인터넷 거버넌스를 말하다

망중립성 이용자포럼

http://nnforum.kr

본 보고서는 국가인권위원회 2013년 인권단체협력사업의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다.

▮ 책을 펴내며 ▮

먼저 망중립성 이용자포럼이 작년 초 “망중립성을 말하다” 출간에 이어 2년 연속 귀중한 자료를 출간하게 된 것을 축하합니다. 특히 이 작업은 개별 조직 내에서 이루어진 것이 아니라, 여러 단체의 협업으로 이루어져 그 의미가 더 크다 하겠습니다. 이는 인터넷 거버넌스와 관련된 출판 작업으로는 세계적으로도 유례가 없을 만큼 값진 성과입니다. 또한, 이 책의 저자 중 30% 가량이 외국인으로 구성되어 있는데, 인터넷 거버넌스가 본래 국제적 성격을 가지고 있다는 점에 비추어 볼 때 아주 좋은 시도라고 생각하며, 앞으로도 이러한 국제적 협업이 계속되기를 기대합니다.

인터넷의 발전과정을 되돌아보면, 대략 10년에서 15년에 한 번씩 커다란 도약이 있었습니다. 먼저 1970년대 초, 미국과 유럽 사이의 협력 관계가 시도되었고, 1980년대 후반에는 미국의 NSFNET이 전 세계 수십 개 국가와 상호연결 됨으로써, 인터넷의 세계화를 촉진했습니다. 이어 1990년대 말에는 도메인 네임과 IP 주소를 중심으로 국제 조직을 만드는 움직임이 있었고, 그 결과 인터넷주소관리기구 ICANN(Internet Corporation for Assigned Names and Numbers)과 지역인터넷등록소 RIR(Regional Internet Registries)들이 등장했습니다.

그리고 2012년 국제전기통신세계회의 WCIT(World Conference on International Telecommunications) 회의를 시작으로 인터넷 조율의 미래에 관한 몬테비데오 선언과 2014년에 브라질에서 개최될 ‘인터넷 거버넌스에 관한 글로벌 멀티스테이크홀더 회의(Global Multistakeholder Meeting on Internet Governance)’ 등이 이어지며 인터넷이 또 한 번 도약할 수 있는 기회가 마련되고 있습니다. 이러한 시기에 인터넷 거버넌스에 대한 건실한 보고서가 출간되는 것은 매우 시기적절한 일입니다. 이 책의 출간을 통해 앞으로 국내에서 또 국제적으로 인터넷 거버넌스에 대한 지속적인 협력의 기회가 만들어질 것을 기대합니다.

전길남

목 차

▮ 제1부

인터넷 거버넌스란 무엇인가

인터넷 거버넌스와 전문성의 정치(*)

김지연[1)]

1. 서론

인터넷 공간 내에서 하나의 도메인네임은 하나의 정보자원(기계문서)만을 지시할 수 있다. ICANN이 관리하는 “A 루트”서버는 도메인네임과 IP주소 목록을 가지고 있고, 전 세계의 모든 DNS는 그 루트서버를 참조한다. “A 루트”서버는 전 세계의 정보자원의 경로를 최종적으로 확인하는 '원본'으로서의 권위를 가진다. ICANN이 인터넷의 통제지점을 관리하고 있다. ICANN은 느슨한 관리 형식이 아니라 직접적이고 위계적인 규제 기구이다. 일반최상위레벨도메인(gTLD) 등록기관이나 대행기관에 대해서 직접적이고도 강력한 규제를 집행하며, 국가코드최상위레벨도메인(ccTLD)에 대해서도 비록 제한적이긴 하지만 중요한 규제를 수행하고 있다(Mueller, 2010:230 ; McLaughlin and Pickard, 2005).

한국은 1986년 .KR도메인을 할당받았고, 당시 인터넷과 도메인네임 체계에 대한 정책은 정부보다는 국제적인 기술 커뮤니티와 교류하던 기술전문가들이 주도하고 있었다. 1990년대 후반, 인터넷이 대중화되기 시작하면서 기술관료들은 도메인네임시스템(DNS)에 주목하기 시작했다. 2004년 "인터넷주소자원에 관한 법률"이 국회를 통과했고, 한국정부 산하에 .KR도메인 관리권한을 두는 것으로 귀결되었다. 이 때 벌어진 논쟁들은 여러 질문들을 불러일으켰고 여전히 해소되지 않은 채로 남아 있다(김지연, 2013). "인터넷 거버넌스란 무엇을 통치하는가?" 그리고 "누가 ICANN에게 그러한 권한을 위임한 것인가?", "인터넷 거버넌스는 공정한가?" 등이 그런 의제들이다. 국내적으로도 ".KR도메인 관리기구의 위상은 무엇이며, 그 통치 대상은 무엇인가?", "인터넷주소자원법의 정통성은 어디에서 오는 것인가?", "전통적인 국가통치 체제와 인터넷 거버넌스 체제는 서로 어떤 관계에 놓여 있는가?" 등이 질문으로 제기되고 있다.

