

국외출장보고서

UNODC 제4차 『사이버범죄 전문가회의』 참가

2018년 4월 2일 ~ 4월 7일

오스트리아, 비엔나

국제전략협력실

I. 출장개요

· 출장자

- 전현욱 국제홍보팀장

· 출장일시

- 2018. 4. 2(월) ~ 2018. 4. 7.(토), (4박 6일)

· 출장지

- 비엔나(Vienna), 오스트리아

· 출장목적

- UNODC 『제4차 사이버범죄 전문가 회의』 참가

· 출장일정

날짜	지역	시간	내용	비고
2일 (월)	서울 - 비엔나	12:50	12:50 서울 출발 17:10 비엔나 도착	
2일 (화)	비엔나	10:00 ~ 13:00	제4차 사이버범죄 전문가회의 참석 - 의제1 2018~2021년 계획안 채택 (a) 개회 (b) 의제 채택 (c) 2018~2021년 계획안 채택 - 의제2 입법과 프레임워크	
		15:00 ~ 18:00	- 의제2 입법과 프레임워크(계속)	
3일 (수)	비엔나	10:00 ~ 13:00	- 의제2 입법과 프레임워크(계속)	
		15:00 ~ 18:00	- 의제2 입법과 프레임워크(계속) - 의제3 사이버범죄 실체법	

4일 (목)	비엔나	10:00 ~ 13:00	- 의제3 사이버범죄 실체법(계속)	
		15:00 ~ 18:00	- 의제4 그 외 사항(Other Matters) - 의제5 보고서 채택	
5일 (금)	비엔나 - 서울	18:40	5일(금) 18:40 비엔나 출발 6일(토) 11:50 서울 도착	익일 도착

II. 출장내용

1. 회의 개최 배경

(1) UNODC는 UN총회 결의 65/230(2010, 12. 21.)에 근거하여 2011년 제1차 사이버범죄 전문가회의를 개최하고 연구 방법론을 확정하여 각국의 사이버범죄 및 대응 현황을 연구하기로 하였으며, 2013년 제2차 회의를 통하여 연구결과의 초안(draft)을 검토하고 이를 발표하고자 하였음.

(2) 그러나 제2차 회의에서는 유럽평의회 『사이버범죄 방지 협약』(일명 부다페스트 협약)을 UN 차원에서 국제 규범화하는 것에 관하여 러시아, 중국 등 일부 회원국의 반발이 있었으며, 이로 인해 연구결과 초안을 승인하는데 합의하지 못함.

(3) 이후 2017년 4월 그간의 상황변화를 반영하기 위하여 제3차 회의를 개최하여 각국의 입장을 다시 조율하였으며, 같은 해 5월 제26차 CCPCJ 연례회의에서는 추후 『사이버범죄 전문가회의』를 정기적으로 개최하여 사이버범죄 대응에 관한 논의를 촉진하고 연구결과의 핵심주제인 ▲입법과 프레임워크, ▲사이버범죄 실체법, ▲법집행과 수사, ▲전자증거와 형사사법, ▲국제협력, ▲범죄예방 등을 체계적으로 검토할 것을 권고함(결의 26/4).

(4) UNDOC는 CCPCJ 결의 26/4에 의거 2018년부터 2021년까지의 사이버범죄 전문가회의에 관한 계획을 확정하였으며, 2018년 4월 개최되는 제4차 회의에서는 상기주제 중 ▲입법과 프레임워크, ▲사이버범죄 실체법에 관하여 논의하기로 함. 이는 UNODC가 『사이버범죄 방지 협약』 관련 문제를 포함하여 장기적 관점에서 사이버범죄 관련 국제공조 강화방안을 새롭게 모색하기 시작하였음을 의미함.

(5) 이와 관련하여 대한민국 정부는 유럽평의회 『사이버범죄 방지 협약』과 관련하여 국가간 이견을 조율하고 이를 국제규범화 하기 위하여 이미 『2013년 제3차 세계사이버스페이스총회』를 개최하는 등 다양한 노력을 기울였으나, 공식적으로는 여러 가지 사정을 고려하여 중립의 입장을 유지해 왔음. 그러나 최근의 상황변화 등을 이유로 대한민국 정부는 이 협약에 가입하는 것을 적극적으로 검토하고 있으며, 중국 등의 입장에도 다소 변화가 있는 것으로 알려짐.

