판 기타 방법으로 제공하거나, 정보통신기술시스템을 통해 아동성학대 또는 아동성착취 자료를 권유, 조달 또는 접근하거나, 정보통신기술시스템 또는 다른 저장매체에 저장된 아동성학대 또는 아동성착취 자료를 소지 또는 통제하거나, 당사국이 별도의 범죄로 규정할 수 있는 위의 범죄에 자금을 지원하는 온라인 아동성학대 또는 아동성착취 자료와 관련된 범죄(Offences related to online child sexual abuse or child sexual exploitation material),[24] 정보통신기술시스템을 통해 아동에 대한 성범죄를 저지를 목적으로 의도적으로 의사소통, 유혹, 길들임 기타 합의를 하는 아동에 대한 성범죄를 목적으로 하는 유혹 또는 길들임(Solicitation or grooming for the purpose of committing a sexual offence against a child), 의도적으로 권리없이 이미지에 묘사된 사람의 동의없이 정보통신기술시스템을 통해 사람의 사적 이미지를 판매, 배포, 전송, 게시 기타 방법으로 제공하는 사적 이미지[25]의 동의없는 배포(Non-consensual dissemination of intimate images), 범죄수익이라는 사실을 알면서 재산을 불법적 출처를 은폐하거나 위장하거나 범죄실행에 연루된 사람을 돕기 위해 재산을 전환하거나 이전하거나 또는 해당 사람의 행위의 법적 결과를 회피하기 위해 범죄실행에 연루된 사람을 돕거나, 범죄수익이라는 사실을 알면서 재산의 진정한 본질, 출처, 위치, 처분, 이동 또는 소유권이나 권리에 대한 은폐 또는 위장의 범죄수익세탁(Laundering of proceeds of crime) 등이다.

---

24) “아동성학대 또는 아동성착취 자료”에는 (a) 실제 또는 시뮬레이션된 성적 활동에 참여하거나, (b) 성적 활동에 참여하는 사람이 있거나, (c) 성적 부위가 주로 성적 목적으로 표시되거나 또는 (d) 고문 또는 잔혹하고 비인도적이거나 품위훼손적 대우 또는 처벌을 받는 경우로 본질적으로 성적인 자료로서 18세 미만의 사람을 묘사, 설명 또는 표현하는 시각적 자료가 포함되며, 서면 또는 오디오 콘텐츠가 포함될 수 있다. 협약 제14조 제2항 참조.

25) “사적 이미지”는 18세 이상의 사람을 사진이나 비디오 녹화를 포함한 모든 수단으로 촬영한 성적 영상녹화물을 의미하며, 그 사람의 성적 부위가 노출되거나 그 사람이 성행위에 참여하고 있으며, 녹화 당시에는 비공개였으며, 묘사된 사람이 범죄 당시 합리적 사생활보호 기대를 유지한 것을 의미한다. 협약 제16조 제2항 참조.

2. 관할권(Jurisdiction)

제3장은 관할권에 관하여 규정하고 있다.[26] 당사국은 범죄가 그 영토 내에서 발생하거나 또는 당사국 국기를 게양한 선박이나 등록된 항공기에서 발생한 경우는 협약상 범죄관할권을 확립하기 위하여 필요한 조치를 한다. 협약에 따라 당사국은 범죄가 그 국민에 대해 발생되거나 또는 그 영토에 상시거주하는 국민이나 무국적자가 행하거나 또는 협약상 규정된 범죄이고 이 범죄를 자국 영토 내에서 행하기 위해 영토 밖에서 행해지거나 당사국에 대해 행해진 경우 등에도 당해 범죄에 대한 관할권을 가질 수 있다.

협약 목적상, 당사국은 피의자가 자국영토에 있고 그가 자국국민이라는 이유로 인도하지 않을 경우 협약상 범죄에 대한 관할권을 갖기 위해 필요한 조치를 하여야 한다. 당사국은 또한 피의자가 자국영토에 있고 해당 범죄인을 인도하지 않을 경우도 범죄 관할권을 갖기 위해 필요한 조치를 할 수 있다.

관할권을 행사하는 당사국이 상대 당사국이 동일한 행위에 대해 수사, 기소 또는 사법절차를 진행하고 있다는 사실을 통보받거나 다른 방법으로 알게 된 경우, 당사국 유관당국은 적절히 협의하여 조치를 조정한다. 협약은 일반 국제법규범을 침해하지 않고 당사국이 국내법에 따라 부여된 형사관할권 행사를 배제하지 않는다.

3. 절차규정(Procedural measures and law enforcement)

협약 제4장은 '절차수단과 법집행'에 관하여 규정하고 있다.[27] 당사국은 협약상 권한과 절차를 특정범죄 수사 또는 소송목적으로 수립하는데 필요한 입법 조치를 하여야 한다. 협약에 달리 규정한 경우를 제외하고, 당사국은 협약상 권한과 절차를 협약상 범죄, 정보통신기술시스템을 통해 저지른 기타 범죄의 전자증거수집 등에 적용해야 한다. 당사국은 협약상 조치를 유보가능한 범죄에만 적용 권리를 유보할 수 있다. 다만 당해 범죄의 범위가 협약상 조치를 적용하는 범죄보다 제한되지 않아야 한다.

당사국은 협약상 권한과 절차의 수립, 이행 및 적용이 국내법에 규정된 조건과 보호조치의 적용을 받도록 보장해야 하며, 국내법은 국제인권법상 의무에 따라 인권을 보호하고 비례원칙을 적용해야 한다. 당사국 국내법에 따라, 이 조건과 보호조치에는 해당

26) Chapter III Jurisdiction.

27) Chapter IV Procedural measures and law enforcement.

절차나 권한의 성격을 고려하여 적절한 경우, 특히 사법적 검토, 효과적 구제책에 대한 권리, 적용을 정당화하는 근거, 해당 권한이나 절차의 범위와 기간의 제한 등이 포함된다.

저장된 전자데이터의 신속한 보존에 관하여, 당사국은 유관당국이 정보통신기술시스템을 통해 저장된 트래픽데이터, 콘텐츠데이터 및 가입자정보를 포함한 특정 전자데이터의 신속한 보존을 명령하거나 이와 유사하게 획득할 수 있도록 필요한 입법조치를 하여야 한다. 이는 특히 전자데이터가 손실 또는 수정 가능성이 특히 높다고 믿을만한 근거가 있는 경우에 해당한다.