본 장에서는 인터넷 거버넌스의 '중심(core)'과 '경계(edge)'를 비교하는 방식을 취할 것이다. 실제로 ‘중심’과 ‘경계’란 명백하게 구분되지 않을 수 있지만, 분석을 위한 방법으로 ICANN의 직접 관리가 관철되는 영역을 '중심'으로 설정하고, 그 외 영역을 '경계'로 정의하

---

* 이 글은 저자의 다른 논문「인터넷거버넌스와 전문성의 정치: 도메인네임시스템(DNS)의 ‘중심’과 ‘경계’, 경제와사회 2013년 여름호」를 기반으로 축약 수정한 것임

1) 고려대학교 과학기술학 박사, 고려대학교 과학기술학연구소 선임연구원, 서울과학기술대학교 강사, spring900@gmail.com

고자 한다. 이 기준으로 본다면 ICANN과 공식적인 계약방식을 취하는 일반최상위레벨도메인(gTLD) 영역은 '중심'에 해당할 것이고, 상대적으로 비공식적이고 우호적 협의를 기반으로 하는 국가코드최상위레벨도메인(ccTLD) 영역은 '경계'에 해당할 것이다. 국가코드최상위레벨도메인의 경우, 전통적으로 "해당 지역 공동체를 대변할 수 있는 자"에게 관리권을 위임하는 방식을 취해왔다. 이 점에서 '중심'에 대한 ICANN의 통치는 직접적인 반면에 '경계'에 대한 ICANN의 통치는 상대적으로 간접적이다[2].

2. DNS의 '중심': 통치의 발명

ICANN으로 대표되는 인터넷 거버넌스는 신자유주의 질서의 확장으로 비판받고 있다. 한스 클라인(Klein, 2002)은 미국정부가 ICANN 체제를 도입하여 정치적 사법권, 처벌, 재산권 등의 자유주의 시장질서를 사이버스페이스 내부로 확장시켰다고 주장했다. 안토노바(Antonnova, 2007) 역시 ICANN이 절차적으로 잘 만들어진 안내 메커니즘이며, 자율규제와 최소한의 정부간섭이라는 규제원리를 전 지구적으로 도입하고 있다는 점에서 신자유주의 노선을 따르고 있다고 지적했다. ICANN 체계가 기본적으로 자유주의적 질서에 따르고 있다는 점에서는 이견이 크지는 않을 것이다(이항우, 2010). 그런데 기업친화적인 정책이나 엘리트 중심주의, 그리고 일반 이용자 참여의 결여라는 것만으로 인터넷 거버넌스를 자유주의적 통치모델이라고 규정하는 것은 충분하지 않다. ICANN 체제는 단순히 미국정부의 위탁관리 기구라기보다는 새로운 통치방식의 창조라는 점에서 주목해야 한다.

1) 도메인네임; 독점적 사용권

뮬러(Mueller, 2004)는 도메인네임과 IP주소를 사거나 팔 수 있다는 점에서 "가상적 부동산(virtual real estate)"이라고 정의했다. 그런데 이들 주소는 엄밀히 말해서 전통적인 의미의 소유 대상이 아니다. 이들 소위 "주소(address)"들은 일종의 메타포이다. 도메인네임 또는 IP주소를 가진다는 것은 그 네트워크 체계 안에서 가상의 '위치'를 가진다는 의미이다. DNS는 도메인네임과 IP주소의 연결목록을 가지고 있다가 인터넷 사용자의 질의에 응답함으로써 경로를 안내한다. 문제는 그 이름이 그 체계 내에서 고유해야 한다는 것이다. 그 시스템이 전체 인터넷 상에서 유일하다면 가장 '이상적'일 것이다.