(6) 한국형사정책연구원은 2013년 제2차 회의에 참석한 바 있으며 금번 제4차 회의에도 초청받음(초청장은 <붙임 1>참조). 우리나라의 유럽평의회 『사이버범죄 방지 협약』 가입 시 필요한 이행입법을 위한 법제정비 등, 예상되는 관련 형사정책 연구수요에 선제적으로 대응하기 위하여 UNODC 제4차 사이버범죄 전문가 회의에 참석함.

2. 회의 개요

- 일시: 2018년 4월 3일 ~ 5일 10:00 ~ 18:00
- 장소: Boardroom D, 4th Floor, Building C, Vienna International Centre
- 참석: 91개 UN 회원국, 3개 국제기구, 학술 및 민간영역 9개 기구 등
(<붙임 2> 참조)



3. 회의 내용¹⁾

회의는 전문가 그룹 부회장이자 제4차 회의의 의장직을 맡은 Andre Rypl (브라질)에 의해 진행됨. 의제1 ‘2018~2021년 계획안 채택’ 회의가 시작되자마자 별다른 의견 없이 통과되었으며, 바로 의제2 ‘입법과 프레임워크’로 넘어감. 부다페스트 협약에 관한 견해 대립으로 인하여 논의가 길어질 것을 예상한 의장이 회의 전반에 걸쳐 신속하게 회의를 진행하려 노력함.

가. 의제2: 입법과 프레임워크

2018년 4월 3-4일 개최된 2,3,4차 회의에서 의제2 “입법 및 프레임워크”를 검토하였음. 우선 첫날 회의에서 Lu Chuanying(중국), George Maria Tyendezwa(나이지리아), Cristina Schulman(루마니아), Pedro Verdelho(포르투갈), Claudio Peguero(도미니카 공화국), Maria Alejandra Daglio(아르헨티나), Mohamed Mghari(모로코)가 전문가 패널로서 입법과 프레임워크와 관련하여 프리젠테이션을 함.²⁾

-
- 1) 부다페스트 협약에 관한 국가 대표단 간 의견 충돌로 인하여 국외출장보고서 제출일 현재(2018.5.3.)까지 논의내용 및 권고사항에 관하여 UNODC 공식 보고서가 확정되지 않았으며, 따라서 이 국외출장보고서는 출장자의 메모와 기억, 회의 말미에 배부된 부분적인 회의록 초안을 토대로 작성되었음. 따라서 이 보고서에 포함된 본 회의의 논의내용 및 권고사항의 내용은 UNODC 공식 보고서와 다소 차이가 있을 수 있음.
 - 2) 각 패널의 발표문은 UNODC 홈페이지(<http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html>, 2018.5.3. 최종방문) 참조.

패널의 발표 이후 각국 대표단들이 발표에 대하여 토론하는 형식으로 회의가 진행되었으며, 각국 대표단들은 발언기회를 얻어 주로 사이버범죄 대응에 관한 자국의 입법 및 정책 동향을 언급하였음. 이들은 성공적인 국내입법 이행지원 및 수사, 기소, 재판, 국제협력에 있어서의 국가역량 마련에 있어서 역량강화 및 기술지원 프로그램의 핵심적 역할과 강조함. 아울러 민간사회 및 민간영역을 포괄하는 학제적 접근법의 중요성도 강조함.

특히 유럽 및 미국 등 부다페스트 협약을 지지하는 국가의 대표단³⁾들은 기존의 부다페스트 협약 및 유엔 초국가적 조직범죄 방지 협약이 사이버범죄에 대한 국내 및 국제 협력 및 대응 마련에 충분하기 때문에 사이버범죄에 관한 추가적인 범세계적, 포괄적 법적 도구는 필요하지 않다는 의견을 제시하였음. 이러한 맥락에서 부다페스트 조약은 유럽 위원회 비회원국을 포함한 당사국에게 효과적인 법적 및 운영 프레임워크를 제공하며 비당사국에게는 국제협력 증진과 관련 형법 및 형사소송법 조항의 조화에 있어서 참고가 된다는 점이 강조되었음. 부다페스트 조약의 이행에 있어서 사이버범죄 조약 위원회(T-CY) 및 유럽위원회의 역량강화 프로젝트인 GLACY의 유용성이 언급되었음. 이 외에도 OAS 및 ECOWAS의 기술지원에 관한 프로젝트도 언급됨. 이와 관련하여 몇몇 발표자는 기본적으로는 부다페스트 협약을 지지하는 듯한 발언을 하면서도 사이버범죄 도구 마련에 있어서 기본 인권의 보호를 위한 적절한 조건과 세이프가드를 포함할 것을 권고하기도 함.

