

방송통신미래전략체계연구 지정 2012-05

# 국제 사이버공간 포럼 대응전략 연구

(A Study on Preparation Strategy of  
International Cyber Space Forum)

2012. 11.

연구기관 : (사)미디어미래연구소



이 보고서는 2012년도 방송통신위원회 방송통신발전기금 방통융합 미래전략체계연구 사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

# 제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『국제 사이버공간 포럼 대응전략 연구』의 연구결과보고서로 제출합니다.

2012년 11월

연구기관 : (사)미디어미래연구소

책임연구원 : 김일환 교수(성균관대학교)

공동연구원 : 김진기 교수(한국항공대학교)

이종관 연구위원(미디어미래연구소)

참여연구원 : 남승용 책임연구원(미디어미래연구소)

김유석 선임연구원(미디어미래연구소)

이종영 선임연구원(미디어미래연구소)

성지연 선임연구원(미디어미래연구소)

전주혜 선임연구원(미디어미래연구소)

안자영 연구위원(미디어미래연구소)

# 목 차

## 요 약 문

제1장 서론 .....	1
제1절 연구의 필요성 .....	1
제2절 연구 목표 및 주요 내용 .....	3
제2장 주요 국제회의 의제 분석 .....	4
제1절 OECD 장관회의 주요 의제 분석 .....	4
1. 1998년 전자상거래 OECD 장관회의 .....	4
2. 2008년 인터넷 경제의 미래에 관한 OECD 장관회의 .....	8
제2절 런던 사이버스페이스 총회 주요 의제 분석 .....	25
1. 2011년 런던 사이버스페이스 총회 개요 .....	25
2. 런던 사이버스페이스 총회 주요 논의내용 .....	28
제3절 2012년 부다페스트 사이버스페이스 총회 의제 분석 .....	34
1. 주요 활동사항 .....	34
2. 주요 의제 .....	36
제3장 사이버공간 관련 글로벌 이슈 분석 .....	40
제1절 사이버보안 및 사이버 범죄 관련 글로벌 이슈 분석 .....	40
1. 사이버 보안 .....	40
2. 사이버 범죄 .....	45
제2절 프라이버시·개인정보 및 아동 보호 관련 글로벌 이슈 분석 .....	56
1. 프라이버시 및 개인정보 보호 .....	56
2. 아동보호 .....	64
제3절 사이버공간의 경제적·사회적 혜택 관련 글로벌 이슈 분석 .....	68

1. 사이버공간의 경제적 혜택 .....	68
2. 사이버공간의 사회적 혜택 및 인권 .....	72
제4장 2013년 세계 사이버스페이스 총회 의제 설정 .....	81
제1절 2013년 세계 사이버스페이스 총회 주제 및 주요 방향 설정 .....	81
1. 추진배경 및 기대효과 .....	81
2. 주제 및 주요 방향 .....	83
제2절 2013년 세계 사이버스페이스 총회 주요 의제 설정 .....	90
1. 기존 회의 주제 및 의제 비교 .....	90
2. 주요 의제 설정(안) .....	91
제5장 결론 .....	96

## 표 목 차

<표 2-1> 1998년 전자상거래 OECD 장관회의 개요 .....	4
<표 2-2> 전자상거래 OECD 회의 의제 .....	5
<표 2-3> 범세계적 네트워크상의 프라이버시 보호에 관한 OECD 장관 선언문 ...	7
<표 2-4> 2008년 전자상거래 OECD 장관회의 개요 .....	9
<표 2-5> 2008년 인터넷 경제의 미래에 관한 OECD 장관회의 의제 .....	11
<표 2-6> 정보통신분야 OECD 선언문, 권고, 지침, 정책원칙 등 현황 .....	19
<표 2-7> 인터넷 경제의 미래를 위한 서울선언문 .....	20
<표 2-8> 2011년 런던 사이버스페이스 총회 개요 .....	25
<표 2-9> 사이버스페이스에 대한 런던 컨퍼런스 의제 .....	33
<표 2-10> 2012 부다페스트 사이버공간 회의 의제 .....	39
<표 3-1> WSIS 원칙 선언 .....	41
<표 3-2> ‘안전하고 신뢰할 수 있는 ICT 환경 촉진’ 분야 실행계획 .....	43
<표 3-3> 최근 5년간 사이버범죄 검거 건수 .....	46
<표 3-4> ‘OECD 프라이버시 가이드라인’ 적용상의 기본원칙 .....	57
<표 3-5> 소셜컴퓨팅 시대의 7대 프라이버시 우려 .....	60
<표 3-6> OECD 권고안 주요 내용(2012년) .....	67
<표 3-7> G20 국가의 인터넷 경제 규모 및 전망 .....	70

<표 3-8> 사이버공간의 경제적 혜택 .....	71
<표 3-9> 사이버공간의 특성과 문화 창달 .....	75
<표 3-10> 사회적 역기능과 통제 .....	76
<표 3-11> 표현의 자유에 대한 규제 유형 비교 .....	77
<표 3-12> 프라이버시 침해 규제 유형 비교 .....	78
<표 4-1> 기존 총회 주제 및 의제 비교 .....	84
<표 4-2> 2013년 세계 사이버스페이스 총회 개도국·NGO·기업 초청(안) .....	87
<표 4-3> 기존 회의 주제 및 의제 비교 .....	90
<표 4-4> 2013년 세계 사이버스페이스 총회 주요 이슈 및 논의 의제(안) .....	95

## 그림 목 차

[그림 2-1] 인터넷 경제의 미래에 관한 OECD 장관회의 슬로건 .....	9
[그림 3-1] 개인정보 침해신고 상담건수 .....	46
[그림 3-2] 월별 악성프로그램 유포 횟수 .....	47
[그림 3-3] 개인정보보호법 제정 전 후의 보호 범위 .....	58
[그림 3-4] 온라인 아동보호 개념 .....	64
[그림 3-5] 온라인상의 아동 위험 요소 .....	65
[그림 3-6] 사이버공간의 사회적 역기능 .....	75
[그림 4-1] 2013 세계 사이버스페이스 주제 선정 방향(안) .....	85

# 요 약 문

## 1. 제 목

국제 사이버공간 포럼 대응전략 연구

## 2. 연구 목적 및 필요성

사이버공간의 기술이 진보하면서 여러 가지 경제적, 사회적 기회와 혜택도 제공을 받았지만 인류는 여러 가지 도전과 위협에도 직면해 있다. 이 같은 배경에서 다음과 같이 사이버공간에 대한 대화의 장을 마련하고 국제 협력을 증진할 필요성이 대두되고 있다. 본 과제는 2013년 사이버공간회의의 의제를 준비하는 과제로 사이버공간에 관한 글로벌 이슈를 분석하고 의제를 선정하는 것을 목표로 한다.

## 3. 주요 국제회의 의제 분석

2008년 서울에서 개최된 OECD 장관회의 개막회의에서는 사회적 네트워킹 및 사용자 제작 콘텐츠, 에너지 효율성과 환경보호, IPv4의 재활용과 IPv6 장려, 인터넷 아키텍처 및 3차원 인터넷 프로젝트, 국제 공조 등이 논의됐다. 이와 함께 라우드테이블에서 경제 성과 및 사회복지 향상, 글로벌 문제 해결을 위한 인터넷, 차세대 통합 네트워크로 전환에 관련된 주요 정책, 융합의 혜택, 창의성 증진, 신뢰의 구축, 글로벌 인터넷 경제 등이 논의됐다. 그 성과로 ‘인터넷 경제의 미래를 위한 서울선언문’이 채택됐다.

2011년 런던 사이버스페이스 총회의 주요 안건으로 경제적 혜택 및 개발, 사회적 혜택, 사이버 범죄, 안전하고 신뢰 가능한 접속 보장, 국제안보 등 모두 5가지 이슈가 대두됐다. 첫 번째 이슈 ‘경제적 혜택 및 개발’ 논의에서는 지적재산권 보호, 정부 규제 對 자율

규제, 동 분야 국제규범 및 원칙 등이 세부 의제로 제시됐다. 두 번째 이슈 ‘사회적 혜택’ 논의에서는 다양성 보장 및 표현의 자유, 정부와 민간의 책임과 균형점, 인터넷 필터링과 사이트 차단이 정당화되는 경우, 인터넷을 통한 정부와 시민 간 협력, 동 분야 국제규범 및 원칙 등이 세부 의제로 제시됐다. 세 번째 이슈 ‘사이버 범죄’ 논의에서는 사이버 범죄 심각성, 사법집행, 사경공조 조약 등이 세부의제로 제시됐다. 네 번째 이슈 ‘안전하고 신뢰 가능한 접속 보장’ 논의에서는 아동보호, 사이버 괴롭힘, 사이버스토킹 등을 비롯해 규제와 자기 규제간 올바른 균형, 개인정보보호 및 프라이버시 문제, 대중의 위험 인식 및 교육, 동 분야 국제규범 및 원칙 등이 세부의제로 제시됐다. 다섯 번째 이슈 ‘국제안보’ 논의에서는 사이버 사건으로 인한 위기, 공격 근원지 확인 문제, 기존 국제법의 효율성, 동 분야 국제규범 및 원칙 등이 세부의제로 제시됐다.

2012년 부다페스트 사이버스페이스 총회에서는 경제성장 및 발전, 사회적 혜택 및 인권, 사이버 보안, 사이버범죄, 국제안보 등 인터넷이 가져오는 다양한 혜택과 위협요인을 논의했다. 표현의 자유, 다양성, 개방성, 투명성 등을 원칙으로, 사이버공간에서의 부작용(범죄, 테러 등)을 최소화하기 위해 국제 및 미-관 협력의 중요성을 강조했다. 그러나 참석자나 논의내용이 유럽과 미국을 중심으로 이뤄져 아시아, 아프리카, 남미 등 개도국의 참여 저조 및 중국 등이 반발했다. 이들은 부다페스트 회의가 런던 회의 이후 참여국가나 의제가 발전되지 못한 점을 지적하며, 사이버공간 회의에 대해 비판적인 입장이다. 따라서 서울회의에는 아시아, 중남미, 아프리카 국가들의 참여를 촉진하는 한편, 이들 개도국의 인터넷 보급률 등 현실에 맞는 의제를 설정할 필요가 있다.

#### 4. 사이버공간 관련 글로벌 이슈 분석

첫째, 사이버 보안과 관련해 최근에는 인터넷 ‘악플’, 사이버범죄, 사이버테러뿐만 아니라 국가안보를 위협하는 수준으로까지 확대되고 있다. 이러한 문제를 해결하기 위해서는 무엇보다 국가간 협력이 필요하다. 또한, 국가 간의 사이버 보안 격차 해소를 위한 공동의 노력이 필요하다. 제3세계 국가들에 인적, 물적, 교육적 지원 활동이 요구된다.

둘째, 사이버범죄는 초국가적 본질과 관할 문제로서 세계 어디서나 공격 시도가 가능하고 여러 국가들 간에 걸쳐 범죄를 실행할 수 있어 전통적 주권국가 관할 개념을 적용하는 것이 불가능하다. 최근 들어 발생하고 있는 여러 가지 형태의 사이버 범죄에는 몇 가지 공통점이 있다. 유출되는 데이터의 양이 상당하고, 치안과 안보가 혼재되어 있으며, 상당히 지능화 되는 추세다.

셋째, 프라이버시 및 개인정보 보호의 보호 필요성이 강하게 제기되고 있다. 정보사회에서의 프라이버시권<sup>1)</sup>을 개인정보통제권으로서 개념을 재구성하는 연구는 ‘자기와 관련된 정보를 통제할 수 있는 권리’라는 적극적, 능동적 권리로 발전하게 됐다. 최근에는 사이버 경제의 확산에 따라 시장에 의한 침해 부분이 더 문제가 되고 있으므로, 시장에 있어서의 개인정보보호 및 프라이버시 침해라는 부분에 대한 논의도 필요하다.

넷째, 20세 미만의 아동 및 청소년의 온라인 및 모바일 등 사이버 공간에 대한 노출이 늘어나고 있으며 이와 관련한 부작용이 지속적으로 발생하고 있다. 이에 따라 사이버 공간에서 아동을 보호해야 할 필요성이 높아지는 추세다. 해외 각국에서는 사이버 공간에 노출되어 있는 아동을 보호할 수 있는 방안을 마련하고 있다.

다섯째, 사이버스페이스의 경제적 혜택으로 비용의 절감, 특히 B2B 거래비용이 상당히 줄어들었다. 수확 체증 현상으로 있어서 사이버스페이스에 통용되는 제품에 대한 물가가 하락한다. 또한, 고용의 증대와 동시에 전통산업에서는 고용이 감소되는 현상이 동시에 발생한다.

여섯째, 런던 회의에서는 인터넷과 사이버 공간이 가져오는 사회적 혜택, 사이버 공간으로 인한 사회적 역작용 또는 문제점, 인터넷에서의 표현의 자유와 규제 간의 균형을 어떻게 달성할 것인가 등이 주요 논의이었다. 부다페스트 회의에서는 ‘인권’이라는 부분이 추가됐다.

---

1) 프라이버시권은 19세기말 당시 미국 언론기관의 유명인사의 사생활에 대한 무차별적 폭로 기사로 인한 법익침해가 기존의 명예훼손으로 인한 법익 침해와는 차이가 있음을 확인하고 새로운 불법행위의 법리를 창안하기 위하여 고안된 권리개념이다.

## 5. 2013년 세계 사이버스페이스 총회 의제 설정

2013년 세계 사이버스페이스총회의 기본방향은 첫째, 1·2차 총회 성과를 기초로 하여 가치를 부가할 수 있는 기회를 만드는 것이다. 둘째, 서울 총회 이전까지 UN 정부전문가 부분, OSCE 각료이사회, OECD, ITU 등 각종 국제 포럼에서 논의되는 내용을 적절히 포함시키도록 한다. 셋째, 한국적 특색도 적절히 가미한다. 넷째, 사이버공간의 다양한 이슈에 대해 국제적인 협력을 강화한다.

2013년 서울에서 개최될 세계 사이버스페이스 총회 주제는 총회의 목적과 방법, 참여 국가 및 주요 논의의제 등을 고려하여 선정할 필요가 있다. 이를 위해서는 다음의 세부적인 다섯 가지 요인을 고려할 필요가 있다. ① 미래지향적 주제 또는 목표, ② 실현 가능한 규범 또는 의제, ③ 전 세계 공통 관심사(의제) 포함, ④ 이용자 중심, ⑤ 사이버스페이스의 성격 등이다. 이와 함께 전 세계의 공통 관심사를 포함할 수 있는 주제 선정이 필요하다. 이는 선진국뿐만 아니라 개도국, 후진국들의 참여를 유도해야 하기 때문이다. 특히, 아시아·중남미·아프리카 등의 개도국을 다수 초청하여, 사이버공간에 대한 논의에서 균형을 잡을 수 있도록 한다.

성과사업으로 첫째, 3회째를 맞는 2013년 총회의 결과 문서로는 가급적 최소한의 원칙적 합의 및 논의 진전사항을 반영한 ‘의장성명’ 또는 ‘선언’을 채택하는 방안이 필요하다. 둘째, 지속적인 총회 개최를 위한 특단의 방안을 고려할 필요가 있다. 이와 함께 지속적인 총회 개최를 위해 사이버스페이스 전담 국제기구의 창설을 검토하고 이를 3회 총회에서 논의하는 것도 고려할 필요가 있다.

런던 사이버스페이스 총회의 주제는 ‘사이버 공간에서 수용 가능한 행동에 관한 규범’이었다. 이때 선정된 주요 경제성장과 개발, 사회적 혜택, 국제 안보, 사이버 범죄, 안전하고 신뢰 가능한 접속 등 5개 의제가 ‘자유, 번영을 위한 신뢰와 안정’을 주제로 한 2012년 부다페스트 총회에서 대부분 유지됐다. 런던회의에서는 사이버공간의 긍정적 측면 및 부정적 측면(hopes and fears)이 논의됐으며, 부다페스트 회의에서는 개도국 역량 강화, 민관협력, 국제·지역기구 역할 등이 검토됐다. 2013년 세계 사이버스페이스 총회에

서도 큰 틀은 계승하되, 회의의 성과를 진전시키고 한국적 특수성을 반영하는 차원에서 일부 보완하는 것이 바람직하다.

우선, 경제적 혜택과 관련된 핵심적인 문제는 디지털 격차문제라고 할 수 있다. 이버 공간의 활용과 경제적 혜택 확산 공유를 위한 디지털 격차 해소와 관련된 국제협력방안에 대한 논의가 경제 분야에서 이뤄질 수 있는 중요한 의제가 될 것이다. 둘째, 사회적 혜택 외에 문화 측면이 강조될 필요가 있다. 특히 아시아권과 중·남미권에서의 공통된 의제를 발굴할 필요가 있다. 셋째, 사이버 보안은 헝가리 회의에서 새로이 채택된 주제로서, 2013년 서울 총회에서도 사이버 보안 의제는 유지할 필요가 있다. 단, 부다페스트 회의에서 가장 쟁점이 됐던 것은 사이버 범죄 협약인데, 이는 각국이 첨예하게 대립하는 부분이기 때문에 협약이 주요 의제로 떠오르는 것은 지양해야 할 것이다. 넷째, 국제안보와 관련해서 현 단계에서는 신뢰구축이 중요하다. 합의를 도출하지 못하더라도 향후 논의의 진전을 이룰 수 있도록 공감대를 마련하여 모멘텀(momentum)을 이어가는 것이 중요하다. 마지막으로 사어비범죄와 관련해서는 사이버공간에서의 중독문제, 초국가적 사이버조직범죄, 안티사이버테러리즘, 새로운 기술과 사이버범죄, 국제 사이버범죄협약, 개인정보와 ‘잊혀질 권리’ 등을 논의할 필요가 있다.

# 제 1 장 서론

## 제 1 절 연구의 필요성

사이버공간의 기술이 진보하면서 여러 가지 경제적, 사회적 기회와 혜택도 제공을 받았지만 인류는 여러 가지 도전과 위협에도 직면해 있다. 이런 가운데 사이버스페이스에서 추구해야 할 핵심 가치, 사이버스페이스를 규율하는 수단 등에 대해 미국을 중심으로 한 서방과 중국, 러시아가 치열하게 패권 경쟁을 하고 있는 상황이다. 이 같은 배경에서 다음과 같이 사이버공간에 대한 대화의 장을 마련하고 국제 협력을 증진할 필요성이 대두되고 있다.

첫째, 사이버공간의 발전과 사회적 역기능간의 격차를 최소화할 필요가 있다. 사이버공간은 지금까지 경험하지 못한 새로운 기회와 혜택을 제공하고 있지만, 동시에 사이버bullying, 사이버범죄, 사이버테러 등 새로운 위협이 대두되고 있다. 한국은 사이버공간이 제공하는 혜택을 그 어떤 국가보다 많이 누리고 있지만, 동시에 정보통신기술로 발생하는 역기능도 많이 경험하고 있다. 사이버공간의 발전으로 인해 다양한 혜택과 기회가 제공되고, 사이버공간을 통한 글로벌 네트워크 환경의 구축은 경제적, 사회적 기회와 혜택을 제공하고 있다. 그러나 사회적으로 사이버 범죄, 사이버 보안, 프라이버시 침해 등 다양한 역기능과 각종 사회적 폐해도 발생하고 있다. 특히 이러한 사회적 폐해가 전 세계적으로 구축된 네트워크를 통해 글로벌화 되면서 심각성은 더욱 증폭되고 있는 상황이다. 따라서 사이버공간의 지속가능한 발전을 도모함과 동시에 각종 사회적 폐단을 최소화할 수 있는 방안 마련을 마련하여 바람직한 사이버공간 문화를 형성할 필요성이 증대되고 있다.

둘째, 사이버공간에서의 제반 문제 해결을 위한 전 세계적 공감대를 형성할 필요가 있다. 사이버공간이 국경 개념이 없다는 점을 감안할 때, 사이버공간에서 발생하는 각종 폐해는 한 국가 내에서만 발생하는 것이 아니라 전 세계적으로 문제가 되는 글로벌 이슈이다. 따라서 전 세계가 하나의 사이버공간에서 연결되고 있는 글로벌 네트워크 시대에

각국의 정부, 산업계, 시민사회 등 다양한 사이버공간 참여자들이 참여하여 전 세계적인 공감대를 형성할 필요가 있다. 해당 이슈들에 대한 포괄적이고 건설적인 논의를 통해 사이버공간 발전 및 제반 문제 해결을 위한 종합적인 대책을 강구할 필요가 있다.

셋째, 사이버공간 규범 및 원칙을 확립할 필요가 있다. 사이버공간의 혜택과 기회를 보장·확대하고 각종 피해를 최소화할 수 있는 사이버공간 규범 및 원칙의 확립이 필요하다. 그동안 사이버 규범에 대한 논의가 부분적으로 진행되어 왔으나, 각각의 이슈 간 상호 연관된 다양한 측면에서 사이버 규범에 대한 포괄적인 논의가 부족했다. 따라서 사이버공간 회의를 통해 각종 글로벌 이슈에 대한 포괄적인 논의를 진행하고 이를 통해서 사이버공간 규범 및 원칙을 조속히 확립할 필요가 있다. 법적 공백과 모호성은 국가간 오해를 확대시키고 악용의 유인이 제공될 가능성이 있다. 따라서 규범 문제에 있어서 공통 기반 추구를 위한 점진적, 이슈별 노력이 요구된다.

넷째, 사이버공간에 관한 국제규범 의제를 준비할 필요가 있다. 2011년 영국 외무성 주관으로 개최된 장관급 회의인 런던 사이버스페이스 회의의 후속회의를 2013년 우리나라에서 개최하기로 결정했다. 이에 따라 2013년 사이버공간회의 의제를 설정하고 2012년 부다페스트 회의 의제에 대한 대응이 필요하다. 사이버스페이스 총회의 성격은 정부, 산업계, 시민사회가 아우르는 사이버공간이 주요 행위자가 모두 참여하는 회의로 기획됐다. 이는 지금까지 UN, ITU, OECD 등의 기구에서 사이버 안보에 대한 논의가 부분적으로 진행됐지만, 상호 연관된 측면을 포괄적으로 다루는 종합 포럼은 부재했다는 문제의식에서 출발한 것이다. 또한, 법적 구속력을 지니는 규범 도출보다는 정치, 외교적 합의 도출을 목표로 하고, 정치적 안보 측면뿐만 아니라 사이버 공간에서의 인권, 경제 사회적 이익 등을 포함한 균형적 논의를 지향한다.

## 제 2 절 연구 목표 및 주요 내용

본 과제는 2013년 사이버공간회의의 의제를 준비하는 과제로 사이버공간에 관한 글로벌 이슈를 분석하고 의제를 선정하는 것을 목표로 한다. 일부 관련 이슈별로 개별적으로 수행된 연구가 있으나, 글로벌 이슈에 대한 종합적이고 포괄적인 연구는 없는 상태이므로 본 연구는 해당 분야에서 선도적인 연구가 될 것이다. 따라서 본 연구는 사이버공간 전반에 대한 이슈 분석 및 글로벌 의제를 설정하는 선도적인 연구로서 그 차별성이 있으며, 향후 사이버공간 관련 타 연구에 영향을 미칠 수 있다는 점에서 높은 의의가 있다.

사이버보안, 프라이버시, 인터넷 윤리 등 정보보호 관련 글로벌 이슈를 분석하고 관련 의제를 발굴하여 정보보호 관련 국내 정책 방안 마련을 본 과제의 목표로 한다. 이를 통해 2012년 부다페스트 사이버스페이스 총회 대응방안을 마련하고 2013년 서울 사이버스페이스 총회 의제를 발굴한다.

본 연구의 목적은 다음과 같다. 첫째, OECD 장관회의, 런던 사이버스페이스 등 주요 국제회의 의제를 분석한다. 둘째, 사이버보안 및 사이버 범죄, 프라이버시 및 개인정보 보호, 온라인 아동보호, 사이버공간의 경제적 사회적 혜택 등 사이버공간 관련 글로벌 이슈를 분석한다. 셋째, 사이버공간회의에 대응하는 국제규범 의제를 설정한다. 여기에는 2012년 헝가리 회의 대응 방안을 마련하고, 2013년 사이버공간회의 주제 및 주요 방향 설정 및 주요 의제 설정이 포함된다.

위와 같은 연구목적을 달성하기 위해 방송통신위원회와 주관연구기관 간의 상시적인 연구협력을 통해 정책수요를 반영한 연구결과를 도출한다. 문헌연구를 통해 OECD 장관회의 등 기존 장관회의 및 사이버공간 회의에서 채택된 정보보호 관련 주요 의제를 발굴·분석하고, 사이버보안, 프라이버시, 온라인 아동보호 등 다양한 정보보호 관련 주요 의제를 분석한다. 또한, 정보보호 관련 전문가들로 구성된 연구반을 운영하여 정보보호 관련 주요 이슈 발굴 및 의제 설정, 전문가 의견을 수렴한다. 이를 통해 본 연구는 정보보호와 관련하여 최근 대두되고 있는 글로벌 이슈를 발굴·분석하고, 사이버공간에 관한 국제적 논의에 지속적·전향적으로 기여할 수 있을 것으로 기대된다.

## 제 2 장 주요 국제회의 의제 분석

### 제 1 절 OECD 장관회의 주요 의제 분석

#### 1. 1998년 전자상거래 OECD 장관회의

##### 가. 배경

1997년부터 OECD 회원국에서 전자상거래를 둘러싼 다양한 문제가 발생하고 소비자 보호문제가 중요한 이슈로 부각되자, ‘세계시장의 관문: 소비자와 전자상거래’를 주제로 포럼이 개최됐다. 또한, 핀란드 투르쿠에서는 ‘글로벌 전자상거래의 장애물 제거’라는 주제로 회의가 열려 전자상거래를 시장 기능에 맡겨야 한다는 전제하에 공익보호와 안정된 법적 환경조성을 위한 최소한의 정부개입이 필요하다는 내용의 10대 원칙을 채택했다. 투르쿠 회의의 문제제기를 바탕으로 1998년 10월 오타와 회의에서는 해결책과 대책을 마련하려는 움직임이 본격화되었으며, 사안별로 정부와 민간부문의 행동계획 책정과 개인정보보호, 소비자보호 과제 및 인증 등에 대한 국제적인 합의도출을 위한 논의를 시작했다. 특히 오타와 회의에서는 소비자보호 문제가 중요한 의제로 제기되고, 네 차례의 전체회의 가운데 두 차례에 걸쳐 소비자보호 문제가 의제로 논의되었다. 이 같은 논의 결과 ‘전자상거래에서 소비자보호 선언’이 채택됐다.

<표 2-1> 1998년 전자상거래 OECD 장관회의 개요

구분	내용
기간	1998년 10월 8일~9일
장소	캐나다 오타와
주제	범세계적인 전자상거래의 실현
참석	OECD 가맹국 장관, 국제기구 대표자, 업계 대표자, 노동관계자, NGO 대표자, 참관(비가맹국 대표자) 등 700여 명

<표 2-2> 전자상거래 OECD 회의 의제

의제	내용
신뢰성 구축	사용자와 소비자의 신뢰구축
기본규칙 설정	디지털 시장질서의 기본 규칙 정립
정보통신 인프라 정비	전자상거래를 위한 정보통신기반의 고도화
경제 사회에 제공하는 이익 최대화	전자상거래 잠재능력의 극대화

나. 주요논의 및 결과

세계적인 전자상거래를 위한 목표 및 공통인식을 열거하고, ‘오타와 선언’ 등 회의에서 합의된 내용을 총괄했다. ‘전자상거래와 소비자보호에 관한 각료선언’을 통하여 전자상거래소비자가 실제 거래와 동일한 수준의 보호를 받아야 함을 천명했다. 그리고 OECD 조세분야 보고서인 ‘전자상거래의 조세 기본체제와 조건’을 승인하고 전자상거래가 기존 거래와 비교하여 더 불리하지 않은 조세대상이 되어야 한다고 선언했다 기존 상거래에서 적용되는 과세원칙을 전자상거래에서도 적용하고, 이러한 과세원칙을 적용하기 위한 수단을 도입하고 변경하는 것이 불가능하지 않다고 제언했다. 과세 기본원칙으로 중립성, 효율성, 확실성과 단순성, 효과성과 공정성, 효율성을 제시했다. 전자상거래 과세에 관한 중립성 원칙<sup>2)</sup>의 중요성과 소비세는 소비지국에서 과세되어야 하며 디지털 재화는 상품의 공급으로 보지 않는다는 원칙을 채택했다. 전자상거래에서 전자인증의 중요성을 인식하고 산업계와 소비자단체가 공동으로 전자인증에 관한 국제수준의 지속적인 활동을 제언했다.

또한, ‘범세계 네트워크에서의 사생활보호 가이드라인’을 채택하여 온라인 환경에도 ‘1980년 OECD 사생활보호 가이드라인’이 적용되어야 한다는 원칙을 확인하고, OECD 8원칙(수집제한, 정보 정확화, 목적 명확화, 이용제한, 안전보호, 공개, 개인참가, 책임)을 바탕으로 프라이버시 보호에 관한 선언을 채택했다. 선언에는 ①인터넷 등 온라인에서도 OECD 8원칙을 기본으로 적용할 것, ②가맹국간의 서로 다른 보호수단을 인정하고

2) 유사한 상황 하에서 유사한 거래를 행하는 납세자는 유사 과세를 받는다.

다양한 접근방법을 조정할 것, ③회원국은 각국의 법과 관행의 틀 안에서 필요한 수단을 강구하며, 특히 법, 자율규제, 행정, 기술적 수단 등으로 프라이버시에 관한 방침 채택을 권장할 것, ④프라이버시 원칙 및 방침을 준수하지 않는 경우에 대처하고 구제를 받을 권리를 확보하기 위해 효과적인 집행제도를 확보할 것 등이 포함됐다.

이를 통해 범세계 전자상거래 진흥을 위한 행동계획이 OECD와 민간업계 그리고 관련 국제기구에 의해 각각 수립되어, 분야별 추진과 협력이 강조됐다. 이용자와 소비자가 신뢰를 얻을 수 있는 디지털시장 형성, 정보인프라 강화, 전자상거래의 혜택 확대를 위해 OECD, 기타 국제기구, 각국 정부, 산업계 등의 대응책을 정리한 행동계획을 책정하고, 구체적으로 OECD 행동계획, 기타 국제기구 활동에 관한 보고, 산업계의 글로벌 행동계획 등을 채택했다.

<표 2-3> 범세계적 네트워크상의 프라이버시 보호에 관한 OECD 장관 선언문(발췌)

(전략)

[14] 회원국은 기본권의 존중을 보장하고, 범세계적 네트워크상에서 신뢰를 구축하며, 개인정보의 국제적 흐름에 대한 불필요한 제한을 방지하기 위하여 범세계적 네트워크상에서의 프라이버시 보호에 대한 회원국의 책무를 재확인한다.

[15] 회원국은 OECD 가이드라인을 기초로 범세계적 네트워크상에서 프라이버시 보호를 보장하기 위해 회원국들에 의해서 채택된 상이한 접근 방식들 간에 교량을 설치하기 위해 노력할 것이다.

[16] 회원국들은 프라이버시 가이드라인이 범세계적 네트워크와 관련하여 효과적으로 이행되는 것을 보장하기 위하여 자국의 법과 관행의 틀 안에서 다음과 같은 조치들을 포함하여 필요한 조치를 취할 것이다.