도메인네임 할당 방법은 기본적으로 선입선출(First-come, First-served)방식이다. 먼저 신청하는 사람이 그 이름을 먼저 사용할 권리를 가진다. 본래 이 시스템은 비상업적으로 출발하였으며 기술 커뮤니티 내에서 사용할 목적으로 개발되었다. 1985년 도메인네임 등록신청이 개방되었고, 사용자가 많아지면서 1996년부터 도메인신청이 유료화 되었다. 유료화 이후에도 선입선출 규칙은 유지되었다[3]. 도메인네임을 신청한 자는 기간별(주로 연간단위)로 정해진 비용을 부담해야 한다. 먼저 선점한 자가 자신의 사용권을 다른 사람에게 되팔 수

2) 2007년 현재 일반최상위레벨도메인 등록자는 105,994 (59.9%)이고, 국가코드최상위레벨도메인 총 등록자는 70,877(40.1%)이다(Park, 2008). 정량적 측면에서 국가최상위도메인주소는 일반최상위도메인주소 만큼이나 많이 사용되고 있고, 국가최상위도메인주소가 단순히 일반최상위도메인주소의 보조적인 의미를 넘어서고 있다.

3) 한편 선입선출원칙이 회계적 원리로부터 유래되었을 가능성도 있다. 회계학에서 선입선출법은 장부상 먼저 입고된 재고를 먼저 출고하는 방식으로 원가주의 평가방법을 말한다.

있다.

이상에서 보듯이 ICANN은 물리적인 물건을 파는 것이 아니라 가상의 이름을 사용할 권리를 대여한다. 그 체계 내에서 고유한 도메인네임을 사용하려면 비용을 지불해야 하고 사용권리가 만료되지 않았는지 주시해야 한다. 사람들이 그런 비용을 감수하는 이유는 그 체계 내에 등록되어야만, 그 안에 있는 다른 사람들-컴퓨터들-이 자신을 알아볼 수 있기 때문이다. 그 체계 내에 포함된 사람들-컴퓨터들-의 수가 무시할 수 없을 정도로 많아지면서 도메인네임은 의미 있는 것이 되었다. 그 세계의 방식대로 만들어진 이름을 가져야만 그 세계 내에서 '존재'할 수 있다.

2) 인터넷기술 커뮤니티; 행위의 발명

DNS의 작동방식이 독점적 특질을 가지고 있음에도 불구하고 사람들에게 흔쾌히 수용되고 성장할 수 있었던 것은 그들의 내러티브에 강한 응집력이 있었기 때문이다. 이는 인터넷 기술 커뮤니티의 부상과 관련이 있다. 오랜 동안 미국정부는 인터넷 기술개발만이 아니라, 인터넷프로토콜을 개발했던 핵심 기술자그룹과 그들 사이의 상호적 네트워킹을 지원했다. 이 기술 커뮤니티는 인터넷의 성장과 함께 국제적으로 확산되었는데, 그들은 스스로 자신의 규범과 절차를 개발했고, 자신들이 자치(self-governing)를 하고 있다고 생각했다.

초기 인터넷 기술 커뮤니티는 칸(Robert Kahn), 서프(Vinton Cerf), 포스텔(John Postel) 그리고 동료 연구자들이었다. 그들은 미국 정부 연구기관의 후원을 받으면서 친밀한 집단을 형성했다[4]. 1986년, NSF(국가과학재단)가 인터넷 백본을 구축하는데 자금을 지원하기 시작하면서 인터넷이 급격히 성장했다. 더불어 발생한 복잡한 기술공학적 문제들을 해결하기 위한 "인터넷 아키텍처(Internet Architecture)"라고 불렸던 기술표준개발 작업팀이 만들어졌다. 그 중 하나가 IETF로 진화했다. 이들은 다른 팀들과 달리 참가자격을 제한하지 않았다. IETF는 매해 4번의 공개회의를 열었는데, 1987년, 5회 회의 때 50명이 참가했고, 1989년에는 200명, 1992년 여름 회의에는 650명이 참석했다(Mueller, 1999; 2004:73-78; Schewick, 2010).