당사국이 저장된 전자데이터를 보존하라는 명령을 받은 사람이 해당 전자데이터의 무결성을 최대 90일까지 보존하고 유지하도록 의무화하는데 필요한 입법조치를 하여 유관당국이 공개를 요청할 수 있도록 해야 한다. 당사국은 그 명령이 이후에 갱신되도록 규정할 수 있다. 당사국은 전자데이터를 보존해야 하는 보관자 등이 해당 절차수행을 국내법에 규정된 기간동안 비밀로 유지하도록 의무화하는데 필요한 입법조치를 해야 한다.

통신데이터의 신속한 보존 및 일부공개에 관하여, 당사국은 협약상 보존해야 할 통신데이터에 관하여 통신전송에 서비스제공자가 관여했는지 여부에 관계없이 통신데이터의 신속한 보존이 가능하도록 보장하며, 당사국 유관당국 또는 당국이 지정한 사람에게 충분한 양의 통신데이터를 신속히 공개하여 당사국이 서비스제공자와 통신 또는 표시된 정보가 전송된 경로를 식별할 수 있도록 보장하기 위해 필요한 입법조치를 하여야 한다.

당사국은 유관당국이 자국영토 내 개인이 정보통신기술시스템이나 전자데이터 저장매체에 저장된 해당 개인이 소유 또는 관리하는 특정 전자데이터를 제출할 수 있도록 하고, 당사국 영토 내에서 서비스를 제공하는 서비스제공자가 소유 또는 관리하는 해당서비스 관련 가입자정보를 제출할 수 있도록 명령하는 권한을 부여하기 위해 필요한 입법조치를 하여야 한다.[28]

당사국은 유관당국이 특정 정보통신기술시스템 또는 그 일부를 검색하거나 유사하게 접근하여 검색하는 전자데이터가 해당 영토 내 다른 정보통신기술시스템 또는 그 일부에 저장되어 있다고 믿을만한 근거가 있고 해당 데이터가 시스템에 합법적으로 접근가능하거나 사용가능한 경우 해당 당국이 신속하게 처리할 수 있도록 필요한

28) 아울러, 당사국은 유관당국이 정보통신기술시스템, 그 일부와 그 안에 저장된 전자데이터 및 전자데이터 저장매체 등을 수색하거나 유사하게 접속할 수 있는 권한을 부여하기 위해 필요한 입법 조치를 하여야 한다. 협약 제25조 참조.

입법 조치를 하여야 한다.

당사국은 기술적 수단을 적용하여 당사국 영토 내에서 수집 또는 기록하고 기존 기술역량 내에서 서비스제공자에게 당사국 영토 내에서 기술적 수단을 적용하여 수집 또는 기록하거나 또는 당사국 영토 내에서 정보통신기술시스템을 통해 전송된 특정통신과 관련된 트래픽데이터를 실시간 수집 또는 기록하는데 유관당국과 협력하고 지원하도록 강제할 수 있는 입법조치를 하여야 한다.

당사국이 국내법상 조치할 수 없는 경우, 해당 영토 내에서 기술적 수단을 적용하여 전송된 특정통신과 관련된 트래픽데이터를 실시간 수집 또는 기록하는데 필요한 입법 조치를 할 수 있다. 당사국은 서비스제공자가 권한의 실행과 관련된 정보를 비밀로 유지하도록 의무화하는 입법 조치를 하여야 한다.

당사국은 국내법상 심각한 범죄와 관련하여 필요한 입법조치를 하여 당사국의 유관당국에 당사국 영토 내에서 기술적 수단을 적용하여 수집 또는 기록하고, 서비스제공자가 기존 기술역량 내에서 당사국 영토 내에서 기술적 수단을 적용하여 수집 또는 기록하고, 유관당국과 협력하여 정보통신기술시스템을 통해 전송된 당사국 영토 내에서 지정된 통신의 콘텐츠데이터를 실시간 수집 또는 기록하도록 강제한다.

당사국은 협약상 범죄에서 발생한 범죄수익 또는 그 가치가 해당 수익가치에 해당하는 재산 및 협약상 범죄에 사용되거나 사용될 예정인 재산, 장비 또는 기타 도구 등 몰수를 국내법상 가능하게 하는데 필요한 조치를 한다. 당사국은 다른 국가에서 피고인의 이전 유죄판결을 고려하는데 필요한 입법조치를 할 수 있으며, 적절한 조건하에 그 목적을 위해 협약상 범죄와 관련된 형사소송에서 해당정보를 사용할 목적으로 필요한 조치를 할 수 있다. 당사국은 국내법에 따라 증언하거나 선의로 합리적 근거에 따라 협약상 범죄에 관한 정보를 제공하거나, 그밖에 수사 또는 사법당국에 협력하는 증인에 대해 잠재적 보복 또는 협박으로부터 효과적으로 보호하기 위한 적절한 조치를 해야 하며, 필요한 경우 그들의 친척 및 그들과 가까운 사람들에 대해서도 적절한 조치를 하여야 한다.[29]

당사국은 협약상 범죄의 피해자에게 지원과 보호를 제공하기 위해 자국 내에서

29) 이 조치는 피고인의 권리와 적법절차를 침해하지 않고, 그들의 신체적 보호를 위한 절차수립, 예컨대 필요하고 실행가능한 범위에서 그들을 이전하고 적절히 그들의 신원과 소재에 대한 정보의 비공개 또는 공개제한을 허용하며 비디오링크 기타 적절한 통신기술을 사용하여 증언을 허용하는 것과 같이 증인의 안전을 보장하는 방식으로 증언을 허용하기 위한 증거규칙을 제공하는 것을 포함한다. 협약 제33조 참조.