중국 및 러시아 등 이를 지지하지 않는 국가의 대표단들은 유엔 프레임워크 내 사이버범죄에 관한 새로운 법적 도구의 필요성을 강조하였음. 일부 발표자는 부다페스트 협약을 지역 차원의 법적 도구로 인식해야 한다고 주장함. 특히 이들은 협약 가입의 비공개적 속성을 언급하면서, 이는 협약 가입이 초청된 국가를 대상으로 한정되어 있으며 당사국의 승인이 필요하다는

3) 마지막 회의에서 공식 회의록에 기존의 부다페스트 협약을 지지하는 발언을 한 국가들을 수식하는 단어를 “many”로 할 것인지 “some”으로 할 것인지 반대의견을 표명한 국가들을 수식하는 단어를 “other”로 하는 것이 적절한지 등에 관하여 유럽 및 미국 등 부다페스트 협약을 지지하는 국가의 대표단과 중국 및 러시아 등 이를 지지하지 않는 국가의 대표단 간에 1시간 이상의 반복적인 토론이 진행되었으며, 논의가 정리되지 않자 의장이 직권으로 “many”와 “other”를 사용하기로 결정하였음.

점을 문제로 지적함. 또한 일부 발표자는 해당 협약의 제32 (b)항은 국제법상 주권 존중의 원칙 상 받아들이기 힘들다고 주장함.

사이버범죄가 더욱 더 초국가적 속성을 띠고 많은 경우에 조직범죄와 연결됨에 따라 일부 발표자는 사이버범죄 근절 활동에 있어서 유엔 초국가적 조직범죄 방지 협약이 관련성을 언급하였음. 전문가 그룹은 또한 사이버안보와 사이버범죄의 관련성과 차이점을 토의하였음. 일부 발표자는 해당 개념들은 정보통신기술의 활용이란 광범위한 도전이란 맥락에서 서로 상이하다고 주장함. 이들은 따라서 이러한 개념들은 유엔의 ITU 또는 GGE에서 토의되는 것이 더 적합하다고 언급함. 반면 일부 발표자들은 그러나 사이버안보 현안은 상호연관된 것으로 사이버범죄를 효과적으로 대응하기 위해서 토의되는 것이 적절하다고 주장함. 또한 민간영역과의 긴밀한 협력과 협정 체결의 중요성이 강조됨.

많은 국가의 대표단들이 UNODC의 사이버범죄에 관한 범세계 프로그램 및 해당 프로그램을 통한 활동에 감사를 표했으며 자국 및 지역 내에서 실시되는 기술지원 및 역량강화 활동을 발표함. 일부 발표자들은 또한 OAS, Africa Union 등의 정부간 기구가 사이버범죄 대응을 위한 입법 및 기타 지원을 제공 중이라고 언급함. 또한 국가 대표단들은 의장 및 전문가 그룹의 위원회 및 사무국에 전문가 그룹회의의 조직 및 준비를 해준 것에 감사를 표함. 많은 발표자들이 전문가그룹의 업무에 대한 지원 의사를 표했으며 일부 발표자들은 금번 회의가 다양한 사법관할의 전문가 간의 다자 토의를 위한 기회를 제공하였다고 언급함. 또한 전문가 그룹 회의가 사이버범죄가 야기하는 공동의 위협에 대한 대응방안을 논의하는데 있어서 효과적인 역할을 담당할 것이라고 주장함. 이러한 점에서 2018-2021년 사이버범죄 전문가회의 개최계획의 채택을 환영하였음.

회의일정 두 번째 날에도 의제 2에 대한 심의를 지속하였음. 각국 대표단들은 특히 ▲사이버범죄 관련 입법에 있어서 특히 전자 증거 관련 국제법과 기준에 따른 인권 보호 방안과 ▲사이버범죄의 예방과 근절에 있어서 사생

활의 권리와 표현의 자유 권리를 균형있게 보장하는 것의 중요성을 강조하였음. 일부 발표자들은 여러 사법관할 내에서 사이버범죄 관련 행위의 범죄화가 높은 수준의 단일화가 이루어지고 있는 점을 언급하고 이가 관련 분야 내 법적 규범의 분산을 줄이는데 크게 기여하고 있다고 밝힘. 현존하는 도전과제로는 ▲공식 및 비공식 협력 활동을 통한 국제협력 증진과 ▲클라우드 컴퓨팅으로 인한 사법 관할의 문제 등이 논의됨.