엔지니어들은 이것을 "DDN 커뮤니티" 또는 "ARPA 커뮤니티"라고 불렀고, 이후에는 "인터넷 커뮤니티" 또는 그냥 "커뮤니티"라고 부르기 시작했다. 그들은 자신의 문화를 개발했는데, 회의 참여자들은 특정 조직을 대표하거나 조직의 위임을 받는 것으로 여겨지지 않았고 단지 개인들로 간주되었다. 이 커뮤니티는 회원제가 아니었고 법인체도 아니었고, 그저 가상적인 형태였다. 누구나 회의를 소집할 수 있고 참여할 수도 있다. IETF 회원이 된다는 것은 IETF 메일링 리스트 상에 있다는 것 말고는 더 이상 아무런 형식도 존재하지 않았다. 그런데도 IETF는 '저절로' 운영되었다. 그들은 스스로 커뮤니티를 형성했고, 자신이 그 커뮤니티를 대변한다고 자부했다. 그들의 기술문서(RFC, Request For Comments)는 누구나 조언할 수 있도록 공개되었으며 배포의 제한도 두지 않았다. 그들 문서는 언제나 국가가 아닌 "인터넷 커뮤니티"를 대리한다고 선언해 왔다[5].

---

4) 이 프로토콜의 명세는 1981년 "RFC 791" 등 공식적인 기술문서의 형태로 등록되었다.

5) 그들의 기술문서(RFC)는 특정한 지식에 접근하는 방식, 온라인에서의 시민의 권리, 혁신 정책의 성공여부, 정치경제적 경쟁 조건, 국가 안보문제 등에 영향을 줄 수 있다. 그리고 어떤 기술회사가 성공할지 여부에도

이제 그들의 기술문서(RFC)는 '인터넷에서 무엇이 실재인가'를 정의하는 새로운 방식이 되었다. 그들은 기술문서를 통해서 자신들의 기술적 경험을 재현했고, 그것을 통해서 동료들과 의사소통했으며 기술규격을 수정하기도 했다. 그들은 기술문서를 통해서 작동 가능한 규칙을 형성해갔고, 그 규칙이 작동하는 가상의 정보체계를 개발했다. 결과적으로 그들은 새로운 행위 규칙을 만들었고, 스스로 그 행위 규칙에 따라 그들의 세계를 구축했으며 그 세계 안에서 행동했다. 그들의 실행은 점점 더 많은 사람들의 행위로 '복제되었고', 많은 사람들에게 그 행위가 스며들면서 그들의 기술문서(RFC)는 표준과 같은 효과를 지니게 되었다. 이제 그들의 행위는 오늘날 수많은 인터넷 접속자들이 일상적으로 하는 행위가 되었다.

3) 프로토콜 사용자; 발명된 '주민'

도메인네임과 IP주소는 기술적으로 프로토콜에 의해 작동한다. 네트워크상에서 프로토콜은 정보의 흐름을 제어하고 정보의 출발지와 목적지를 특정하고, 정보를 재현하기 위해 컴퓨터 장치가 포함해야 할 공통의 데이터 형식, 인터페이스, 네트워킹 합의, 절차들을 특정한다. 프로토콜은 소프트웨어 코드도 아니고 물리적인 생산물도 아니다. 그것은 문자와 숫자로 된 '언어'이다. 이것은 지리적인 장소나 제조사들에 관계없이 이 프로토콜을 사용하는 장치들 사이의 상호운용성을 가능하게 해준다(DeNardis, 2009). 그런 점에서 기술적 프로토콜은 현실 세계의 규약과 유사하다. 사회문화적 규약들이 현실세계의 언어로서 인간의 상호작용 질서를 제공한다면, 기술적 프로토콜은 이진법 스트림으로 질서를 제공한다. 그런데 기술적 프로토콜들은 일단 결정되고 나면 사회규약과는 달리 최종 사용자에게는 보이지도 않고 만질 수도 없는 것이 된다.

TCP/IP는 대표적인 인터넷 프로토콜이다. 역사적으로 TCP/IP 프로토콜은 전자메일규약(SMTP)이나 파일전송규약(FTP)과 같은 다양한 프로토콜들과 가족 형태의 분류학적 체계를 형성했다. 이들 프로토콜들은 인터넷 사용에 필요한 형식과 절차에 관한 질서이며, 이들 프로토콜들을 통해서만 이질적인 네트워크들은 하나의 네트워크인 것처럼 연결될 수 있다. 웹문서들이 DNS 상에 등재된 도메인네임을 사용할 때만 가상 세계 안에 존재할 수 있는 것처럼, 컴퓨터 장치는 IP주소를 사용할 때에야 비로소 네트워크 위에 '존재한다'. 물론 사용자들은 원하는 정보에 접근하기 위해서는 해당 IP주소나 도메인네임을 미리 알고 있어야 한다. 그러나 사용자가 프로토콜이 처리되는 과정을 직접 이해할 필요는 없다.