[17] 범세계적 네트워크상에서 프라이버시 보호를 위해 재량껏 활용할 수 있는 수단과 온라인 프라이버시 이슈에 관한 이용자 교육 및 계몽을 촉진하는 조치,

[18] 법적, 자율규제적, 행정적 또는 기술적 수단을 막론하고 범세계적 네트워크와 관련된 OECD 프라이버시 가이드라인을 효과적으로 이행하는 프라이버시 정책의 채택을 조장하는 조치,

[23] 이용자에 대한 프라이버시 정책의 온라인 통지를 촉진하는 조치,

[24] 온라인을 통한 국제적 정보이전에 관하여 계약적 해결책의 이용과 계약적 해결모델을 개발하도록 권장하는 조치,

[25] 온라인에서 프라이버시 보호 기술의 이용을 촉진하는 조치,

[26] 법과 기준의 위반을 다루고 피해구제에 대한 접근을 보장해 줄 수 있는 효과적인 집행 메커니즘의 이용가능성을 보장해 주는 조치,

[27] 회원국은 이 선언문 목표의 추진정도를 2년 이내에 점검하고, OECD 프라이버시 가이드라인에 기초하여 범세계적 네트워크상에서 개인정보의 보호를 보장하기 위한 추가조치가 필요한지를 평가하기로 동의한다.

더 나아가 OECD는 다음과 같은 행동을 취할 것임을 선언하며,

[28] 범세계적 네트워크상에서 프라이버시를 보호하고 이 선언문의 목표를 달성하기 위한 노력과 경험을 보고하는 효과적인 방법에 관한 회원국들의 정보교환을 지원한다.

[29] 회원국들에 의해서 채택된 상이한 프라이버시 보호 접근방식을 참고하고 회원국들과 민간부문의 경험을 토대로 하여, 범세계적 네트워크와 관련된 OECD 프라이버시 가이드라인의 이행과정에서 제기된 문제점을 점검하고 가이드라인의 이행에 필요한 지침을 제공한다.

[30] 범세계적 네트워크상에서 프라이버시가 보호될 수 있도록 산업과 기업의 활동에 협력한다.

[31] 이 선언문의 목표와 관련하여 프라이버시 보호 분야의 주요 발전 및 문제점을 주기적으로 검토한다.

(후략)

## 2. 2008년 인터넷 경제의 미래에 관한 OECD 장관회의

### 가. 배경

1998년 캐나다 오타와 ‘전자상거래에 관한 장관회의(Ministerial Conference on Electronic Commerce)’ 이후 인터넷 세계는 새로운 기술의 출현, 차세대 네트워크의 도입, 새로운 융합의 진전 등으로 중대한 전환기를 맞이했다. 1998년 이후, OECD는 소비자 보호 가이드라인을 개발하고, 1980년 OECD 프라이버시 가이드라인의 글로벌 네트워크 실질 이행 방안 등 ‘전자상거래에 관한 장관회의’ 후속 조치를 위해 노력했다. 이에 OECD ICCP 위원회가 2005년 ‘인터넷 경제의 미래에 관한 OECD 장관회의’의 첫 배경문서인 ‘인터넷의 미래 확보: 컨버전스와 정책일관성 필요’를 통해 더 나은 미래를 구현하기 위해 인터넷 관련 정책의 일관성을 갖출 필요가 있음을 주지하고 장관회의를 개최할 것을 촉구했다.

OECD는 인터넷의 잠재력을 충분히 인지하고 ‘인터넷의 미래’에 관한 장관급 회의 개최를 결정하고, 2006년 3월 8일 미국 National Science Foundation과 공동으로 프랑스 파리에서 ‘인터넷의 미래(Future of the Internet)’를 주제로 워크숍을 개최했다.

OECD 장관회의 유치 경쟁에는 한국, 포르투갈, 캐나다가 합류하여 경쟁했다. 2006년 10월 2~5일 헝가리 부다페스트에서 열린 OECD 정보통신정책위원회(Committee for Information, Computer and Communication Policy, ICCP)의 51차 정례총회에서 대한민국으로 정하고, 2006년 12월 14일 제1146차 OECD 이사회 총회에서 개최지와 개최 날짜를 최종 결정했다. 1997년 이후 OECD 장관회의는 OECD 본부인 프랑스 파리를 제외하고 8회 개최되었으며, 5회는 유럽지역, 2회는 캐나다, 1회는 중동지역인 요르단에서 개최되어 OECD 장관회의의 지역적 안배와 성공적인 개최를 위해 대한민국으로 결정했다.

2007년 3월 16~17일 제52차 OECD ICCP 위원회 정례총회에서 기존의 OECD ICCP 위원회의 배경 문서의 제목인 ‘인터넷의 미래(The Future of the Internet)’를 인터넷 자체의 미래상이 아니라 인터넷을 기반으로 하는 정치, 경제, 사회, 문화 전반에 대한 인터넷 경제를 논하자는 OECD 회원국들의 요청을 반영하여 ‘인터넷 경제의 미래(The Future of the Internet Economy)’로 변경했다.

<표 2-4> 2008년 전자상거래 OECD 장관회의 개요

구분	내용
기간	2008년 6월 17일~18일
장소	서울 코엑스
주제	미래 경제 성과와 사회복지 향상, 융합에 따른 혜택, 창의성 증진, 신뢰구축 및 글로벌 인터넷 경제
주요행사	개막식 및 개막회의, 라운드 테이블, 전문가 패널 및 정부수석대표회의, 폐막식 각국 장관 및 대표, 비즈니스, 시민단체, 인터넷 기술 전문가 등 70개국 2,278명 참석

[그림 2-1] 인터넷 경제의 미래에 관한 OECD 장관회의 슬로건



나. 주요논의

1) 인터넷을 활용한 혁신을 보여주는 다양한 분야의 사례 논의

에너지 효율을 증진하는 IT 기술을 통해서 친환경 제품의 생산과 유통의 사례를 공유하고, 환경과 IT에 관한 국제 동향 소개 및 협업을 통해 지역적 문제의 해결 사례를 공유했다. 또한, 인터넷의 협동모델이 주는 시너지 효과에 관해 논의하고, 인터넷 상의 혁신 및 창의성 증진이 문화적 테두리에서 발생되고 있음을 확인하고 가치 변화에 대해 논의했다.

## 2) 융합의 혜택에 대한 평가 및 정책 논의

융합의 정의는 기술, 정책, 사회적 함의를 포괄하고 있으며 인터넷 관련된 시장에 대한 자유로운 진입을 의미한다. 온라인상의 소비자의 권익을 신장하면서 시장 경쟁 정책과의 균형적 발전을 동시에 이룰 수 있는 방안을 논의했다. 차세대 네트워크의 개발 및 확충은 인터넷 경제의 기본과제로서 새로운 인터넷 서비스의 도입 및 정착을 위한 제도적 정비, 시골지역으로 확대하기 위한 기간 투자의 유치방안을 논의했다. 네트워크 사업자, 콘텐츠 사업자, 이용자 간의 이익관계를 균형적으로 세울 수 있는 지적재산권과 같은 제도 정비를 추진했다.

## 3) 국제공조

인터넷상의 침해적 행위를 방지하기 위해 각 국 정부 간 협력 체계를 세우고 제도적 정비를 통해 이행할 수 있는 방안을 논의했다. 개발도상국의 인프라 구축, 정보통신 기술교육, 서비스의 호환 등을 위해서 선진국과의 협력적 노력을 지속적으로 추진했다. 또한, 온라인상의 소비자의 권익을 신장하기 위한 소비자 보호시스템 구축 이행방안을 논의했다.

## 4) 개도국의 인터넷 경제의 확충

개발도상국의 인프라 구축, 정보통신 기술교육, 서비스의 호환 등을 위해서 선진국과의 협력적 노력을 지속적으로 추진했다. 인터넷이 대중적 미디어로서 시민 중심의 사회적 연대감을 형성시키고, 문화적 다양성을 증진하며, 시민들의 정치적 참여 기회의 확대에 대한 논의를 진행했다.

## 5) 인터넷 거버넌스

인터넷 주소 고갈의 현황을 정확하게 예측할 수 있도록 하는 자료의 필요성을 확인하고, 각 국가의 입장의 차이를 고려한 다양한 중장기 대책을 논의했다. 인터넷 기술의 호환과 융합을 위해 정부 및 이해관계자 중심의 분권적 노력의 필요성에 대해 논의했다.

<표 2-5> 2008년 인터넷 경제의 미래에 관한 OECD 장관회의 의제

개막 회의	사회적 네트워킹 및 사용자 제작 콘텐츠	
	에너지 효율성과 환경보호	
	IPv4의 재활용과 IPv6 장려	
	인터넷 아키텍처 및 3차원 인터넷 프로젝트	
	국제 공조	
라운드 테이블	경제성과 및 사회복지 향상	인터넷 경제는 미래의 경제 및 사회적 인프라에 핵심적 역할
		글로벌 문제 해결을 위한 인터넷
		차세대 통합 네트워크로 전환에 관련된 주요 정책
	융합의 혜택	융합의 정의
		융합을 위한 정책 환경 조성
		회원국의 융합 환경을 소개
	창의성 증진	창의성에 관한 의견
		ICT 및 인터넷에 기반을 둔 창의적 연구와 혁신
	신뢰의 구축	신뢰 구축을 위한 정책 마련 필요성
		신뢰구축을 위한 국제 공조
		소비자 권리 강화 및 보안문화 구축을 통한 인터넷 신뢰사회 구축
		인터넷 신뢰사회 구축을 위한 보안 문화 구축
	글로벌 인터넷 경제	디지털 격차 해결을 위한 국제협력
		글로벌 인터넷 경제를 위한 국제 협력

다. 개막회의 의제 및 논의

1) 사회적 네트워킹 및 사용자 제작 콘텐츠

인터넷으로 인해 미디어 영역에서는 디지털 기기와 함께 성장한 ‘디지털 네이티브(digital native)’와 ‘프로슈머(prosumer)’가 등장했다. 이들은 기존의 매체가 제공하는 콘텐츠를 수동적으로 소비하지 않고 적극적으로 미디어 콘텐츠를 검색, 소비 및 생산한다. 인터넷을 통해 불특정 다수의 사람들이 동시에 정보를 교환하면서 사람들이 자신의 의사를 직접적으로 표현할 수 있게 됨에 따라 정치문제에도 직접적으로 참여하게 되어 직접 민주주의가 실현되며 권력이 일반시민에게로 이동하고 있다.

## 2) 에너지 효율성과 환경보호

IT를 환경에 접목한 ‘Green IT’는 IT를 활용하여 에너지의 소비를 줄이는 동시에 효율성을 높일 수 있으므로 사회 전반의 에너지 소비 절감에 크게 기여할 수 있다. 에너지 효율을 제고하고 지구 온난화를 해결할 수 있는 IT분야의 기여 방안의 하나로 ‘Green IT’가 추진되고 있다. 친환경 제품의 순 영향(net impact)을 가시화하여 생산자와 소비자가 에너지 효율을 제고하는 활동이나 환경 친화적인 제품을 생산 및 소비하는 것에 대한 동기를 부여한다. 마일리지 제공 등을 통한 동기부여와 이를 통한 환경 친화적인 제품의 생산, 유통 및 구매를 증진한다. 여러 국가에서 ‘Green IT’의 개념을 채택하고 다양한 방법으로 실현하고 있다. 일본이 ‘Green IT Initiative’ 전략을 발표했고, 덴마크는 ‘Green IT Action Plan’을 발표하는 등 많은 나라들이 IT 산업을 신성장 동력으로 보고 있다. IT를 환경에 접목한 ‘Green IT’는 IT를 활용하여 에너지 소비를 줄이는 동시에 효율성을 높일 수 있으므로 사회 전반의 에너지 소비 절감에 크게 기여할 수 있다.

## 3) IPv4의 재활용과 IPv6 장려

정부와 기업은 IPv4에서 IPv6로 이전을 촉진하여 3년 내에 고갈될 인터넷 주소 자원 문제에 적극적으로 대처해야 하며, 직접적이고 장기적 해결책을 제공해야 한다. 당시 유럽집행위원회는 2010년까지 유럽 인터넷 사용자 중 25%는 IPv6에 접속할 수 있어야 한다는 실제적 목표를 설정, 공공서비스와 유력 웹사이트의 IPv6 이전을 앞당기도록 장려했다. 나아가 유럽집행위원회는 국제인터넷주소관리기구(ICANN)에 국제표준도메인명(Internationalized domain name) 도입과 다양성을 인정하는 인터넷 활용을 위한 기회 제공을 지속적으로 역설했다.

## 4) 인터넷 아키텍처 및 3차원 인터넷 프로젝트

모바일 이용률 증가 및 인터넷 이용 주체를 연결하는 애플리케이션의 증가로 인터넷 인프라에 구축되어야 할 효율적인 새로운 아키텍처 솔루션 개발이 시급한 문제로 대두되고 있다. 인터넷은 초당 100메가바이트 데이터 전송률을 염두에 두고 설계한 것이 아

니므로 확장성, 라우팅, 보안 및 신뢰가 당면과제임을 강조했다. 이와 관련하여 비비안 레딩 유럽집행위원회 위원은 ‘미래의 인터넷’에서 시민들의 행복과 기업이 지구촌에 선보일 혁신 잠재력을 그려내는 차원에서 2013년까지 3억 유로를 투자할 계획임을 언급하면서 지구촌의 모든 파트너들이 동참해 줄 것을 요청했다.

## 5) 국제 공조

선진국과 개발도상국 간의 정보통신 격차는 무선 인터넷을 통해 효과적으로 해소할 수 있을 것으로 전망되며, 정보격차의 효과적인 해소를 위해서 정부 간 공조가 필수적이다. 모바일 통신이 빠르게 확산되면서 인터넷을 위한 인프라의 부족 문제를 효과적으로 보완하고 있다. 은행이나 상거래를 위한 인프라가 현격하게 부족한 개발도상국의 사용자들은 무선 인터넷에 의존하는 경향을 보인다.

기술의 발전과 확산을 위해 혁신적인 환경을 조성하는데 있어서 국제 공조가 필요하다. 혁신적인 기업 활동을 증진하기 위해서 기존의 장벽을 허물고 규제의 틀을 보완할 필요성이 있으며, 이러한 노력을 통해 국가 간 투자가 촉진되고 서비스의 호환이 증진될 전망이다. 광대역과 이동성으로 인해 인터넷의 잠재력은 더욱 커지고 있으나, 인터넷의 부정적인 측면들에 적절히 대응하지 못할 경우 이러한 잠재력은 사라지거나 위협 받을 수 있다. 실제로 프라이버시 침해, 저작권 침해 등 악의적인 활동들이 인터넷 환경의 신뢰를 저해할 수 있다. 2007년 봄, 에스토니아 네트워크에 대한 대규모 공격으로 인한 서비스 전송 중단으로 온라인 서비스가 교란되고, 에스토니아 로컬 네트워크가 지구촌 인터넷망으로부터 고립된 것을 계기로 유럽의 각국은 네트워크 공격이 국가경제와 사회구조에 미칠 수 있는 여파에 대해 인식하고 있다.

모든 국가가 상호 네트워크로 연결되어 있다는 점에서 지구촌이 인터넷 공격에 대한 경각심을 높일 필요가 있다. 국가 간의 정치적·경제적 분쟁으로 네트워크에 대한 공격이 벌어질 수 있으므로 지역 간에 정책 및 보안 관련 협력의 틀에서 대처 필요하며, 인터넷의 미래 및 인터넷으로 인해 창출되는 가치를 보호하기 위해 국제적 공조 노력이 필수적이다.

## 라. 라운드테이블 의제 및 논의

### 1) 경제성과 및 사회복지 향상

인터넷 경제는 미래의 경제 및 사회적 인프라에 핵심적 역할을 담당한다. 정부, 교육, 보건, 도로, 항구 및 금융 등 거의 모든 분야에서 정보 통신이 핵심적 기술로서 사용될 것이다. 정보통신기술정책은 공공정책 분야인 노동, 재정, 금융 등과도 연계성을 지니게 된다. 벨기에는 인터넷을 통해서 e-banking, e-health, e-voting 등을 실현하고 있으며, 인터넷 인프라의 무한한 적용가능성을 소개했다. 인터넷 기술을 통해 대 국민 서비스를 향상하고, 시민과 정부의 간격을 줄이고 정부가 국민의 요구에 적절하게 대처할 수 있게 됐다. 일반시민들은 균등한 기회를 갖고 인터넷을 사용하며, 인터넷은 사회 및 경제적 참여 기회 등을 획득하는 대중적 매체로서 역할이 커지고 있다. 이를 통해 인터넷 서비스의 핵심은 시민 중심이라는 원칙을 상기시켰다. 아프리카의 경우, 인터넷을 통해서 연대감을 형성하고 있으며 'Digital Solitary Fund'를 마련하여 기반을 확충하고 있다.

### 2) 글로벌 문제 해결을 위한 인터넷

정보통신기술을 통해 사회적 문제 및 범세계적인 문제를 해결하고 경제적 성과를 달성할 수 있는 방안을 계속적으로 모색해야 한다. 범세계적인 문제에는 다양한 이해관계자가 존재하기 때문에 주요 국가의 정책 관행을 살피고 국가 간의 협력을 도모할 수 있는 노력이 필요하다.

### 3) 차세대 통합 네트워크로 전환에 관련된 주요 정책

가장 기본적인 과제로 VoIP 및 IPTV 등의 인터넷 기반 서비스를 적극적으로 도입하고 인터넷을 국토의 도서, 시골, 산간 지역으로 확대하기 위한 인프라 확충 정책이 근본적인 방안으로 제시됐다. 활발한 투자 및 경쟁이 존재하는 네트워크 시장으로 투자 친화적인 환경을 조성하고 네트워크 사용자에게 대한 서비스를 향상시키며, 소비자 권익 증진도 함께 병행되어야 한다. 인터넷이 지향하는 시장은 독점 혹은 과점이 아닌 경쟁적 시장이

며, 경쟁적 네트워크 시장을 기반으로 서비스 가격을 합리화 하고 새로운 서비스를 도입해야 한다. 정부의 통신 인프라에 대한 규제의 합리화로 시민들이 정부의 정책원리에 대한 정확한 이해를 도모할 수 있도록 하며, 비합리적인 정책에 대한 자유로운 토론을 유도한다.

#### 4) 융합의 혜택

융합이란 단순히 네트워크와 네트워크 간의 통합 뿐 아니라 네트워크를 비롯한 기기 및 서비스들 간 통합의 현상으로 모든 신기술에 대해서 개방적이며, 이러한 기술들 간의 정책적인 융합 및 통합 노력을 비롯하여 기술적 혁명이 아닌 사회적 포괄을 의미한다. 융합과 관련된 어떤 요소가 인터넷의 발달을 가져왔는지 설명하는 것이 중요하다.

따라서 기술적 및 제도적으로 독립적이었던 네트워크를 서로 호환하며 통합하는 차세대 네트워크로 전환하는 등 융합을 위한 정책 환경을 조성해야 한다. 융합의 네트워크에서 모든 사용자가 혜택을 누릴 수 있도록 하는 것이다. 네트워크에 대한 자유로운 접근(access)을 저해하지 않도록 지원하는 장기 정책적 방향을 설정하고, 네트워크 사업자와 콘텐츠 사업자 간 수입 모델의 균형적 발전을 위한 지원이 필요하다. 융합 환경을 반영하여 자유로운 시장 진입을 보장하고, 개방적인 환경을 구축하는 것이 가장 중요하다.

규제 및 모든 관련 제도는 투명해야 하며 투자를 유인할 수 있도록 제도적 정비를 시행해야 한다. 3년 이내에 전 세계적으로 IPv4 주소가 고갈될 것으로 예상되며, IPv6로의 전환 시에 기존의 IPv4와의 호환성 문제가 발생하는 한편, IPv6에 대한 수요가 충분하지 않기 때문에 현재 IPv6에 대한 적극적인 투자가 이루어지고 있지 않고 있다. 이에 IPv4와 IPv6의 공존 상태를 어느 정도 유지하면서 IPv6로의 자연스러운 전환이 필요하며 무엇보다도 IPv4 주소고갈의 상태를 정확하게 파악하는 매우 중요하며 이에 맞추어 분명한 대안을 수립해야 한다.

#### 5) 창의성 증진

창의성은 문화적인 측면에서도 고려해야 하며, 창의성은 혁신을 중요시 여기는 문화의

커다란 테두리에서 발생함을 인지해야 한다. 창의성은 사회에 새로운 가치를 심어주는 행위이며, 도덕적인 측면도 신중하게 고려되어야 개발되어야 한다. 창의성은 일반적인 환경에서는 드러나지 않으며, 좀 더 구체적이고도 유일한 환경에서 발생된다.

ICT를 통해서 정보의 수집과 배포가 용이하게 되었고, 특히 정보의 자유로운 흐름을 가능하게 할 수 있으며, 이는 새로운 아이디어를 찾아내는데 매우 유용한 도구가 되었다. 또한, 네트워크상에 존재하는 수많은 객체들의 협업을 유도하며, 협업을 통해서 작업의 시너지 효과를 기대할 수 있다.

ICT의 접근성 및 지불 능력 확보를 위해 네트워크의 접근을 비롯해 콘텐츠를 확보할 수 있도록 해야 한다. 또한, 공공기관이 보조금 등과 같은 수단을 통해서 대중에게 콘텐츠를 값싸게 제공해야 한다. ICT 활용을 통해서 민족, 언어 및 종교의 다양성 유지에 기여해야 하며, 개인이 속한 커뮤니티가 매우 중요하며, 이러한 커뮤니티를 기반으로 새로운 아이디어와 혁신적 요소가 창출된다. ICT를 통해 경제의 지속적 발전을 도모해야 하며, 특히 민간 부문과 연계하여 지속적 발전을 도모하여야 한다. 아일랜드의 경우 210개의 다국적 ICT 기업 및 660개의 아일랜드 기업이 경제의 지속적 발전에 기여하고 있다.

환경의 보호는 경제의 지속적 발전에서 중요한 요소이며 정보통신기술이 환경보호에 크게 기여할 수 있다. 인터넷을 활용하여 기후 변화 문제를 해결하는 등 정보통신산업이 좀 더 환경 친화적으로 변화되는 것이 요구된다. 유럽의 북해 국가들은 원격 화상회의를 통해서 이산화탄소의 방출량을 실제로 줄인 경험이 있다. 정부는 창의라는 가치를 직접적으로 창출하지는 않지만 하나의 모델을 제시하는 역할을 담당할 수 있는 것이다.

인터넷이 개방적 플랫폼으로 되기 위해서는 정부의 역할이 중요하며, 정부는 친환경 기업에 대한 동기를 부여하여 기업의 혁신 모델을 유도하여야 한다. 한국의 ‘다음(Daum)’ 사례를 살펴보면, Daum은 한메일 및 카페 서비스를 통해서 국내 최대의 포털 사이트로 성장한 사례로서 웹에서 객체들의 협동이 어떤 방식으로 일어나는지에 대한 탐구적 선택을 만들었다. 글로벌 뉴스는 모든 사람이 기자가 되어서 실제 정보를 전 세계 지역으로부터 지원받아서 운영되며, 하루에 65,000명이 약 3,000개의 콘텐츠를 제공하고 있다. ICT는 인구 문제의 해결에도 이바지하고, 고령화 사회와 관련하여 정보통신 부문에 여

성 인력들이 참여할 것을 촉구하고 있다.

## 6) 신뢰의 구축

인터넷은 개방성, 익명성, 글로벌성(global reach), 그리고 유비쿼터스 속성을 가지고 있다. 인터넷의 이러한 장점으로 인터넷이 벽촌 주민부터 대규모의 글로벌 기업까지 인류의 삶의 질을 향상시킨다는 것에 대해 인터넷 보급 수준이 각기 다른 나라 대표, 인터넷 기술 전문가 및 모든 이해관계자들이 공감대를 형성하게 되었다. 그러나 이러한 인터넷의 속성으로 인터넷이 사고나 유해환경에 취약하고, 인터넷으로 이루어지는 경제 및 사회적 활동이 증가하는 만큼 그 위험도 증가하고 있다.

스팸, 프라이버시, 악성 소프트웨어, 디지털 신원관리, 소비자 보호 등과 같은 인터넷의 위험요소들이 점점 심화되고 복잡해지고 있으며, 이러한 유해 환경으로부터 소비자의 권익을 강화시키고, 인터넷의 악의적 이용 및 남용으로부터 청소년을 보호하는 것이 중요하다고 강조되고 있다. 지속적으로 정보 보안 문화에 대한 콘텐츠와 정책을 개발해야 하며, OECD 이사회 권고안에서 촉구된 바와 같이 핵심정보인프라를 보호하는 것도 중요하다. 인터넷이 경제의 촉진제로서의 역할을 하기 위해서는 신뢰 구축이 우선되어야 하고, 다양한 이해관계자간 협력을 통한 인터넷상의 신뢰 구축 필요성에 대해 모든 이해당사자들이 동의하고 있다. 인터넷으로 인한 혜택을 모든 국가가 누리듯이 그 어느 국가도 인터넷의 신뢰 보장에 관한 도전과제에서 자유로울 수 없다.

이에 인터넷의 신뢰성을 위협하는 요소들에 효과적으로 대처하고 스팸, 악성소프트웨어, 프라이버시 및 소비자 보호 등의 문제해결을 위해서는 국제공조 체제를 구축하여야 한다. OECD를 비롯한 아태경제협력체(Asia Pacific Economic Cooperation, APEC) 외 국제전기통신연합(International Telecom Union, ITU)에서도 인터넷의 신뢰성과 관련된 국제공조에 강력하게 지지했다. 유럽평의회(COE) 사무차장은 ‘사이버 범죄 협약(Convention on Cybercrime)’ 체결과 같은 공식적인 방법으로 사이버 위협에 공동으로 대처할 것을 주문했다. 프라이버시와 보안문제는 단순한 기술 범죄가 아니라 인권, 민주주의, 법치주의, 신뢰 일체가 포함된 복잡한 사안이며, 한 국가만으로는 대처가 어려우므로 국가 간

의 공조가 필요하다. 국제소비자보호집행기구 네트워크(International Consumer Protection Enforcement Network)나 런던액션플랜(London Action Plan)과 같은 비공식적인 방법 및 각국의 신뢰 구축과 사이버 테러, 국가 안보, 개인의 자유보장 사례를 공유하는 데 동의했다.

인터넷이 많은 사람들에게 교육, 정보, 정치, 의료 등의 분야에서 상당한 기여를 하고 있는 오늘날, 사용자가 인터넷을 신뢰하고 위협으로부터 보호를 받을 수 있어야 한다. 인터넷에는 국경이 없으므로 온라인에서도 오프라인과 같은 수준의 소비자 보호 시스템 구축이 필요하며 이를 위한 법안이 신속히 마련되어야 한다.

인터넷은 현대의 일상생활에서 매우 중요하기 때문에 인터넷에 접속하지 못하게 하는 것은 개인을 시민사회로부터 단절하는 것과 같으며, 이에 프라이버시, 지적재산권을 보호하면서 미성년자 보호 및 개발도상국의 문맹 퇴치에 노력할 필요가 있다. 노인과 어린이의 인터넷 사용의 습득 및 용도가 매우 다르기 때문에 소프트웨어나 기기를 개발하는 부문에서 현재 안고 있는 정보통신기기 문맹퇴치에 대한 난제를 극복할 수 있도록 처음 설계 단계부터 각각의 개별 상황에 대처할 수 있도록 만들어져야 한다.

인터넷 신뢰사회 구축을 위하여 보안에 대한 인지도를 높여야 하며, 이 과정에서 인적 요소를 간과하지 않도록 유의해야 한다. 보안 문화를 위해 국가 간의 협력은 물론이고 전에는 협력하지 않았던 이해당사자들과의 협력도 필요하다.

## 7) 글로벌 인터넷 경제

다양한 방법으로 인터넷 접근이 가능해지고 있으며, 인터넷은 생산의 방식을 바꿨으며, 인터넷 사용 방식이 바뀌어가면서 새로운 모델이 탄생하고 있다. 특히 엔터테인먼트 부분(동영상, 음악을 전 세계로 유통)의 사이버 시장이 구축되고 많은 사람들이 저가의 인터넷 광고와 거래를 통해서 매출에 기여하고 있으며 주문형 마케팅이 가능케 되었다. 인터넷 경제는 개도국에 큰 기회를 가져다 줄 것이며 지식의 생산, 접근 등을 완전히 바꿀 수 있으나, 이 모든 것은 인터넷 접속이 가능한지 여부에 따라 좌우될 수 있다. 참가자들은 이제 정보격차는 극복할 수 있으며, 광대역격차를 극복하는 게 중요하다고 강조

했다. 이를 극복하기 위해서는 민간투자와 공공분야의 공동노력이 필요하며, 협력을 바탕으로 개선이 이뤄지면 ICT 분야가 발전할 것이라고 기대했다. 이를 위해서는 정책결정과정에서 여러 분야의 이해관계자들이 참여해야 하며, 중요한 이해 당사자들은 정부, 기술전문가, 시민단체로 확장된 인터넷의 신뢰를 보장해야 한다.

<표 2-6> 정보통신분야 OECD 선언문, 권고, 지침, 정책원칙 등 현황

연도	명칭	비고
1980	프라이버시 보호 및 개인데이터의 국경간 유통에 관한 OECD 지침(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)	
1985	국경간 데이터 유통에 관한 OECD 선언문(OECD Declaration on Transborder Data Flows)	
1992	정보시스템 보안에 관한 OECD 지침(OECD Guidelines for the Security of Information Systems)	2002년 개정
1997	암호정책 지침에 관한 OECD 이사회 권고(OECD Recommendation of the Council concerning Guidelines for Cryptography Policy)	
1998	전자상거래를 위한 인증에 관한 OECD 장관선언문(OECD Ministerial Declaration on Authentication for Electronic Commerce)	전자상거래에 관한 OECD 장관회의에서 채택
1998	범세계적 네트워크에 있어서의 프라이버시 보호에 관한 OECD 장관선언문(OECD Ministerial Declaration on the Protection of Privacy on Global Networks)	오타와 장관회의에서 채택
1998	전자상거래를 위한 OECD 행동계획	오타와 장관회의
1999	전자상거래에 있어서의 소비자 보호를 위한 OECD 지침 (OECD Guidelines for Consumer Protection in the Context of Electronic Commerce)	
2002	정보시스템 및 네트워크 보안에 관한 OECD 지침: 보안 문화를 향하여(OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security)	1992년 지침의 개정
2002	온라인 프라이버시: 정책 및 실제에 관한 OECD 지침 (Privacy Online: OECD Guidance on Policy and Practice)	
2003	국경간 상거래의 사기 및 기망으로부터의 소비자 보호를 위한 OECD 지침(OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders)	

연도	명칭	비고
2004	브로드밴드 개발에 관한 OECD 이사회 권고(OECD Recommendation of the Council on Broadband Development)	
2006	<ul style="list-style-type: none"> <li>▪ OECD 스팸방지 정책 및 조치 권고 툴킷(OECD Anti-Spam Toolkit of Recommended Policies and Measures)</li> <li>▪ 스팸방지법 집행에 있어서의 국경간 협력에 관한 OECD 권고(OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam)</li> </ul>	
2007	전자인증에 관한 OECD 권고 및 전자인증에 관한 OECD 지침(OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication)	
2007	프라이버시 보호법 집행에 있어서의 국경간 협력에 관한 OECD 권고(OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy)	
2007	소비자 분쟁해결 및 피해보상에 관한 OECD 이사회 권고(OECD Recommendation of the Council on Consumer Dispute Resolution and Redress)	
2008	인터넷경제의 미래를 위한 서울 선언문(The Seoul Declaration for the Future of the Internet Economy)	
2008	CII 보호정책에 관한 이사회 권고안(Recommendation of the OECD Council on the protection of critical information infrastructures)	
2008	공공분야 정보의 접근확대와 효과적인 활용을 위한 이사회 권고안(Recommendation of the OECD Council for enhanced access and more effective use of public sector information)	
2010	ICT와 환경에 관한 OECD 이사회 권고(OECD Recommendation of the Council on ICT and Environment)	

<표 2-7> 인터넷 경제의 미래를 위한 서울선언문

(전략)

우리는 인터넷 및 관련 정보통신기술에 의해 경제, 사회 및 문화 전 영역의 활동을 망라하는 인터넷 경제가 다음과 같은 기능을 통하여 모든 시민의 삶의 질을 제고시킬 우리의 역량을 강화할 것이라는 비전을 공유한다.