적절한 조치를 해야 하며, 특히 보복위협이나 협박의 경우에 그러하다. 당사국은 국내법에 따라 협약상 범죄의 피해자에게 보상과 배상에 대한 접근을 제공하기 위한 적절한 절차를 수립해야 한다. 당사국은 국내법에 따라 피해자의 의견과 우려가 피고인의 권리를 침해하지 않도록 가해자에 대한 형사소송단계에서 제시되고 고려될 수 있도록 해야 한다. 이러한 범죄의 피해자를 위한 지원, 특히 신체적·심리적 회복을 위해 관련 국제기구, 비정부기구 및 시민사회와 협력한다. 이상의 규정을 적용함에 있어 당사국은 아동을 포함한 피해자의 연령, 성별 및 특정상황과 필요를 고려해야 하며, 당사국은 국내법과 일치하는 범위에서 협약상 내용을 제거하거나 접근불가능하게 하는 요청을 준수하도록 보장하기 위한 효과적 조치를 하여야 한다.

4. 국제협력(International Cooperation)

협약 제5장은 국제협력에 관하여 규정하고 있다.[30] 국제협력원칙상 당사국은 협약 및 형사사건 관련 국제협력에 관한 국제기구 및 국내법에 따라 협약에 명시된 범죄의 수사와 기소, 그리고 해당범죄로 인한 수익의 동결, 압수, 몰수 및 반환, 협약에 규정된 범죄의 전자증거 수집, 획득, 보존 및 공유, 중대한 범죄에 대한 전자증거 수집, 획득, 보존 및 공유 등을 포함한 사법절차에 협력해야 한다.

개인데이터를 이전하는 당사국은 국내법과 국제법에 따라 이를 수행하며, 개인데이터보호에 관한 법률을 준수하여 데이터를 제공할 수 없는 경우 개인데이터를 이전할 필요가 없다. 개인데이터 전송이 협약에 위배될 경우 당사국은 적절한 조건을 붙여 요청에 답할 수 있으며, 당사국은 개인데이터 전송을 위한 양자간 또는 다자간 협정을 체결하도록 권장된다. 전송된 개인데이터는 수신된 당사국 법률하에서 적절히 보호되어야 한다. 당사국은 협약에 따라 취득한 개인데이터를 제3국이나 국제기구로 전송하기 위하여 원래 전송한 당사국의 승인을 서면으로 받아야 한다.

범죄인인도 요청대상자가 그 영토에 있는 경우, 협약상 범죄에 적용되며 인도요청 범죄는 요청당사국과 피요청당사국 모두의 국내법에 따라 처벌가능해야 한다. 인도가능한 범죄에 부과된 징역 기타 구금의 최종형을 집행하기 위하여 인도가 요청되는 경우, 국내법에 따라 인도를 허가할 수 있으며, 협약에 규정된 범죄 중 자국 국내법으로 처벌할 수 없는 범죄에 대하여 인도를 허가할 수 있다.

30) Chapter V International cooperation.

당사국은 협약상 범죄에 관한 특정범죄 수사, 기소 또는 사법절차 목적 또는 협약상 범죄와 관련하여 전자증거를 수집, 획득 및 보존하기 위해 24/7 네트워크, 즉 하루 24시간 주7일 이용가능한 연락처를 지정한다. 유엔사무총장은 이 연락처를 통보받고 지정된 연락처의 최신등록부를 보관하며 매년 당사국에 최신연락처목록을 배포한다. 이 지원에는 기술적 조언제공, 저장된 전자데이터보존, 증거수집 및 정보제공, 용의자 위치파악, 또는 비상상황을 피하기 위한 전자데이터제공 등 조치를 용이하게 하거나 피요청당사국 국내법 및 관행이 허용하는 경우 직접수행이 포함된다. 당사국은 24/7 네트워크 운영을 위해 훈련된 인력이 사용가능하도록 해야 한다.[31)]

당사국은 다른 당사국에 협약상 당사국 영토 내에 위치한 정보통신기술시스템을 통해 저장된 전자데이터의 신속보존을 명령하거나 다른 방법으로 획득하도록 요청할 수 있으며, 요청당사국은 전자데이터의 수색 또는 유사한 접근, 압수 또는 유사한 확보 또는 공개에 대한 상호 법적 지원요청을 제출할 수 있다. 요청당사국은 협약에 규정된 24/7 네트워크를 사용하여 정보통신기술시스템을 통해 저장된 전자데이터의 위치와 관련된 정보 및 적절한 경우 서비스제공자의 위치에 대한 정보를 구할 수 있다.

협약상 특정통신에 관한 통신데이터(Traffic Data)를 보존하라는 요청을 실행하는 과정에서 요청당사국이 다른 당사국의 서비스제공자가 통신전송에 관여했음을 발견한 경우, 요청당사국은 해당 서비스제공자와 통신이 전송된 경로를 식별하는데 충분한 양의 통신데이터를 요청당사국에 신속히 공개해야 한다.

당사국은 다른 당사국에게 요청당사국 영토 내에 있는 정보통신기술시스템을 통해 저장된 전자데이터를 수색하거나 유사하게 접근하고, 압수하거나 유사하게 보호하고, 공개하도록 요청할 수 있다. 이에는 협약상 보존된 전자데이터가 포함된다. 요청당사국은 협약상 관련 국제문서와 법률을 적용하여 요청에 응답한다. 요청은 관련데이터가 특히 손실 또는 변경되기 쉽다고 믿을만한 근거가 있는 경우 또는 문서와 법률이 신속한 협력을 규정하는 경우 신속히 응답해야 한다.

당사국은 협약상 범죄를 퇴치하기 위한 법집행조치의 효과성을 강화하기 위해 국내법과 행정체계에 따라 긴밀히 협력해야 한다. 당사국은 국제형사경찰기구를 포함한 기존채널을 고려하여 자국의 유관당국, 기관 및 서비스간 의사소통채널을 강화하

31) 당사국은 국내법의 범위에서 기존 공인연락처 네트워크를 사용하고 강화할 수 있다. 이에는 국제형사경찰기구의 컴퓨터관련범죄에 대한 24/7 네트워크가 포함되며, 이를 통해 신속한 경찰간 협력 등 정보교환을 제공한다. 협약 제41조 참조.

고 필요한 경우 확립하여 협약상 범죄의 모든 측면에 관한 정보의 안전하고 신속한 교환을 위한 효과적 조치를 하여야 한다. 협약상 범죄에 연루된 것으로 의심되는 사람의 신원, 소재 및 활동 기타 관련자의 위치, 범죄실행으로 얻은 범죄수익 또는 재산의 이동, 범죄실행에 사용되거나 사용될 의도가 있는 재산, 장비 기타 도구의 이동 등을 조사하는데 다른 당사국과 협력해야 한다.