다만 사용자는 반드시 IP주소로 작동하는 컴퓨터 장치와 함께 있어야 한다. 컴퓨터 장치와 응용프로그램들이 기술문서에 의해 정의된 방식으로 도메인네임을 처리해준다. 사용자와 컴퓨터 장치는 양쪽 모두 개별적으로는 어떤 완성된 행위를 할 수 없다. 그들은 정해진 프로토콜을 통하여 긴밀하게 연결된 상태로 하나의 행위에서 다음 행위로 자신들의 합성적 행위를 이어간다. 그들은 네트워크 안에서 '하나의 존재'처럼 행동한다. 이 질서 안에서는 사용자도 기계장치도 '프로토콜 사용자'라는 점에서 동등하다. 그들은 인터넷기술 커뮤니티에 의해 실험되고 창조된 인공적 실재이며 사회적 신체이다.

프로토콜 사용자가 된다는 것은 그 프로토콜을 정의하는 기술문서의 지배와 통치를 승인

관여할 수 있다.

한다는 것을 의미한다. 최초의 프로토콜 사용자는 기술 커뮤니티, 또는 프로토콜 개발자들이었다. 그들이 정의해낸 새로운 행위는 다른 사용자들에게 학습되고 복제될 수 있었을 뿐만 아니라 흔쾌히 수용되었다. 최초의 기술전문가들로 이루어졌던 인터넷 커뮤니티는 자기 자신을 원형으로 하여 다수의 '프로토콜 사용자'들을 복제해내는데 성공했다.

프로토콜 사용자들은 기술규격에 따라 행위를 하기 때문에 언제나 측정가능하다. 그들이 언제 어떤 프로토콜을 사용하여 어떤 정보에 접근했는지, 얼마나 많이 정보에 접속하는지, 얼마의 빈도로 해당 정보를 방문하는지, 그리고 그들이 어떤 정보를 따라 다음 정보로 이동했는지 등을 쉽게 확인할 수 있다. 프로토콜 사용자들의 행위에 대한 지식은 그들의 행위에 대한 관리를 가능하게 해준다. 인터넷 거버넌스는 전통적인 통치시스템 보다 자신의 통치대상에 대해 잘 알 수 있는 조건을 이미 내재적으로 구비하고 있다.

그들이 바로 인터넷 거버넌스가 발명해낸 새로운 통치대상이다. 이들 통치대상-주민-은 두 개의 이질적인 세계가 중첩되는 영역에 자리하고 있다. 하나는 TCP/IP 프로토콜이라는 기술적 질서의 세계이고, 다른 하나는 언어라는 기호학적 질서의 세계이다. 32비트의 숫자들의 나열로 구성된 IP주소는 기계장치에게는 적절한 것이었지만 사람들에게는 가독성이 없었다. 그래서 숫자기호를 언어(문자)기호로 번역하는 방식을 도입한 것이다. 도메인네임은 기술적 프로토콜 내부로 일상적인 언어(문자)의 사용을 끌어들여옴으로써 사용자들에게 시스템접근의 편리성을 제공했고, 이와 더불어 사용자가 쉽게 확대될 수 있었다.

그런데 주목할 것은 여기에서 말하는 '언어(문자)'란 영어라는 점이다. 이는 초기 인터넷 기술 커뮤니티가 영어사용자였기 때문이다. 그들은 언어적 측면에서는 영어문자가 가지고 있는 의미를 공유하는 동질적 사회문화 집단이었다. 결과적으로 DNS는 영어만을 전제하여 구성되었으며 그 외 다른 언어는 전혀 고려되지 못했다.

4) ICANN의 통치와 자율성

미상무부의 인터넷 정책은 크게 자유경쟁과 인터넷 거버넌스로 대변된다. 이 두 가지 원칙은 일반적으로 미국 정부가 인터넷상에서 발생하는 문제에 직접적인 개입을 하지 않는다는 것으로 해석되었다. 그러나 DNS에 대한 미국 정부의 지위는 논쟁적이다. ICANN 체제가 출범할 당시 인터넷 자원에 대한 미상무부의 관점은 "미국정부 투자의 결과"라는 것이었다(NTIA, 1998). 기술 커뮤니티가 의도한 것은 아니지만, 그들의 프로젝트들은 미국 정부의 재정지원에 의해 운영되었으므로 불가피하게 그 프로젝트의 결과물에 미국정부의 권한이 체화되었다. GAO(2000) 보고서에 따르면 미상무부는 “A 루트" 서버에 대한 정책적 권위를 ICANN에게 이전할 계획이 없으며, 그러한 통제권을 이전할 시나리오를 개발하거나 환경을 조성한 적도 없다. 미국정부의 이런 경향은 최근에도 여전히 유효한 것으로 알려졌다.