- o 고용, 생산성, 교육, 의료 및 공공 서비스 분야에서 새로운 기회를 제공하고 환경 및 인구 문제를 해결한다.

- 기업과 공동체를 형성하는 주요 원동력으로서의 역할을 하며, 보다 긴밀한 글로벌 협력을 도모한다.
  - 시민 참여에 있어서 의견의 다양성을 증진하고 투명성, 책임의식, 프라이버시 및 신뢰를 제고하는 새로운 형태를 가능케 한다.
  - 온라인 상거래 소비자 및 사용자의 권리를 강화한다.
  - 정보 시스템, 네트워크와 그 사용자들에 적용되는 보안문화 의식을 보강한다.
  - 다양한 부문에서 연구, 국제적 과학협력, 창의성 및 혁신을 위해 주요 플랫폼을 개발한다.
  - 언제 어디서나 정보통신 네트워크에 끊임 없이 접속할 수 있도록 함으로써 새로운 경제 및 사회 활동, 애플리케이션과 서비스를 위한 기회를 창출한다.
  - 수십억 인구, 기계 및 개체를 연결하는, 빠르고, 안전하며, 언제 어디서나 접속 가능한 네트워크에 기반을 두는 글로벌 정보사회를 증진한다.
- 우리는 법, 정책, 자율 규제 및 소비자 권리 강화 간의 적절한 균형을 통하여 다음 과제를 추진할 것을 합의한다.
- 인터넷 접속 및 활용을 전세계로 확산시킨다.
  - 인터넷 기반의 혁신, 경쟁, 그리고 사용자의 선택권을 향상시킨다.
  - 핵심정보인프라를 보호하며 새롭게 대두되는 위협에 대응한다.
  - 온라인환경에서의 개인 정보를 확실히 보호한다.
  - 지적재산권에 대한 중요성을 분명히 인식한다.
  - 개개인, 특히 소외계층과 기타 취약 집단을 보호하는 신뢰할 수 있는 인터넷 기반 환경을 보장한다.
  - 국제적 사회·윤리 규범을 중시하고 투명성과 책임의식을 제고하는 안전하고 책임 있는 인터넷의 사용을 장려한다.
  - 인프라 투자, 초고속 접속, 그리고 혁신적 서비스 및 애플리케이션 개발을 장려하는 융합에 대하여 시장 친화적인 환경을 조성한다.

우리는 인터넷 경제의 발전에 기여하기 위하여 다음의 사항들을 추진할 것을 선언한다.

- a) 다음과 같은 정책을 통해 디지털 네트워크, 기기, 애플리케이션 및 서비스의 융합을 촉진한다.
  - 공정 경쟁을 보장하는 규제 환경을 조성한다.
  - 인터넷의 개방성, 분권화, 역동성이라는 속성과 이의 지속적인 확대를 가능케 하고 혁신, 호환성, 참여 및 접근의 용이성에 기여하는 기술 표준의 개발을 지지한다.
- 대용량 정보 및 통신 인프라의 개발과 국내 및 국경간 인터넷을 통한 서비스의 제공을 위하여 투자와 경쟁을 장려한다.
- 브로드밴드 네트워크 및 서비스가 각국의 실질적인 보급범위와 이용의 극대화를 달성하도록 개발되어야 한다.
- 공공의 목적을 고려하면서 인터넷 접속과 새롭고 혁신적인 서비스의 도입을 활성화하기 위하여 보다 효율적인 주파수 이용을 장려한다.
- 현재의 지속적인 IPv4 주소자원의 고갈을 감안하여, 특히 민간부문의 IPv4 주소 대량이용자들뿐만 아니라 정부 또한 새로운 단계의 인터넷 프로토콜인 IPv6를 시의 적절하게 채택함으로써

써 이의 도입을 장려한다.

o 인터넷 애플리케이션, 단말기, 그리고 콘텐츠에의 연결, 접근 및 사용에 있어서의 선택권과 서비스 품질과 비용에 대한 명확하고 정확한 정보를 제공하여 소비자와 기업이 융합의 혜택을 누릴 수 있도록 보장한다.

b) 다음과 같은 정책을 통해 인터넷의 발전, 활용 및 적용에 있어서의 창의성을 증진한다.

o 정보의 자유로운 유통, 연구, 혁신, 기업가 정신 및 기업혁신을 장려하는 개방적인 환경을 유지한다.

o 과학 관련 데이터 및 문화 유산에 대한 작업 등의 공공부문 정보와 콘텐츠를 디지털화하여 더욱 폭넓게 접근할 수 있도록 한다.

o 인터넷 및 관련 정보통신기술에 대한 기초 및 응용 연구를 장려한다.

o 대학, 정부, 공공 연구기관, 사용자와 기업이 혁신적인 협업 네트워크를 통해 공조하고, 실험적인 인터넷 설비를 공유하여 활용하도록 장려한다.

o 콘텐츠 제작자와 저작권자가 창작물을 생성, 유통하는 과정에서 그 혜택이 제작자와 사용자 및 경제 전반에 돌아갈 수 있도록 동기를 부여하는 혁신적인 접근방식으로 디지털 무단복제 근절을 위한 공동의 노력을 기울인다.

o 디지털 콘텐츠의 제작, 배포 및 활용에 있어서 제작자의 권리와 사용자의 이익을 충분히 인정하는 새로운 협업 모델과 사회적 네트워크를 장려한다.

o 인터넷과 연관된 정보통신기술을 충분히 활용하고, 나아가 정보통신기술과 디지털 및 미디어에 대한 이해도를 더욱 배양할 수 있도록 인력양성을 강화한다.

c) 다음과 같은 정책을 통해 신뢰성 및 보안을 강화한다.

o 국내외 핵심정보인프라를 보안 위협으로부터 보호한다.

o 우리 경제 및 사회의 증대되는 수요와 필요를 충족하기 위하여 인터넷, 관련 정보통신 시스템 및 기기의 복원력과 보안성을 강화한다.

o 모든 이해당사자들이 예방, 보호, 정보 공유, 대응, 영업 지속성 및 회복을 위해 나아가는 단계로서 국내 및 국제적인 공조를 통하여 온라인상의 악의적인 활동을 줄인다.

o 디지털 신원 및 개인정보 보호와 온라인상의 개인 프라이버시가 확보되어야 한다.

o 효율적인 소비자 보호체계를 구축하고 온라인 상거래에서 야기되는 경제적 손해에 대해 적절하게 배상하는 등 공정하고, 접근하기 용이하며, 효율적인 분쟁 해결 절차의 실질적인 접근을 통하여 소비자들이 혜택을 받을 수 있도록 해야 한다.

o 인터넷을 사용하는 미성년자들을 보호하고 지원하기 위해 인터넷이 미성년자에게 미치는 영향에 대한 이해도를 높이는데 있어 정부, 민간부문, 시민단체 및 인터넷 기술 전문가 집단이 협력을 증진한다.

o 새롭게 대두되는 보안 위협을 해결하기 위한 연구를 장려한다.

d) 다음과 같은 정책을 통해 진정한 글로벌 인터넷 경제가 이루어질 수 있도록 보장한다.

o 인터넷 및 관련 정보통신기술에 대한 폭넓은 접근 기회가 특히 개발도상국 국민들에게 보다 많이 주어질 수 있도록 지원한다.

- 인터넷 및 관련 정보통신기술이 장애인 및 특별한 도움이 필요한 사람들에게 보다 나은 서비스를 제공할 수 있다는 잠재력을 인식한다.
- 인터넷 경제의 성공적인 성장을 도모하고 이를 통해서 특히 경제적 여건이 열악한 지역 및 주민에게 발전의 기회를 제공하기 위해서는 경쟁적인 환경이 중요하다는 점을 인식한다.
- 능력, 교육, 기술 수준이 상이한 사람들을 사회 및 경제적으로 더욱 폭넓게 포용하고 문화와 언어의 다양성을 보존하기 위해 고유의 콘텐츠 제작과 다국어 번역을 촉진하고 모든 공동체가 인터넷 및 관련 정보통신기술 네트워크를 사용하도록 장려한다.
- 인터넷의 무결성 및 안정성을 보장하는 동시에 다국어 도메인 이름의 도입을 촉진한다.
- 사이버 보안 증진, 스팸 근절, 프라이버시 및 소비자 및 미성년자 보호를 위하여 관련 분야에서 정부와 법 집행 당국의 국가간 협력을 증진한다.
- 에너지 효율 제고, 기후변화 대처 등 글로벌 도전과제를 해결하기 위해 인터넷의 잠재력을 활용한다.

우리는 OECD 정책권고문인 「인터넷 경제의 미래를 위한 정책 형성」을 환영하고, 그 중요성을 인식하며, OECD 회원국 및 비회원국이 인터넷 경제에 대한 정책 개발 시 이를 고려하는 것은 매우 바람직하다.

우리는 모든 이해관계자들과 협력하여 우리 경제와 사회가 직면하는 미래의 도전과제 및 기회와 본 선언문의 연관성을 유지하기 위하여, 우리가 본 선언문에서 도달한 결정을 이행하고 또한 적절하게 검토할 것을 약속한다.

우리는 OECD가 본 선언문에 명시된 목표를 다양한 이해관계자들과 협력하여 다음과 같이 발전시키기를 바란다.

- 인터넷 경제의 미래 발전상 즉, i) 혁신과 생산성, 그리고 경제 성장의 원동력으로서 인터넷 및 관련 정보통신기술이 맡고 있는 중요한 역할과 공헌, ii) 가상 세계, 센서 기반 네트워크 및 사회적 네트워킹 플랫폼과 같은 최신 인터넷 기술, 애플리케이션 및 서비스가 경제·사회·문화에 미치는 영향 등을 분석한다.
- 이러한 분석을 바탕으로 인터넷 경제의 미래 발전을 위한 정책, 규제 원칙, 지침, 기타 방안, 모범 사례를 개발하고 발전시킨다.
- 인터넷 및 관련 정보통신기술이 기후변화에 대처하고 에너지 효율을 증진하는데 미치는 영향을 연구한다.
- 인터넷 보안 및 안정성에 대한 위협 근절, 국가간 교류 증진, 정보 접근성 확대와 같은 영역에서 인터넷 경제의 정책 목표를 달성하기 위해 중재자를 포함한 여러 당사자들의 역할을 검토한다.
- 인터넷의 사용 행태 변화 및 경제 성과와 사회 복지에 미치는 영향에 대해 신뢰할 수 있는 척도를 마련하고, 시민과 기업, 그리고 관련 기관이 인터넷 및 관련 정보통신기술 네트워크, 접속, 사용 행태의 변화를 측정하기 위한 통계 시스템을 개선한다.
- 기술, 시장, 이용자의 사용 행태가 변화하고 디지털 신원의 중요성이 점차 증대하고 있다는 점을 감안하여, 현재 OECD가 소비자 보호 및 권리 강화, 개인 프라이버시와 보안 개선을 위해 취하고 있는 방안을 평가한다.

- 융합된 통신 네트워크의 개발 및 이용을 위한 정책 입안시, 지침이 되는 ○ ECD의 방안을 개발할 것을 권고한다.
- 전자 정부 및 공공부문 개혁과 관련된 도전과제와 모범 사례를 검토하기 위하여 여러 전문 분야간 연구를 계속한다.
- 보다 효율적인 국가 간 협력을 위한 방안과 메커니즘을 지원한다.
- 본 선언문과 OECD 정책권고문인 「인터넷 경제의 미래를 위한 정책 형성」을 G8, 국제전기통신연합(ITU), 세계지적재산권기구(WIPO), 국제연합교육과학문화기구(UNESCO) 등 모든 유관 국제 단체 및 국제기구에 배부한다.
- 아시아-태평양 경제협력체(APEC), 유럽평의회(Council of Europe), 그리고 인터넷 거버넌스 포럼(IGF)과 같은 인터넷 기술 전문가 집단, 민간부문, 시민단체들과 협력적인 관계와 상호 공조를 강화한다.
- 본 선언문 채택 후 3년 이내, 그리고 그 이후에도 필요 시 본 선언문과 관련하여 국가 및 국제적 단계에서 이루어진 발전사항을 검토한다.

## 제 2 절 런던 사이버스페이스 총회 주요 의제 분석

### 1. 2011년 런던 사이버스페이스 총회 개요

#### 가. 배경

사이버공간의 기술진보는 인류의 생활방식을 혁명적으로 변화시켰으며, 사이버공간의 발달로 인한 전 지구적 차원의 네트워크 사회 출현은 커다란 경제적·사회적 기회와 혜택을 제공한 동시에 도전과 위협을 야기하고 있다. 2011년 런던 사이버스페이스 총회는 전 세계적으로 급격히 발전하고 있는 네트워크 시대에 사이버공간의 주요 행위자들이 참여하는 포괄적 대화 기회제공과 사이버공간 발전에 따른 기회를 보장·관리하기 위한 대책을 강구하기 위해 개최했다.

사이버공간의 중요성이 증가함에 따라 사이버 범죄도 증가하고 있는 시점에서 전세계 사용자들이 직·간접적으로 참여하여 논의하는 장을 마련한 것이다. 사이버공간에 대한 의존도가 점증하고 있는 현실에서 사이버공간에서의 허용 또는 금지되는 행동에 대한 시급한 합의 도출이 회의 개최의 궁극적 목적이다. 2011년 2월, 뮌헨안보회의 당시 영국 헤이그 외교장관은 2011년 7월 60여 개국에 ‘사이버공간에 관한 런던 회의’ 초청장을 발송했으며, 전 세계 네티즌들을 대상으로 트위터와 페이스북 등 소셜미디어를 통해 의견이나 질문을 받고, 사전에 선별된 의견과 질문은 회의기간 중 발표하고 의제에 반영했다.

<표 2-8> 2011년 런던 사이버스페이스 총회 개요

구분	내용
기간	2011년 11월 1일~2일
장소	Queen Elizabeth II Conference Center
주제	사이버공간에서 허용 가능한 행동 규범
참석자	정부(60개국) 및 국제기구(에스토니아 대통령, 불가리아 부총리, 네덜란드·스웨덴 외교장관, 인도 통신장관, 보츠와나 법무장관, ITU 사무총장, UNDP 총재, 세계은행 부총재 등), 재계·학계·민간단체(위키피디아 공동창업자, ICANN(도메인관리기구) 회장, 페이스북 부회장, 마이크로소프트 부회장 등)

## 나. 주요논의

모든 인터넷은 미래에 대해 긍정적인 전망을 지원하는 반면, 다양한 방법으로 그것의 잠재력에 도달하는 것을 방해받을 우려가 있다. 주변을 제한하거나 제한된 인터넷 액세스와 범죄자와 국가 행위자에 의한 디지털 네트워크의 악의적인 사용 증가에 대한 우려가 그것이다. 디지털 시대의 장점은 세계의 모든 민족과 경제로 확장되는 미래를 지원하는 것과 사이버스페이스와 관련한 책임을 세계적으로 공유할 수 있다는 것이다.

런던 컨퍼런스에서 등장한 공통의 목표는 정부의 통제 혹은 검열에 의해 억제당하지 않고, 혁신과 경쟁이 번창하고, 투자와 기업이 보장되는 사이버 공간의 형성이다. 이를 위해 정부, 산업, 인터넷 이용자의 책임의 균형을 확립하고 공동의 노력으로 함께 작동하는 인터넷 지배구조에 대한 모델을 형성하였다. 이번 회의에서는 주요 안건으로 경제적 혜택 및 개발, 사회적 혜택, 사이버 범죄, 안전하고 신뢰 가능한 접속 보장, 국제안보 등 모두 5가지 이슈가 대두됐다.

첫 번째 이슈 ‘경제적 혜택 및 개발’ 논의에서는 지적재산권 보호, 정부 규제 對 자율 규제, 동 분야 국제규범 및 원칙 등이 세부 의제로 제시됐다. 두 번째 이슈 ‘사회적 혜택’ 논의에서는 다양성 보장 및 표현의 자유, 정부와 민간의 책임과 균형점, 인터넷 필터링과 사이트 차단이 정당화되는 경우, 인터넷을 통한 정부와 시민 간 협력, 동 분야 국제규범 및 원칙 등이 세부 의제로 제시됐다. 세 번째 이슈 ‘사이버 범죄’ 논의에서는 사이버 범죄 심각성, 사법집행, 사경공조 조약 등이 세부의제로 제시됐다. 네 번째 이슈 ‘안전하고 신뢰 가능한 접속 보장’ 논의에서는 아동보호, 사이버 괴롭힘, 사이버스토킹 등을 비롯해 규제와 자기 규제간 올바른 균형, 개인정보보호 및 프라이버시 문제, 대중의 위험 인식 및 교육, 동 분야 국제규범 및 원칙 등이 세부의제로 제시됐다. 다섯 번째 이슈 ‘국제안보’ 논의에서는 사이버 사건으로 인한 위기, 공격 근원지 확인 문제, 기존 국제법의 효율성, 동 분야 국제규범 및 원칙 등이 세부의제로 제시됐다.

런던 사이버스페이스 총회 결과 발표된 의장성명은 세부의제별 주요 논의내용과 함께 향후 방향을 제시하고 있다. 제1차 총회에서는 인터넷을 통한 공정하고 지속가능한 성장 유도, 정보에 대한 접근과 의견의 교환, 혁신과 투자의 촉진, 소외집단의 사회 및 경제활

동에 대한 참여의 증대 등의 잠재적 혜택이 기대됨과 동시에 네트워크로 연결된 세계는 이러한 잠재적 혜택을 침해할 수 있는 심각한 도전과 위협을 야기하고, 모두에게 영향을 미치고 있다는 사실에 주목했다. 또한 안전한 디지털 환경은 정부 단독으로 조성될 수 없으며, 전 세계 시민사회, 산업계의 이해가 반영되어야 한다고 보았다. 하지만 이러한 위협에 대응하는 과정에서 보안문제 개선을 명목으로 기본적인 인권 침해가 발생해서는 안 된다는 입장이었다.

2011년 초 사이버공간에서의 정부조치에 관한 7개 원칙을 제안한 바 있다. 7개 원칙을 살펴보면, 첫째, 정부는 사이버공간에서 국제법에 준하여 행동해야 하며, 둘째, 능력, 기술, 신뢰, 기회 측면에서 사이버공간에 접근할 수 있는 능력을 모두가 가지고 있어야 하며, 셋째, 사이버 공간의 이용자들이 언어, 문화, 사고의 다양성에 대한 존중과 관용을 보여야한다는 것이다. 넷째, 사이버공간이 혁신과 사고, 정보 및 표현의 자유로운 흐름에 대해 개방적인 상태를 유지하도록 해야 하며, 다섯째, 사생활에 대한 개인의 권리를 존중하고 지식재산에 대한 적절한 보호조치를 취해야하고, 여섯째, 온라인상의 범죄위협에 대해 모두가 공동으로 대응해야 하며, 끝으로 네트워크, 서비스 및 콘텐츠 투자에 대한 공정한 수익이 보장되는 경쟁적인 환경이 촉진되어야 한다는 것이다.

런던회의는 이들 원칙에 대한 보다 심도 있는 논의와 추가 작업이 필요한 의제를 설정하는 출발점으로, 이들 의제들이 성공적인 결과를 낳기 위해서는 런던회의에서 논의된 동반관계(partnership)가 기반이 되어야함을 강조했다. 또한 안전하고, 활력 있고, 신뢰할 수 있는 글로벌 디지털 환경을 조성하기 위해서는 동반관계가 비배제적, 협력적 및 공동의 노력이 지속되는 것을 바탕으로 이루어져야 함을 지적했다.

이번 회의의 여러 이슈 가운데 핵심 의제로 떠오른 ‘사이버 안보’와 관련한 국가 간 갈등 예방 문제에 대해 대부분의 국가는 사이버 공간의 불투명성에 대해 공감하고 신뢰구축 수단에 한계에 있음을 동의했다. 또한 이해관계가 달라 대립각을 세웠던 영국과 미국, 러시아와 중국 간의 대립 양상이 표면화되지 않았다. 주최국인 영국을 비롯해 이들 국가들은 글로벌 규범의 필요성을 인식하고, 이를 도출하기 위해서 대화와 협력의 중요성을 강조했다.

## 2. 런던 사이버스페이스 총회 주요 논의내용

### 가. 경제성장 및 발전

런던회의는 크게 5개 주제를 심도 있게 다루었는데, 경제 성장 및 발전, 사회적 이익, 안전하고 신뢰할 수 있는 환경, 국가 간의 보안문제, 사이버 범죄 등이 이에 포함된다.

우선 경제 성장 및 발전 주제는 세계경제의 성장과 발전을 위해 사이버공간의 이익을 안전하게 달성할 수 있는 방법, 지식재산의 보호와 활용, 혁신 및 시장창출간의 균형유지 방법, 규제와 재정정책의 투명성 및 예측 가능성 보장과 기술발전에 대한 적응 방법, 정부규제와 산업 자율규제, 향후 진전방안, 국가간 분쟁 방지 및 관리 방안 등의 내용을 담고 있다. 경제성장의 엔진과 촉진제로서 인터넷의 핵심적 역할 특히, 개도국에서의 역할, 폭넓은 집단 간의 사이버공간상의 기회 공유, 사이버공간의 안전성과 신뢰성 확보의 중요성에 공감하고, 네트워크, 서비스, 콘텐츠에 대한 투자를 촉진하고 공정한 수익을 보장받을 수 있는 경쟁 환경과 성과물 보호를 강력하게 지지하였다. 동시에 정부와 상업적 검열로부터의 사이버공간의 자유를 강조하고, 투명한 정책수립, 표준개발 및 규제절차 등을 통한 자유롭고 공정한 경쟁에 대해 지지하였으며, 사이버공간상의 무역에 대한 불필요한 장벽 제거를 요구하였다. 한편, 2011년 6월 OECD의 인터넷정책수립 원칙과 같은 인터넷 및 성장에 관한 기존의 노력에 관심을 가지고 관련 노력에 모든 이해당사자의 참여가 중요하다고 지적하였다. ICT 개발 지원을 통한 정보격차 감축 글로벌 노력을 요구하고, 인터넷의 MDGs 달성을 위한 역할을 환영하였으며, 개방적이고 경쟁적인 시장이 핵심임을 강조하였다.

이와 관련해 중국은 지적재산권 침해 방지를 위하여 검열 메커니즘을 운영하고 있으며, e-commerce 활성화를 위하여 공급자와 구매자간 신뢰 형성이 필요하다는 의견을 제시했다. 러시아 전기통신연합은 인터넷을 통한 경제성장을 위하여 개인 정보 접근의 자유와 공익 간 균형을 이룰 수 있는 다중이해관계자가 참여하는 입법이 필요하다는 의견을 제시했다. 네덜란드 외교부는 인터넷의 개방성, 창조성이 기존 경제활동의 혁신을 가능하게 하여 경제를 번영·촉진시키지만, 사이버 공간상 권리침해에 대응하기 위하여 정

부와 시민사회가 책임을 공유하는 공동의 노력이 필요하다는 의견을 제시했다.

#### 나. 사회적 혜택

사회적 이익과 관련한 주제는 지식의 권능과 정부 서비스에 의한 잠재이익 극대화 방안, 민주주의에 대한 신뢰와 표현의 자유 강화를 위한 방안, 정부의 개입효과 극대화 방안, 사회면의 부정적 영향 대응방안 등의 내용을 다루었다. 인터넷으로 인한 긍정적이고 전환적인 사회적 이익에 공감하였으며, 특히, 사회적 매체로서 표현과 결사의 자유에 대한 기여를 환영하고, 청년층 참여의 중요성 강조하였다. 또한 사이버상의 보안을 강화하기 위해 인권이 희생되어서는 안된다는 점에 합의하였으며, 사이버공간상의 이익과 자유보장을 극대화하기 위해 정부뿐만 아니라 업계와 시민사회의 참여가 필요하다고 지적했다. 그리고 빠른 기술발전 속도를 고려하고 인터넷의 역동성을 반영하기 위해서 투명하고 안정적인 자율규제체제를 최적의 기반으로 고려하였다. 사이버공간의 이용자들은 언어, 문화 및 사고의 다양성을 존중하고 관용성을 보여야 한다는 원칙에도 강력한 지지를 표명하였다. 한편, 이러한 원칙이 표현과 결사의 자유에 대한 억압을 은폐하는 수단이나 인터넷의 분리주의 주장의 수단으로 악용되어서는 안된다는 점을 강조했다.

이에 대해 영국은 새로운 서비스를 통해 실시간으로 시민의 정책 관심도 및 의지를 파악할 수 있고, 사이버 공간을 통한 민·관 상호작용은 정부조직을 유연하게 만들 수 있다는 의견을 제시했다. EC는 E-house를 추진할 예정이라고 밝히고, ICT를 통한 사회적 혜택을 늘리는 방안에 대해 시민단체, 민간사업자 및 수혜자가 공동으로 협력해야 한다고 제안했다. 에스토니아는 정부 정책의 개방성 및 책임성을 확보하여 부패를 줄여야 한다는 의견을 제시했다.

#### 다. 안전하고 신뢰 가능한 접속 보장

사이버공간에 대한 안전하고 신뢰할 수 있는 접근 보장방안, 안전하고 신뢰할 수 있는 온라인 활동에 대한 인식제고 및 교육 촉진방안(특히, 취약그룹), 악용 방지 및 차별 혹

은 불필요한 간섭 없이 개인의 적법한 이용을 보장할 수 있는 방법 등을 다루었다. 인터넷의 경제적 및 사회적 이익을 지원하기 위한 글로벌 상호 운용성과 활력, 정부, 업계 및 시민사회간의 공동노력의 필요성에 대해 일반적으로 공감하고, 이와 관련한 ICANN 역할의 중요성을 인식하고 이해관계자들의 참여를 요구하였다. 사이버공간상의 보안, 안전, 활력 및 신뢰의 확보에 있어서 민간 부문의 핵심적 역할을 인식하고, 정부가 개방적인 인터넷을 통하여 개인의 콘텐츠 및 서비스에 대한 접근을 보장하고 악용되는 것으로부터 이용자들을 보호하기 위해 민간부분과 공동노력을 할 책임이 있음을 논의하였다. 하지만 규제의 경우 국제적 법적 의무에 기반을 둔 경우에만 허용하기로 하였다.

이와 관련해 중국은 디지털 격차로 세계경제 불균형의 심화가 우려되며, 평등한 사이버 공간 접근 기회를 제공하기 위해 UN 차원에서 정책 및 이행 방안을 모색하고 있다고 밝혔다. 호주 법무부는 정부가 규제보다는 사이버 위협에 대한 대국민 교육 및 홍보 등 자율적 거버넌스 토대를 마련하는 것이 중요하다고 강조했다. UN ITU는 인터넷 사용자 증가로 인해 사이버 공격에 대한 취약성이 증대함에 따라 앞으로 국가들 간에 사이버 공격에 대한 일반 원칙을 수립하는 한편, 국내법상 이행 방안을 마련하는 등의 대응 역량을 강화해야 한다는 의견을 제시했다. ICANN은 원자폭탄 못지않은 사이버 공간의 위협에 대하여 다중이해관계자가 참여해 안보 중심의 네트워크를 조성하고, ICANN 내 실무 그룹을 참여시켜 시스템을 개선할 것을 제안했다.

#### 라. 국제 사이버안보

국가 간 보안 부문에서는 국가 간의 문제를 예방하고 완화시킬 방법, 다른 분야의 국가 간 안보 및 분쟁방지 노력에서의 교훈, 적절한 행동원칙의 개발과 이행방법, 향후 논의를 위한 적절한 논의의 장 등에 대해 논의했다. 각국 정부는 인터넷상에서 균형적으로 행동해야 하며, 국가간 관계를 규율하는 기존의 국제규범 및 전통적 관행에 따라야 함을 강조했고, 신뢰를 구축하고, 오해를 방지하기 위해 협력과 공동의 노력이 강화되어야 함을 역설했다. 또한 향후 시급히 이루어져야 할 사안으로 UN 정부전문가집단(UN Group

of Government Experts), OSCE 등을 통한 공동의 이해와 합의된 공동의 접근방법 및 신뢰구축 조치를 개발하기 위한 실질적인 조치를 취하는 것이라는데 합의했다.

이에 대해 미국의 마이크로소프트(MS)는 표현의 자유를 위한 익명성과 역기능 방지를 위한 책임성간 조화가 필요하다는 의견과 함께 사이버 범죄에 대한 국제공조가 어렵기 때문에, 부다페스트 협약의 확대가 필요하다는 의견을 제시했다. 또한, 클라우드에서 정보 보안은 민간 차원의 ISO와 같은 표준을 확보해야 한다고 제안했다. 카스퍼스키랩은 기존 부다페스트 조약보다는 새롭고 강력한 글로벌 차원의 협력 체계 구축이 필요하다는 의견을 개진했다. 한편, 중국 대표단은 어린이 포르노물만을 금지하고 있는 부다페스트 협약은 글로벌 규범 수립을 위해 유럽이 중심이 되어서 UN을 비롯해 모든 국가가 참여하여 논의하는 것이 필요하다고 밝혔다. 또, 보츠와나 검찰은 개도국의 사이버 범죄가 급증하고 있다고 밝히고, 사이버 범죄와 관련해 정부가 민간에 대하여 열린 태도로 접근하는 것이 필요하다는 의견을 제시했다. 한국 경찰수사연구원은 최근 정부 인프라를 대상으로 한 공격이 증가하여 사이버포렌식 기술 및 디지털미디어 분석 표준화 등에 대한 글로벌 공조가 필요하다고 밝혔다.

#### 마. 사이버범죄

사이버 범죄 주제에서는 사이버 범죄 예방을 위한 개인, 민간부문, 정부의 책임과 각국이 사이버 범죄에 대응하고, 관련 국제적 활동을 지지하기 위해 동등한 법규정을 갖추도록 하는 방법, 필요한 부문에 적절한 수준의 투자를 유인하는 방법, 인터넷중개자들이 유해프로그램(malware, botnets) 확산방지를 위해 해야 할 역할, 그리고 기기, 시스템 및 서비스 설계에 있어서 효율적인 비용으로 발전적인 보안책 구축을 유도하기 위한 유인책 등의 내용을 논의하였다. 사이버범죄는 경제 및 사회적 복지에 중대한 위협요소로, 시급한 공동 대응노력이 요구되는 상황으로 인식되었다. 온라인범죄가 국경을 넘어 발생함에 따라 사이버범죄로부터 안전지대는 없으며, 사이버범죄의 위협에 대해 공동 대응을 해야 한다는 원칙을 강력하게 지지했다. 또 사이버범죄에 대한 대응지침으로 오프

라인에서 허용될 수 없는 것은 온라인에서도 허용될 수 없다는데 강력한 지지 표명하였다. 즉, 온라인과 오프라인 세계를 하나로 인식한 것이다. 사이버범죄에 관한 부다페스트 협약의 원칙들에 대해 일반적 지지를 표명하고, 이 협약에 대해 일부의 문제제기가 있었으나, 새로운 수단에 대한 협상이 필요성에 대한 의견은 거의 없었다. 정부와 업계 모두 사이버범죄 예방을 위한 더욱 강화된 노력이 필요하다고 지적했다. 예를 들어, 업계는 더욱 보안성이 강화된 기기, 시스템 및 서비스를 제공해야 한다는 것이다. 또한 정부는 온라인을 통한 서비스를 강화하고 있기 때문에 관련 정부조달 및 온라인서비스 제공 등에 있어서 주도적인 역할을 할 수 있음을 강조했다.