당사국은 협약상 범죄와 관련하여 범죄 수사, 기소 또는 사법절차의 대상이 되는 양자간 또는 다자간 협정과 약정의 체결을 고려해야 한다. 유관당국은 공동수사기관을 설립할 수 있다. 이러한 협정이나 약정이 없는 경우, 공동수사는 사례별로 합의하여 수행될 수 있다. 당사국은 해당 조사가 수행될 영토의 당사국 주권이 충분히 존중되도록 보장해야 한다.

당사국은 협약상 범죄실행을 통해 취득되거나 관련재산에 대해 협약상 법적 지원을 제공하기 위해 국내법에 따라 자국의 유관당국이 다른 당사국 법원이 발행한 몰수명령을 시행할 수 있도록 필요한 조치를 하고, 관할권이 있는 경우 유관당국이 자금세탁범죄 또는 자국관할권 내 범죄에 대한 재판을 통해 또는 자국 국내법상 허가된 절차를 통해 외국에서 발생한 재산의 몰수를 명령할 수 있는 조치를 하며, 유죄판결 없이도 해당재산을 몰수할 수 있도록 필요한 조치를 하는 것을 고려해야 한다. 이는 가해자가 사망, 도주 또는 부재로 기소될 수 없는 경우 등 적절한 경우에 해당한다.[32]

Ⅴ. 국내법의 개정 방안

1. 협약규정과 국내법규정의 비교

협약가입을 위해서는 구체적으로 협약의 실체적 규정과 절차적 규정을 면밀히 분석하여 국내법과 충돌하거나 국내법상 흠결이 있는지 살펴봐야 한다.

협약의 실체적 규정으로는 전술한 바와 같이 협약에서 사이버범죄로 규제하려는 모든 유형에 대해 국내법에서도 사이버범죄로 규제되는지 비교분석할 필요가 있다.

32) 협약상 당사국이 몰수한 범죄수익 또는 재산은 당사국이 국내법과 행정절차에 따라 처분한다. 협약상 다른 당사국 요청에 따라 조치할 때, 당사국은 국내법이 허용하는 범위에서 요청이 있는 경우, 몰수된 범죄수익 또는 재산을 요청당사국에 반환하는 것을 우선 고려하여 범죄 피해자에게 보상을 제공하거나 범죄수익 또는 재산을 이전의 합법적 소유자에게 반환할 수 있도록 한다. 협약 제52조 참조.

조약 제2장에서 사이버범죄로 규제되는 유형을 나열하면, 불법접속, 불법가로채기, 전자데이터 방해, 정보통신기술시스템 방해, 장치오용, 정보통신기술시스템관련 위조, 정보통신기술시스템관련 도난 또는 사기, 온라인 아동성학대 또는 아동성착취 자료와 관련된 범죄, 아동에 대한 성범죄목적의 유혹 또는 길들임, 사적 이미지의 동의없는 배포, 범죄수익세탁 등이다. 이들 사이버범죄 목록을 국내법에서 분류하듯이 정보통신망침해범죄, 정보통신망이용범죄, 온라인불법콘텐츠로 묶어서 살펴보면 불법접속, 불법가로채기, 전자데이터 방해, 정보통신기술시스템 방해, 장치오용 등은 정보통신망침해범죄[33]에 해당하고, 정보통신기술시스템관련 위조, 정보통신기술시스템관련 도난 또는 사기, 온라인 아동성학대 또는 아동성착취 자료와 관련된 범죄, 아동에 대한 성범죄목적의 유혹 또는 길들임 등은 정보통신망이용범죄[34]에 해당하며, 사적 이미지의 동의없는 배포는 온라인불법콘텐츠범죄[35]에 속할 것이다.

협약에 열거된 사이버범죄의 유형은 각 유형마다 매우 구체적 설명이 수식어로 붙어 있는데 이 점은 우리나라 법제상 사이버범죄 유형에 상세한 수식어 설명이 붙어 있지 않은 것과 크게 대비된다. 예컨대, 정보통신망법 제48조는 정보통신망 침해행위 등의 금지라는 타이틀로 금지되는 사이버범죄를 규정하고 있는데, 그 규정을 보면 다음과 같다.

> 제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
> ② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.
> ③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.
> ④ 누구든지 정당한 사유 없이 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하거나 이를 전달·유포하여서는 아니 된다.

이 조항을 보면 "정당한 접근권한 없이 또는 허용된 접근권한을 넘어"라는 두 가지

33) 이에 관한 논문으로 전응준/신동환, "정보통신망 침입행위 관련 연구 - 정보통신망법 제48조 제1항을 중심으로 -", 문화미디어엔터테인먼트법 제14권 제1호, 중앙대학교 법학연구원 문화·미디어·엔터테인먼트법연구소, 2020, 151-182쪽 참조.

34) 이에 관한 논문으로 김한균, "사이버성범죄·디지털성범죄 실태와 형사정책", 이화젠더법학 제9권 제3호, 이화여자대학교 젠더법학연구소, 2017, 27-57쪽 참조.

35) 이에 관한 논문으로 홍남희, "'좋아요'로 공유되는 범죄영상 - 소셜플랫폼을 통한 불법·유해콘텐츠 유통실태와 쟁점", 언론중재 제145호, 언론중재위원회, 2017, 20-31쪽; 김예정/송봉규, "성인사이트에서 디지털 성범죄 실태와 대책", 한국범죄심리연구 제18권 제2호, 한국범죄심리학회, 2022, 21-36쪽 등 참조.

요건을 수식어로 붙여 정보통신망 침입금지를 규정하였고 악성프로그램의 경우도 “정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손, 멸실, 변경, 위조하거나 그 운용을 방해할 수 있는”이라는 수식어를 붙여 그러한 악성프로그램을 전달 또는 유포해서는 안 된다고 규정하고 있다. 이 부분과 관련된 사이버범죄협약의 규정을 보면 다음과 같다.