ICANN은 민간 이해당사자들과 전문가 중심으로 의사결정이 이루어지지만 미국정부의 의지로부터 자유로울 수 없었다. 때문에 ICANN은 투명성과 공정성의 결핍이라는 비판을 받아왔고, 대안적 관리기구의 필요성이 제기되어 왔다. 그러나 비판자들의 주장처럼 DNS에 대한 미국정부의 권한의 성격이 일방적이라고 보기는 어렵다. 사실 ICANN 체제를 미국정부가 설립했다고 하는 평가도 부분적으로만 진실이다. ICANN이 미국정부의 양해각서에 의

한 프로젝트 관계이고 계약문서상으로 미국정부의 위탁자라고하더라도, ICANN의 지위는 단순한 위탁운영자에 머물지 않는다.

첫째 그들의 기술적 조정 및 운영은 IETF와 같은 기술 커뮤니티에 의해서 오랜 동안 누적되어온 기술적 규격 위에서 작동하기 때문이다. 그들 내에서 작동하는 규칙은 이미 독자적이다. 그들의 기술문서(RFC) 체계는 다른 외부의 문서를 참조하기 보다는 자신들의 문서를 참조하는 것으로 충분하다. 이는 DNS의 기술적 운영이 자율성을 가지고 있음을 의미하며 결과적으로 구체적인 기술적 결정에 대해 미국정부의 의지가 언제나 결정적일 수는 없다.

둘째, ICANN의 통치대상은 프로토콜 사용자들이며 이는 미국정부의 통치대상-미국시민-과 다른 고유한 영역이다. ICANN 체제의 정통성은 초기 인터넷 기술 커뮤니티의 형식에서 기원하고 있다. 그리고 ICANN의 의사결정 절차에 의해 결정된 규약은 전 지구적으로 '프로토콜 사용자'들의 행위를 규제하게 된다. 의사결정 방식에서도 ICANN과 미국정부는 상이하다. 먼저 DNS 관련 이해당사자 집단이나 기술 커뮤니티가 의제를 제기하여야만 비로소 의사결정 절차가 시작될 수 있다. 미국정부의 지위가 상당히 결정적이라고 하더라도 ICANN 의사결정 절차 내에서 미국정부가 선제적으로 공식적인 의제를 발의하기는 어렵다. 이처럼 통치 방식이 다르고 통치대상이 다르기 때문에 ICANN을 단순히 미국정부의 위탁협력자라고만 할 수 없다.

셋째, 도메인네임시스템(DNS) 전체에 대해 독자적인 소유권을 주장할 수 있는 명백한 주체가 없다는 점이다. 비록 미국정부가 "A 루트" 서버에 대해서 소유권적 권리를 암시한다 하더라도 그것은 전체 거버넌스의 부분일 뿐이다. 더구나 미국정부는 자신의 권리를 명백히 주장할 수도 없다. DNS 구조는 기술적으로 단순한 시스템이다. 누구든지 구축할 수 있고 운영할 수 있다. 미국정부가 DNS에 대한 전반적 권리를 주장한다면 현재의 인터넷 거버넌스를 수용했던 사람들은 그 세계를 떠날 가능성이 있다. 그렇다면 그 세계는 더 이상 권리를 주장해야 할 만큼 매력적이지 않게 될 것이다.

ICANN 체제가 기술적 자율성과 통치방식 및 통치대상의 고유성이 있다는 점을 인정한다면, 인터넷 거버넌스는 미국정부 내 하위 시스템이라기보다는 일정한 독자성을 가진다고 보아야 한다. DNS 운영에 대한 미국정부의 권한은 소유권이나 지배권이라기보다는 일종의 '거부권'에 가깝다. 물론 거부권이더라도 그것은 중요한 권력 효과이다. 미국정부는 DNS 운영에 있어서 ICANN 체제가 수립한 정책을 '최종적으로' 허용할 것인지 거부할 것인지를 결정할 수 있는 잠재적 권위를 가지고 있다. 유럽을 중심으로 대안적 도메인 관리기구 논의가 제기되고 있지만, 기술적 어려움이 거의 없음에도 불구하고 이에 대한 미국정부의 입장은 단호한 거절이었다. ICANN이 생산한 규칙이 미국정부의 이해관계에 위배된다면 최종적으로 집행되기 어렵다는 점에서 미국정부는 그 규칙의 범위를 경계 짓는다.