이 같은 5개 주제에 대한 논의과정에 대해 참가자들은 런던회의가 정부뿐 아니라 업계 및 시민사회의 대표들을 포괄하여 동반자적 관계에 기반을 둔 광범위하고 건설적인 논의였다고 평가했다. 그리고 후속회의를 통해 안전하고, 개방적인 사이버공간에 대한 공통의 비전 구축 강화를 기대했다.

이와 관련해 미국 백악관은 조약 형식을 통한 사이버안보 확보 노력은 기술의 진보를 따라가지 못한다고 전제하고, 정부 POC 설정을 통한 국가 간 CERT 통로 확보와 함께 인터폴과 G8 공조 및 부다페스트 조약의 확대가 필요하다고 밝혔다. 반면, 중국 대표단은 일부 국가만의 합의로 시작된 부다페스트 조약에 다른 국가가 가입하는 경우 어떤 장점이 있는지 의문을 제기했다. 러시아 외교부 역시 ICT 역기능과 관련해 무엇보다 국제 규범 형성이 시급하지만, 기존의 법적 수단이 현실을 제대로 고려하지 못하는 문제점이 있으므로 각 국가들이 냉전적 사고에서 벗어나 모두 한 배에 탄 상황에서 공동의 합의가 필요하다고 의견을 제시했다. 한편, 프랑스 네트워크정보보안청은 인터넷을 e-G8에서 주요 의제로 설정하고, 국가 CERT간 POC 설정을 통한 대화 창구 구축이 필요하다는 의견을 밝혔다. 독일 연방내무부 및 정보기술위원회는 IT의 실패는 국가에 실질적 위협이 된다고 인식하고 있다고 밝히고, 사이버공간에서 국가 간 갈등 해결을 위해서는 백서 교류, CERT 협력 및 POC 설정을 통한 CBM을 구축을 위해 노력해야한다는 의견을 제시했다. 또한, 인도 외교부는 국가 사이버안보전략 검토, 미국과 ICT 협력 및 국가 CERT간 협의체 운영 등에 노력하고 있다고 밝히고, 글로벌 사이버 규범 형성을 위해서는 민간과 시

민사회 모두가 참여하는 전체적인 시각을 견지할 필요가 있다고 의견을 제시했다. 한국의 국제안보대사는 익명성과 근원지 추적의 어려움, 합의된 규칙 부재 등 국가 간의 상호 신뢰가 없는 사이버 공간의 특수성에 대해 국가 간에 공동으로 인식하고 CBM을 구축 하는 것이 필요하다는 의견을 개진했다.

<표 2-9> 사이버스페이스에 대한 런던 컨퍼런스 의제

경제성장과 개발	사이버공간에서의 지적재산권
사회적 혜택	인터넷과 사이버공간이 가져오는 사회적 혜택
	사이버공간으로 인한 사회적 문제
	인터넷에서의 표현의 자유와 규제간 균형
사이버범죄	사이버범죄의 정의
	사이버범죄의 심각성
	사이버범죄 관련 국제협약
안전하고 신뢰 가능한 접속 보장	사이버 안전(Cyber Safety)
	개인정보보호 및 Privacy 문제
국제 사이버 안보	사이버 보안
	국제 보안 및 충돌 방지
토론	능력배양
	네트워크 연결성
	온라인상의 사생활 및 데이터 보호
	온라인 사법권
	인터넷 인프라 투자
	사이버 범죄

## 제 3 절 2012년 부다페스트 사이버스페이스 총회 의제 분석

### 1. 주요 활동사항

#### 가. 회의 개요

2012년 10월, 부다페스트에서 개최된 사이버공간 회의의 주제는 ‘자유와 번영을 위한 신뢰와 안전(With Trust and Security for Freedom and Prosperity)’이며 런던회의의 연장선 상에서 5개 세부 의제를 설정했다. 세부 의제는 경제성장과 발전, 사회적 혜택과 인권, 사이버 보안, 국제 안보, 사이버 범죄로 구성됐다.

각국 외교부/정통부 장·차관, 국제기구, NGO, 학계, 기업 등 약 800여명이 참가했다. 주로 유럽과 미국 등 서방국가가 참가했으며, 아시아권에서는 한국, 일본, 중국, 인도, 사우디아라비아, 싱가포르, 태국, 필리핀 등 일부 국가만 참석했다.

개막식에 이어 이틀간 3개의 총회(Plenary Session)와 5개의 패널토의가 이뤄지고, 거의 유사한 주제의 7개 워크숍이 동시 진행됐다. 부대행사로 전사회, 청년포럼이 개최됐다. 회의는 각 세션별로 좌장을 두고 발표자의 10~15분 내외 발표 및 방청객 2~3명 정도의 질의응답 형식으로 진행됐다. 거의 모든 발표가 원고 배포나 프리젠테이션 자료 없이 영어로 이뤄졌으며, 프랑스나 중국 발표자의 경우 영어동시통역이 제공됐다.

#### 나. 회의 참석결과

경제성장 및 발전, 사회적 혜택 및 인권, 사이버 보안, 사이버범죄, 국제안보 등 인터넷이 가져오는 다양한 혜택과 위협요인을 논의했다. 표현의 자유, 다양성, 개방성, 투명성 등을 원칙으로, 사이버공간에서의 부작용(범죄, 테러 등)을 최소화하기 위해 국제 및 미-관 협력의 중요성을 강조했다.

미국과 유럽측은 현재의 인터넷 거버넌스 체제의 유지 및 인터넷에 대한 최소규제 원칙을 주로 주장한 반면, 중국, 브라질 등 일부 개도국은 사이버회의에 대해 비판적이며, UN이나 ITU 등 국제기구에서 해당 이슈에 대해 논의할 것을 주장했다.

정부대표단은 총회 전체회의, 세부 분과회의 및 워크숍 등에 적극 참여하여 사이버공간에 대한 참가국간 포괄적 대화를 통한 협력을 강화했다. 2013년 10월, 서울에서 개최하는 차기 총회에서 논의될 수 있는 사이버공간 관련 참가국의 주요 관심사 등 최근 동향을 파악했다. 차기 총회에서 한국이 사이버공간 논의의 주도권을 가질 수 있도록 정보수집 및 분위기 확산에 주력했다.

또한, 분과회의 및 부속행사 등을 통해 사이버공간 이슈에 관련된 국제적 감각을 익히고, 사이버보안 관련 패널토의 등 토론에 국내 전문가가 참여하여 한국의 앞선 사이버보안 체계 등을 홍보했다. 이와 함께 정부대표단 참여 부처와의 협력 및 공조를 강화했다.

그러나 참석자나 논의내용이 유럽과 미국을 중심으로 이뤄져 아시아, 아프리카, 남미 등 개도국의 참여 저조 및 중국 등이 반발했다. 이들은 부다페스트 회의가 런던 회의 이후 참여국가나 의제가 발전되지 못한 점을 지적하며, 사이버공간 회의에 대해 비판적인 입장이다. 따라서 서울회의에는 아시아, 중남미, 아프리카 국가들의 참여를 촉진하는 한편, 이들 개도국의 인터넷 보급률 등 현실에 맞는 의제를 설정할 필요가 있다.

따라서 2013 서울회의에서는 의제설정, 발표자 및 패널 구성 등에 미국, 영국, 러시아, 중국 등과 사전 협의를 통해 보다 많은 국가가 공감할 수 있도록 해야 한다. 또한, 한국적인 의제를 설정하여 선진국과 개도국간 가교 역할을 수행할 필요가 있다.<sup>3)</sup>

---

3) 한편, ITU가 주최하는 세계정보통신회의(12월)에서 인터넷 거버넌스 관련 후속 논의가 이뤄질 것으로 보인다. 관계기관 및 부처 의견수렴을 철저히 하여 대응할 필요가 있다.

## 2. 주요 의제

### 가. 경제성장과 발전

인터넷 경제의 성장이 글로벌 국가들에게 혜택이 될 수 있도록 유도하는 정책 방향, 경제성장과 생산성의 향상 및 콘텐츠의 발전 등을 위해 요구되는 사항, 전 세계적인 디지털 콘텐츠의 발전과 혁신적 서비스를 확산시키기 위해 필요한 정책 방향 등을 다음과 같이 논의했다. 첫째, 인터넷 경제 발전의 글로벌 혜택과 관련해, 인터넷 접속의 확대 외에 인터넷에 의한 혜택의 확산과 수용 촉진을 위한 광범위한 디지털 콘텐츠와 혁신적인 어플리케이션, 서비스 등의 발전을 지원하는 정책 방향과, 사이버 공간 자체의 혁신을 뒷받침할 수 있는 요인을 모색했다. 둘째, 경제성장과 생산성 향상 및 콘텐츠의 발전 요인과 관련해, 국제 접속료(초고속인터넷 요금), 네트워크 발전과 사회경제적 혜택 간의 관계에 대한 실체적 자료를 바탕으로 도출될 수 있는 정책과, 이를 바탕으로 인터넷 경제에 개도국의 참여를 높일 수 있는 방안을 논의했다. 셋째, 디지털 콘텐츠의 발전과 혁신적 서비스의 확산과 관련해, 디지털 및 모바일 콘텐츠 및 어플리케이션 등의 혁신적 서비스가 동태적인 온라인 생태계를 구축하도록 하는 방안과, 해당 분야에 혁신을 가장 효과적으로 확산시킨 정책이나 접근 방법을 분석했다.

### 나. 사회적 혜택과 인권

인터넷의 개방성과 투명성 및 사회적 진보 간의 관계에 대한 논의, 소셜 네트워크에 의한 정치참여, 사이버 보안이나 범죄에 대한 대응 및 인터넷 거버넌스 등이 인권에 미치는 영향, 보안과 인권 간의 균형 달성을 위한 국제 협력, 인권이나 접근에 대한 보호를 증진하는 모범 사례 및 인권에 대한 의무가 사이버 공간에서도 동일하게 적용되도록 하는 방안을 모색했다. 첫째, 인터넷의 개방성과 투명성 및 사회적 진보와 관련해, 인터넷을 통한 참여 확대에 따른 보편적 접근권 및 사회 발전, 인터넷에서 표현의 자유를 보장할 수 있는 방안, 인터넷을 통한 교육, 의료, 프라이버시, 반부패, 인권 보호 신장 방안을 논의했다. 둘째, 소셜 네트워크에 의한 정치 참여와 관련해, 소셜 네트워크를 통한 정

치 참여와 소외의 배제, 사이버 공간에서 위협 및 기회와 인터넷에서의 행동규범에 대한 인식 제고 방안을 논의했다. 셋째, 사이버 보안 및 범죄 대응 등이 인권에 미치는 영향 즉, 정부의 인터넷 거버넌스나 보안, 범죄 대응 조치들이 인권에 미치는 영향과 이에 따른 인권에 대한 시각을 글로벌 차원에서 명확히 할 수 있는 방안을 논의했다. 넷째, 보안과 인권 간의 균형 달성을 위한 국제 협력에 관해서는 언론, 집회, 표현의 자유, 정보에 대한 접근권 등 기본권을 신장시킬 수 있는 방안 및 사이버 공간에서의 프라이버시 및 개인정보 보호 방안을 논의했다. 다섯째, 모범 사례 공유 및 인권에 대한 의무의 사이버 공간 적용 의무화와 관련해 유엔 인권이사회에서 최근 합의된 사항에 따른 국가 및 국제 인권 관련법의 의무 적용 등을 논의했다.

#### 다. 사이버 보안

국가들의 사이버 보안 문제를 총체적으로 해결, 개선하기 위한 모델을 모색했다. 첫째, 모범 사례와 실효성 있는 지침 및 지원 사례를 공유하고 네트워크 시스템의 보안, 개인정보보호 및 신뢰 구축을 위한 바람직한 균형 달성 방안을 모색했다. 둘째, 사이버 보안의 주요 흐름, 정부, 기업, 국민들에 의해 개발·구축된 모범 사례, 사용자에게 대한 인식 제고 및 보안지식 등 국제 협력방안 및 사례를 공유했다. 셋째, 국제 협력 및 신뢰 구축 방안과 CERT(Computer Emergency Response Team) 및 민간 부문에서 논의되고 있는 대표적인 도전 과제와 해결 방안을 논의했다.

#### 라. 국제 안보

모두를 위한 경제 사회 발전을 지지할 수 있도록 믿을만하고 안정적이며 상호정보교환이 가능하고 열린 환경으로 사이버스페이스를 보존하기 위한 공통의 이해와 책임을 공유했다. 증진된 국제 공조는 사이버스페이스에서의 국가 행위의 적절함에 대한 공감대를 형성하고, 갈등으로 인한 위협을 줄이고 협동 과정을 통한 자신감을 형성하기 위해 디자인된 실질적인 방안의 이행이다. 국제 사회는 수년전부터 이와 같은 위협(사이버스

페이스로부터)을 인지하고 있었다. 패널 논의 사항은 지도자들이 그들의 제안들을 제출하기 위해 상이한 관점을 표출하면서 국가 간에 다른 관점들을 소개하고 그들이 도출한 함의를 이해하고 공유했다. 또한 일반적인 주제와 실제적인 결론을 추구하는 관점으로 각 국가가 제시한 이론들이 모두를 위한 신뢰와 안전을 고취할 수 있는 실제 방안으로 이행되기 위해 요구되는 과정을 모색했다.

#### 마. 사이버 범죄

사이버 범죄와 연관된 가장 중요한 문제점을 조사하고 사이버 범죄에 대응하기 위한 실질적인 해결책을 확정하는 방안이 논의됐다. 발표자들은 지역적 혹은 국제적 기구 관점에서 부상하고 있는 위협을 확정할 것이고 모바일 인터넷 접근과 관련된 위협에 대해서 토론하며, 널리 퍼져있는 지적재산권 침해에 대해 탐색했다. 발전하고 있는 법적 체제와 훈련, 법 집행 기관들의 준비, 그리고 효과적인 국제적 공조 보장과 관련된 능력배양을 위한 도전과 필요성, 그리고 해결책을 모색했다. 상시 감시 네트워크와 같은 성공적인 시발점을 모색하며 비공식적 국제 법 집행 공조 노력뿐만 아니라 디지털 증거가 전통적 법 제도에 적용될 수 있도록 하는 방안을 모색했다. 또한, 효과적인 사이버범죄 법의 개발과 시행에 대한 모범 사례를 모색했다.

<표 2-10> 2012 부다페스트 사이버공간 회의 의제

구분	주요 논의내용
대주제	‘자유와 번영을 위한 (사이버 공간의) 신뢰와 안전’ With Trust and Security for Freedom and Prosperity
(의제1) 경제성장과 발전	①인터넷 경제의 성장이 글로벌 국가들에게 혜택이 될 수 있도록 유도하는 정책 방향 ②경제성장과 생산성의 향상, 콘텐츠의 발전 등을 위해 요구되는 사항 ③전 세계적인 디지털 콘텐츠의 발전과 혁신적 서비스를 확산시키기 위해 필요한 정책 방향 등
(의제2) 사회적 혜택과 인권	①인터넷의 개방성, 투명성, 사회적 진보 간의 관계에 대한 논의 ②소셜 네트워크에 의한 정치참여 ③사이버 보안/범죄 대응, 인터넷 거버넌스 등이 인권에 미치는 영향 ④보안과 인권 간의 균형 달성을 위한 국제 협력 ⑤인권보호 관련 모범 사례 및 인권에 대한 의무가 사이버 공간에서도 동일하게 적용되도록 하는 방안
(의제3) 사이버 보안	o 국가들의 사이버 보안 문제를 총체적으로 해결, 개선하기 위한 모델 모색 - 모범 사례와 실효성 있는 지침 및 지원 사례를 공유하고 네트워크 시스템의 보안, 개인정보보호 및 신뢰 구축을 위한 바람직한 균형 달성 방안을 모색 - 사이버 보안의 주요 흐름, 정부, 기업, 국민들에 의해 개발·구축된 모범 사례, 사용자에게 대한 인식 제고 및 보안지식 등 국제 협력 및 사례 공유, 도전과제와 해결방안
(의제4) 국제안보	o 사이버스페이스를 믿을만하고 안정적이며 상호정보교환이 가능하고 열린 환경으로 보존하기 위한 공통의 이해와 책임 공유 - 국가간 국제안보에 관한 견해차이 등 공유, 각 국가가 제시한 이론들이 모두를 위한 신뢰와 안전을 고취할 수 있는 실제 방안으로 이행될 수 있는지 모색
(의제5) 사이버 범죄	o 사이버범죄와 연관된 가장 중요한 문제점을 조사하고 사이버범죄에 대응하기 위한 실질적인 해결책을 확정하는 방안 - 지역 혹은 국제적 기구 관점에서 사이버범죄 관련 내용을 확정하고 모바일 인터넷 접근 관련 위협, 지적재산권 침해에 대해 논의 - 발전하고 있는 법적 체제와 훈련, 법 집행 기관들의 준비, 그리고 효과적인 국제 공조 관계에 대한 모색, 디지털 증거의 법제도 적용방안 모색

## 제 3 장 사이버공간 관련 글로벌 이슈 분석

### 제 1 절 사이버보안 및 사이버 범죄 관련 글로벌 이슈 분석

#### 1. 사이버 보안

##### 가. 국제적 논의 동향

정보통신기술이 발달하면서 정치·경제·문화·사회적으로 사이버공간에 대한 의존도가 급격히 증가함에 따라 사이버공간의 혜택과 동시에 사이버위협에 대한 취약성 및 사회적 역기능 등의 부작용도 동반하고 있다. 최근에는 인터넷 ‘악플’, 사이버범죄, 사이버테러뿐만 아니라 국가안보를 위협하는 수준으로까지 확대되고 있다. 이러한 문제를 해결하기 위해서는 무엇보다 국가간 협력이 필요하다. 국제사회는 사이버범죄 예방·대응, 국가간 사이버안보 문제 해소를 위한 투명성·신뢰 제고, 사이버안보 규범 확립 등의 주요 의제에 대해 국제협력을 위한 노력을 다각도로 모색하고 있다.

##### 1) 국제연합(UN)에서의 사이버안보 논의

국제연합(UN)은 정보안보 정부 전문가 그룹(GGE: Group of Governmental Experts on Information Security)을 통해 사이버안보 확보를 위한 국가간 규범 문제를 논의하고, 2005년 과 2009년에 각각 그 논의 결과에 대한 보고서를 제출했다.

우선 정보보안의 기존의 위협 사항 또는 향후에 예상되는 잠재적 위협 사항이 21세기 가장 심각한 도전 과제 중 하나로 꼽힌다. 안보와 관련해 개인, 기업, 국가 인프라 및 정부 등 모든 집단이 공격 대상이며, 이는 국제 사회 전반의 심각한 위협 요인이 되고 있다. 이런 문제를 개선하기 위해서는 국가, 민간부분, 시민사회 간 광범위한 국제협력이 중요하다. 또한, 보고서는 위협 경감 및 핵심 인프라 보호를 위한 국가 간 대화를 강화해야 하고, 신뢰 구축, 정보 교환이라든지 개도국의 역량 강화 등이 필요하다고 권고했다.

## 2) 국제전기통신연합(ITU)에서의 논의

국제전기통신연합(ITU)은 전기통신에 관한 UN의 전문 기구로서, 2001년 ITU 이사회 결정에 따라 출범한 정보사회세계정상회의(W SIS; World Summit on Information Society)를 2003년 제네바(1차), 2005년 튀니지(2차)에서 개최했다. 여기에서 ‘WSIS 원칙 선언(Declaration of Principles)’을 채택하고, 신뢰할 수 있는 프레임워크 강화가 정보사회의 발전과 ICT 이용자들 간의 신뢰 구축의 선결 요건이며, 모든 당사자들이 협력하는 글로벌 사이버 보안 문화가 시급하다는 것을 강조했다. 그리고 신뢰할 수 있는 프레임워크에는 정보보안, 네트워크 보안, 인증 관련된 부분, 사생활 및 소비자보호 등이 포함되는 것으로 규정했다. WSIS 원칙 선언의 부제는 ‘모두를 위한 정보사회의 핵심 원칙’이며, 11가지의 원칙들의 분야를 명시하고 있다. 그중 ‘ICT 활용에 있어서 신뢰와 안전 구축’이라는 사이버 보안 문제를 핵심원칙에 포함하고 있다.

### <표 3-1> WSIS 원칙 선언

- 1) ICT4D 촉진에 있어서 정부와 모든 이해당사자들 역할
- 2) 소외 없는 정보사회를 위한 필수기반(정보통신 인프라)
- 3) 정보와 지식에 대한 접근
- 4) 능력배양
- 5) ICT 활용에 있어서 신뢰와 안전 구축
- 6) 여건 조성
- 7) 모든 생활측면의 혜택을 위한 ICT 어플리케이션
- 8) 문화 다양성 및 정체성, 언어 다양성 및 로컬 콘텐츠
- 9) 미디어
- 10) 정보사회의 윤리적 측면
- 11) 국제 및 지역협력

ITU에서는 사이버 보안 문제를 구체적으로 다루기 위해 2007년 ITU 글로벌 사이버 보안 아젠다(GCA; ITU Global Cybersecurity Agenda)를 출범시켰다. 이는 WSIS의 실행계획(WSIS Action Line) 중 ‘ICT 활용에 있어서 신뢰와 보안 구축’의 선도적인 역할을 담당하기 위한 것이다. GCA는 법적조치, 기술 및 절차적조치, 조직구조, 능력배양, 국제협력 등

5가지 추진 분야를 기반으로 구체적인 행동의 필요성과 방향을 제시했다. 아울러 사이버 보안과 관련해서 온라인 아동보호와 관련된 인센티브(COP; Child Online Protection)를 정리했다. 인터넷 보급과 이용이 빠르게 확산되는 상황에서 보편적인 수단이 되었고, 특히 어린이들 또한 온라인상에서 노출되어 온라인 위험이 증가하고 있는 상황에서 미래세대에 대해서 안전한 사이버세계 기반 수립이 필요하다는 측면에서 이런 과제를 설정·운영하고 있다.

### 3) 경제개발협력기구(OECD) 및 아태경제협력체(APEC)에서의 논의

OECD의 사이버보안 관련 논의는 정보통신정책위원회(ICCP) 산하 정보보호작업반(WPISP)에서 프라이버시 및 정보보호 분야의 회원국 정책경험 공유, 상호조화를 위한 협력과 정책개발을 중심으로 이뤄진다. 최근의 논의 현안이나 추진사업을 보면 ‘개인정보의 경제학’이라는, 개인정보의 경제적 가치나 유출에 따른 손실이나 사회적 비용, 가치 사슬 등에서 프라이버시 및 정보보호 관련된 지표개발, 국제적인 비교 가능성이나 정책적 근거 개선을 위한 논의가 주로 이뤄지고 있다. 또한, 1980년 ‘OECD 프라이버시 보호 가이드라인’을 발표했으며, 스마트 모바일 시대에 맞춰서 업데이트 논의가 이뤄졌다. 그리고 회원국의 사이버보안 전략 및 사례 비교분석, 봇넷 대응정책 개발, 디지털 ID 관리 등에 관한 논의를 진행하고 있다.

APEC에서는 정보통신작업반 TELWG의 보안및변영운영그룹(PSPG)에서 사이버보안 및 사이버상에서의 신뢰 제고, 사이버범죄 방지, 스팸·스파이웨어 대응, 비상·보안사고대응팀(CERTs/CSIRTs) 관련 인력 개발·능력 배양, 사이버보안 인식제고, 비즈니스 퍼실리테이션(business facilitation) 관련된 논의가 이뤄지고 있다. 최근 추진사업으로는 아태지역의 사이버보안 정책 동향 워크숍, 사이버범죄 전문가그룹회의, 인터넷 서비스사업자(ISP) 자발적 사이버보안 실행규범, 도메인명 서비스보안 확대(DNSSEC) 관련 워크숍, ICT 역기능 예방교육 및 훈련 프로그램 등이 진행됐다. 2012년에는 APEC TELWG 회의에서 인터넷 거버넌스와 관련된 논란이 있었다. 러시아는 신규 사업 과제로 웹3.0 도입 관련된 새로운 인터넷 지배구조 거버넌스 부분을 제안했는데, 이에 대해 한국을 포함한

상당수의 국가들이 우려를 표명했다. 기존의 웹2.0 상황에서 충분히 사이버보안 문제를 논의하고 협력해야 할 부분이 아직 많은 상황이기 때문에, 이 부분에 대해서는 논의를 유보한 상황이다. 2010년 오키나와 정보통신장관회의(TELMIN8)에서 APEC TEL 전략적 실행계획(TEL Strategic Action Plan)은 2010년에서 2015년까지 정보통신 분야에서 중점 추진과제로 ‘안전하고 신뢰할 수 있는 ICT 환경 촉진’ 등의 과제를 명시했다.

<표 3-2> ‘안전하고 신뢰할 수 있는 ICT 환경 촉진’ 분야 실행계획

- |  |
|--|
| <ol style="list-style-type: none"> <li>1) 안전하고 신뢰할 수 있는 ICT 환경 촉진 전략 개발 및 확산</li> <li>2) 사이버보안 모범사례 보급, 정보공유, 기술협력, 교육훈련</li> <li>3) 사이버보안 인식 제고, 능력배양</li> <li>4) 다양한 이해당사자 참여 및 협력</li> <li>5) 온라인상의 위협으로부터 취약그룹(특히, 어린이) 보호</li> <li>6) 정보교류 촉진을 통한 안전하고 생산적인 인터넷경제 육성</li> </ol> |
|--|

4) 부다페스트 사이버범죄 협약

인터넷상의 모든 범죄행위에 대해 상세한 규정을 두고 이를 처벌하도록 하고 있다. 컴퓨터 시스템이나 데이터에 대한 불법 접속, 지적재산권 침해, 컴퓨터 사기, 컴퓨터바이러스 개발 및 유포, 아동 포르노그래피 배포 등을 범죄행위로 규정하고 조약 참가국들이 국내법으로 이를 금지하도록 의무화했고, 사이버범죄 수사 상호 협력 의무 등을 규정했다. 부다페스트 사이버범죄 협약에 서명한 국가들은 사이버범죄에 대응하기 위해 법규정을 표준화하고, 핫라인을 설치하는 등 국제공조체제를 구축하고 있다.

5) 사이버공간에 관한 런던회의

2011년 11월 1일부터 2일까지 이틀간 영국에서 ‘사이버공간에 관한 런던 회의’(London Conference on Cyberspace)가 처음으로 개최됐다. 런던 회의는 새로운 범세계적 이슈로 대두되고 있는 사이버규범 문제를 정부, 학계, 산업계 등 다양한 행위자들이 모두 참여하여 경제·사회·범죄·안보 등 사이버공간상의 제반 이슈에 대해 논의하는 최초의 대규모

각료급 종합포럼이다. 60개국 국가 장관급 또는 고위급 정부대표, 국제기구 대표, 학계, 산업계, 시민사회 대표 700여명이 참석해 경제, 사회, 범죄, 안전, 안보 등 다양한 영역에서의 사이버 규범 문제를 논의했다. 런던회의에서 2012년 헝가리에 이어 한국이 2013년 후속 회의를 개최하는 것으로 결정됐다.

#### 나. 사이버 보안 격차 해소

미국, 중국, 독일, 영국 등 사이버 범죄 상위 20개국이 있다. 인터넷 이용이 쉽기 때문에 범죄에서 상위권을 차지하는 것도 마찬가지이다. 인터넷 정보 접근이 용이할수록 사이버 범죄의 위험이 증가한다는 것이다. 따라서 정보격차 뿐만 아니라 국가간의 보안 격차를 해소할 필요가 있다.

런던에서는 정보격차에 대해서는 이야기를 했지만 보안 격차에 대해서는 적절하게 언급되지 않았다. 하지만 보안이 뒷받침되지 않는 정보격차 해소는 보안 위협의 노출을 초래할 수 있다. 인터넷 이용이 높고 보안 수준이 낮은 국가들은 다른 국가에 대한 어떤 공격에 활용에 될 수 있다는 것이다. 따라서 국가 간의 사이버 보안 격차 해소를 위한 공동의 노력이 필요하다. 제3세계 국가들에 인적, 물적, 교육적 지원 활동이 요구된다.

## 2. 사이버 범죄

### 가. 논의의 배경

#### 1) 사이버범죄의 정의

사이버범죄(cyber crime)는 컴퓨터, 통신, 인터넷을 악용하여 사이버공간에서 행하는 범죄이며, 범행목적에 따라 사이버 테러형과 일반 범죄형으로 분류된다. 정보통신망으로 연결되는 컴퓨터 시스템이나 사이버공간을 이용해 다른 사람한테 피해를 주고 건전한 사이버 문화에 해를 끼치는 행위를 의미한다. 일반 범죄와 달리 빠른 시간안에 불특정 다수에게 많은 악영향을 미치며, 사이버공간 특성상 정보 발신자를 특정하기 어렵고, 전자 정보의 증거 인멸 및 수정이 용이하기 때문에 범죄 수사에 어려움이 많다. 사이버범죄는 국내는 물론 해외에서 동시에 발생하는 특성을 갖고 있어 이를 대처하기 위해선 국제적인 형사 사법의 규칙도 요구된다.

사이버범죄는 범행목적에 따라 사이버 테러(해킹, 서비스 거부 공격, 바이러스 유포, 악성프로그램, 메일폭탄)와 사이버범죄사기(통신, 게임), 불법복제(음란물, 프로그램), 불법/유해사이트 (음란·도박·폭발물·자살), 명예훼손죄, 모욕죄, 개인정보침해, 사이버스토킹, 사이버성폭력, 협박/공갈 등으로 분류된다. 사이버범죄는 초국가적 본질과 관할 문제로 세계 어디서나 공격 시도가 가능하고 여러 국가들 간에 걸쳐 범죄를 실행할 수 있어 전통적 주권국가 관할 개념을 적용하는 것이 불가능하다. 또한, 사이버범죄자와 피해자 사이에는 범죄가 실행되는 동안 어떠한 형태의 물리적 접근을 필요로 하지 않는다는 특징이 있다.

게다가 단기간에 대규모, 다중 피해가 나타날 수 있어 한 번의 범죄 실행 행위로 불특정 다수가 피해자가 발생할 수 있으며, 실행 속도 또한 물리적 범죄에 비해 빠르게 일어난다. 또, 사이버공간의 기본적 익명성과 프록시, VPN 등을 이용한 IP 세탁으로 범죄자가 손쉽게 신원을 감출 수 있다.