> 의도적으로 정보통신기술시스템의 전체 또는 일부에 대한 권리없이 접속하는 불법접속(Illegal access), 의도적으로 권리없이 정보통신기술시스템에서 비공개 전자데이터 전송을 기술적 수단으로 가로채는 불법가로채기(Illegal interception), 의도적으로 권리없이 저질러진 전자데이터의 손상, 삭제, 악화, 변경 또는 억제 등 전자데이터 방해(Interference with electronic data), 의도적으로 그리고 권리없이 저질러진 전자데이터의 입력, 전송, 손상, 삭제, 악화, 변경 또는 억제를 통해 정보통신기술시스템의 기능을 심각하게 방해하는 정보통신기술시스템 방해(Interference with an information and communications technology system), 이상의 범죄를 목적으로 설계 또는 개조된 프로그램을 포함한 장치 또는 정보통신기술시스템에 접근할 수 있는 비밀번호, 액세스증명, 전자서명 또는 유사한 데이터를 취득, 생산, 판매, 사용을 위한 조달, 수입, 배포 기타 방식으로 제공하는 장치의 오용(Misuse of devices).

몇 개밖에 안 되는 수식어를 갖고 있는 우리 법률규정과 비교할 때 상세하고 다양한 침해유형을 열거하고 있는 사이버범죄협약의 규정은 절대로 동일한 규정이라고는 볼 수 없을 만큼 차이가 크다. 우선 ‘의도적으로(intentionally)’라는 수식어가 없는 우리 법률은 고의이든 과실이든 모두 규제대상일 수 있는 반면, 협약은 ‘의도적으로’라는 수식어로 고의범죄만을 단속대상으로 함을 명백히 밝히고 있다. 또한 우리 법률은 ‘정당한 사유없이’라는 수식어를 가지고 있는데 반해, 협약에는 이런 수식어는 붙이고 있지 않다. 정당한 사유라는 것은 수사관이나 법관에 의해 얼마든지 자의적인 해석이 가능한 수식어이기 때문에 죄형법정주의를 기초로 하는 형사법 규정상 바람직하지 않은 표현임에도 불구하고 우리나라 법제도하에서는 형사법 출범 초기부터 상당히 애용되어 온 관용적 표현이기도 하다. 협약에서는 이러한 수식어는 사용하지 않고 그 대신 매우 구체적인 범죄행위 유형을 나열하고 있다. 우리는 “정당한 권한없이 또는 허용된 접근권한을 넘어”라고 표현하고 있는데 정당한 권한의 개념도 불확실하고 허용된 접근권한도 사실은 애매한 표현이다. 협약은 이러한 표현을 사용하지 않고 구체적 행위유형을 나열하되 예컨대 ‘권한없이’라는 말 대신 ‘권리없이’라는 표현을 쓰고 ‘정보통신망에 침입’하는 것이 아니라 ‘정보통신기술시스템에 접속하는’ 행위를 금지하고 있고, 또한 “정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손・멸실・변경・위조하거나 그 운용을 방해할 수 있는”이라는 표현이 아니라 “전자데이터의 전송을 기술적 수단으로 가로채는”이라던가 “의도적으로 권리

없이 행해진 전자데이터의 손상, 삭제, 악화, 변경 또는 억제 등 전자데이터의 방해" 또는 "의도적으로 권리없이 행해진 전자데이터의 입력, 전송, 손상, 삭제, 악화, 변경 또는 억제를 통해 정보통신기술시스템의 기능을 심각하게 방해하는"이라고 표현하여 보다 구체적인 수식어로 설명하였고 또한 "이상의 범죄를 목적으로 설계나 개조된 프로그램을 포함한 장치 또는 정보통신기술시스템에 접근할 수 있는 비밀번호, 액세스증명, 전자서명 또는 유사한 데이터를 취득, 생산, 판매, 사용을 위한 조달, 수입, 배포 기타 방식으로 제공하는" 행위 등을 정보통신망침해행위, 즉 사이버범죄로 규정하고 있는 것이다.

또한 사이버사기와 관련한 규정으로 협약규정과 국내법규정을 비교하면 다음과 같다. 먼저 협약규정을 다시 보면, 아래와 같다.

> 의도적으로 권리없이 전자데이터를 입력, 변경, 삭제 또는 억제하여 가짜데이터를 생성하고, 합법적 목적상 진짜인 것처럼 간주되거나 조치되도록 의도하는 정보통신기술시스템관련 위조(Information and communications technology system-related forgery), 의도적으로 권리없이 전자데이터의 입력, 변경, 삭제 또는 억제, 정보통신기술시스템의 작동에 대한 간섭, 정보통신기술시스템을 통해 사실적 상황에 대한 사기로 사람이 하지 않을 일을 하거나 하지 않게 하여 자신 또는 타인을 위해 권리없이 금전 기타 재산의 이득을 얻으려는 사기적 또는 부정직한 의도로 타인에게 재산손실을 초래하는 정보통신기술시스템관련 도난 또는 사기(Information and communications technology system-related theft or fraud).

여기서 정보통신기술시스템관련 위조는 통계위조 등 뿐 아니라 가짜뉴스를 포함하는 광범위한 내용으로 보이는데, 우리 법률에는 허위의 데이터에 관한 범죄유형은 규정되어 있지 않고 다만 타인에게 손해를 야기하기 위한 허위의 통신규정은 존재한다.

> 전기통신기본법 제47조(벌칙) ① 삭제
> ② 자기 또는 타인에게 이익을 주거나 타인에게 손해를 가할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 3년이하의 징역 또는 3천만원이하의 벌금에 처한다.
> ③ 제2항의 경우에 그 허위의 통신이 전신환에 관한 것인 때에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
> ④ 전기통신업무에 종사하는 사람이 제3항의 행위를 한 때에는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하고, 제2항의 행위를 한 때에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

일반적인 내용으로 공익을 해하는 허위의 통신에 대한 범죄규정이 제1항에 있었으나 위헌결정으로 삭제되었고, 다만 자기 또는 타인에게 이익을 주거나 타인에게 손해를 가할 목적으로 하는 허위의 통신만을 범죄로 규정하고 있다. 아울러 허위의 내용이 전신환에 관한 것이거나 전기통신업무에 종사하는 사람의 행위인 경우를 추가로 규