2009년 ICANN과 미상무부는 양자의 관계를 “이행확인(Affirmation of Commitments)” 형태로 전환했고[6], 동시에 ICANN과 UNSCO 사이에 “국제도메인네임 개발을 위한 협력협정(CA)”을 맺었다. 이로써 ICANN은 그동안 미상무부에게만 보고서를 제출했던 것과 달리,

6) http://www.icann.org/ko/about/agreements/aoc/affirmation-of-commitments-30sep09-ko.htm

모든 주체에게 연간보고서를 공개하기 시작했다. 일련의 협정들은 ICANN의 조정업무가 특정 주체에 의해서 영향을 받지 않음을 명시적으로 선언하는 것이었다. 이는 미국 이외 다른 여러 나라 정부들과 관련자들이 미국주도의 인터넷 거버넌스 체제를 비판했기 때문이고, DNS관리에 있어서 ICANN이 가지는 고유한 거버넌스가 존재함을 확인하는 것이기도 하다. ICANN 체제는 미국정부라는 강력한 환경으로부터 외재적인 영향을 받지만, 동시에 그런 외적 개입으로부터 차단된 독자적인 통치 시스템으로서 일정한 자율성을 얻어가고 있다.

3. DNS의 '경계'; 통치의 변이

시장계약 관계에 기반을 두는 일반최상위레벨도메인(gTLD)이라는 ICANN 체제의 '중심' 영역과 대비하여, 국가코드최상위레벨도메인(ccTLD)이라는 '경계'영역은 비공식적인 우호관계를 기반으로 작동한다. 이는 달리 말하자면, ICANN 체제와의 관계에서 일반최상위레벨도메인(gTLD)보다 국가코드최상위레벨도메인(ccTLD)이 상대적으로 독립적으로 움직일 수 있다는 의미이다. '경계'영역은 '중심'의 규칙만이 아니라, '경계'가 가지는 독자적인 규칙이 중첩되어 나타나므로 현상의 복잡성이 크다. 그런 점에서 경계영역의 복잡성은 그 체제를 오히려 입체적으로 증명해줄 수 있다. '경계'에서의 시점이야말로 보다 더 넓은 조망을 가능하게 해주기 때문이다. 특히 한국의 DNS 관리체제는 전통적인 정부시스템과 인터넷 거버넌스라는 두 개의 이질적인 통치시스템이 조우하고 충돌했던 역사적 과정을 함축하고 있다.

1) SDN 커뮤니티와 거버넌스

한국의 인터넷기술 커뮤니티는 "SDN(System Development Network)"으로부터 기원한다. SDN은 컴퓨터국산화프로젝트를 진행하던 전길남 박사의 제안으로 진행되었다. 당시 한국정부는 컴퓨터 및 통신장비의 국산화에 관심이 높았던 반면에 컴퓨터 네트워킹은 주요한 관심사가 아니었다. 때문에 다만 "컴퓨터국산화 프로젝트를 원활하게 수행하기 위해서 관련 연구자들 사이의 협력을 촉진"한다는 취지로 전자기술연구소(KIET)와 서울대학교 사이의 통신선을 연결하는 재정지원을 받을 수 있었는데(전길남, 2012-10-27), 이것이 SDN이다.

그 즈음, 한국데이터통신(주) 및 대학연구소들이 통합망 연구를 수행하고 있었다. 이 개별적인 시스템들이 SDN에 연결되기 시작했고 KAIST SALab이 네트워크 관리를 담당했다. 1986년, KAIST SALab은 존 포스텔에게 국가코드 도메인네임을 신청했다. 포스텔은 RFC 규정에 준하여 한국에 ".KR"이라는 국가도메인을 부여했고 전길남은 .KR 국가도메인 관리자가 되었다. 1989년, 한국통신 등 11개 기관이 컨소시엄 형태로 '하나(HANA)'망을 구성했고, SDN과 연결되었다. 이즈음 SDN 가입기관은 약 30여개에 이르렀고 기술전문가들 사이의 일상적인 협력이 필요해지면서 자연스럽게 네트워크 담당자들 사이의 모임이 시작되었다. 네트워크는 늘 문제가 발생했고 "하루라도 서로 얘기를 하지 않으면 저절로 죽었다"(전길남, 2012-12-08). 그들 사이의 정기적인 모임은 커뮤니티로 발전했는데, 네트워크 운영자, 엔지니어, 사용자 그룹이 중첩되는 시기였다. 여기서는 그들을 'SDN 커뮤니티'라고 부를 것이다(오익균, 2012-12-12).