## 2) 사이버범죄의 심각성

### ① 국내 현황

국내 사이버범죄는 2006년 70,545건에서 2010년 103,809건으로 약 47% 증가했다. 유형별로는 인터넷 사기(35,104건), 불법 복제판매(17,885건) 등 일반 사이버범죄가 85.6%로 대다수를 차지하고 있다. 디도스 등 대규모 공격 현황을 살펴보면, 2009년 7월, 국내 21개 국외 14개 사이트를 대상으로 하는 디도스 공격이 발생했고, 해당 사이트 접속불가, 좀비 PC감염, 하드디스크 손상 등 피해를 초래했다. 2011년 3월에는 국내 40개 사이트를 대상으로 디도스 공격이 발생하여 2009년과 유사한 피해내역이 확인되었다.

<표 3-3> 최근 5년간 사이버범죄 검거 건수

'06년	'07년	'08년	'09년	'10년
70,545	78,890	122,227	147,069	103,809

유해사이트 접속현황을 살펴보면, 음란, 도박, 폭발물·자살 선동 등을 불법(유해) 사이트로 규정, 2010년 해당 사이트 운영 등 총 8,611건이 검거됐고. 2011년 6월 13일~26일간 보건복지부·환경부와 공동으로 사이버명예경찰 협조 등을 통해 조사한 결과, 인터넷 폭발물·자살 선동 게시물 6,932건이 발견됐다.

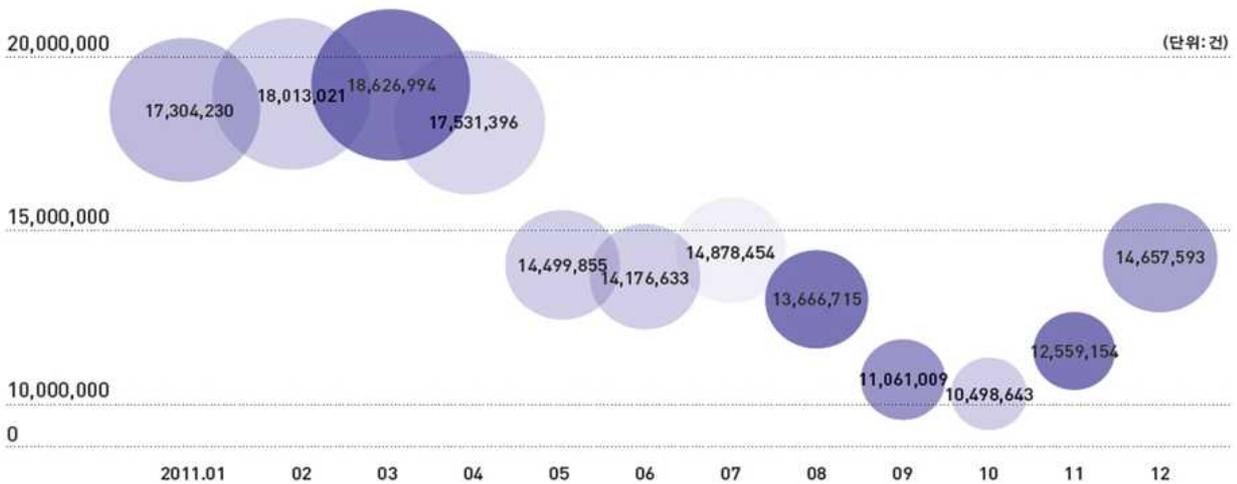
[그림 3-1] 개인정보 침해신고 상담건수



출처: KISA 인터넷통계정보검색시스템

또한, 국내의 경우 악성 프로그램 제작 및 유포와 관련해 연구목적이나 학술목적 등으로 인해 제작하는 것 자체에 대해서는 처벌규정을 두고 있지 않다. 2011년 12월, 약 1,400만 건의 악성프로그램이 유포됐다는 자료가 있다. 그중에서도 Java 플랫폼에 대한 공격이 가장 많고, HTML이나 운영체제(OS) 자체에 대한 공격 또한 늘어나고 있다. 상대적으로 해킹 등에 취약한 Windows XP를 많이 사용하고 있는 국내의 특수한 환경 때문에, 같은 공격이라도 더욱 치명적으로 작용할 수 있다.

[그림 3-2] 월별 악성프로그램 유포 횟수



출처: 안철수컴퓨터바이러스연구소 통계자료

인터넷 본인확인제에 대해 헌법재판소가 2012년 8월, 위헌 결정을 내렸다. 일정규모 이상(일일 평균 이용자수 10만 명 이상)의 인터넷게시판을 설치·운영하는 정보통신서비스 제공자의 본인확인 조치의무, 정보 게시자만이 아니라 열람자도 본인 확인의 대상에 포함, 6개월 이상 본인확인정보를 보관해야 한다는 본인확인제의 내용이 목적과 수단의 불균형에 해당한다는 이유로 위헌 결정을 내린 것이다.

## ② 국제 동향

보안업체 시만텍의 연구에 의하면 2010년 사이버범죄로 인한 금전적 피해액이 1,140억

달러(약 122조원)에 달하고 4억 3,100만명이 피해를 당했다. 인터넷을 이용하는 성인의 3분의 2가 넘는 69%가 사이버범죄 피해 경험을 가지고 있다. 이는 매초마다 14명, 매일 1백만명 이상이 사이버범죄의 피해자가 되고 있음을 의미한다. 주요 사이버범죄 유형을 살펴보면, 컴퓨터 바이러스 및 멀웨어(악성 소프트웨어) (54%), 온라인 사기(11%), 피싱 메시지(10%) 등이 있다. 2010년에는 2억8,600만개의 Malware 변종이 발견되었으며, 전년 대비 19% 증가한 수치이다.

사이버범죄 대응의 기본 원칙은 첫째, 신속·정확한 범정부차원의 보안 대비체제를 구축하는 것이다. 이때 평상시와 긴급상황시를 구별해 대응하도록 한다. 미국의 경우 영장주의 원칙의 예외를 인정하고 있다. 둘째, 실체법, 절차법적인 요구를 수용할 필요가 있다. 컴퓨터 범죄의 수사 및 소추를 방해하거나 지연하는 절차적, 관할적인 여러 가지 장애물을 제거하거나 최소화하기 위한 강력한 입법적 조치를 서두르지 않으면 안 될 시점이다. EU 회원국들뿐만 아니라 미국, 일본, 캐나다 등 여러 국가가 참여하는 다국적 협약인 ‘EU 사이버범죄 방지 조약’에 가입하는 것을 고려할 필요가 있다. 해당 조약 가입 시 이행이 필요한 입법적 정비도 필요하다. 셋째, 전문가 양성과 자격제도를 운영할 필요가 있다. 즉, 전자적 증거의 수집과 분석에 관한 국제적 기준을 마련해야 한다.

#### 나. 새로운 범죄화의 요구와 수용

##### 1) 사이버 공간의 범죄 유형과 국제조약

사이버 공간에서의 문제는 법률적, 실체법적 측면에서 보면 통신수단의 완전성(completeness), 통신수단의 건전성(soundness), 거래 안전(e-commerce security)과 저작권 보호(copyright protection)를 확보하는 것이다. 통신수단의 완전성은 일반적으로 ‘정보자산의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 유지하는 것’으로 정의할 수 있다. 통신수단의 건전성을 확보하는 차원에서 아동포르노 제작, 이용, 배포, 전송 등 행위에 대한 처벌과 표현의 자유 보장과의 한계가 문제로 대두된다. 또, 거래 안전과 저작권 보호를 위해 컴퓨터 데이터나 시스템의 정상적인 작동을 방해하는 행위에 대

한 실체법적인 보완이 필요하다.

앞서 언급한 EU사이버범죄 방지조약은 이 같은 범죄 유형과 관련해 다음과 같은 규정을 두고 있다. 첫째, 통신수단의 완전성을 침해하는 형태의 범죄에 대해 EU사이버범죄 방지조약은 제2조(불법접속), 제3조(불법감청), 제4조(데이터침해), 제5조(시스템방해), 제6조(장치의 남용), 제7조(컴퓨터 관련위조)에 이르기까지 컴퓨터 데이터와 시스템에 대한 침해, 장치의 남용 등 행위를 범죄로 규정하도록 요구하고 있다. 둘째, 거래의 안전성과 저작권을 침해하는 형태의 범죄에 대해 제8조에서 타인의 재산에 손실을 입히거나 자신 또는 타인의 경제적 이익을 획득할 목적으로 권한 없이 고의로 컴퓨터 데이터를 입력, 변경, 삭제 및 은폐하거나, 컴퓨터 시스템의 정상적인 작동을 방해하는 행위를 범죄로 규정하는 입법을 요구하고 있다. 제10조에서는 고의로, 상업적 규모로, 컴퓨터 시스템을 이용하여 저작권을 침해하는 행위를 형사 처벌하도록 하고 있다. 셋째, 통신수단의 건전성을 침해하는 형태의 범죄에 대해 제9조는 컴퓨터 시스템을 통하여 배포할 목적으로 아동 포르노를 제작하거나 이용하도록 제공하는 행위, 이를 배포·전송하는 행위, 컴퓨터 시스템을 통해 아동 포르노를 획득하거나 저장매체나 시스템상에서 아동 포르노를 소지하는 행위에 대한 처벌하도록 규정하고 있다.

## 2) 국내 사이버범죄 처벌 규정

국내에서는 현행법으로 불법접속 행위에 대해서는 처벌규정이 있다.<sup>4)</sup> 그렇지만 불법접속행위에 대해서는 정보통신회선을 통한 경우로 한정되어 있으므로, 사내 LAN을 통하여 서버에 접속하는 행위도 부정접속죄로 처벌하도록 보완할 필요가 있다.

또한, 데이터 침해 및 컴퓨터 관련 위조·변조에 대해 형법상 공문서에서 사용하는 전자기록 등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해하는 경우 처벌하도록 하고 있다(제141조). 전자기록의 위작·변작죄에 대한 처벌 규정을 형법에 포함시켰지만, 아직도 문서위조에 대한 처벌공백이 많다. 예를 들어, 사전전자기록 자체의 손

---

4) 정보통신망법상 불법침입죄(제72조제1항제1호), 비밀침해죄(동 제1조 제11호), 형법상 비밀침해죄(제316조), 공무상비밀표시무효죄(제140조 제3항)

괴행위와 공전자기록 무형위조의 경우 입법적 보완이 필요하다.

더 큰 문제는 악성 프로그램의 제작행위에 대해서는 처벌규정이 없다는 것이다. 다만, DoS(Denial of Service) 혹은 DDoS(Distributed Denial of Service)라고 하는 공격에 의한 서비스 방해 행위에 대하여 형법상 컴퓨터 업무방해죄(제314조제2항)로 처벌하고, 정보통신망법 제48조 제2항, 제71조 제9호에 처벌 규정을 마련해 놓았을 뿐이다. 앞서 언급한 것처럼, EU 사이버방지 조약은 이에 대해 입법하도록 권고하고 있다. 연구목적이나 학술목적은 제외하더라도 악성프로그램의 제작하는 행위에 대해서는 입법적 보완이 필요하다. 악성 프로그램의 작성·사용행위는 컴퓨터에 의한 정보처리의 정당성에 대한 신뢰를 저해하는 행위로서 처벌의 필요성이 매우 크다. 악성 프로그램의 제작행위를 예비죄 형태보다는 본범형식으로 신설 규정하는 것을 고민해야 한다.

컴퓨터 사용 사기죄에 대해서는 형법상 컴퓨터 등 사용사기죄(제347조의2)를 규정하고 있으나, 객체를 재물이 아닌 재산상 이익으로 한정하고 있다. 게임아이템 같은 것은 아직 절도의 대상, 물건이 아니기 때문에 절도죄가 성립되지 않는다. 단, 물건은 아니지만 재산상 이익은 된다는 측면에서 사기죄를 적용하거나 거래에 대한 부가가치·세금을 부과하지만, 이를 훔쳐가는 행위나 빼어가는 행위는 물건이 아니라는 이유로 절도나 강도로 처벌할 수 없다는 것이다. 따라서 재산상 이득에 한정하지 않고, 재물도 컴퓨터 사용사기죄의 대상이 될 수 있도록 형법을 개정할 필요가 있다.

또한, 아동 포르노 관련 범죄에 대한 처벌 규정이 미약하다. 미국의 경우 아동포르노 관련범죄에 대하여 평균 115월의 징역으로 강력히 처벌하고 있으며, 이는 살인죄(253월), 납치 및 인질강요(199월)에 이어 3번째로 높은 형량평균치에 해당된다. 또한, 포르노 파일 등을 전송하는 행위에 대해 파일은 물(物)이 아니기 때문에 형법상 음란물 제작 반포죄로 처벌하기 어렵다. 대신 정보통신망법 위반 등으로 처벌하는 실정이다. 이처럼 형법상에 아직 들어오지 못한 전자적 거래에 대한 고민이 필요하다. 음란물 등에 ‘전자기록 등 특수매체기록’을 추가하고 전시 또는 상영 외에 ‘전송’한 자도 처벌하도록 입법적 보완이 필요하다. 이와 함께 형법상 특수매체기록도 음란‘물’의 대상에 포함시켜야 한다.

#### 다. 절차법적 개선사항

사이버범죄와 관련된 증거는 무체정보성, 변조 용이성, 원본과 구별 불가능성, 대량성, 전문성이라는 특성을 갖고 있다. 기존의 유체 증거물을 전제로 한 엄격한 강제 처분 법정주의의 적용과 한정된 증거수집방법만으로는 체계적 대응이 미흡한 실정이다. 이와 관련해 EU사이버범죄 방지조약은 절차법 규정으로서 적용범위와 요건, 컴퓨터 데이터의 신속한 보존조치, 컴퓨터데이터의 제출명령, 압수수색, 실시간 수집 등에 대해 특별한 규정을 두도록 하고 있다. 그러나 국내에서는 절차법적으로 미비한 점이 많다.

첫째, 전자적 기록 등의 압수·수색과 관련해 현행 형사소송법(제106조 제3항 및 제4항)은 디지털 증거에 대한 수색·압수·검증과 관련해 원칙적 선별압수, 예외적 정보저장 매체압수로 규정하고 있는데, 이와 관련해 최근 컴퓨터 압수·수색 현장에서 압수·수색의 방법에 관해 분쟁이 빈발하다. 예외적인 전자저장매체 등의 압수를 보다 포괄적으로 열거하는 방식의 입법적 보완이 필요하다. 또한, 원격조작에 의한 증거수집 및 보전을 인정하는 것에 대해서도 고민해야 한다.

둘째, 전자기록 등의 보존 및 비밀유지 요청에 관해, EU사이버범죄 방지조약 제16조는 통신데이터를 포함해 저장된 컴퓨터데이터의 신속한 보존 명령 및 필요한 입법적 조치를 취하도록 하고(제1항), 해당 컴퓨터 데이터를 소유 내지 지배하는 사람에게 확대(제2항), 보관자 또는 컴퓨터 데이터를 확보해야 하는 자에게 기밀유지 의무를 부과하도록 했다(제3항). 또한, 동 조약 제17조는 트래픽 데이터를 긴급히 보존해야 할 필요가 있을 때, 이에 개입하는 서비스제공자와 관계없이 신속한 보존이 가능하도록 요구하고, 이를 수사기관에게 신속히 공개하는 절차를 마련하도록 하고 있다.

셋째, 기록 후 제출 명령 제도와 관련해 침해의 정도가 높은 수색 및 압수절차의 대안적인 방법으로 서비스 제공자나 그 밖의 사람에 대해 제출명령을 위한 입법적 조치가 요구된다. EU사이버범죄 방지조약 조약 제18조 제1항은 특정한 컴퓨터 데이터를 소유하고 있거나 이를 관리하는 자와 서비스제공자에 대해 특정데이터와 가입자정보에 관한 제출명령을 규정하고 있다.

넷째, 저장된 컴퓨터 데이터의 수색·압수, 원격조작과 관련해 EU사이버범죄 방지조약 제19조 제1항은 자국 영토 내에 있는 컴퓨터 데이터를 수색하거나 이와 유사한 방식으로 접근할 수 있도록 법적 근거를 마련하도록 했다. 제2항은 중앙서버에 연결된 단말기를 통하여 접속된 단말기를 통해 필요한 정보를 다운로드 받거나 백업 받은 후 압수할 수 있도록 규정했다. 제3항은 이를 위해 컴퓨터시스템 또는 그 일부 또는 컴퓨터저장매체를 압수하거나 이와 유사한 방법으로 보존, 컴퓨터 데이터를 복제하고 반환, 관련된 컴퓨터데이터의 무결성을 유지하도록 하는 규정을 마련하도록 했다.

다섯째, 피처분자에 대한 협조요청과 관련해 일정한 자에게 EU사이버범죄 방지조약 제19조 제1항, 제2항에 언급하고 있는 조치를 수행할 수 있도록 하기 위해 합리적인 기준에 따라서 필요한 정보를 제공하도록 했다. 또한, 정보제공의무자에게 저장된 컴퓨터 데이터에 대한 원활한 수색을 위해 협조하도록 요구할 수 있도록 했다.

여섯째, 실시간 송수신 데이터와 통신내용데이터의 수집에 관해 EU사이버범죄 방지조약 제20조, 제21조는 통신내용데이터를 실시간 수집할 수 있도록 규정할 것을 요구하고 있다

일곱째, 네트워크를 이용하는 경우 국제간의 관할권 문제가 발생할 여지가 크다. EU사이버범죄 방지조약 제22조에 따르면, 속지주의를 원칙으로 하면서 컴퓨터 시스템을 공격한 자와 피해를 입은 시스템이 자국의 영역 내에 있는 경우 당사국은 관할권을 가지며, 공격 받은 컴퓨터 시스템이 자국의 영역 내에 있다면 공격자가 영역 외에 있는 경우라도 관할권을 행사할 수 있다. 단, 자국민이 자국 영역 외에 있더라도 자국법에 따라 관할권을 행사할 수 있도록 함으로써 보충적으로 속인주의를 가미했다. 또한, 동 조약에 의한 범죄에 2개국 이상이 관할권을 주장하는 경우 상호 협의하도록 했다.

#### 라. 긴급상황 대비 특례법 제정

미국은 수정헌법 제4조의 영장주의 요건의 예외로 다음과 같은 ‘예외적 상황’(exigent circumstances)의 경우 영장 없는 수색과 압수를 제한적으로 허용하고 있다. 이때 예외적 상황이라 함은 증거가 파괴될 위험이 임박하였을 때, 경찰 또는 대중을 위험에 처하게

할 때, 경찰이 현장에서 용의자를 추격 중일 때, 영장발부 이전에 도주의 우려가 있을 때 등이 해당된다(Georgia v. Randolph, 547 U.S. 103 (2006)).

미국은 9/11 테러 이후 수사기능 강화 특별법(USA Patriot Act)을 제정해 정보기관과 수사기관의 사전 정보수집절차상의 방해요인을 최대한 제거하고, 수사기관의 전화, 전자우편에 대한 감청 및 의료·재무기록 열람권한 대폭 강화 등 강력한 감시권한을 부여했다. 외국인의 미합중국 영토 내 첩보활동을 수사할 때의 제한 완화, 이동감청제도 도입, 비밀수색제도 명문화 등이 이에 포함된다.

이동감청제도(roving wiretap)란, 기존 감청제도의 한계를 극복하기 위해 영장주의에 변화를 준 것이다. 감청대상자가 휴대전화를 교체하거나 거주지를 이전하는 경우, 기존에는 새로운 감청영장이 필요했으나, 이동감청제도의 도입으로 감청대상을 물리적, 사법적으로 ‘따라다니면서’ 감청하는 것이 가능하게 됐다. 특정한 전화회선이나 전자우편 계정을 명시하지 않은 채, ‘용의자가 사용하는 모든 유선·휴대전화 및 인터넷 계정’ 등의 형식으로 포괄적 기재를 허용하는 것이다.

비밀수색제도(sneak and peek)란 영장집행의 고지를 집행 후로 연기하는 제도로서, 수색대상지의 소유자·거주자의 동의를 받지 않고 사전에 고지하지 않고 비밀스럽게 침입하여 수색하는 방법이다. 비밀수색에서 발견한 증거품은 압수할 수 없지만 비밀수색으로 획득한 정보를 근거로 차후에 압수수색영장을 발부받아 집행할 수 있다. 손쉽게 범죄의 증거를 은닉 가능한 사이버 테러리즘 사건의 경우 비밀수색제도가 강력한 도구로 기능할 수 있다.<sup>5)</sup>

긴급사태라는 것이 특별한 이례적인 상황이라 할 수 있겠지만, 국내에서도 언제든지 사이버테러와 같은 것이 올 수 있다는 점에서 관련 법·제도적 준비가 필요하다. 구체적

---

5) 미국 법원은 비밀수색이 적법하다고 판시했다(United States v. Simons, 206 F.3d 392 (4th Cir. 2000)). 수정헌법 제4조에는 그 통지에 대한 언급이 일절 없으며, 비밀스러운 침입과 그에 필연적으로 수반되는 통지의 지연 또한 기술하고 있지 않기 때문에, 수정헌법 제4조의 요구조건을 충족한 이상, 공정성과 중립성을 갖춘 판사가 상당한 이유에 기해 발부한 영장으로 이루어진 수색은 그 통지가 45일간 지연되었다고 하여 헌법에 위반되었다고 볼 여지가 없다는 것이다.

으로 총괄기관, 영장주의 예외, 비밀수색, 이동감청 등 특별장치마련에 관한 내용이 포함 되어야 할 것이다.

#### 마. 포렌식 전문가 양성과 자격제도

디지털 포렌식 전문가란, 수색·압수 현장에서 증거의 특성에 따라 최적의 방법론을 제시하고 실행할 수 있는 특수 수사요원이다. 미국 제9순회항소법원은 수사와 독립된 중립적인 ‘컴퓨터 요원’이 이러한 작업을 수행해야 함을 명확히 밝히고 있다.

디지털 포렌식에 대한 수요는 계속 증가하고 있다. 수사관의 전문적 분석 능력과 분석 결과의 신뢰성에 대한 요구가 증대되고, 전문가 의견이 소송에서 차지하는 비중이나 중요성이 강조되는 것이다. 디지털 증거의 신뢰성과 직결된 문제이기도 하다. 미국에서는 디지털 포렌식이 컴퓨터 등 특수기록매체에 저장된 디지털 증거에 관한 적정절차로서 소송당사자의 의무로 간주되고 있다. 따라서 디지털 포렌식 전문가의 역량을 강화하고 공신력 및 통용성을 제고시킬 수 있는 자격제도의 운영이 필요하다. 인터넷에서의 법률 행위에 대한 자격증 제도, 디지털증거를 법정에서 제출하는 적정한 절차에 관한 연구 및 이를 다루는 전문가 제도도 마련해야 한다. 국제 소송 관계에서는 이런 전문가가 자료를 제출하는 것이다.

#### 바. 사이버범죄의 최근 동향과 전망

최근 들어 발생하고 있는 여러 가지 형태의 사이버 범죄에는 몇 가지 공통점이 있다. 첫째, 유출되는 데이터의 양이 상당하다는 것이다. 구글의 통신정보 도청사건, 옥션 사이트 해킹에 따른 고객정보 유출, GS칼텍스 하청업체의 개인정보 유출 등 개인정보 데이터가 대규모로 유출되고 있다. 둘째, 금융기관 해킹 등의 경우 금전적인 치안과 관계된 이슈인지, 경제 인프라를 상당히 불안하게 만들어서 사회 전반적의 위협을 야기하려는 안보적 차원의 위협인지 판단하기 어렵다. 적어도 초기 단계에서는 치안과 안보가 혼재되어 있다. 셋째, 금융기관이나 국가기관을 사칭하는 피싱의 경우도 상당히 지능화 되

는 추세다. 피싱 사이트를 사이버경찰청이나 검찰청 홈페이지와 비슷하게 만들어서 개인정보를 체계적으로 입수하는 등 지능화된 사례들이 발생하고 있다.

이처럼 치안과 관련된 부분 외에도 사이버 안보와 관련해 허위사실 유포를 통한 심리전, 해킹 공격을 통한 시스템 마비 또는 기밀 유출, 디도스 공격을 통한 서비스 중단 및 사회혼란 야기 등 사이버전 혹은 테러의 유형이 나타나고 있다. 국가 기반시설에 바이러스 살포, 댐·공항·철도·전력·원자력 등에 대한 시스템 마비, 중요한 기밀유출 등도 초기에는 단순 사이버 범죄 같지만 사이버안보의 문제가 내포돼 있을 수 있다. 이처럼 사이버스페이스에는 다양한 사이버 범죄의 위협이 존재한다. 조직 범죄자, 국가기관, 산업 스파이 등 사이버 안보를 위협하는 주체와 동기도 다양하다. 결국 최근의 사이버 범죄 동향은 치안과 안보의 혼재, 주체와 동기의 다양화로 요약할 수 있다.

## 제 2 절 프라이버시·개인정보 및 아동 보호 관련 글로벌 이슈 분석

### 1. 프라이버시 및 개인정보 보호

#### 가. 국제적 논의 동향

정보통신기술의 발전으로 컴퓨터에 의한 대량의 데이터 처리가 가능해짐에 따라 개인정보의 보호, 특히 전산 처리되는 개인정보의 보호 필요성이 강하게 제기되고 있다. 정보사회에서의 프라이버시권<sup>6)</sup>을 개인정보통제권<sup>7)</sup>으로서 개념을 재구성하는 연구는 ‘자기와 관련된 정보를 통제할 수 있는 권리’라는 적극적, 능동적 권리로 발전하게 됐다.

프라이버시 개념에는 인격권, 친교관계 비공개권, 비밀성의 원리, 자신에 대한 접근 통제권, 개인정보 자기결정권<sup>7)</sup> 등이 포함된다. 정보화가 진전될수록 개인정보 자기결정권의 중요성이 증가하고 있다. 정보사회에서의 개인정보는 상품화 되어 거래의 대상으로서 경제적 가치를 갖기 때문에 시장기능에 입각한 자율규제만으로는 보호되기 어렵다.

프라이버시와 개인정보보호는 안전하고 신뢰 가능한 접속 보장을 위해서도 논의가 필요하며, 기존에는 이런 프라이버시의 침해라는 부분이 정부 정책의 효율성이라는 부분에서 일부 침해가능성이 존재했으나, 최근에는 사이버 경제의 확산에 따라 시장에 의한 침해 부분이 더 문제가 되고 있으므로, 시장에 있어서의 개인정보보호 및 프라이버시 침해라는 부분에 대한 논의도 필요하다.

#### 1) OECD에서의 프라이버시 및 개인정보보호 논의

OECD는 1980년에 개인정보의 보호에 대한 국제적 동향과 관련하여 ‘개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인’을 채택하여 각국의 노력과 국내입법을 제정, 권고했다. OECD 프라이버시 가이드라인의 검토를 진행하는 자발적 그룹 의장은

---

6) 프라이버시권은 19세기말 당시 미국 언론기관의 유명인사의 사생활에 대한 무차별적 폭로 기사로 인한 범익침해가 기존의 명예훼손으로 인한 범익 침해와는 차이가 있음을 확인하고 새로운 불법행위의 법리를 창안하기 위하여 고안된 권리개념이다.

7) 다른 사람이나 기관에 공여된 자신의 개인 정보의 유통과 활용과정에 관여할 수 있는 권리

자발적 그룹의 보고서를 중심으로 작업반의 논의 현황과 향후 일정에 대해 설명했다.

<표 3-4> ‘OECD 프라이버시 가이드라인’ 적용상의 기본원칙

- o 수집제한의 원칙 : 합법적이고 공정한 절차에 의하고 가능한 경우에는 알리거나 동의를 얻은 연후에 수집하여야 함
- o 정보내용정확성의 원칙 : 이용목적에 부합하는 것이어야 하며 필요한 범위안에서 정확하고 완전하며 최신의 것이어야 함
- o 목적명확화의 원칙 : 수집목적은 늦어도 수집시까지 명확화 되어야 함. 그 후의 이용은 목적의 실현 또는 목적과 양립하여야 하고 목적 변경시마다 명확화될 수 있는 것으로 제한되어야 함
- o 이용제한의 원칙 : 주체의 동의가 있는 경우 법률의 규정에 의한 경우를 제외하고 명확화된 목적이외의 목적을 위하여 개시,이용,기타사용에 제공되어서는 안됨
- o 안전확보의 원칙 : 개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 함
- o 공개의 원칙 : 개인데이터와 관련된 개발, 실시, 정책에 대해 일반적인 공개정책을 취해야 함
- o 개인참가의 원칙 : 개인은 데이터관리자가 자기에 대한 데이터를 갖고 있는지 여부에 대하여 확인을 받은 권리, 개인에 대한 데이터를 본인에게 통지하도록 하는 권리, 자기에 대한 데이터에 대하여 이의를 제기하고 그 이의가 인정되지 않을 경우에 그 데이터를 소각, 수정, 안전화, 보완하게 하는 권리를 갖고 있음
- o 책임의 원칙 : 데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따른 책임이 있음

2) UN에서의 프라이버시 및 개인정보보호 논의

UN은 1990년 ‘전산처리된 개인정보 파일의 규제지침’을 발표했으며 이는 회원국들이 개인정보에 대하여 입법 등을 통해 규율하고자 할 때 참고하여 각국의 실정에 맞는 이행 방안과 절차를 채택하도록 하고 있다.

본 가이드라인은 개인정보 파일을 규율하는 다음의 여섯 가지 원칙을 제시하고 있다. 첫째는 합법성과 공정성의 원칙, 둘째, 정확성 원칙, 셋째, 목적구체화의 원칙, 넷째, 개인접근의 원칙, 다섯째, 비차별 원칙, 여섯째는 안정성 원칙이다. 예외적으로 국가안보·공공질서·공중보건 또는 공중도덕과 관련된 정보처리는 제1원칙부터 제4원칙의 적용을 받지 않는다.

### 3) EU에서의 프라이버시 및 개인정보보호 논의

EU에서도 개인정보보호에 관하여 강력한 정책을 추진하고 있으며, 1995년 ‘개인데이터의 처리와 개인데이터의 자유로운 유통과 관련된 개인정보 지침’을 채택했다. 이는 경제활동이나 행정목적, 기타 모든 영역에 있어서 개인정보를 수집하고 축적·이전하는 활동에 적용된다. 이에 EU는 본 지침을 보완하기 위해 1997년 ‘정보통신부문에서의 개인정보 처리 및 프라이버시 보호에 관한 지침’, 1999년 ‘정보고속도로에서 신상정보의 수집 처리와 관련한 개인의 보호를 위한 지침’을 채택했다. EU는 프라이버시 관련 지침(Directive)을 2012년 개정해 2014년부터는 레귤레이션(Regulation)으로 강화한다. EU 회원국에 관련 개별법이 없더라도 자동적으로 상위법으로 지배하는 위치를 갖는 것이다.