정하고 있다. 허위통신의 내용이 매우 특화되어 있는 것이다. 그러나 협약의 경우 “의도적으로 권리없이 전자데이터를 입력, 변경, 삭제 또는 억제하여 가짜데이터를 생성하고, 합법적 목적상 진짜인 것처럼 간주되거나 조치되도록 의도하는 정보통신기술시스템 관련 위조”라고 표현하고 있어 위헌의 소지를 제거한 매우 구체적인 범죄유형을 규정하고 있다. 또한 사이버절도와 사이버사기를 규정한 협약의 내용은 “정보통신기술시스템을 통해 사실적 상황에 대한 사기로 사람이 하지 않을 일을 하거나 하지 않게 하여 자신 또는 타인을 위해 권리없이 금전 기타 재산의 이득을 얻으려는 사기적 또는 부정직한 의도로 타인에게 재산손실을 초래하는 정보통신기술시스템 관련 절도 또는 사기”라고 상세히 규정하고 있는데 우리 법률은 사이버절도에 관하여는 규정을 두고 있지 않으며, 사이버사기 규정도 별도로 입법하지 않고 일반 형법상 사기죄 규정을 적용하고 있어 죄형법정주의를 위반한다는 지적을 받기도 한다. 형법은 사기죄에 관하여 아래와 같이 규정하고 있어 협약의 구성요건과 서술방식이 상당히 다름을 알 수 있다.

제347조(사기) ① 사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
② 전항의 방법으로 제삼자로 하여금 재물의 교부를 받게 하거나 재산상의 이익을 취득하게 한 때에도 전항의 형과 같다.

이밖에 청소년성보호에 관한 규정 및 사이버음란물 규정도 협약과 우리 법률규정과 구성요건이 상당히 다르다. 협약의 규정을 먼저 살펴보면 다음과 같다.

정보통신기술시스템을 통해 아동에 대한 성범죄를 저지를 목적으로 의도적으로 의사소통, 유혹, 길들임 기타 합의를 하는 아동에 대한 성범죄를 목적으로 하는 유혹 또는 길들임, 의도적으로 권리없이 이미지에 묘사된 사람의 동의없이 정보통신기술시스템을 통해 사람의 사적 이미지를 판매, 배포, 전송, 게시 기타 방법으로 제공하는 사적 이미지의 동의없는 배포

이에 반하여 우리 법률의 규정은 다음과 같다.

아동청소년성보호법
제15조(알선영업행위 등) ① 다음 각호의 어느 하나에 해당하는 자는 7년 이상의 유기징역에 처한다.
2. 아동·청소년의 성을 사는 행위를 알선하거나 정보통신망에서 알선정보를 제공하는 행위를 업으로 하는 자
제15조의2(아동·청소년에 대한 성착취 목적 대화 등) ① 19세 이상의 사람이 성적 착취를 목적으로 정보통신망을

> 통하여 아동·청소년에게 다음 각 호의 어느 하나에 해당하는 행위를 한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
> 1. 성적 욕망이나 수치심 또는 혐오감을 유발할 수 있는 대화를 지속적 또는 반복적으로 하거나 그러한 대화에 지속적 또는 반복적으로 참여시키는 행위
> 2. 제2조 제4호 각 목의 어느 하나에 해당하는 행위를 하도록 유인·권유하는 행위
> ② 19세 이상의 사람이 정보통신망을 통하여 16세 미만인 아동·청소년에게 제1항 각 호의 어느 하나에 해당하는 행위를 한 경우 제1항과 동일한 형으로 처벌한다.

아동의 성보호에 관하여 협약은 "정보통신기술시스템을 통해 아동에 대한 성범죄를 저지를 목적으로 의도적으로 의사소통, 유혹, 길들임 기타 합의를 하는 아동에 대한 성범죄를 목적으로 하는 유혹 또는 길들임(grooming)"으로 요건을 서술한 반면에, 우리 법규정은 "성적 욕망이나 수치심 또는 혐오감을 유발할 수 있는 대화를 지속적 또는 반복적으로 하거나 그러한 대화에 지속적 또는 반복적으로 참여시키는 행위"라고 규정하고 있는데, 협약은 의사소통, 유혹, 길들임 등이라고 구체적 유형을 서술하고 있지만, 우리 규정은 성적 욕망이나 수치심 또는 혐오감을 유발할 수 있는 대화라고 표현하고 있어 매우 애매한 상황이다. 성적 욕망, 수치심, 혐오감이 누구의 것인지 실제 재판에서는 가해자와 피해자를 기준으로 판단하지 않고 뜬금없이 제3자의 생각을 기준으로 판정하는 경우도 있는 상황이다.

아무튼, 이상에서 살펴본 바와 같이, 죄형법정주의[36]라는 형사법원칙의 규정상 구체성을 따져볼 때 국내법 규정은 협약의 규정과 비교할 때 매우 간단하고 허술하기까지 하다는 느낌을 가질 수밖에 없는 상황이고,[37] 협약에서 금지하는 행위유형과 비교할 때 그 구체적 행위가 우리나라 법규정에도 해당되는 행위인지 확실히 구별하기가 쉽지 않을 것으로 전망된다. 우리나라 법률규정을 협약규정과 합치될 수 있도록 전문가태스크포스를 구성하여 면밀한 검토분석이 필요한 이유이다. 사이버범죄규정의 취지는 어떻든 협약이나 우리 법규정이나 거의 같은 것이므로 같은 내용의 행위금지라며 법해석을 통해 해결할 수 있다는 의견도 있는데, 죄형법정주의를 대원칙으로 하는 형사법규정이니만큼 보다 면밀한 합치성 여부를 검토하여 만반의 가입준비를

36) 형사법상 죄형법정주의에 관하여는 허일태, "죄형법정주의의 연혁과 그 사상적 배경에 관한 연구", 법학논고 제35호, 경북대학교 법학연구원, 2011, 115-148쪽; 이경재, "영미형법상 죄형법정주의", 법학연구 제21권 제3호, 충북대학교 법학연구소, 2010, 159-180쪽 등 참조.

37) 필자는 사이버범죄 처벌에 관하여 사이버사기, 사이버모욕, 사이버도박 등 3자의 경우 처벌규정 없이 형법규정을 그대로 적용하는 부분에 대해 죄형법정주의 위반이므로 규정신설이 필요함을 여러 차례 지적한 바 있다. 정완, "사이버범죄의 주요 쟁점과 대응책에 관한 소고", 홍익법학 제17권 제3호, 홍익대학교 법학연구소, 2016, 365-392쪽 참조.