이와 관련하여 전문가 그룹은 데이터의 초국가적 접근에 대하여 토의하였음. 발표자들은 해당 주제에 관한 토의가 사이버 범죄 수사에 있어서 사법관할 간의 협력을 증진하고 모범사례를 도출하는데 도움을 줄 것으로 기대함. 아울러 발표자들은 또한 주권 존중의 원칙에 대하여 토의할 필요성을 제기하였으며, 이는 다른 사법 관할에 위치한 데이터에 대한 접속 등의 행위가 주권 존중의 원칙과 어떻게 조화될 수 있을 지에 관한 문제가 해결되어야 한다고 주장함. 이 외에도 많은 발표자들은 기술 발전 및 범죄 양상에 대응하기 위해서는 사이버범죄 대응입법이 기술적으로 중립적인 용어를 사용해야 한다는 점을 언급하였으며, 인터넷을 활용한 중오범죄에 대한 대응의 중요성도 강조함. 또한 발표자들은 사이버범죄 대응입법이 기술지원 및 역량강화 활동을 통하여 뒷받침 되어야만 효과적일 수 있음을 강조하였음.

이러한 논의를 통하여 의제2 ‘입법과 프레임워크’에 관하여 참석자들은 다음과 같은 권고사항을 도출하여 CCPCJ(The Commission on Crime Prevention and Criminal Justice)에 제출하기로 함.

(a) 개별 회원국은 지속적으로 발전하는 기술에도 불구하고 미래를 향해 유효한 법률 조항을 만들어 내기 위하여 단순한 수단이 아니라 불법의 본질에 해당하는 행위를 범죄화해야 하며, 이 때 기술적으로 중립적인 법적 용어를 사용한다. 회원국은 여러 사이버범죄 활동을 명시할 때 일관된 용어를 사용하여, 가능한 범위 내 형사사법 기관 및 사법부가 관련법을 정확히 해석할 수 있도록 한다.

(b) 개별 회원국은 사이버범죄 대응을 위한 입법 시 대응에 필요한 조건 및 자국의 환경에 맞게 입법하되 타국의 주권을 존중하여야 한다. 사이버범죄 근절을 위

해 국제협력을 촉진하되 주권 존중이 장애요소로 인식되지 않고 근본적인 출발점이 되어야 한다. 클라우드 등 데이터의 전자 전송 및 저장의 휘발성 문제에 적절하게 대응하기 위해서는 전자 데이터 및 증거에 대한 적시적 접근을 보장하기 위한 회원국 간의 혁신적 및 확장된 사법공조 논의가 필요할 수 있다.

(c) 범죄 피난처의 존속을 막기 위해 회원국은 가장 광범위한 범위 내의 수사, 증거 수집, 기소, 재판, 그리고 필요시 인터넷 상의 불법자료의 삭제 등에서 공조를 지원한다. 회원국은 사이버범죄 또는 전자 증거가 연루된 기타범죄에서 처벌 구성요건이 서로 다르더라도 수사 또는 증거 등의 국제공조를 제공할 경우 가능한 범위 내에서 높은 수준의 유연성을 보장한다.

(d) 회원국은 관련 정책 입안 및 입법 시 인권 보호와 국가안보, 공공안전, 제3자의 권리가 균형 있게 조화를 이루도록 해야 한다. 사이버범죄의 수사, 기소, 재판을 위해 특정 행위를 범죄화하고 절차에 있어서 법적 권리를 부여할 때 적법 절차, 사생활, 시민권, 인권이 일관되게 보장되어야 한다. 다만 국가 정책 및 법안은 다양한 수단으로 실현될 수 있으므로 사이버안보라는 큰 범위의 개념에 대한 총체적인 이해를 바탕으로 한 적절한 사이버범죄 정책을 공유하며, 이와 동시에 범죄행위에 대응하면서 동시에 범죄를 예방하고 피해자에 대한 지원을 제공하며 사이버범죄 피해로부터 일반 시민을 보호할 수 있도록 노력하여야 한다. 사이버범죄 근절을 위한 국제협력의 기반을 창출하기 위하여 회원국은 사이버공간의 공동 미래를 만들어가는 문화를 증진하기 위해 노력하여야 한다.

(e) 회원국은 행위의 본질이 범죄화될 수 있는 경우라면 국내 법제의 완전한 조화 없이도 국제 협력을 추진하여야 하며, 여러 형태의 협력을 단순화하고 촉진하기 위해서 법제가 충분한 범위 내에서 호환 가능하게 해야 한다.

(f) 회원국은 범죄 행위가 발생한 지역과 해외 관할에서 동일한 행위가 범죄행위로 규정되는지 여부와 상관없이 자국의 시민 또는 거주자에 대해서 국내법의 역외적용을 위한 법률을 마련한다.