[그림 3-3] 개인정보보호법 제정 전 후의 보호 범위



### 4) 국내에서의 프라이버시 및 개인정보보호 논의

국내에서는 최근의 개인정보 침해가 대형화·지능화·다양화추세에 있으며 개인정보 보

호 관련 일반법 미비로 법 적용 사각지대가 발생한다는 지적에 따라, 2011년 개인정보 보호법을 제정하여 개인정보 보호에 대한 규정을 마련하고 있다. 개인정보보호법 시행 이후 개별법이 없는 경우라도 공공·민간부문의 모든 개인정보처리자를 대상으로 보호의 무가 적용되며 컴퓨터 등에 의해 처리되는 정보 외에도 수기문서를 포함하여 보호범위가 확대됐다.<sup>8)</sup>

## 나. 프라이버시 및 개인정보보호 관련 글로벌 이슈

### 1) 스마트폰 개인정보 무단 수집

미국 이동통신사들이 판매한 1억5천만여대의 스마트폰 가입자들의 개인정보를 무단으로 수집하는 기능을 가지고 있는 별도의 소프트웨어(캐리어IQ)가 설치된 사실이 드러났다. 국내에서도 삼성전자 갤럭시 시리즈에 기본적으로 탑재되어있는 앱에 개인정보 수집 권한이 포함되어 있다는 주장 제기됐다. 스마트폰을 통한 정보유통 증대가 네트워크 트래픽 증대로 이어지면서 이동통신사들이 패킷감청(Deep Packet Inspection)기술을 도입하기 시작했다. 당초 이 기술은 네트워크의 품질관리라는 목적에서 도입된 것이지만, 이를 통해 스마트폰을 통해 유통되는 각종 정보들의 내용까지 감시·감청이 가능하게 된 것이다. 공적 측면에서 불특정 다수의 프라이버시가 침해될 수 있으며, 사적 측면에서도 맞춤형 광고 등에 패킷정보가 활용될 수 있다. 또한 패킷정보를 분석할 경우 정보를 분석하여 개인 식별에 활용할 위험이 존재한다.

### 2) 구글의 사파리 개인정보 침해

미 연방통상위원회(FTC)에 따르면 구글이 PC에 쿠키를 심어 애플 사파리에 내장된 정보보호 기능을 우회하도록 한 개인정보 침해 혐의가 사실로 드러났다. 애플 사파리에는 제3자 쿠키를 차단하는 기능이 있으나 구글은 온라인광고에 특수한 코드를 설치해 이러한 기능을 우회해 정보를 수집해온 것이 발각된 것이다. 일일 침해 1건당 1만 6,000달러

---

8) 2010년 1억 건 이상의 개인정보 침해사고가 발생하였으며, 해킹 및 내부직원 유출 또는 담당자 부주의 등이 주요 원인으로 조사되고 있다.

의 벌금을 부과할 수 있어 미국 언론들은 대략 1,000만달러 이상의 벌금이 부과될 것으로 보고 있다.

### 3) SNS의 사용자 정보수집

<월스트리트 저널>이 인기 있는 100개의 페이스북 앱을 조사한 결과 대부분의 앱이 지나치게 많은 개인정보와 사용자의 친구 정보까지 수집하고 있는 것을 발견했다. 앱의 성격에 맞지 않는 개인정보를 요구한다거나 친구정보까지 수집하게 되는데, 친구들은 자료수집에 대한 동의절차를 거치지 않았으며 사용목적에 대해서도 통보를 받지 못했으므로 프라이버시 권리와 관련하여 문제가 발생할 소지가 있다. WSJ의 조사결과, 대부분의 페이스북 앱은 타겟광고를 위해 필요한 이메일, 위치, 성적취향, 종교 및 정치견해, 사진, 생일 등을 수집하고 있는 것으로 밝혀졌다. 무료 앱이라 하더라도 ‘행태기반 마케팅’을 통한 수익창출을 위해 개인정보를 수집하고 있었던 것이다.

#### <표 3-5> 소셜컴퓨팅 시대의 7대 프라이버시 우려

- 관리자의 부적절한 개인정보 이용
- 법적 요구에 따른 개인정보 공개
- 불충분한 보안 대책
- 디자인/설계상의 결함이나 오류에 따른 고의적 프라이버시 침해
- 사회적 추론에 따른 개인정보 노출
- 특정 이용자 행태를 꾸준히 추적해 그의 개인 정보를 밝혀내는 경우
- 사회적 영향력을 활용해 비밀정보를 취득하는 경우

### 4) 잊혀질 권리

‘잊혀질 권리’란 온라인에서는 사진, 구매정보, 거래정보, 개인의 성향 등 개인정보의 이전이 용이하므로, 개인의 자기정보 소유권 강화 및 개인정보 보호를 위하여 온라인기업, SNS 등 개인의 동의하에 제공된 개인정보 뿐 아니라 인터넷 신문기사, 개인블로그, 포털사이트에 올라와 있는 개인정보에 대한 삭제를 요구할 수 있는 권리이다. 유럽에서

는 ‘잊혀질 권리’에 대한 법제화가 추진 중에 있다. ‘개인정보 보호에 관한 지침’ 개정 초안에는 정보의 삭제 권한을 개인이 갖도록 하는 내용이 포함될 것으로 전망되고 있다. ‘잊혀질 권리’ 개정안은 유럽연합에 서버를 두고 있는 인터넷 서비스 업체에만 적용하는 것이 아니다. 역외에 서버를 두고 있더라도 유럽연합 거주자에게 인터넷 서비스를 제공하는 경우 일괄적으로 이 법의 적용을 받게 된다. 이에 대해 미국은 정-재계 모두 강력히 반발하고 있다. 미국 상무부는 개정안이 상업적 목적을 위한 정보처리의 상호운용을 막고 동시에 소비자 정보 보호를 막게 될 것이라고 주장하며 개정안에 반대하고 있다.

한편, 2011년 1월 스페인의 개인정보보호원은 일간 엘파이스(El Pais)를 비롯한 신문기사 중 약 100건에 대해 명예훼손 가능성이 있다며 구글에 해당 기사링크 중단을 요구하여 인터넷 이용자가 ‘민감한 기사’에 접근하지 못하도록 요구했다. 구글은 이에 반발하여 검색엔진과 같은 중개자가 다른 곳에서 생산된 콘텐츠를 검열하라고 요구하는 것은 개인의 사생활을 보호하지 못하고 자유로운 표현을 침해한다면서 기사 링크 제한 요구에 반발했다. 또, 2010년 10월 구글의 스트리트뷰와 관련해 스페인 당국이 개인정보 침해를 거론하며 구글을 마드리드 법원에 제소했으며, 2009년 독일범죄자들이 위키피디아를 상대로 자신들의 이름을 삭제해 달라는 소송을 제기한 바 있다.

##### 5) 구글의 개인정보 통합

구글이 지메일, 구글플러스, 유튜브 등 자사의 60여개 이상의 서비스의 개인정보를 통합한다고 발표하여 ‘빅브라더’ 논란이 촉발됐다. 구글의 발표와 함께 미 하원의원 8명이 공개질의서를 보낸 데 이어, 10여명의 의원들이 구글의 법률고문과 공공정책이사를 불러 비공개 설명을 듣기도 했다. 또한, 미국 주요 시민단체의 경우 구글의 ‘정보권력 독점’을 우려하며 반대의사 표명했다. 한 회사가 특정소비자에 대한 총체적인 정보를 수집하는 것 자체가 소비자 사생활에 대한 심각한 피해이며 아직 어린 청소년의 경우 향후 취업 등에 큰 불이익을 받을 수 있다는 것이다. EU는 이러한 정책에 강력히 반발하며 구글의 새로운 정책이 소비자에게 미칠 영향에 대한 조사 종료시까지 서비스 개시 연기를 요청하였으나 구글이 이를 거부했다. 국내에서도 한국개인정보보호협의회에서 구글이

모든 개인정보를 통합관리 할 경우 개개인을 특정할 수 있기 때문에 개인 프라이버시 침해가 있을 수 있다고 지적하며, 구글의 개인정보 취급방침 개정 철회를 촉구했다.

#### 다. 프라이버시 보호 국제 협약 필요

프라이버시의 경우 유럽, 미국, APEC 등 각 지역마다 그 수준이 상이하다. 유럽에서 프라이버시 권리는 인간의 존엄권(human-dignity right)인 반면, 미국에서는 프라이버시 권리가 ‘소비자를 보호하는 권리’로 이해된다. 미국에서는 권리장전의 ‘표현의 자유’가 우선인데 반해, 유럽에서는 ‘프라이버시’가 우선인 것이다.<sup>9)</sup>

또한 미국은 공공부문은 프라이버시로 되어 있고 필요에 따라 개별법을 두고 통제한다. 그래서 주로 소비자의 프라이버시에 관한 관할도 미국연방통상위원회(Federal Trade Commission)에서 한다. 반면 EU에서는 프라이버시가 정보 자체를 보호하자는 개념으로 인식되고 있으며, 공공부문과 민간부문이 개인정보에서 기본법으로 되어 있고, 기본법과 함께 감독 기구를 의무적으로 설치할 것을 명시한다. 또한, EU에서 개인정보가 다른 나라로 유통되었을 때, 제3국의 프라이버시 법제 수준이 적절하거나 동일하지 않을 경우에는 정보를 주지 못하도록 되어 있다.

2000년대 들어서 미국의 요청으로 미국과 EU간 협약을 통해 세이프 하버 협정(Safe Harbor Agreement)을 발표했다. 세이프 하버 협정은 미국과 유럽 연합(EU) 간에 맺은 개인 신상 정보(PII)의 전송에 관한 협정으로 미국 상무성의 세이프 하버에 등록하고 이를 준수하는 기업들은 EU에서 미국으로 전송되는 개인정보를 위한 적절한 보호 조치를 취한 것으로 간주된다. 협정 내용에는 고지, 선택, 접근, 제3자 전송, 보안, 데이터 무결성 및 법률 시행 등 7개항의 원칙이 있다.

하지만 여전히 미국과 EU의 법체계가 다른 상황이다. 특히 EU는 2014년부터 지침에서 규정으로 개정이 된다. 규제의 경우, EU회원 개별국은 이에 대한 개별법이 없다 하더라도 자동적으로 상위법으로 지배하는 위치를 갖는다. 구글의 개인정보 통합정책에 대

---

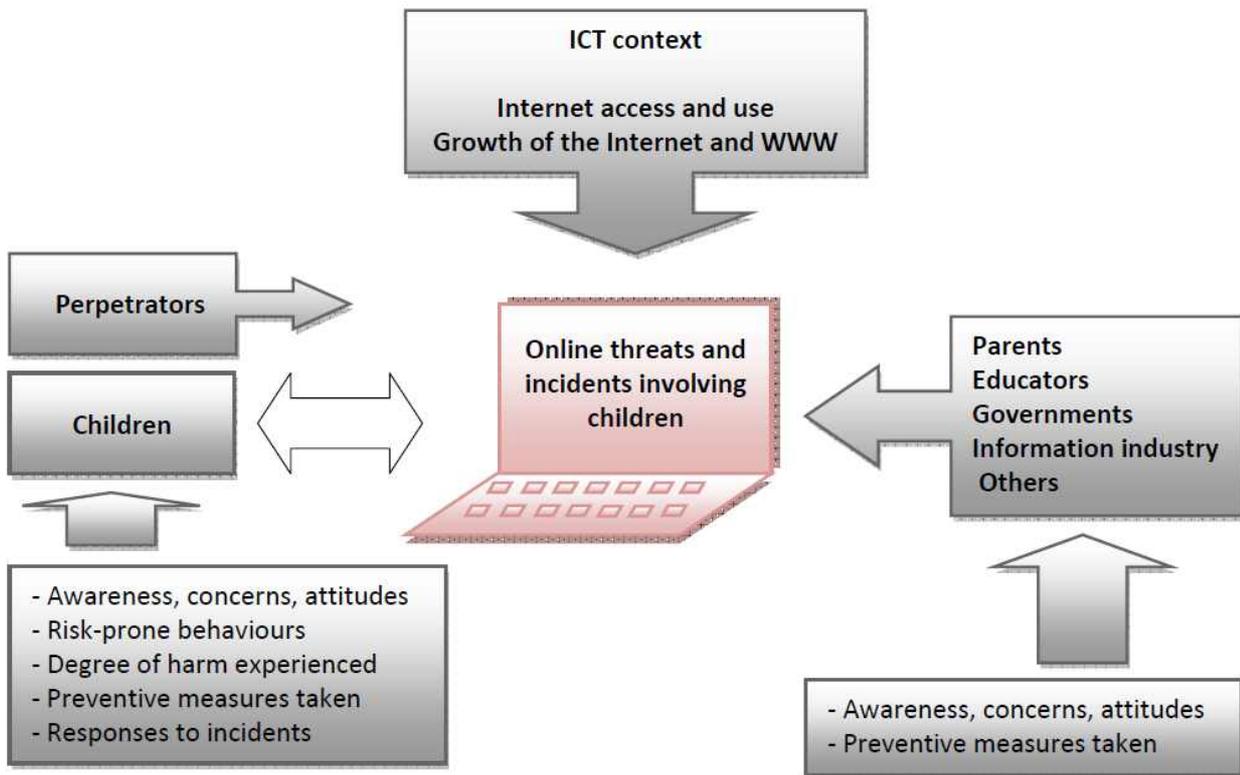
9) 출처: ‘When American and European Ideas of Privacy Collide’, 뉴욕타임즈, 2010.

해서도 미국과 EU는 심각한 개인 프라이버시 침해에 반발하는데 반해, 인도와 캐나다는 ‘실용적 접근’이라며 이에 대해 긍정적인 입장을 보이는 등 국가별 대응이 다르다. 이처럼 프라이버시에 대해 주요 국제기관 개인정보보호 국제규범을 통한 노력은 진행되고 있지만 수준이 상이하기 때문에 프라이버시 보호 국제 협약이 필요한 상황이다.

## 2. 아동보호

20세 미만의 아동 및 청소년의 온라인 및 모바일 등 사이버 공간에 대한 노출이 늘어나고 있으며 이와 관련한 부작용이 지속적으로 발생하고 있다. 이에 따라 사이버 공간에서 아동을 보호해야 할 필요성이 높아지는 추세다. 해외 각국에서는 사이버 공간에 노출되어 있는 아동을 보호할 수 있는 방안을 마련하고 있다.

[그림 3-4] 온라인 아동보호 개념

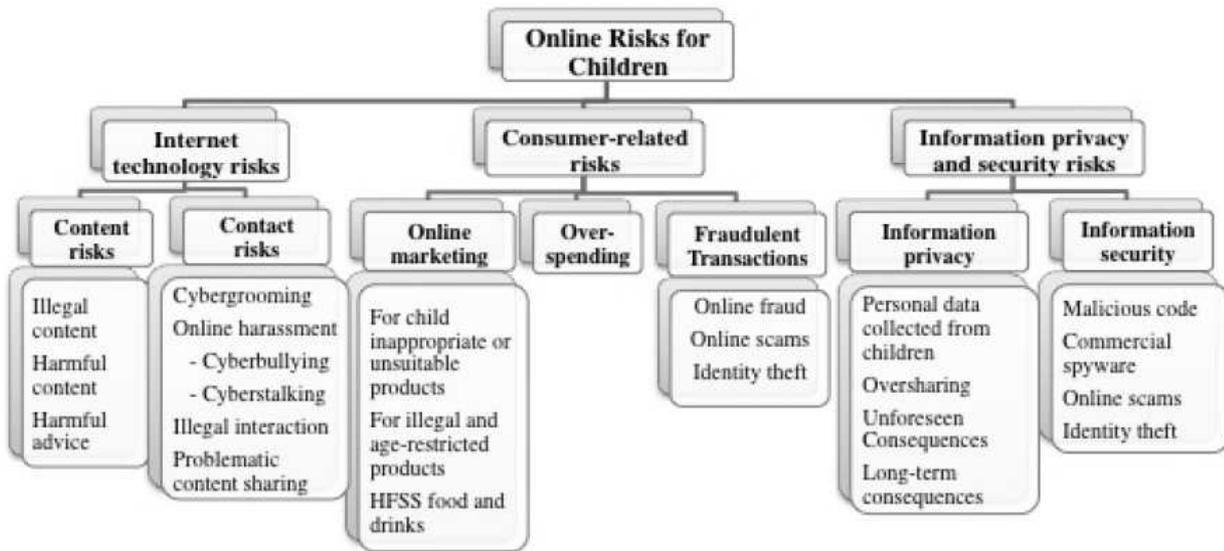


출처: ITU(2010)

ITU에서는 아동이 인터넷에 노출될 가능성이 커진 상황이기 때문에 학부모, 교육자, 정부 및 기타 정보 산업에 종사하는 모든 이해당사자들의 적극적인 개입이 필요하다는 입장을 견지한다. 현재 상황은 아동들이 유해 콘텐츠, 사이버 상에서 일어나는 커뮤니케이션상의 위협, 미성년자의 범위에서 해결할 수 어려운 과소비(온라인 및 모바일 게임 결제 등) 등 여러 가지 위협에 직면하고 있다. OECD는 아동이 처한 이러한 위협을 인터

넷의 기술적인 위험(Internet technology risks), 소비자 관련 위험(consumer-related risks), 정보보안 위험(information privacy and security risks) 등으로 접근한다.

[그림 3-5] 온라인상의 아동 위험 요소



출처: OECD(2011)

아동과 관련된 인터넷 피해는 크게 게임 중독, 언어폭력, 인터넷 성매매 관련 정보 등과 같은 유해콘텐츠 노출 등으로 구분할 수 있다. 인터넷의 보급과 확산으로 인해 아동들에게 노출도가 높아진 유해 콘텐츠는 스마트폰의 보급으로 인해 더욱 노출도가 증대되는 상황이다. 또한 게임중독으로 인해 아동들이 정상적인 일상생활을 영위하지 못하는 경우가 늘어나고 있다. 온라인 게임 중독은 행위 측면에서 폭력행위를 모방할 수 있다는 있다는 측면에서 위험성이 크며 스마트폰의 보급으로 인해 상시적으로 게임에 접속할 수 있다는 점에서 심각성이 더해진다.

또한, 사이버 공간에서의 언어폭력이 갈수록 심각해지고 있는 상황이다. 언어폭력에 의한 사이버 공간에서의 커뮤니케이션 부작용으로 인해 아동들의 정상적인 의사소통에 지장을 주는 사례 발생하고 있다. 온라인 공간을 통해 벌어지는 성매매, 섹스팅(sextin g)<sup>10)</sup> 등 사이버공간에서 이루어지는 청소년들의 무분별한 사이버 성행위가 문제가 되고

있는 상황이다.

OECD, ITU, EU 등에서는 온라인 위협에 노출되어 있는 아동들을 위한 대책을 마련하기 위해 가이드라인을 제정하고 있다. OECD는 산하 정보보호작업반에서 2012년 2월 16일 온라인상의 아동들이 직면한 위협과 각국의 보호 정책을 분석하여 온라인상 아동보호에 관한 이사회 권고안을 마련하여 발표했다. 또한 OECD는 이전부터 사이버 공간 상에 노출된 아동의 위협에 대해 관심을 기울여 왔으며, 2011년에 "The Protection of Children Online" 발표했다. 이와 관련하여 2008년 6월 서울 OECD 정보통신장관회의에서 인터넷 이용 아동에 대한 보호와 지원을 강화하기 위해 정부, 민간, 인터넷 기술 분야 간 협력이 필요함을 강조하고, 사이버 보안, 스팸 근절, 개인정보 보호 및 미성년자 보호 개선 분야에서 범국가적 협력을 촉구했다. 또한 OECD와 APEC은 '서울 선언문' 이행을 위해 2009년 4월, 싱가포르에서 공동 심포지움을 개최했으며, OECD 정보통신정책위원회 산하 정보보호작업반(WPISP)에서는 온라인상 아동들이 직면한 위협과 각국의 보호 정책을 분석, 위의 분석결과를 토대로 2011년과 2012년에 권고안을 발표했다.

ITU는 Global Cybersecurity Agenda(GCA)를 발족하여 사이버 위협에 대한 국제적 대응 강화 협력 체계를 구축하고 아동보호를 위해 GCA 하에 Children Online Protection(COP) 이니셔티브에 착수했다. COP의 세부목표는 첫째, 사이버공간상의 아동에 대한 주요 위협 및 취약점 파악하고 둘째, 사이버공간에서의 아동보호 이슈에 대한 인식을 제고하고 셋째, 위협을 최소화하는데 도울 수 있는 실용적 도구의 개발 및 보급하고, 넷째, 국제사회 내 이와 관련 지식 및 경험 공유하는 것을 목표로 삼고 있다.

EU의 경우에는 Safer Internet Programme을 통해 아동들의 안전한 인터넷 이용을 보장하고, 온라인상에서 자신을 보호할 수 있는 권한을 부여하기 위한 EU 차원의 활동이 활발히 진행되고 있다. EU의 Safer Internet Programme은 소셜 네트워킹과 유해 콘텐츠를 포함한 사이버불링(bullying)과 그루밍(grooming)과 같은 불법적 행위에 대처하고 있다.

---

10) 섹스팅은 휴대전화로 나체사진을 보내거나 성적인 암시가 있는 사진을 보내는 행위를 의미함

<표 3-6> OECD 권고안 주요 내용(2012년)

[온라인상 아동보호에 관한 정책 수립시 정부와 다른 모든 이해당사자들에 대한 권고]

- 정부와 모든 이해관계자는 보다 안전한 온라인 환경을 조성하고, 정책 수립을 통한 위험 평가 및 최소화 의무
- 온·오프라인에서 위험을 최소화하는 과정에서 부모가 1차적 역할과 책임이 있다는 사실 인식
- 비례의 원칙에 따라, 아동은 물론 그 밖의 인터넷 이용자들에 대한 인터넷 이용의 기회를 제약하지 않으면서 온라인 위험에 대한 보호를 극대화
- 표현의 자유, 개인정보보호 및 정보 접근권, 정보 공유권과 같은 민주주의의 기본권에 부합
- 아동의 연령, 발달정도, 사회적 취약성을 고려한 유연성과 빠르게 진화하는 기술에도 적용할 수 있는 지속가능성이 존재

[국가 차원의 정책 수립시 정부에 대한 권고사항]

- 공공 및 민간분야 이해당사자들의 의견을 수렴하고, 일관성·통일성 있는 정책 추진
- 부모 및 아동 교육을 통한 인식제고, 조사 등을 통한 증거에 기반한(evidence-based) 정책을 지원하고 해당 정책을 정기적으로 평가
- 아동의 권리 및 인터넷 이용자의 자유를 존중하는 연령확인 시스템, 프라이버시 보호수단 기술의 개발 및 적용을 장려

[국제적 차원에서 정책 수립시 권고사항]

- 온라인상 아동 보호를 위한 핫라인 네트워크 등 국제 네트워크를 강화하고, 국제적 비교 분석을 위한 정보 공유
- OECD, APEC, IGF, ITU 등을 비롯하여 비정부 이해당사자를 포함해 다양한 국제적·지역 기구의 업무에 협력

출처: 한국인터넷진흥원(2012)

### 제 3 절 사이버공간의 경제적·사회적 혜택 관련 글로벌 이슈 분석

#### 1. 사이버공간의 경제적 혜택

##### 가. 사이버공간의 특징

사이버공간의 특징은 다음과 같이 5가지로 정리할 수 있다. 첫째, 사이버스페이스는 정보의 공유와 확산이 아주 용이하다. 네트워크를 통해서 그동안 있었던 정보의 비대칭성이 해소됨에 따라 정보의 공유와 확산이 빠르고, 전파속도도 빠르다는 특징을 갖고 있다. 둘째, 공간개념이 소멸되고 있다. 네트워크를 통해서 그동안 제약으로 있었던 공간적인 제약문제가 해소된다. 셋째, 네트워크 효과가 나타난다. ‘멧칼프 법칙’에 따르면, 네트워크의 가치는 네트워크 사용자 수의 제곱에 비례한다. 켈리의 법칙은 인터넷 가치는 사용자 수의 승수에 비례한다는 것이다.  $n$ 의  $n$ 승으로 사용자에게 따라 인터넷의 가치가 증가한다고 표현한다. 넷째, 사이버스페이스의 특징은 융합기능이다. 컴퓨팅, 통신서비스, 콘텐츠산업, 지식산업 등의 제반 서비스와 기기와 산업이 융합하는 공간이라고 할 수 있겠다. 또 하나는 예측이 상당히 어렵다는 점이다. 과거에는 예측 가능하던 것들이 전파의 속도, 공간적인 제약의 해소 이런 것들로 인해서 사이버스페이스에서는 예측할 수 없는 사건과 이벤트들이 수시로 발생하고 사라지기도 한다. 다섯째, 수확 체증의 법칙이 존재하는 공간이다. 과거 제조업 중심의 사회에서는 기본적인 고용 비용, 기본적으로 필요했던 고정비용 문제가 사이버스페이스에는 통용되지 않고 있다. 단위 생산량을 늘리더라도 그에 따른 비용이 크게 늘어나지 않는다. 대표적으로 소프트웨어를 한번 개발하는데까지는 많은 비용이 들어가지만, 그 이후에는 거의 비용이 발생하지 않는다. 사이버스페이스의 가치가 사용자수의 제곱에 비례한다는 것은 링크의 개수가 그만큼 늘어나는 것이고, 변동비용은 상대적으로 아주 작다는 것이다.

##### 나. 사이버공간의 경제적 환경

사이버스페이스 상에서는 경쟁력의 변화가 나타난다. 과거에 비해 속도와 커스터마이

즈가 중요한 화두가 된다. 또한, 기존 경쟁 상황 안에서 가격경쟁이 상당히 격화된다. 예를 들어, 인터넷 포털사이트에서 가격을 다 비교해 주기 때문에, 자연스럽게 가격에 대한 경쟁이 심화되고 있다. 진입 장벽이 낮아지고 상대적으로 기득권 유지가 어렵다. 이는 과거 전통적인 산업과의 차별점이다. 대체 제품과 서비스의 위협이 증가하기도 하고, 경우에 따라 감소하기도 한다. 이처럼 정보의 불균형이 해소됨에 따라 공급자의 협상력이 상당히 약화되고, 상대적으로 구매자의 협상력이 대폭 강화된다. 온라인상에서는 정보의 비대칭성이 해소되고, 공간적인 제약, 선택의 전환이 아주 용이하게 된다. 이에 따라 전환비용이 감소되고, 구매자의 영향력이 증가하게 된다.

#### 다. 사이버공간의 경제적 혜택

사이버스페이스의 인터넷 경쟁, 디지털경제의 확산으로 인해 진입장벽이 상당히 약화되었다. 비용의 절감, 특히 B2B 거래비용이 상당히 줄어드는 경제적 혜택이 있었다. 수확 체증 현상으로 있어서 사이버스페이스에 통용되는 제품에 대한 물가가 하락한다. 또한, 고용의 증대와 동시에 전통산업에서는 고용이 감소되는 현상이 동시에 발생한다.

소비자 행태 역시 변화했다. 과거에는 물건을 사려면 돌아다녀야 했지만, 이제는 책상에 앉아서 원하는 상품을 검색하고 구매한다. 공급자 측면에서도 과거에는 대량생산으로 원가를 줄이는 개념이었지만, 이제는 커스터마이징 하는 것이 기업이나 공급자의 이슈가 되고 있다.

시장에도 상당히 많은 변화가 있었다. 시장에서는 과거의 중간 유통업체가 상당히 중요한 역할을 했지만 최근에는 직거래 같은 것들이 나타나고 있다. 중간 유통업체의 역할이 상당히 감소하면서, 시장에서 기업과 소비자 간의 거리가 단축되고 있는 것이다. 이에 따라 과거에는 경제활동에서 지역성이 상당히 중요했지만, 지금은 사이버스페이스 상에서 지역성이라는 것이 별로 중요하지 않게 되었다. 인터넷을 통해 경제활동의 수요 시간도 단축되고 있다. 거래의 소요시간이 굉장히 단축되고 있다.

장소에 구애 없이 개인 간의 커뮤니케이션이 활성화되기 때문에, 개인의 추천이나 사

용 후기 등 그리고 상호작용이 거래에 영향을 미치고 있다. 그리고 SNS가 활성화됨에 따라 영향이 확대되고 있다. 이런 것들이 개발도상국의 입장에서 본다면 성장의 새로운 기회가 될 수 있을 것이란 이야기도 나오고 있다.

<표 3-7> G20 국가의 인터넷 경제 규모 및 전망

	2010			2016			연평균 성장률 (CAGR)
	GDP	인터넷 경제규모	GDP 비중(%)	GDP	인터넷 경제규모	GDP 비중(%)	
G20	54.9	2.300	4.1	79.9	4.200	5.3	10.8
EU27	16.2	0.619	3.8	20.0	1.133	5.7	10.6
미국	14.5	0.684	4.7	18.6	1.000	5.4	6.5
영국	2.3	0.187	8.3	2.8	0.347	12.4	10.9
한국	1.0	0.075	7.3	1.4	0.114	8.0	7.4
일본	5.5	0.258	4.7	6.6	0.372	5.6	6.3
중국	5.9	0.326	5.5	12.4	0.852	6.9	17.4
인도	1.7	0.070	4.1	4.3	0.242	5.6	23.0
프랑스	2.6	0.073	2.9	3.1	0.105	3.4	6.1
독일	3.3	0.100	3.0	3.9	0.157	4.0	7.8

단위: 조달러

출처: BCG(2012) 재구성

2010년을 기준으로 G20 인터넷 경제 규모는 약 2조 3천억 달러로 전체 GDP의 4%에 해당된다. 인터넷경제란, 경제주체가 인터넷을 통해 제품이나 서비스 생산 활동에 참여해 창출한 부가가치를 평가한 합계로서, 포털 서비스, 모바일인터넷 서비스, 인터넷 게임, 인터넷 बैं킹, 인터넷 TV방송 등이 포함된다. 2016년에는 4조 2천억 달러 정도로 약 2배 성장해 전체 GDP의 5.3%를 차지할 것이라는 예측된다. 2016년의 경제규모로만 보면 미국, 중국, 일본, 인도 다음의 세계 5위 정도 수준으로 인터넷경제가 성장할 것이라는 전망이다. 국내의 경우 2010년 GDP의 7.3%였는데, 2016년에는 8.0%가 될 것으로 보인다.

<표 3-8> 사이버공간의 경제적 혜택

구분	내용
성장의 촉진	IT 산업 :1991-99년 23.4%성장
진입장벽의 완화	완전경제, 투명경제
비용의 절감	B2B 거래비용 절감효과
수요의 증대	공급곡선 하향 이동, 기업 투자 촉진
물가의 하락	수확체증 현상, 관리·물류·유통 비용절감
고용의 증대	정보통신산업 고용창출 churning effect
소비자 형태의 변화	'Sit & Search', 'Roam & Receive'
공급 형태의 변화	mass-production → mass-customization
시장의 변화	중간유통업체 소멸, 기업-소비자간 거리단축
변화의 가속화	경제활동의 지역성 탈피, 글로벌화, 경제활동의 소요시간 단축
상호작용의 증가	장소의 구애 없는 개인간 커뮤니케이션, SNS 활성화 및 영향력 확대
개방성 확대	정부, 기업 보유 정보의 개방화
시간적 제약의 탈피	365일 비즈니스, 거래 소요시간 단축
개발도상국의 성장기회	전세계 상대, 부유 고객 근접

출처: 2012~2013 사이버스페이스 총회 준비 워크숍 자료집

## 2. 사이버공간의 사회적 혜택 및 인권

### 가. 국제적 논의 현황

#### 1) 2011 런던 사이버스페이스 총의에서의 논의

사이버공간에 대한 의존도가 계속 높아지고 있는 상황에서 사이버공간에서 허용되거나 또는 금지되는 행동에 대한 합의 도출과 규범에 대한 논의가 필요하다는 취지에서 ‘사회적 혜택’이라는 부분이 의제로 포함됐다. 런던 사이버스페이스 총회에서 논의된 사회적 혜택은 크게 세 부분으로 구성되어 있다. 첫째, 인터넷과 사이버 공간이 가져오는 사회적 혜택, 둘째, 사이버 공간으로 인한 사회적 역작용 또는 문제점. 셋째, 인터넷에서의 표현의 자유와 규제 간의 균형을 어떻게 달성할 것인가 등이 주요 논의 사항이었다.