해야 할 것으로 사료된다. 검토가 필요한 협약의 규정과 국내법 규정은 사이버범죄의 실체적 규정뿐 아니라 절차규정과 국제협력 규정 등 다수의 규정이 존재하는바 여기서 모든 규정을 상세히 검토하기는 어려우므로 추후의 법개정 작업반에서 빠짐없이 검토하기를 기대한다.

2. 합리적 개정작업으로서의 사이버형법전 입법 제안

전술한 바와 같이 협약규정에 맞도록 국내법의 사이버범죄규정들을 일일이 찾아서 개정하는 작업이 필요한만큼 쉬운 작업이라고는 할 수 없다. 그 이유는 기본적으로 사이버범죄협약은 단일규정인데 우리 사이버범죄규정들은 이 법, 저 법에 산발적으로 흩어져 있기 때문이다. 이러한 차원에서 국내 사이버범죄관련 법률도 통합하여 '사이버형법'으로 단일법전화하면 어떨까 제안하고자 한다. 사이버범죄통합법률 제정의 필요성에 관해서는 이미 여러 차례 제안한 바 있고[38] 필자 이외에도 이런 제안을 하는 학자들이 더 있다.[39] 이에 사이버범죄협약 가입을 위해 관련 법규정을 개정하는 차원에서 사이버범죄기본법의 입법필요성을 함께 강조하고자 한다.

기본적으로 기본적인 사이버범죄유형을 규정하고 있는 정보통신망법만 해도 정보통신망침입, 사이버공격, 악성프로그램, 사이버명예훼손규정, 사이버음란물규정, 사이버스토킹 규정 등이 여기저기 흩어져 규정되어 있어 잘 찾아봐야 하고, 그 밖의 많은 사이버범죄규정은 성폭력처벌법상 통신매체이용음란행위와 몰래카메라촬영 및 허위영상물반포 등, 청소년성보호법상 아동·청소년의 성을 사는 행위를 알선하는 정보를 정보통신망에 제공하거나, 성년자의 아동청소년에 대한 성착취목적의 대화 등, 정보통신기반보호법상 주요정보통신기반시설 침해행위 등, 주민등록법상 허위의 주민등록번호를 만들거나 사용하는 행위 등, 형법상 사이버모욕과 사이버도박 및 사이버사기와 컴퓨터사용사기 등, 저작권법상 인터넷송신 등 저작권침해행위, 전기통신기본법상 타인에게 손해를 발생하기 위한 허위통신, 전기통신사업법상 전기통신의 타인사용, 전자금융거래법상 다른 가맹점명으로 전자화폐거래를 하는 행위 등, 국민체육진흥법상 프로그램이용 입장권 부정판매, 정보통신망발행 투표권 등을 이용

38) 디지털타임스, "사이버범죄 통합법 제정 필요하다", 2017. 11. 27, <https://www.dt.co.kr/contents.html?article_no=2017112802102251607001>, 검색일: 2025. 3. 16. 참조.

39) 단일법으로 '사이버범죄처벌법'을 제정하자는 의견은 강석구/이원상, 사이버범죄 관련 법령정비 방안(연구총서 13-B-02), 한국형사정책연구원, 2014, 180쪽 참조.

한 도박행위 등 무수히 많다. 현재로서는 이들 관련 규정을 일일이 다 검토하여 사이버범죄협약 규정과의 합치성을 따져봐야 하는 작업이 필요불가결한 상황이다.

요컨대 이러한 다양한 수많은 사이버범죄규정들을 한데 모아 예컨대 '사이버범죄기본법'으로 단일화하여 각 사이버범죄규정을 면밀히 검토하여 개정작업을 병행하면 좋을 것으로 사료된다.[40] 특히 단일화할 법령의 이름과 관련하여 필자는 이를 '사이버형법'으로 명명하면 이상적이지 않을까 생각한다. 일반범죄에 관한 형법전이 있고 사이버범죄에 관한 사이버형법이 있다면 형법전의 균형이 맞을 것이기 때문이다.

VI. 결어

이상에서 국제연합 사이버범죄협약의 채택과 가입에 대한 분석을 통해 사이버범죄의 정의와 현황, 협약의 채택과정과 협상쟁점, 유럽협약과의 비교, 조약가입의 법적 및 정치적 영향을 다루고 이를 통해 국제사회가 직면한 사이버범죄의 복잡성과 이에 대응하기 위한 국제협력의 필요성을 강조하였다. 아울러 우리나라가 조약가입을 위한 법개정작업을 함에 있어서 어려운 부분을 살펴보고 해결점을 제시하였다.

사이버범죄는 국가의 경계를 넘어 발생하며 그 피해가 세계적으로 확대되고 있다. 이러한 범죄는 단순한 개인의 문제가 아니라 국가안보와도 직결된다는 점에서 국제사회의 공조가 필수적이다. 본문에서 서술한 바와 같이, UN 사이버범죄협약은 이러한 공조의 틀을 제공하며, 국제사회가 통일된 대응전략을 마련하는데 매우 중요한 역할을 하고 있다. 조약의 채택과정과 협상쟁점은 국제정치의 복잡성을 드러낸다. 각국은 자국의 주권과 안전을 보호하기 위해 조약의 조항에 대해 다양한 입장을 취하고 있어 협상의 주요쟁점이 되고 있다. 특히 법적 표준의 조화와 데이터보호, 개인정보 처리에 대한 논의는 여전히 지속되고 있는 주요과제다.

국제연합 사이버범죄협약은 사이버범죄에 대한 국제적 대응을 위한 중요한 초석을 마련하고 있다. 그러나 협약의 실질적 효과를 극대화하기 위해서는 각국의 적극적 참여와 협력이 필수적이다. 또한 빠르게 변화하는 기술환경에 발맞춰 협약내용을

40) 단일법으로 '사이버범죄기본법'을 제정하자는 의견의 모델은 '유럽사이버범죄협약'이다. 이 협약에는 사이버범죄에 관한 실체법규정뿐 아니라 절차법규정, 국제공조 등 사이버범죄의 주요 내용이 모두 규정되어 있으므로 우리나라도 이런 메커니즘을 채택하여 사이버범죄관련 규정이 통합운용될 필요가 있다고 한다. 강석구/이원상, 위의 책, 182-186쪽 참조.