(g) 회원국은 국제협력을 위하여 여러 상이한 국제법적 근거를 사용할 수 있다. 이는 상호호혜, 양자 또는 다자 조약 그리고 기타 협정 등이다. 또한 사이버범죄 분야에서 높은 수준의 역량을 보유한 회원국은 자국의 역량 또는 기반시설에 비례하여 타국에 대한 법적 지원 제공에 있어서 더 큰 책임을 부담하여야 한다.

(h) 회원국은 사이버범죄에 있어서 관련 현안이 적절히 고려될 수 있게 보장하는

사이버범죄 관련 법제 마련이 결정될 경우 정부간 이해관계자, 민간 및 시민사회 등을 포함한 모든 관련 이해관계자와 빠른 시일 내 협의한다.

(i) 회원국은 사이버범죄 근절에 있어서 강력하고 신뢰할 수 있는 민관 협력을 창출하여야 하며, 이러한 협력에는 정부 법집행 당국과 통신서비스제공업체 (CSPs) 간의 협력을 포함한다. 이는 협력의 강화 및 증진에 유용한 바, 필요시 민관 협력 또는 MoU 체결을 통하여 구축한다.

(j) 회원국은 회원국의 사법부 및 검찰 그리고 디지털 포렌식 전문가들의 인식제고뿐만 아니라 민간기구의 사이버범죄 및 범죄대응에 관한 인식제고를 목표로 하는 UNODC의 교육적 프로젝트 및 프로그램을 지원하여야 한다. 회원국은 역량강화 도구 또는 전자지식관리 플랫폼을 활용하여 민간사회의 사이버범죄의 파급에 관한 인식제고를 촉진한다.

(k) 사이버범죄 대응을 위한 효과적인 법제 마련, 제정, 이행은 역량강화 및 기술 지원 프로그램으로 지원되어야 한다. 회원국은 자국 내 역량강화를 위한 적절한 자원을 분배한다. 사이버범죄 관련 법안의 적절한 이행에는 경찰, 검찰에 대한 훈련뿐만 아니라 공공인식의 제고를 위한 캠페인도 포함된다. 국제협력은 회원국의 사이버범죄 관련 범죄행위의 수사 및 기소 역량이 증가될수록 강화될 수 있다.

(l) UNODC는 회원국, 특히 개발도상국의 역량강화 활동 및 노력을 적극 지원한다. 이러한 역량강화 활동 지원은 정치적으로 중립적이며 부패로부터 자유로워야 한다. 이는 회원국의 자발적인 참여와 충분한 협의를 거쳐야 한다. 역량강화 활동은 다음을 포함한다:

- (i) 법관, 검찰, 수사관, 법집행 당국에 대한 사이버범죄 수사 훈련, 전자증거 취급, 무결성(chain of custody), 그리고 포렌식 수사
- (ii) 사이버범죄 및 전자증거에 대한 법안의 초안 작성, 개정, 이행
- (iii) 사이버범죄 수사부서 구성 및 관련 절차에 대한 지침 제공

(m) UNODC는 역량강화 활동이 분산되지 않도록 하기 위해서 Council of Europe 또는 OAS와의 긴밀한 협력 및 시너지 효과를 모색한다.

(n) 회원국은 전문가 그룹을 플랫폼으로 활용하여 참고 법안, 조항, 관할에 관한 문제, 특수수사기법, 전자증거의 휘발성 및 이로 인한 증거의 법적효력 문제 등

에 있어서 정보 및 모범사례를 지속 공유한다.

(o) 회원국은 유엔 및 전문가 그룹 플랫폼을 통하여 보편적인 관행 및 규칙을 연구한다.

(p) 회원국은 전문가 그룹 또는 UNODC의 임무에 정기적인 사이버범죄 동향 분석을 추가하는 방안의 가용성 및 가능성을 검토한다.

(q) 회원국은 유엔 프레임워크에 관한 회원국의 우려 및 이해를 반영한 사이버범죄 관련 국제법적 도구를 개발한다.

(r) 회원국은 부다페스트 협약 등 사이버범죄 관련 현존하는 다자 법적 도구에 가입하거나 활용하도록 권고되는 바, 이는 이 협약이 적절한 국내 및 국제적 사이버범죄 대응을 마련하는데 모범적인 모델로서 인정되기 때문이다.

(s) 유엔 초국가적 조직범죄 방지 협약 등 현존하는 법적 도구 및 매커니즘을 더 많은 국가가 활용하여 국제협력을 강화하여야 한다.