런던회의에서 사회적 혜택과 관련해 도출된 사항은 크게 4가지다. 첫째, 사회적 혜택으로서 상호관계성이 증가한다는 것이다. 상호관계성의 증가는 결국 사이버공간이 사회적 자본으로 작용한다는 것으로 이해할 수 있다. 사회적 자본은 ‘멧칼프의 법칙’과 ‘리츠의 법칙’에 따라 연결망이 조금 심화될수록 거기에 따른 가치는 배증하거나 승수로 증가한다.

둘째, 새로운 공론 영역으로서의 사이버 공간이다. 의견이나 정보수렴의 통로로 사이버공간이 활용되고, 특히 SNS의 확산에 따라서 정보나 의견의 전파가 용이하다. 런던회의 당시에는 아랍중동권의 자스민 혁명이 글로벌 이슈였기 때문에, 특히 SNS를 통한 정치적 참여로써의 공론장의 기능 측면이 강조됐다.

셋째, 시간-공간 제약을 극복한 서비스 이용으로 전자상거래의 일반화, 이러닝(e-learning) 및 디지털 콘텐츠 이용의 편의성이 논의됐다.

넷째, 인터넷을 통한 정부 서비스(전자정부)의 확산에 따라 참여에 의한 민주주의적 가치가 확대된다. 그리고 표현의 자유와 권리침해라는 상충되는 부분에 대해, 표현의 자유와 규제간의 조화 노력을 통한 사회적 합의를 위해 이용자에 대한 권익보호, 배려, 시장과 정부 간의 공동노력이 필요하다.

따라서 런던회의에서는 사이버 공간의 사회적 혜택을 증진하기 위해 국가 간의 공동

노력이 필요한 4가지 규범을 제시했다. 첫째, 자국이나 국제법을 준수해야 한다. 둘째, 이용자들은 언어, 문화, 사상 및 사고의 다양성을 존중하고 관용적 태도(‘톨레랑스’적인 태도)를 견지할 필요가 있다. 셋째, 사이버공간의 혁신에 대한 개방, 사상과 사고의 자유로운 이동, 정보와 표현의 자유를 보장할 필요가 있다. 넷째, 프라이버시에 대한 개인의 권리 보장 및 보호, 지적재산권에 대한 보호 조치를 제공해야 한다.

## 2) 2012 부다페스트 회의에서의 논의

2012년 부다페스트 회의 의제에서는 사회적 혜택이라는 부분은 유지하면서 ‘인권’이라는 부분이 추가됐다. 그 이유는 첫째, 2012년 런던회의에서 사이버인권에 대한 보호, 보장 방안에 대한 의제 설정 요구가 제기됐기 때문이다. 둘째, 사이버공간의 사회적 혜택 외에 인권이라는 인류의 보편적 가치를 강조함으로써 사이버공간에서 최근 대두되고 있는 정보인권 및 프라이버시의 침해에 대한 공통의 노력을 모색한다는 것이다. 셋째, 개도국에서 정보인권이나 프라이버시 침해의 가능성이 높고, 최근 개인정보 침해가 계속 증가하고 있으며, 개인정보나 인권이 사이버공간 안에서는 경제적 가치로 전환돼서 거래되고 있다는 점이 반영된 것으로 보인다. 넷째, 기존의 사이버공간의 혜택(사회적 자본, 교육확대, 정보격차 해소 등)에 사이버공간의 사회적 문제점(표현의 자유 침해, 프라이버시 침해, 사이버 플레이밍(flaming)과 불링(bullying) 등)에 대응한 인권 의제가 추가되었다는 점에서 의의가 있다.

그렇다면 글로벌 차원에서 사이버공간의 인권 의제는 4가지 정도로 정리할 수 있다. 첫째, 국가 간의 이념 차이에 의해서 정부 및 기관에 의한 표현의 자유나 프라이버시 침해에 대한 부분이다. 둘째, 사이버공간 및 시장의 확대에 따라 인권적 요소의 금전적·경제적 거래가 많이 일어나면서 인권적인 요소가 경제적인 요소 때문에 침해받는 양상에 대한 것이다. 셋째, 표현의 자유와 사회적 플레이밍·사이버 불링 등에 대한 규제와의 균형 문제다. 넷째, 사이버 공간에서의 반인류적인 인종차별주의, 사이버공간의 매카시즘, 선동주의 등을 억제하기 위해 인권적인 요소와 가미해서 규범체계를 확립할 필요가 있다.

## 나. 사회적 혜택

### 1) 로컬에서 글로벌 차원의 사회적 자본 구축

사회적 혜택의 범위는 매우 넓기 때문에, 추가로 발굴해야 될 의제라는 관점에서 4가지 정도로 접근할 수 있다. 그중 첫째는 로컬에서 글로벌 차원의 사회적 자본구축이라는 부분의 의제를 고민해야 한다는 것이다. 기본적으로 사회적 자본이라는 것은 상호 인지하는 관계적 존재로써 연결망이 형성하게 되는데, 이 연결망을 통해 개인 간, 집단 간의 연결망을 통해서 창출되고 형성되는 자본을 의미한다. 예를 들어 ‘집단지성’이라고 하는 것들이 자본화 된다는 것이다. SNS와 같은 사이버 네트워크의 확산은 지역 및 국가 공동체의 경계를 초월하는 탈 지역적 사회적 자본의 출현을 가능케 하고, 국가간 글로벌화된 연계망은 ‘약한 유대’를 기반으로 하면서 사회적 자본 축적에 보다 효율적이다. 동질적 관심과 가치관이 이질적 경험을 통해서 신뢰를 기반으로 해서 결합될 때, 사회적 자본이 가장 효과적으로 발생한다. 예를 들어, 글로벌적인 관점에서 동질적인 가치관이나 규범체계가 있다고 가정하고, 이를 공유하면서 그 연결망이 신뢰를 통해서 형성되어 있을 때는 굉장히 높은 사회적 자본효과의 축적효과가 발생한다는 것이다. 이것은 글로벌화 되는 사이버 공간의 지향점이라고 할 수 있다.

### 2) 사이버 공간의 특수성과 문화 창달

국내의 특수성을 반영하면 사이버 공간의 특수성과 문화 창달이라는 부분도 강조할 필요가 있다. 특히, 한국은 높은 인터넷 보급률과 인터넷 문화가 형성돼 있고 한류로 대표되는 콘텐츠가 있기 때문에, 사이버공간에서의 문화 창달과 사이버 공간에서의 사회문화적 혜택이라는 부분으로도 연결될 수 있다.

### 3) 사이버공간의 사회적 역기능

사이버공간의 사회적 역기능은 중독, 콘텐츠의 유해성, 사이버폭력, 권리침해, 왜곡 등 5가지 정도로 범주화 할 수 있다. 이중에서 콘텐츠의 유해성, 사이버폭력, 사이버권리침해, 왜곡(인종차별, 선동행위) 등이 글로벌 차원에서 논의될 수 있는 이슈일 것이다.

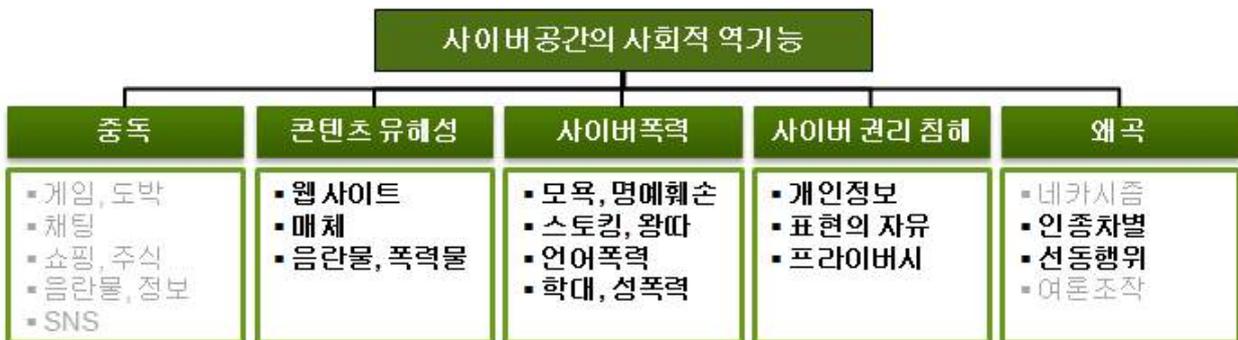
<표 3-9> 사이버공간의 특성과 문화 창달

문화의 특성			문화의 영향	
문화형성	문화전파	문화내용	장점	단점
익명성	-	탈억제	자기표현, 정체 실험	무책임성, 무절제
개방성	-	다양성	지위의 평등화, 참여기회 확대	무임승차, 집단규범 약화
연결성	전파성	-	공동체 형성, 정보 공유	탈개인화, 비검증 정보 확산
초월성	-	가상성	장벽 극복, 사고실험	현실 유리, 현실 도피
선명성	-	극단성	역할이해	고정관념, 비정상적 행위

#### 4) 사회적 역기능과 통제

이러한 역기능이 있을 때 어떤 식의 통제가 이뤄질 것인지도 이슈가 될 수 있다. 사이버 역기능이나 일탈의 요인은 구조적 요인, 문화적 요인, 개인적 요인 등 3가지 정도로 볼 수 있다. 구조적 요인은 사회구조상에서 법규의 미비라든지 구조적 특성을 의미하는 것이고, 문화적 요인은 어떤 국가에서는 그것이 큰 흠이 되지 않는데 다른 문화에서는 흠이 될 수 있는 것들이 해당된다. 또 개인적인 부분도 원인이 될 수 있다.

[그림 3-6] 사이버공간의 사회적 역기능



\* 굵게 표기된 사항은 글로벌 의제로써 다뤄질 필요가 있는 이슈

기존의 사이버 공간이나 오프라인 공간에서의 거버넌스 구조는 법령을 통한 정부주도 형이었고, 전문가 집단에 의한 거버넌스 구조를 가졌다. 그러나 익명성, 연결성, 가상성,

극단성 등의 특성이 있는 사이버 공간에서는 현실 공간과 달리 법적 규제 효력이 크게 감소할 수 있다. 사회통제 기제 역시 공식적 통제보다는 비공식적 통제가 상대적으로 크게 작용한다. 이에 따라 최근에는 이용자나 시장에 의한 거버넌스로 이동하고 있다. 이는 결국 이용자의 입장에서 자정능력을 배양해야 한다는 필요성이 존재하는 것이고, 시장에 있어서는 자율규제라는 부분이 굉장히 중요하다는 논리로 연결된다.

<표 3-10> 사회적 역기능과 통제

구분	일탈의 차원		주요 요인	통제 방향
	기술적 차원	규범적 차원		
개인정보 침해	의사소통/접근/ 거래/시스템	법규범	아노미, 통제기제 실패	법규 정비, 규범 내면화
사이버 범죄	의사소통/접근/ 거래/시스템	법규범	구조적 긴장	공식통제 강화
유해정보 유통	의사소통/접근	민습	아노미, 통제기제 실패, 부분문화	법규정비, 규범 내면화, 정보문화

#### 다. 사회적 혜택과 인권

정보 인권의 주요 권리목록은 표현의 자유, 프라이버시권, 정보 공유의 권리, 정보 접근권 등 4가지 범주가 해당된다. 사이버공간에서 인간의 행동을 제한하는 요소는 법, 시장, 규범, 기술(암호)이 있다.

##### 1) 표현의 자유

표현의 자유는 국가기관에 의한 검열이나 이런 것을 통해 제한될 수 없다는 것이 원칙이다. 단, 정보의 생산이나 수용 단계에서 자율 규제나 기술적 규제를 통해 일부 보호될 수 있다는 것이 일반적이다. 정보의 생산단계에서의 규제는 억압적 검열로서 최근 위헌 판결이 난 ‘인터넷 실명제’ 같은 경우가 해당된다. 정보 수용단계에서는 억지적 검열로서 ‘내용 등급제’가 해당된다. 전자의 경우는 표현의 자유를 침해하는 것이고, 후자의 경우에는 알권리를 침해하는 형태로 나타나게 된다. 기본적으로 표현의 자유에 대한 억압

적 검열은 굉장히 부적절하다. 인터넷 실명제와 관련해서 공익에 기여하는 바가 많지 않은 상황에서 오히려 표현의 자유를 침해했다는 것이 헌법재판소의 판결 요지였다. 따라서 사이버공간에서의 표현의 자유에 대해 정부나 특정기구가 인위적으로 개입해서 억압적인 형태로 규제하는 것은 바람직하지 않다는 것이 다수설이다.

<표 3-11> 표현의 자유에 대한 규제 유형 비교

규제 구분	과정 구분	규제 유형	특징
억압적 검열	정보 생산 단계	인터넷 실명제 등	표현의 자유 침해 (위헌적 요소)
억지적 검열	정보 수용 단계	인터넷 내용 등급제 등	알권리 침해

## 2) 사이버공간과 프라이버시

프라이버시 개념에는 인격권, 친교관계 비공개권, 비밀성의 원리, 자신에 대한 접근 통제권, 개인정보 자기결정권<sup>11)</sup> 등이 포함된다. 정보화가 진전될수록 개인정보 자기결정권의 중요성이 증가하고 있다. 정보사회에서의 개인정보는 상품화되어 거래의 대상으로서 경제적 가치를 갖기 때문에 시장기능에 입각한 자율규제만으로는 보호되기 어렵다.

기존에는 이런 프라이버시의 침해라는 부분이 정부 정책의 효율성이라는 부분에서 일부 침해가능성이 존재했으나, 최근에는 사이버 경제의 확산에 따라 시장에 의한 침해 부분이 더 문제가 되고 있다. 구글의 국내 개인정보법 위반 소지 여부, 페이스북의 개인 사진으로 광고하는 행위, 위법적으로 개인정보를 유통 또는 거래하는 행위 등이 새로운 형태의 프라이버시 침해 유형이라고 볼 수 있다. 프라이버시에 대한 침해 가능성이 국가나 기관뿐만 아니라 시장에도 확산되었기 때문에, 향후 논의는 시장에 있어서의 프라이버시 침해라는 부분을 조금 더 논의할 필요가 있다. 또한, 프라이버시와 관련된 규제에는 다음과 같이 정부주도형, 규범주도형, 시장주도형이 있는데, 각각의 장단점을 혼합하는 것이 중요하다.

11) 다른 사람이나 기관에 공여된 자신의 개인 정보의 유통과 활용과정에 관여할 수 있는 권리

<표 3-12> 프라이버시 침해 규제유형 비교

규제 구분	규제 유형	특징
정부 주도	법제도의 강제력에 의한 개인 사생활 보호	가장 효율적이나 감시체제에 이용될 우려
규범 주도	이용자의 사회적 규범에 의한 사생활 보호	가장 이상적이나 실효성에 의문
시장 주도	자기 이해의 실현을 위해 개인 사생활 보호 (이용자들에게 이익제공 등)	정보인권이나 개인정보 보호의 가치를 금전적 또는 시장기능에 위임하는 것의 문제

### 3) 사이버공간에서의 인권 보호

표현의 자유는 국가의 개입과 간섭을 배제하려는 소극적 성격으로서, 사이버 공간에서 무제한적으로 허용될 수 없고, 일정한 요건 하에서 제한이 필요하다. 반면, 프라이버시는 권리의 보호를 위해 국가의 적극적 관여가 요구되는 적극적 성격으로서 효율적 국가행정과 기업 경영의 명분하에 침해될 가능성이 있기 때문에 일정 수준의 규제가 필요하다. 즉, 표현의 자유는 제한으로 접근해야 하고, 프라이버시는 규제로 접근하는 것이 현 상황에서 가장 타당한 것으로 보인다.

특히 글로벌 체제에서는 표현의 자유와 프라이버시가 상충되는 결과를 야기할 수 있다. 예를 들어, 2012년 런던올림픽에서 펜싱 심판의 페이스북 테러와 같은 경우가 해당된다. 한편에서는 표현의 자유이지만, 상대방의 입장에서는 인권 침해이기 때문이다. 문화권을 건너서 이 같은 행위가 발생하기 때문에, 국가 간의 분쟁으로도 확장될 수 있는 요소가 있다. 따라서 글로벌화 된 사이버공간에서의 인권은 위협요소의 억제, 그리고 보편적 공통규범의 합의가 매우 중요하다.

### 4) 사이버공간에서의 인권 관련 기타 의제

이 외에도 정보인권의 가장 보편적 범주인 표현의 자유와 프라이버시를 침해하는 최근의 다양한 행위 유형이나 부작용의 억제가 이슈화 될 수 있다. 사이버공간에서 빈번하게 발생하는 인종차별이나 인종혐오, 문화적 차이나 충돌 및 문화 혐오 현상, 플레이밍이나 소외 등이 이에 포함된다.

라. 기본 의제와 관련된 신규 의제 발굴

1) 사이버공간의 문화적 혜택

한국의 경우 사이버공간의 확대에 따른 문화전파와 문화 창달, 문화적 혜택 등을 강조할 필요가 있다. 과거 글로벌 문화의 수용자적 입장이던 우리나라가 한류의 확산으로 인해 문화 주도자의 지위가 됨에 따라, 사이버공간의 문화적 혜택과 관련된 의제를 발굴, 강조해야 하는 것이다. 문화적 혜택이라는 부분은 한국의 문화적 특수성을 충분히 반영할 수 있는 세부 의제가 될 수 있다.

2) 사이버공간에서의 공통 규범

다음으로 사이버 공간에서 추구되어야 할 인류의 공통 규범과 관련된 의제를 발굴하되, 아시아나 개도국을 포섭할 수 있는 의제나 규범이 필요하다. 런던 2011 회의의 경우 선진국이 개도국에 대한 ‘시혜’적 관점으로 접근하는 것이 일부에서 관찰되는데, 2012 회의나 2013 서울 회의의 경우 개도국이나 비서구 관점에서 접근하는 것이 바람직할 것이다. 특히, 인종, 문화적 차이에 의한 사이버공간의 역작용에 대한 의제를 강조할 필요가 있다.

3) 사이버공간의 역작용에 대한 글로벌 규범 제안

사이버공간의 역작용에 대한 글로벌 규범을 제한할 필요가 있다. 국내의 경우 이런 역작용 사례가 많고, 이에 대한 정부의 노력이나 정책 사례가 풍부하다는 점에서 주도적으로 글로벌 규범을 제안할 수 있을 것이다. 글로벌한 개념에서는 사이버공간의 사회적 혜택이나 인권에 대해 역내 법제도의 적용이 어려운 경우가 있으므로, ‘서울 선언문’ 등의 형식으로 규범적 차원으로 접근하는 것이 중요하다.

4) 사이버공간의 사회적 혜택 및 인권 의제의 범위

사이버공간의 사회적 혜택 및 인권 의제는 그 범위가 매우 방대함에 따라 다양한 세부

의제 관련 전문가 풀을 구성하고 의제를 발굴하는 것이 필요하다. 기존의 의제 분석 외에도 주최국의 입장에서 새로운 의제를 발굴할 필요가 있기 때문에, 사회적 혜택이나 인권의 다양한 이슈와 관점에서 접근하는 것이 바람직하다.

## 제 4 장 2013년 세계 사이버스페이스 총회 의제 설정

### 제 1 절 2013년 세계 사이버스페이스 총회 주제 및 주요 방향 설정

#### 1. 추진배경 및 기대효과

##### 가. 개최 제안 및 추진배경

2011년 9월, 제66차 유엔총회를 계기로 개최된 한·영 외교장관 회담 시 헤이그(Hague) 외교장관은 ‘사이버공간에 관한 런던 회의’의 후속회의를 한국에서 개최할 것을 제안했다. 2011년 10월, 영국 캐머런(Cameron) 총리는 이명박 대통령 앞 서한을 통해 후속회의 개최 제안 사실을 상기시키면서 한국 정부에 검토를 요청했다.

한국은 2010년 유엔 전자정부평가 1위, 2011년 ITU 정보통신기술 발전지수 1위를 차지하는 등 디지털기술 수준과 이에 기반한 정치·경제·사회·문화적 혜택 면에서 IT 분야의 세계적 선도국이다. IT 인프라 및 이용률 관련 국제지수 순위를 보면, 초고속인터넷 인프라는 세계 최고 수준(2011년)<sup>12)</sup>이며, ITU ‘ICT 발전지수’ 종합 1위 및 ‘ICT 이용도’ 부문 1위 (2011년)<sup>13)</sup>이다. 정보통신발전지수(ITU)<sup>14)</sup>와 전자정부준비지수(UN)<sup>15)</sup> 역시 세계 1위를 기록하고 있다. 또한, 2010년 11월 서울 G20 정상회의, 2011년 11월 부산 세계개발원조총회, 2012년 3월 서울 핵안보정상회의에 이르기까지 다양한 범세계적 문제 해결을 위한 주요 고위급 대형 국제회의를 연달아 개최하고, 의장직을 수임하면서 축적한 성공적 회의 개최 경험은 물론 이견 조정 및 성과 도출을 통해 입증한 외교력을 국제사회가 인정한 것으로 풀이된다.

이번 회의를 서방국가에서 계속 개최하기보다는 세계 경제의 주목을 받고 있는 아시

---

12) 초고속인터넷 평균 접속속도 OECD 1위(약 16Mbps), 인구 100명당 무선 초고속인터넷 가입건수 OECD 1위(89.8명), 유무선 초고속인터넷 접속 가구 비율 OECD 1위(95.9%)

13) 가정에서의 인터넷 접속가구 비율 1위, 무선 브로드밴드 가입자 1위, 유선 브로드밴드 가입자 4위 등 최상위권 기록

14) 2007년 1위('07)→2위('09)→3위('10)→1위('11)

15) 5위('05)→6위('08)→1위('10)

아에서, 특히 IT 강국인 한국에서 개최할 경우 전 세계적 관심과 협력을 조직화할 수 있을 것이라는 기대도 작용했다.

이 같은 제안에 대해 한국은 IT 강국으로서의 위상 제고, 향후 국제사회의 사이버규범 논의 주도 기회, 2013년 안보리의장국 수임 시 국가적 의제로 추진 가능성 등의 긍정적 기대효과를 고려해 개최의사를 통보했다. 단, 예산사정을 고려해 관계부처 간 합의를 통해 2013년 회의를 개최하는 것으로 의사를 전달했다.

#### 나. 회의 개최 시 기대효과

서울 사이버스페이스 총회를 개최함으로써 기대할 수 있는 효과는 다음과 같다. 첫째, 새로 부상하는 주요 국제 이슈인 사이버스페이스에 대한 논의에 대한 주도권을 선점한다는 것이다. 특히 2013년 사이버스페이스 총회, 2014년 ITU 전권회의<sup>16)</sup>를 연속해서 개최함으로써 사이버 IT 분야의 정책 논의의 주도국으로 위상을 확립할 수 있을 것으로 기대된다. 서방과 중국·러시아가 팽팽하게 대립함으로써 논의가 거의 진전되지 않고 있는 사이버스페이스에 대한 국제 규범 분야에 대한 논의를 촉진하는 역할을 담당하는 것이다. 둘째, 이 과정에서 국익에 부합하는 국제 규범 및 창출에 기여할 수 있도록 입장을 반영할 수 있다. 아울러 국내 IT 업체들의 해외진출 확대를 위한 기회로 활용할 수도 있다. 셋째, 시민사회 NGO 및 네티즌들의 참여를 장려함으로써 사이버 보안 의식을 증진하고 책임감 있는 사이버 공간 활용 문화의 정착에도 기여할 수 있다.

---

16) 방송통신위원회가 준비하고 있는 2014년 ITU 전권회의는 부산에서 개최될 예정

## 2. 주제 및 주요 방향

### 가. 기본 방향

2013년 세계 사이버스페이스총회의 기본방향은 첫째, 1·2차 총회 성과를 기초로 하여 가치를 부가할 수 있는 기회를 만드는 것이다. 둘째, 서울 총회 이전까지 UN 정부전문가 부분, OSCE 각료이사회, OECD, ITU 등 각종 국제 포럼에서 논의되는 내용을 적절히 포함시키도록 한다. 셋째, 한국적 특색도 적절히 가미한다. 넷째, 사이버공간의 다양한 이슈에 대해 국제적인 협력을 강화한다.

차기 총회를 준비함에 있어서 고려해야 할 사항은 다음과 같다. 첫째, 결과문서 (Outcome document)와 관련해 1·2차 총회의 성과를 진전시키기 위해 ‘의장요약’ 차원을 넘어 ‘의장선언’ 채택을 목표로 할 필요가 있다. 둘째, 아시아에서 개최되는 총회인 만큼 유럽과 미국 등 서구 중심의 회의가 아니라 아시아, 중남미, 아프리카, 중동 개도국 등이 참가할 수 있도록 초청국가를 다변화 하는 것이 바람직하다. 셋째, 지역별 워크숍 및 Open debate 등 부대행사를 사전 개최하는 방안도 고민할 필요가 있다. 넷째, 한·미·영 3자 협의 및 Friends Group을 가동하여 준비과정에서부터 적극적인 참여를 유도한다. 특히 한국(Convener & Momentum-Creator), 영국(Initiator), 미국(Facilitator)의 역할 분담이 중요하다. 다섯째, 민간 분야와의 협력을 강화할 필요가 있다. 마지막으로 의제개발이 중요하다. 기존 회의처럼 선진국 중심의 의제보다는 개도국도 참여할 수 있는 의제를 개발해야 한다.

### 나. 주제 선정 방향(안)

2013년 서울에서 개최될 세계 사이버스페이스 총회 주제는 총회의 목적과 방법, 참여 국가 및 주요 논의의제 등을 고려하여 선정할 필요가 있다. 이를 위해서는 다음의 세부적인 다섯 가지 요인을 고려할 필요가 있다. ① 미래지향적 주제 또는 목표, ② 실현 가능한 규범 또는 의제, ③ 전 세계 공통 관심사(의제) 포함, ④ 이용자 중심, ⑤ 사이버스페이스의 성격 등이다.

사이버스페이스는 그동안 빠르게 성장, 발전해 왔으며, 앞으로도 사이버스페이스 뿐만 아니라 타 산업 성장의 핵심이다. 이는 ICT 기술의 발전으로 인해 다양한 분야가 사이버스페이스와 연결되어 있기 때문이다. 따라서 사이버스페이스는 현재의 성장보다 미래의 발전에 중추적인 역할을 수행한다. 즉, 2013년 세계 사이버스페이스 총회는 현재의 문제가 아닌 미래의 발전상을 제시할 수 있는 주제를 선정할 필요가 있다. 또한 총회 준비 고려사항에서도 언급한 것처럼, 2013년 세계 사이버스페이스 총회의 목적을 명확히 한다면, 그 목표에 맞는 주제를 설정하는 것도 고려해야 한다.

실현가능한 규범 또는 의제 요인은 총회의 주제가 다양한 의제가 설정되고 논의될 것이기 때문에 이를 전부 포함하는 것은 어려운 일이다. 런던 총회에서는 ‘허용 가능한 행동규범’, 부다페스트 총회에서는 ‘신뢰와 안전’이라는 키워드를 사용했으나 서울 총회에서는 이러한 방식을 채택할 것인지의 여부를 결정해야 한다.

<표 4-1> 기존 총회 주제 및 의제 비교

구분	주제	주요 의제
보장 차원	자유와 번영(부다페스트)	경제성장, 사회적 혜택(런던, 부다페스트)
보호 차원	허용가능한 행동규범(런던) 신뢰와 안전(부다페스트)	보안, 범죄, 테러, 국제안보(런던, 부다페스트) 인권(부다페스트)

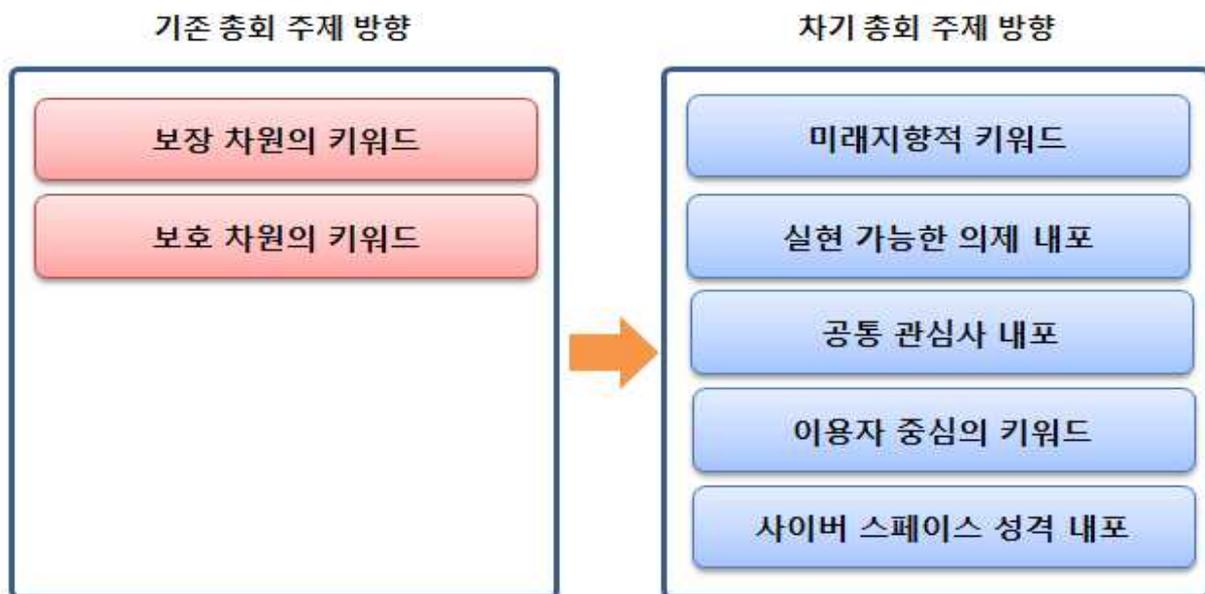
이와 함께 전 세계의 공통 관심사를 포함할 수 있는 주제 선정이 필요하다. 이는 선진국뿐만 아니라 개도국, 후진국들의 참여를 유도해야 하기 때문이다. 그러나 해당 국가들의 관심사가 정확히 공통적인 주제를 찾는 것은 사실상 불가능하다. 부다페스트 총회에서는 ‘자유와 번영’이라는 용어를 사용했는데 이와 유사하게 선진국의 관심을 얻을 수 있는 용어와 개도국에 필요한 용어를 나열하여 사용하는 것이 바람직하다.

두 차례에 걸친 사이버스페이스 총회의 주제나 의제를 살펴보면, 다분히 공급자 입장에서 선정되었다고 볼 수 있다. 두 차례 회의에서 논의된 의제는 주로 경제성장, 사회적 혜택과 같은 보장 차원에서의 의제와 인권, 보안, 범죄, 테러 등 보호 차원에서의 의제가

선정되었으며, 주제의 경우도 이와 유사하다. 보호 차원의 의제가 중시되면서 주제 자체도 사이버스페이스 상에서 나타나는 행동양식을 규정하려는 측면에서 주제가 선정되었다. 그러나 사이버스페이스의 이용자는 능동적, 적극적 이용자이기 때문에 이를 적절히 반영할 필요가 있다. 즉, 2013년 세계 사이버스페이스 총회의 주제는 공급자 입장에서의 주제보다는 이용자 중심의 사이버스페이스 총회라는 것을 부각하는 것이 필요하다.