지속적으로 검토하고 개정할 필요가 있다. 향후에도 지속적으로 협약의 효과성을 평가하고, 사이버범죄에 대한 혁신적 대응방안을 모색해야 할 것이다. 이 논문은 UN 사이버범죄협약의 중요성과 그 적용에 따른 과제를 조명함으로써 국제사회가 직면한 사이버보안문제해결에 기여하려는 목적에서 작성하였다. 이 노력이 결실을 맺기 위해서는 법적・기술적・정책적 측면의 통합적 접근과 지속적 국제협력이 요구되는바, 이를 통해 보다 안전하고 신뢰할 수 있는 사이버환경을 구축하는데 기여할 수 있을 것이다.

참고문헌

1. 단행본

강석구/이원상, 사이버범죄 관련 법령정비 방안(연구총서 13-B-02), 한국형사정책연구원, 2014.

2. 학술지

김예정/송봉규, “성인사이트에서 디지털 성범죄 실태와 대책”, 한국범죄심리연구 제18권 제2호, 한국범죄심리학회, 2022, 21-36쪽.

김한균, “사이버성범죄・디지털성범죄 실태와 형사정책”, 이화젠더법학 제9권 제3호, 이화여자대학교 젠더법학연구소, 2017, 27-57쪽.

박재성, “사이버범죄 국제조약의 동향-부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로-”, 저스티스 제185호, 한국법학원, 2021, 246-284쪽.

송도언/전성은/강영신, “사이버 문제행동에 관한 문헌 연구-개념적 정의를 중심으로-”, 현대사회과학연구 제25권, 전남대학교 사회과학연구소, 2021, 1-27쪽.

윤지영, “생성형 AI 시대의 사이버범죄와 형사법적 대응”, 법학연구 제34권 제1호, 연세대학교 법학연구원, 2024, 373-399쪽.

이경재, “영미형법상 죄형법정주의”, 법학연구 제21권 제3호, 충북대학교 법학연구소, 2010, 159-180쪽.

이영준, “유럽의회(Council of Europe)의 사이버범죄방지를 위한 국제협약(案) 소고”, 형사정책연구 제46권, 한국형사법무정책연구원, 2001, 5-30쪽.

전응준/신동환, “정보통신망 침입행위 관련 연구 - 정보통신망법 제48조 제1항을 중심으로 -”, 문화미디어엔터테인먼트법 제14권 제1호, 중앙대학교 법학연구원 문화・미디어・엔터테인먼트법연구소, 2020, 149-182쪽.

정 완, “사이버범죄의 주요 쟁점과 대응책에 관한 소고”, 홍익법학 제17권 제3호, 홍익대학교 법학연구소, 2016, 365-392쪽.

조기영, “사이버범죄의 현황과 대책”, 동북아법연구 제13권 제3호, 전북대학교 동북아법연구소, 2020, 441-466쪽.

진우경/권헌영, “UN 사이버범죄협약의 초안과 국내법의 비교에 관한 연구”, 치안정책연구 제37권 제4호, 경찰대학 치안정책연구소, 2023, 99-136쪽.

허일태, “죄형법정주의의 연혁과 그 사상적 배경에 관한 연구”, 법학논고 제35호, 경북대학교 법학연구원, 2011, 115-148쪽.

홍남희, “‘좋아요’로 공유되는 범죄영상-소셜플랫폼을 통한 불법・유해콘텐츠 유통 실태와 쟁점”, 언론중재 제145호, 언론중재위원회, 2017, 20-31쪽.

3. 신문기사

법률신문, “UN사이버범죄방지협약 성안, 이젠 국내법 마련할 차례”, 2024. 8. 14, <https://www.lawtimes.co.kr/opinion/200508>, 검색일: 2025. 3. 16.

Digwatch, “Comparative analysis: the Budapest Convention vs the UN Convention Against Cybercrime”, 2024. 10. 22, <https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime>, 검색일: 2025. 3. 16.

The Record Recorded Future News, Alexander Martin, “Final negotiations on UN cybercrime treaty underway in New York”, 2023. 8. 23, <https://therecord.media/un-cybercrime-treaty-negotiations-new-york>, 검색일: 2025. 3. 16.

UN News, “UN General Assembly adopts milestone cybercrime treaty”, 2024. 12. 24, <https://news.un.org/en/story/2024/12/1158521>, 검색일: 2025. 3. 16.

[Abstract]

A Study on the Adoption and Accession of the UN Convention on Cybercrime

Choung, Wan*

The recent adoption of the UN-led Convention on Cybercrime is playing an important role in establishing a legal framework for the international community to jointly respond to cybercrime.

First, the adoption of the UN Convention on Cybercrime was achieved through complex negotiations among several countries. The convention includes the definition of cybercrime, cooperation mechanisms between countries, and harmonization of law enforcement and judicial procedures, which enables a unified response at the global level.

The convention clarifies the scope of cybercrime and provides specific provisions on key issues such as cyberattacks, data theft, online fraud, and digital evidence collection. In addition, the convention promotes information sharing and technical support among member states, enabling more effective responses to cybercrime. Through this, each country is expected to be able to strengthen its own legal and technical capabilities.

The UN Convention on Cybercrime will continue to develop and evolve in line with the changing technological environment. To this end, the Convention should evolve to adapt to new types of cyber threats, including regular review and update mechanisms. In addition, cooperation between international organizations and the private sector should be strengthened for the successful implementation of the Convention.

In short, the UN Convention on Cybercrime is an important milestone in the international response to cybercrime and is expected to have a positive impact on global security and economic stability. However, cooperation and coordination of the international community are essential for the successful implementation and continuous development of the

* Professor, Kyung Hee University Law School

Convention. This paper aims to contribute to the establishment of future cybercrime response strategies by deeply analyzing the meaning and prospects of the Convention in this regard.

[Key Words] UN Convention on Cybercrime, International Cooperation, Cybersecurity, Cybercrime, Global Security, Law Amendment Plan