(t) 전문가 그룹의 후원 하에 회원국은 현존하는 지역적 도구 및 국내법에서 국제적으로 적용할만한 대응방안을 탐구하고 이를 통해 타국이 참고할만한 법제, 조항을 마련하도록 노력한다.

나. 의제3: 사이버범죄 실체법

2018년 4월 4-5일 개최된 4, 5차 회의에서 전문가 그룹은 의제3 “사이버범죄 실체법”에 관하여 논의하였음. 두 번째 주제에 관하여 Malini Govender (South Africa), Li Jingjing (중국), Vadim Sushik (러시아), Eric do Val Lacerda Sogocio (브라질), Marouane Hejjouji (모로코), Norman Wong (캐나다)가 전문가 패널로서 프리젠테이션을 함⁴⁾

4) 각 패널의 발표문은 UNODC

홈페이지(<http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html>, 2018.5.3. 최종방문) 참조.

패널 발표 이후 많은 발표자들이 패널발표에 대한 토론 형식으로 자국의 사이버범죄 범죄화 관련 입법에 대해 언급하였음. 많은 국가의 대표단은 컴퓨터 시스템의 기밀성, 무결성, 가용성을 표적으로 하는 범죄, 개인정보 관련 범죄, 테러 목적의 인터넷 사용 등의 핵심 사이버범죄행위를 열거하여 자국의 형사입법 상황에 관하여 발표하였음. 이미 많은 국가들이 상기 범죄행위들을 자국의 형사법체계에서 처벌하고 있음. 이에 관하여 일부 국가의 대표단들은 국가들마다 범죄화된 불법의 본질에 해당하는 행위가 동일한 이상, 국제공조를 위해서 동일한 범주로 유형화할 필요는 없을 것이라고 주장하기도 함.

아울러 각국 대표단들은 실체법에 관한 논의임에도 불구하고 실체법의 집행에 있어 필요하다는 이유로 다소 논점을 이탈하여, 앞에서 열거된 범죄를 수사함에 있어 전자증거의 법적 효력에 관한 절차법의 정비가 사이버범죄의 대응에 필수적이라고 주장하였음. 또한 법집행 담당자, 법관, 검사에 대한 적절한 훈련이 필요하다고 덧붙임. 더 나아가 관할권 간의 전자증거 공유의 필요성도 제기되었으나 해당 논의가 다시 부다페스트 협약의 국제규범화 문제로 번져 생산성없는 논의가 반복되려는 경향을 보이자 의장에 의해서 논의의 범위가 다소 제한되기도 함.

각국의 발표자들은 사이버 활동의 범죄화를 위한 입법 및 법안 마련의 경험을 공유하였음. 특히 몇몇 전문가들은 특정 행위의 범죄화를 위한 새로운 법안의 마련이 필요하다는 점에 대하여 언급함. 반면 기존의 법안 및 법제가 신종 사이버범죄 행위의 범죄화에 적절하고 충분하다는 주장도 있었음. 다만 다수 국가의 대표단들은 새로운 정보통신기술의 발전으로 인하여 새롭게 등장하는 사이버범죄의 유형에 대해서도 범죄구성요건이 적용될 수 있도록 하기 위하여 기술적으로 중립적 용어를 사용하는 구성요건이 만들어질 필요가 있다는 점을 주장함. 또한 범죄동향에 상응하여 다양한 구성요건을 입법할 필요가 있음을 언급하였으며, 암호화폐와 사물인터넷, 다크넷 등 새로운 유형의 범죄행위들에 적용될 수 있도록 적절한 구성요건이 마련되어야 한다고 주장함.

더 나아가 참석자들은 사이버범죄에 적절하게 대응하기 위해서는 인터넷서비스제공자(ISP)의 협조가 필수적이라는 점에 공감하고, 법집행에 협조한 ISP의 면책과 법집행 과정에서의 인권 보호 장치가 필요하다는 점에 대해서도 논의함. 더 나아가 전문가 그룹은 법집행 협조하지 않은 ISP에 대한 제재 부과 및 민간 기업의 협조를 이끌어 낼 방안도 논의됨.

일부 발표자들은 사이버범죄를 예방하기 위하여 공공 인식 제고 캠페인 및 아동에 대한 사이버범죄 위험 인식 제고 교육의 필요성이 제기됨. 또한 사이버범죄 활동의 예방을 위한 법집행 당국의 역량 강화를 위한 국제적 자원 배분의 필요성도 언급됨.