마지막으로 사이버스페이스의 성격이나 역할이 명확히 나타낼 수 있는 주제의 선정도 고려할 필요가 있다. 런던 총회 주제처럼 사이버스페이스라는 용어를 그대로 사용하는 것은 바람직하지 않다. 사이버스페이스 그자체로 미래지향, 공간 확장 등의 의미를 내포하고 있으나 보다 구체적인 사이버스페이스의 성격을 규명하고 한 단계 격상하여 표현해주는 것이 바람직하다. 일반적으로 사이버 페이스는 개방, 공유, 참여의 성격을 가지므로 이러한 용어들이 내포될 수 있는 주제를 선정할 필요가 있다.

[그림 4-1] 2013 세계 사이버스페이스 주제 선정 방향(안)



다. 행사 개요

회의 명칭은 국제회의라는 것을 강조하는 차원에서 ‘세계 사이버스페이스 총회’로 하

고, 영문 명칭은 ‘Seoul Conference on Cyberspace’로 정했다.

개최 시기는 런던회의(11월 1일), 부다페스트 회의(10월 4일) 개최 일자를 고려하되, 주요 국제회의 일정 등과 중복되지 않도록 했다. 이에 따라 다른 정상·장관급 회의가 예정되지 않은 2013년 10월로 결정했다.

개최 장소는 학계·기업·NGO의 참여 편의성, 주변시설, 회의 주제 등을 감안해 서울 삼성동 코엑스(COEX)로 정했다.

초청 규모는 부다페스트 총회보다 10여국 정도를 확대하여 80여개국에서 약 1,200명이 참석하는 행사로 준비하도록 한다. 차기 총회 개최국과 전자정부 중점사업대상국 등 정상 2~3명을 비롯해 7~80개국 정부 대표 500여명이 참가할 것으로 예상된다. 특히, 아시아·중남미·아프리카 등의 개도국을 다수 초청하여, 사이버공간에 대한 논의에서 균형을 잡을 수 있도록 한다. 아시아에서는 차기 총회 개최 후보지인 인도를 비롯해 아세안지역 안보포럼(ARF, Asean Regional Forum)의 사이버공간 신뢰구축 세미나 참가국을 중심으로 초청하고, 중남미에서는 태평양동맹(Pacific Alliance) 4개국 등, 아프리카에서는 인터넷 보급률이 높은 세네갈을 비롯해 구글의 인터넷 보급 사업 대상 지역을 위주로 초청한다. 이 외에도 정보격차 해소, 사이버 보안, 프라이버시 보호 등을 위해 활동하는 국제적 NGO와 글로벌 검색업체, 보안업체, 인터넷 신용결제 업체 등을 초청한다.

본회의는 전체회의와 분과회의로 구성하고, 부대행사로 IT산업 전시회, 전자정부 전시회, 학술 워크숍, 청소년 온라인포럼 등을 진행한다. 모든 참석자들이 자유롭게 의견을 개진하는 포럼 형식으로 준비한다.

총회 의제와 관련해 가급적 서방과 중국·러시아, 선진국과 개도국의 이해를 포괄하는 균형적인 의제를 선정하되, 런던·부다페스트 총회에 비해 차별화되고 진전된 논의를 가능케 할 한국적 아젠다를 발굴하도록 한다. 이를 위해 관계부처 협의회를 개최하고, 민간자문단 운영을 통해 의제 발굴을 추진할 예정이다.

<표 4-2> 2013년 세계 사이버스페이스 총회 개도국·NGO·기업 초청 후보국가(안)

구분	국가	비고
아시아 (13개국)	인도	차기 사이버스페이스 총회 개최 후보지
	말레이시아	한국과 ARF 사이버공간 신뢰구축 세미나 공동개최('12.9)
	필리핀	ARF 사이버공간 신뢰구축 세미나 참가
	싱가포르	ARF 사이버공간 신뢰구축 세미나 참가, 인터넷 보급 1위
	인도네시아	ARF 사이버공간 신뢰구축 세미나 참가
	태국	ARF 사이버공간 신뢰구축 세미나 참가
	베트남	ARF 사이버공간 신뢰구축 세미나 참가
	라오스	ARF 사이버공간 신뢰구축 세미나 참가
	캄보디아	ARF 사이버공간 신뢰구축 세미나 참가
	미얀마	ARF 사이버공간 신뢰구축 세미나 참가
	몽골	ARF 사이버공간 신뢰구축 세미나 참가
	파키스탄	ARF 사이버공간 신뢰구축 세미나 참가
	사우디아라비아	중동 최대 인터넷 사용자수
중남미 (7개국)	멕시코	태평양동맹(Pacific Alliance) 4개국
	칠레	태평양동맹(Pacific Alliance) 4개국, 중남미 최대 인터넷 보급
	페루	태평양동맹(Pacific Alliance) 4개국
	콜롬비아	태평양동맹(Pacific Alliance) 4개국
	브라질	낙후된 인터넷 인프라
	아르헨티나	낙후된 인터넷 인프라
	베네수엘라	낙후된 인터넷 인프라
아프리카 (7개국)	세네갈	아프리카 최대 인터넷 보급률(6%), 구글의 인터넷 보급
	남아프리카공화국	구글의 인터넷 보급 사업 지역
	나이지리아	구글의 인터넷 보급 사업 지역
	가나	구글의 인터넷 보급 사업 지역
	베냉	아프리카연합(AU) 의장국
	케냐	동아프리카 공동체(EAC) 의장국
	이집트	반정부시위, 인터넷 접속 차단
NGO (7개)	OLPC	One Laptop Per Child 운동, 저가 노트북 제공, 정보격차 해소
	PL	Privacy International, 프라이버시 침해 감시단체(47개국)
	ISOC	Internet Society, 인터넷 분야 최대 민간 국제기구
	EFF	Electronic Frontier Foundation, 디지털시대 권리 보호
	EPIC	Electronic Privacy Information Center, 사생활 보호단체(美)
	CDD	Center for Digital Democracy, 온라인 사생활 보호운동(美)
기업 (6개)	Google	미국 글로벌 검색업체
	Gemalto	디지털 보안업체, WEF 사이버 회복력 파트너십 참여
	PayPal	미국 인터넷 신용결제 시스템
	KASPERSKY Lab	러시아 글로벌 보안업체
	McAfee	컴퓨터 안전 대책업체
	CISCO	글로벌 보안업체

## 라. 성과 사업(안)

첫째, 3회째를 맞는 2013년 총회의 결과 문서로는 가급적 최소한의 원칙적 합의 및 논의 진전사항을 반영한 ‘의장성명’ 또는 ‘선언’을 채택하는 방안에 대한 고민이 필요하다. 기존 1, 2회 총회에서는 이보다 낮은 수준에서 ‘의장요약’이 채택됐다. 의장요약은 총회 시 논의된 내용의 단순 요약에 지나지 않는다. 따라서 2013년 세계 사이버스페이스 총회의 위상을 제고하기 위해서라도 의장 성명이나 서울선언문 등을 채택하는 것이 바람직하다.

둘째, 지속적인 총회 개최를 위한 특단의 방안을 고려할 필요가 있다. 사이버스페이스가 제공하는 혜택이나 이 안에서 발생하는 각종 폐단은 단기적으로 종료되는 이슈가 아니다. 앞서도 언급한 것처럼 사이버스페이스는 미래지향적인 성격을 갖고 있으며 빠르게 변화하고 있고, 점차 확장되고 있는 추세이다. 따라서 해당 이슈들을 변화에 맞게 검토하고 대응할 수 있는 지속적인 논의가 필요하며 이를 위해서는 사이버스페이스 총회도 지속적으로 개최될 필요가 있다.

현재 3회 개최국만 결정된 상태이며, 사실상 향후 개최국은 결정되지 않았다. 3회 총회에서 차기 개최국을 선정할 것으로 예상되나, 총회 개최 준비 기간을 고려하면 이는 조금 늦은 감이 있다. 따라서 3회 총회에서 4회 및 5회 총회 개최국을 선정하여 보다 건실한 총회가 지속될 수 있도록 제안하는 것이 필요하다.

이와 함께 지속적인 총회 개최를 위해 사이버스페이스 전담 국제기구의 창설을 검토하고 이를 3회 총회에서 논의하는 것도 고려할 필요가 있다. 현재 사이버스페이스와 관련된 논의 기구는 ITU, OECD 등 다양하다. 그러나 각 기구의 목적과 역할이 다양하고 핵심 사업이 아니기 때문에 다소 부차적인 논의로 이루어지고 있으며, 그 위상도 상대적으로 낮다. 그러나 사이버스페이스의 중요성을 감안한다면, 국제 공조가 분산되는 것보다는 하나의 중심적 기구를 설립하여 운영하는 것이 바람직하다. 다만, 국제기구 창설 여부는 기수 설립에 따른 제반 준비 작업 및 자원 마련이 어렵다는 문제가 있어 총회 개최국에서 결정할 수 있는 사안이 아니고 부담이 있기 때문에 3회 총회에서는 제안 수준에서 논의하는 것이 바람직할 것으로 보인다.

국제기구 창설이 가능하다면, 세부적으로 워킹그룹이나 TF를 정례화 하는 방안도 고려할 수 있다. ITU 등 대부분의 국제기구 또는 국제적 논의기구에서는 실제로 워킹 그룹을 통해 세부적인 이슈를 논의하고 그에 따른 대응방안을 마련하고 있다. 그러나 현재 사이버스페이스 총회는 실무협의 차원의 논의가 적절하게 이루어지지 않고 있어 현실적인 이슈나 대응방안 마련이 어려운 상태다. 따라서 사이버스페이스 총회가 역할을 명확히 규정하고 위상을 제고하기 위해서는 워킹그룹을 통해 정례화 된 논의의 장을 마련하는 것이 반드시 필요하다. 이는 국제기구 창설 → 워킹그룹 운영의 순서가 될 수도 있고, 국제기구 창설이 어렵다면 워킹그룹 운영 → 국제기구 창설의 순서로 추진하는 것도 가능하다.

두 번째 성과사업이 가능하다는 전제를 한다면, 첫 번째 성과 사업인 서울 선언문은 총회 논의 의제를 중심으로 하는 선언문과 함께 지속적인 사이버스페이스 총회 개최에 대한 국가간 합의문을 채택하거나 서울 선언문에 포함하는 것도 가능할 것으로 보인다. 이 경우, 총회의 시작을 알리는 Keynote speech는 Global Network Governance(안)의 역할이라는 측면에서 진행될 수 있으며, 폐회를 알리는 Closing remark는 서울 선언문이 될 수 있다.

만약 두 번째 성과사업안인 사이버스페이스 전담 국제기구의 창설이 어렵다면, 개별적인 이슈별로 협약 가입 및 센터 설립도 고려할 필요가 있다. 예를 들면, 사이버안보 연구·교육·훈련 등을 위한 ‘국제사이버안보센터’ 설립을 검토하는 것이다. 핵안보정상회의 개최 시에도 국제핵안보교육·훈련센터를 후속사업으로 추진한 바 있다. 국제사이버안보센터 설립은 국제사회 기여, 우리의 위상 증진, 기업진출 발판 마련 등 여러 측면에서 바람직하다. 단, 아시아 지역 사이버 보안 교육·훈련센터가 말레이시아에서 운영되고 있으므로, 차별화 하는 방안을 고민해야 한다.

## 제 2 절 2013년 세계 사이버스페이스 총회 주요 의제 설정

### 1. 기존 회의 주제 및 의제 비교

런던 사이버스페이스 총회의 주제는 ‘사이버 공간에서 수용 가능한 행동에 관한 규범’이었다. 이때 선정된 주요 경제성장과 개발, 사회적 혜택, 국제 안보, 사이버 범죄, 안전하고 신뢰 가능한 접속 등 5개 의제가 ‘자유, 번영을 위한 신뢰와 안정’을 주제로 한 2012년 부다페스트 총회에서 대부분 유지됐다. 런던회의에서는 사이버공간의 긍정적 측면 및 부정적 측면(hopes and fears)이 논의됐으며, 부다페스트 회의에서는 개도국 역량 강화, 민관협력, 국제·지역기구 역할 등이 검토됐다. 2013년 세계 사이버스페이스 총회에서 큰 틀은 계승하되, 회의의 성과를 진전시키고 한국적 특수성을 반영하는 차원에서 일부 보완하는 것이 바람직하다.

단, 지난 회의의 경우 발표자 수가 많은 반면 토론이 거의 진행되지 않아 각 의제에 대한 합의나 공감대를 도출하기 어려웠다는 지적이 제기됐다. 발표내용 역시 하나의 주제에 집중해서 합의를 이루기 위해 서로 공유되고 토의하는 것이 아니라, 각자 자기가 생각했던 분야의 이야기를 낭독하는 형식으로 진행됐다. 차기 사이버스페이스 총회에서 논의를 진전시키고 일정 부분 합의나 공감대를 이루기 위해서는 5개 분야별로 중점 발표 및 토론 의제에 대한 구체적인 고민이 필요하다. 본 행사에 앞서 주요국과 사전 워크숍 등을 개최함으로써 분야별 세부의제를 구체화하는 방안도 고려할 만하다.

<표 4-3> 기존 회의 주제 및 의제 비교

	런던회의	부다페스트 회의
주제	사이버공간에서 허용 가능한 행동 규범	자유·번영을 위한 신뢰와 안전
의제1	경제성장 및 발전	
의제2	사회적 혜택	사회적 혜택 및 인권
의제3	안전·신뢰 접속(인터넷 거버넌스 포함)	사이버보안: 예방·대응·복원
의제4	국제안보	
의제5	사이버범죄	

## 2. 주요 의제 설정(안)

### 가. 경제성장 및 발전

우선, 선행연구, 주요 국제기구 활동내용 등에 대한 워크숍 개최 등을 통해 사이버공간의 경제적 혜택 관련 모범사례를 공유할 필요가 있다. 사이버공간 활용 및 경제적 혜택 공유를 위한 디지털 격차 해소, 사이버공간의 신뢰 강화를 위한 연계/관련 국제협력 방안을 논의하도록 한다. 또한 인터넷중개자의 역할과 책임을 논의할 필요가 있다.

경제적 혜택과 관련된 핵심적인 문제는 디지털 격차문제라고 할 수 있다. 인터넷 경제의 혜택에 대해서 국가마다 체감인식의 차이가 상당히 크다. OECD 회원국의 가계 브로드밴드 보급률은 2011년 기준 평균 70% 정도고 한국은 98%에 이르는 반면, 상당수의 개발도상국은 10% 이하인 경우가 많다. 따라서 사이버 공간의 활용과 경제적 혜택 확산 공유를 위한 디지털 격차 해소와 관련된 국제협력방안에 대한 논의가 경제 분야에서 이뤄질 수 있는 중요한 의제가 될 것이다. 디지털 격차 해소가 경제적 기회 부여의 요체가기 때문이다.

### 나. 사회적 혜택과 문화

우선, 사이버공간의 영향력을 고려할 때 사회적 혜택이라는 대의제는 유지하는 것이 바람직하다. 사이버공간의 발전에 따른 경제, 사회, 문화, 정치 부문의 변화를 고려할 때 사회적 혜택 의제는 유지가 필요하다. 인권 의제의 경우 표현의 자유 외에 개인정보 보호 및 자기통제권, 프라이버시권도 같이 논의될 수 있다. 단, 인권 의제의 경우 부다페스트 총회의 한계를 고려해 논의 범위를 조정할 필요가 있다.

또한, 사회적 혜택 외에 문화 측면이 강조될 필요가 있다. 사이버공간은 문화수용자와 문화형성자라는 속성을 동시에 갖는 것은 물론 문화전파의 탈국경적인 속성을 갖는다. 특히 인류 공통의 가치를 논의하기 위해서는 사이버공간에서 상대방의 문화에 대한 관용(tolerance) 의식이 제고될 필요가 있다. 사이버공간에서의 인종차별 및 혐오, cyber bullying, flaming, 문화 혐오 및 멸시 등의 문제가 사이버공간의 인류 보편적 가치를 위협

하는 이슈로 등장하고 있기 때문에, 사이버공간에서의 올바른 문화, 타 국가들의 문화에 대한 관용과 이해, 사이버공간을 통한 다양성의 증대 등을 세부의제로 설정하면서 ‘사회 문화적 혜택’이란 의제로 확대할 필요가 있다.

한편, 사이버스페이스 총회가 갖고 있는 근본적 문제점을 극복하기 위해서는 공통의제를 발굴하는 것이 중요하다. 기존 런던 및 부다페스트 총회는 서방(유럽 및 미국) 중심의 논의구조를 갖고 있었기 때문에, 비서방 국가가 소외되거나 대칭적이고 균형 있는 공론장이 되지 못했다. 특히, 해당 의제의 경우 인권 의제가 부각되고, 표현의 자유라는 이슈를 중심으로 논의구조가 형성되면서 중국, 러시아 등의 국가들의 반발이 있었다. 서울 총회에서는 표현의 자유를 반드시 논의하되, 문화 의제나 규범체계, 국제협력 체계 등을 통해 비서방 국가들의 주장을 논의할 수 있는 장을 제공할 필요가 있다. 공통적인 세부 의제 안은 사이버문화 창달, 문화적 뜰레랑스 인식 제고, 사이버공간의 보편적 가치, 사회적 혜택 제고를 위한 국제협력 체계 등이 있다.

사이버 이슈에 대해서는 한국의 위상이 상대적으로 높다는 점을 고려할 때, 서울 총회에서 적절한 의제 설정이 이뤄진다면 본 의제에 대한 참여가 높을 것으로 전망된다. 사회적 혜택이나 문화 관련 이슈 설정을 통해 아시아 국가의 참여를 높일 필요가 있으며, 특히 아시아권과 중·남미권에서의 공통된 의제를 발굴할 필요가 있다. 이와 함께 사회적 혜택의 대의제와 세부의제를 조속히 공개함으로써 관심을 제고하고, 발제 및 토론자 선정 시 서방-비서방-아시아권의 균형을 도모하는 것이 중요하다.

#### 다. 사이버보안

사이버 보안은 헝가리 회의에서 새로이 채택된 주제로서, 2013년 서울 총회에서도 사이버 보안 의제는 유지할 필요가 있다. 사이버 보안 관련 주요 의제로는 국가별 정보보호 정책, 국제기구별 정보보호 현안(침해사고 대응, 개인정보보호, 스팸 등), 침해사고 관련 지역별 CERT 그룹 현안(FIRST, APCERT, ASEAN CERT, OIC-CERT, GCC-CERT, 아프리카 & 남미지역 대표 CERT), 침해사고 예방을 위한 국가/기구별 정보공유 체계(한국,

미국, 일본, IMPACT, 맥아피, 시만텍) 등을 논의할 필요가 있다.

한편, 워크숍을 통해 국가별 정보보호 우수사례 발표, 글로벌 기업의 정보보호 정책(맥아피, 시만텍, 시스코, MS 등 정보보호 업체), 참가자들을 대상으로 정보보호 교육 과정 운영(부다페스트 협약 소개 및 적용 사례, 중국 & 러시아 정보보호 협약 소개 및 적용 사례, 침해사고 사례), 국가별 정보보호 관련 연구개발 과제 소개 등을 진행할 수 있다. 단, 부다페스트 회의에서 가장 쟁점이 됐던 것은 사이버 범죄 협약인데, 이는 각국이 첨예하게 대립하는 부분이기 때문에 협약이 주요 의제로 떠오르는 것은 지양해야 할 것이다.

#### 라. 국제안보

현 단계에서는 국제 안보 논의에서 신뢰구축이 중요하다. 국제안보 논의에서는 CBMs가 핵심이 될 것으로 전망되나, 현재 양 진영간 대립구도를 감안할 때, 당장 합의를 도출하는 것은 어려울 것으로 예상된다. 지금까지 UN GGE, OSCE, ARF 차원에서 논의되었던 조치들의 공통분모만을 포함하는 낮은 수준의 원칙적 합의 정도만 가능할 것으로 예상된다. 합의를 도출하지 못하더라도 향후 논의의 진전을 이룰 수 있도록 공감대를 마련하여 모멘텀(momentum)을 이어가는 것이 중요하다.

우선, UN GGE, OSCE, ARF 차원의 CBMs 등 현재 여러 국제기구 차원에서 이루어지고 있는 논의 결과물 및 진행상황을 서울 총회 논의에 적절히 반영할 필요가 있다. UN GGE는 2013년 1월, 제네바에서 보고서 초안에 대해 본격적으로 논의할 예정이다. 참가국간 합의가 이루어질 경우 2013년 8월에는 보고서가 채택될 수 있을 것으로 예상된다. 그러나 서방국가와 중·러간 입장 차이가 여전하다(단, 러시아는 실용적 접근, 중국은 이념적 접근). 보고서가 채택되지 않더라도 GGE 활동은 계속될 것으로 보인다. UN GGE 보고서 채택 여부와 무관하게 GGE 내에서의 논의 사항을 계속하여 서울 총회 국제 안보 관련 주제로 반영할 필요가 있다.

OSCE는 2012년 12월 각료이사회를 앞두고 최근 합의문서가 거의 도출될 수 있었으나, 러시아가 막판에 인터넷 콘텐츠 검열 및 인터넷 거버넌스 이슈를 제기함으로써 교착상

태에 직면했다. 따라서 OSCE 내에서의 논의동향을 지속적으로 예의 주시할 필요가 있다. 한편, ARF에서는 호주가 2013년 중 '사이버공간에서의 국가간 충돌 예방 및 신뢰 발전을 위한 조치에 관한 작업계획' 제안할 예정이다.

한국으로서는 원칙적으로 서방측 입장을 지지하나, 개최국으로서 균형적 자세를 견지할 필요가 있다. 신뢰구축조치 우선적 실시 필요성을 강조하고, 기존 국제인도법·전쟁법 내용 중 사이버공간에 적용 가능한 요소들을 정리하여 구속력 없는 규범으로 성안하는 방안의 가능성을 검토해야 한다.

국가안보 관련 부처들이 사이버안보에 대해 대외적으로 단일한 입장을 표명할 필요가 있다. 이를 위해 사이버공간 관련 국제법에 대한 심도 있는 분석을 통해 범정부 차원의 의견 조율, 국익 극대화 방안을 마련 및 공식 입장 수립이 필요하다. 또한 미국을 포함한 우방국과의 사전 협의를 거쳐 대외적으로 발표하도록 한다. 한편, 사이버스페이스총회를 비롯한 다양한 양자 혹은 다자 협의체에 전략적으로 참여할 필요가 있다. 단, 사이버 무기를 규제하는 국제법을 제안하는 것은 미국을 포함한 우방국들로부터 우리 정부가 사이버공간과 관련하여 중·러의 입장을 지지하는 것으로 오해 받을 소지가 있다.

#### 마. 사이버범죄

사이버공간에서의 중독문제(온라인 게임, 온라인 도박, 포르노그래피 등), 초국가적 사이버조직범죄(해킹(스파이아이나 제우스) 등), 안티사이버테러리즘(Anti-Cyberterrorism), 새로운 기술과 사이버범죄(스마트폰, 클라우드 컴퓨팅, 빅데이터 등), 국제 사이버범죄협약(International Convention on Cybercrime), 개인정보와 잊혀질 권리 등을 논의할 필요가 있다.

<표 4-4> 2013년 세계 사이버스페이스 총회 주요 이슈 및 논의 의제(안)

주요 이슈	논의 의제(안)
이슈1: 경제적 혜택 및 개발	사이버 공간의 활용 및 경제적 혜택 사례 공유
	글로벌 디지털 격차 해소
	사이버 공간의 신뢰 광화를 위한 국제협력
	인터넷 중개자의 역할과 책임
	시장의 창출과 지적권 보호 사이의 균형
	ICT와 개도국 경제성장
	선진 기술의 개도국 이전
이슈2: 사회문화적 혜택과 문화	사이버 공간을 통한 표현의 자유, 다양성의 증대
	개인정보보호(문화적 접근), 프라이버시권 보호(문화적 접근)
	자기통제권, 잊혀질 권리
	사이버 문화의 창달
	사이버 공간에서의 문화 이해 및 관용(문화적 tolerance 인식 제고)
	사이버 공간에서의 보편적 가치 보호
	사회적 혜택 제고를 위한 국제협력 체계 구축
	표현의 자유와 규제간의 균형
	정부의 역할과 민간의 역할 및 협력 체계
정보의 개방과 공유	
이슈3: 사이버범죄	사이버 범죄 대응을 위한 국제 공조
	사이버 범죄 대응을 위한 민-관 협력
	사이버 범죄 사례 및 대응 사례 공유
	개도국 역량강화 지원
	국가적 사이버조직범죄 예방
	신 기술과 사이버 범죄
이슈4: 사이버 보안	사이버보안의 기본 원칙 설정
	사이버 보안 모범 사례 공유
	사이버 보안 강화를 위한 국제 협력 체계
	침해사고 예방을 위한 정보공유 체계 구축
	국가별 정보보호 정책, 국제기구별 정보보호 현안
	개인정보보호(기술적 측면), 프라이버시권 보호(기술적 측면)
	선진 기술의 개도국 이전
이슈5 국제안보	사이버 공간에서의 국가간 충돌 예방
	국가간 신뢰 구축, 신뢰구축조치(CSBM) 우선적 실시 필요성
	사이버 안보 위협 대응을 위한 국제 규범
	사이버 안보 제고를 위한 민-관 협력
	사이버 분쟁 가능성 및 사례 공유
이슈6 이용역량 증진	인터넷 윤리(국가별, 수준별)
	인터넷 이용 역량 강화
	인터넷 중독 예방

## 제 5 장 결 론

사이버 공간을 둘러싼 다양한 이슈들이 인터넷의 탈공간성이란 속성에 의해 개별 국가의 이슈가 아니라 글로벌 이슈화하고 있다. 특히 인터넷 거버넌스 측면에서는 서방진영(미국, 유럽, 일본, 호주 등)과 비(非) 서방진영(중국, 러시아, 브라질, 인도 등) 간의 의견 대립이 첨예하고 나타나고 있다. 본문에서 언급한 바와 같이 그 요지는 서방진영은 다중이해당사자 모델(Multi-stakeholder model)을 주장하나, 비서방진영은 국제기구를 통한 통합 논의를 주장하고 있다. 즉, 비서방 진영에서는 ITU 논의 구조와 같이 국제기구 체 내에서 인터넷 거버넌스에 대한 논의 구조를 주장하고 있는 것이다.

우리나라의 경우 다중이해당사자 모델을 묵시적으로 따르고 있긴 하나 그 역시 아직 명확한 것은 아니다. 2013년 서울 사이버스페이스 총회는 이에 따라 우리나라의 리더십이 요구되고 있는데 양측의 참여한 대립을 여하히 조정·중재하여 생산적인 논의를 이끌어 가는가가 매우 중요하다. 특히 사이버스페이스 총회에 대한 회의적 시각, 즉, ‘서방진영을 중심으로 하는 그들만의 총회’라는 인식을 불식시키고 총회의 지속가능성에 동력을 부여하는 것이 우리나라의 핵심 역할이라 할 것이다.

또한 2013 서울 사이버스페이스 총회의 구체적인 결과물 도출 역시 중요한데, 국가간 구체적인 합의문 도출이 현실적으로 어렵다고 하더라도, 느슨한 수준의 선언문을 도출할 수 있도록 노력을 기울여야 할 것이다. 예를 들어 구체적인 이슈에 대한 합의 수준은 아니더라도 향후 사이버스페이스 총회의 발전 방향이나 논의 방향을 제시하는 ‘느슨한 수준의’ 선언문 도출을 도모할 수 있다. 이를 통해 향후 사이버스페이스 총회에서 한국의 위상 및 영향력을 강화하는 것을 기대할 수 있다.

본문에서 언급하지 않았으나, 추가로 고려할 수 있는 사항으로, 이러한 느슨한 수준의 선언문을 도출하기 위해서는 사전 국제 워크숍을 활용하는 방안을 고려할 수 있다. 사이버스페이스 총회는 정무적 논의를 중심으로 이루어지는 측면이 존재하기 때문에 관련분야의 타 국제회의에 비해 정책적 접근이나 논의가 부족하다는 특징이 있다. 따라서 정책

과 정부·외교 논의의 균형 달성을 위해 사전 워크숍 등을 통해 정책적, 전문적 논의가 선행될 필요가 있다. 이를 위해 사전 워크숍이 WG(Working Group) 또는 SG(Study Group)의 역할을 수행하도록 유도하고, 이슈 및 방향에 대해 사전 합의를 유도하도록 하는 것이 바람직할 것이다. 전술한 바와 같이 사이버스페이스 총회가 총회 중심의 논의구조를 형성함에 따라 기존 논의가 되풀이 되고 진영 간 대립적 ‘자기 주장’만 존재한다. 따라서 워크숍을 통해 상호 이해 및 사전 조율이 요구되며, 워크숍을 통해 의제 도출 및 의제에 대한 공동의 관심사를 도출할 필요가 있다. 이를 위해 사전 워크숍을 의제별로 분리하여 의제에 대한 사전 공지 효과와 논의를 추진하도록 하는 것이 필요하다. 워크숍의 논의 방식은 각 워크숍 회차별로 별도의 의제를 논의하도록 하고, 다양한 국가의 참여와 논의를 유도하며, 각 워크숍에서 도출된 결과를 보고자(Rapporteur)가 서울 총회의 전체 회의(Plenary Session)나 개별 의제 회의(Panel Discussion)에서 보고하면서 자연스럽게 선언문을 도출하도록 유도하는 것이 바람직할 것이다.

2013년 서울 사이버스페이스 총회는 새 정부 들어 갖는 첫 번째 대규모 국제회의이고, 그 연장선에서 2014년 ITU 전권회의의 개최가 예정되어 있다. 따라서 서울 총회가 높은 중요성을 갖고 있으며, 특히 새정부 들어 우리나라의 국격을 향상시키는데 좋은 기회가 될 수 있다. 예를 들어 2012 부다페스트 총회에서는 타 유럽 국가들에 비해 비교적 성공적으로 유럽 금융위기를 극복했다는 점이 홍보됨과 동시에, 부다페스트 사이버범죄 협약 10주년이란 점에서 헝가리가 사이버 공간의 안전과 신뢰에 기여를 했다는 점이 홍보·부각되었다. 우리나라의 경우 인터넷 강국, 특히 인터넷 인프라 강국이라는 점에서 타 국가들의 관심 대상이 되어 왔다. 그러나 한편으로는 사회적 혜택이나 인권, 표현의 자유 측면에서는 인프라 수준에 비해 다소 열위에 있다는 점도 지적되고 있다. 따라서 서울 총회를 계기로 대한민국이 사이버스페이스에서의 인프라 강국뿐만 아니라 인터넷을 통한 경제적, 사회적, 문화적 혜택을 추구하는 나라이고, 안전하고 신뢰 가능한 인터넷 공간 구축에 선도적인 국가라는 점이 강조되어야 할 것이다. 이를 통해 국내 인터넷 산업에 대한 홍보 외에 국격의 제고라는 효과를 기대할 수 있을 것이다.

방통융합미래전략체계연구 지정 2012-05

## 국제 사이버공간 포럼 대응전략 연구

---

2012년 11월 15일 인쇄

2012년 11월 15일 발행

발행인 방송통신위원회 위원장

발행처 방송통신위원회

서울특별시 종로구 세종로 20

TEL: 02-750-1114

E-mail: [webmaster@kcc.go.kr](mailto:webmaster@kcc.go.kr)

Homepage: [www.kcc.go.kr](http://www.kcc.go.kr)

---