이러한 논의를 통하여 의제3 ‘사이버범죄 실체법’에 관하여 참석자들은 다음과 같은 권고사항을 도출하여 CCPCJ에 제출하기로 함.

- (a) 회원국은 많은 온라인 범죄에 오프라인 범죄 구성요건이 적용될 수 있음을 인지하고 국내 및 국제법에 현존하는 조항을 적용하여야 한다.
- (b) 회원국은 사이버범죄 행위를 적절하게 처벌하기 위하여 국내 법제를 개선하고 법집행 당국의 수사에 있어서 적법절차를 마련하여, 사생활 등 기본권과 인권을 보호한다.
- (c) 회원국은 정보통신기술을 남용하는 신종 사이버범죄에 대응하기 위하여 일반적으로 적용되는 형법에 의존하지 않을 수 있도록 사이버범죄에 대한 별도의 구성요건을 마련한다.
- (d) 회원국은 널리 인식된 국제적 기준을 고려하여 컴퓨터 네트워크 및 데이터의 기밀성, 무결성, 가용성을 침해하는 핵심 사이버범죄 행위를 범죄화한다.
- (e) 범죄행위에 이르지 못하는 사소한 법익침해에 해당하는 사이버 행위는 민사 및 행정 규제로 다룬다.
- (f) 회원국은 다음 행위유형의 범죄화를 검토한다.

- 암호화폐의 범죄적 사용 등의 신종 사이버범죄, 다크넷에서의 범죄행위, 사물 인터넷관련 범죄, 피싱, 악성소프트웨어 배포 및 이용 범죄
- 리벤지 포르노 등 개인정보의 유출
- 테러를 목적으로 한 인터넷 이용
- 증오범죄 및 폭력적 극단주의를 유발시키기 위한 인터넷 이용
- 사이버범죄에 대한 기술 지원
- 불법 온라인 플랫폼 개설 또는 사이버 관련 범죄를 목적으로하는 정보 공개
- 컴퓨터 시스템에 대한 불법적 접속 또는 해킹
- 컴퓨터 시스템 또는 데이터에 대한 불법적 손해야기
- 불법 데이터와 시스템 방해
- 장비의 불법적 사용
- 컴퓨터 관련 위조 또는 사기(행사)
- 아동에 대한 성적 학대 및 착취
- 지식재산권 침해

(g) 회원국은 정보체계의 기밀성, 무결성, 가용성에 대한 핵심 범죄 행위에 관한 사이버범죄 실체법의 국제적 조화에 특히 유의해야 하며, 정보통신기술을 활용한 일반 범죄 관련 법제의 국제적 조화는 특정 범죄 유형을 다루는 별도의 포럼에서 논의한다.

(h) 회원국은 인터넷서비스제공자(ISP)의 광범위한 활동을 범죄화하는 것을 피해야 하며 특히 이러한 규제가 생각 또는 신념의 표현을 부적절하게 제한하는 경우에 유의해야 한다. 회원국은 인터넷서비스제공자 등 민간 기업과 법집행 당국과의 협력을 증진하고 특히 대부분의 인터넷서비스제공자가 인터넷 플랫폼이 범죄에 악용되는 것을 방지하는데 이해관계를 지니고 있다는 점을 인식한다.

(i) 회원국은 증거 관련 국내법적 프레임워크를 채택하고 이행하여 범죄 수사 및 기소에 있어서 전자 증거의 법적 효력 및 해외 법집행 당국과의 적절한 전자 증거 공유 등을 인정한다.

(j) 회원국은 유엔 초국가적 조직범죄 방지 협약을 활용하여 범죄수사에 필요한 정보 및 증거 수집을 도모한다.

(k) 회원국은 사이버범죄 수사에 있어서 24/7 가용 가능한 협력 채널을 구축한다.

(l) 인터넷서비스제공자의 법집행 비협조의 범죄화와 관련하여 회원국은 이로 인한 민간 부문에 대한 부정적 효과와 표현의 자유 등 기본권 침해에 유의한다.

(m) 회원국은 사이버범죄의 효과적 대응을 위해서 현존하는 인권 프레임워크를 고려하고 사이버범죄 형사절차에서 법적 정당성, 필요성, 비례성의 원칙을 존중한다.

(n) 회원국은 연구를 통하여 사이버범죄의 근원적인 활동의 동향을 확인해야 하며 전문가 그룹 또는 UNODC에 사이버범죄 동향연구 임무를 부여하는 것을 고려한다.

(o) 회원국은 피해자조사 및 잠재적 피해자에 대한 정보제공 및 역량강화를 목적으로 하는 사이버범죄에 대한 포괄적 대응전략의 채택을 고려한다.

3. 맺음말

사이버범죄 협약(부다페스트 협약)의 국제규범화 문제는 여전히 국제적 합의를 이루지 못하고 있으며, 지지하는 국가들의 입장과 반대하는 국가들의 입장이 여전히 평행선을 그리고 있음. 출장자가 참여했던 2013년 제2차 회의에서 연구보고서 초안을 승인하지 못하고 회의가 중단된 이유가 바로 이 협약에 대한 해결될 수 없는 견해 차이였음. 본 회의에 참석하기 전에는 2017년에 전문가회의가 재개된 이면의 사정이 이와 같은 국가들간의 견해 차이를 극복기 위한 것인지 여부가 명확치 않았으나, 이번 회의를 통해 결국 양측의 입장이 더 강화되고 있음을 확인할 수 있었음.

미국, 유럽 등을 비롯하여 협약을 지지하는 국가들은 2013년 2차 회의 이후로 71개국(UN 가입국의 37%)가 협약에 가입했으며, 약 70% 이상의 UN 회원국들이 이 협약을 자국의 사이버범죄 관련 실체법과 절차법 개선의 가이드라인으로 이용하고 있다고 주장하면서, 이 협약의 국제규범화는 이미 돌이킬 수 없는 추세라고 주장하였음.

반면 러시아, 중국 등 이 협약에 반대하는 국가들 역시 세력을 규합하고 있음. 특히 2001년 결성된⁵⁾ SCO(Shanghai Cooperation Organization)를 중심으로 사이버범죄 관련 지역적 국제규범을 마련하고 있으며, 이러한 점을 논거로 부다페스트 협약 또한 CoE(Council of Europe)의 지역적 규범에 불과한 것으로 평가절하하면서, 부다페스트 협약이 ▲인권에 대한 고려가 부족하고, ▲주권 우선의 원칙과 충돌하며, ▲2001년에 제정된 이후로 새로운 기술발전을 반영하지 못하다는 근본적 문제가 있을 뿐만 아니라, 형식적으로도 ▲가입을 위해서는 CoE의 승인을 얻도록 하는 것이 합리적이지 않다는 이유로 UN 차원에서 다수의 지역적 협약들을 종합적으로 고려하여 새로운 다자협약을 마련할 것을 주장하였음. 아울러 회의 중 언급된 바로는 이번 회의를 비롯하여 앞으로 열릴 사이버범죄 전문가회의의 비용을 중국 측이 부담한다고 하였음. 이러한 사실은 협약에 반대하는 국가들의 입장이 상당히 정리되고 강화되고 있음을 방증하는 것으로 생각됨.

이번 회의에 법무부에서는 국제형사과 김남수 검사가 파견되었으나 일정상 첫날 회의에만 참석하고 이후의 회의는 오스트리아 대사관에 법무협력관으로 파견되어 비엔나에 상주하는 조주연 검사가 참석함. 회의 기간 중 김남수 검사, 조주연 검사 그리고 외교부 주오스트리아대사관 겸 주빈국제기구대표부 최태호 참사관과 우리나라의 협약 가입 추진 상황에 관하여 논의하였으며, 특히 형사소송법 및 통신비밀보호법의 개정 등 이행입법 문제에 관하여 의견을 나누었음. 정부 측에서는 특히 기본권 제한과 밀접한 관련이 있는 강제수사 수단을 강화하는 방향의 절차법 개정이 다소 부담스러운 점이 있으며, 따라서 현행 절차법과 판례 등에 근거한 수사실무의 강제수사방법이 협약이 제시하는 입법 기준에 어긋나지 않다는 점을 명백히 하여 협약 가입을 추진하고 있음. 협약 가입 필요성 및 사이버범죄 관련 수사 방법의 개선방안에 대한 검토 필요성에 관하여 의견을 같이 하였으며, 앞으로 협약 가입 및 이행입법 필요 여부와 관련하여 정책연구를 통하여 법무부와 지속적으로 논의를 이어가기로 함.

5) 바르샤바 조약기구를 대체하는 국제기구로 1996년 러시아, 중국, 카자흐스탄, 키르기스스탄, 타지키스탄 등 5개국이 결성한 상하이 파이브(Shanghai Five)가 전신임. 현재는 인도, 파키스탄이 가입하는 등 대체로 반미, 친중, 친러 성향의 국가들의 연합체로 발전하고 있음.