이후 이 커뮤니티가 확장되어 공식적 명칭을 가지게 된 것이 1991년 학술전산망협의회(ANC)이다[7]. 당시 DNS 기능은 있었지만 지금과는 달리, 가입기관 네트워크 관리자들에게 주기적으로 "hosts.txt"파일을 보내어 각각 업데이트하는 방식으로 이루어졌다(박태하, 2012-11-30). 망 가입기관들이 늘어나면서 기술적인 조정만이 아니라, 누가 관리할 것인지, 비용을 누가 낼 것인지를 조율하는 문제들이 더 빈번히 부상했다. 학술전산망협의회(ANC) 회원들은 자신의 위상 설정 문제를 고민하기 시작했고, 논의과정에서 당시 체신부의 공식적 위임을 받아야할 필요가 제기되기도 했다(ANC-91-011). 1994년에는 한국전산망협의회(KNC)로 확대·개편되었고, 자생적으로 정책 조정 절차도 구체화했다. 1996년까지 활동했던 한국전산망협의회(KNC)는 총 461개의 문서를 생성했는데 이 문서들은 당시의 거버넌스의 주요 의제들을 담고 있다(KNC-94-154).

한편 1994년 학술전산망협의회(ANC) 16차 회의 의결에 따라, 한국망정보센터(KRNIC) 운영기능을 한국전산원에 이관하기로 했다. 이에 체신부는 이를 공식적으로 승인하기 위해 “한국망정보센터기능의 한국전산원 이관·수행”이라는 제목의 공문을 한국전산원에 발송했다(한국전산원, 1997). 그 해 8월 한 달 동안 KAIST와 한국전산원사이에서 업무 인수· 인계가 이루어졌다. 그러나 .KR 도메인에 대한 거버넌스 권한은 여전히 한국전산망협의회(KNC)에게 있었고, 한국전산원은 한국전산망협의회(KNC) 사무국 역할을 맡았다(KNC-94-163).

2) 이질적인 통치의 병존

한국전산망협의회(KNC)의 정책기능은 1997년 NIC위원회에 승계되었다. 1998년 정부산하기관 경영혁신방안이 추진되었는데, 그 일환으로 한국전산원 내에 있던 한국망정보센터(KRNIC) 기능이 분리되어, 1999년 “재단법인 한국인터넷정보센터(KRNIC)”가 되었다. 이 과정은 정보통신부 인터넷정책과(김광수)와 한국인터넷협회(전길남), NNC(박치항), 정보통신진흥협회(박석규), 웹마스터클럽(손정윤), Name Committee(이수연) 등이 민간기구 운영원칙에 합의함으로써 이루어졌다. 당시 당사자들 사이에서는 .KR도메인에 대해서 한국인터넷정보센터(KRNIC)가 운영관리를 담당하고 인터넷주소위원회(NNC)가 정책결정을 담당한다는 암묵적 합의가 있었다(송관호, 2012-11-15). 이것이 암묵적 신뢰관계였기 때문에 이후 법제정 논쟁과정에서 상호관계를 상이하게 해석하는 현상이 발생했다.

1999년 6월 도메인 등록이 유료화 되었고, 도메인주소 등록에 대한 대중적 관심이 높아지면서 도메인 등록자 수가 급증했다. 이 시기를 즈음하여 정통부의 .KR도메인에 대한 관심도 구체화되었다. 그러자 정보통신부와 인터넷주소위원회(NNC)는 빈번한 충돌하기 시작했다. 대표적인 사례로는 지역도메인 영문표기법 변경문제에 관한 의견 충돌을 들 수 있다. 2000년, 문화관광부는 한국어의 로마자 표기법을 변경·고시했는데, 이때 "Pusan"은 "Busan"이 되었다. 이에 자방자치단체에서는 2단계 도메인네임을 변경해 줄 것을 한국인터넷정보센터(KRNIC)에 요청했다.

담당자들은 이 문제를 인터넷주소위원회(NNC)에 상정했다. 그런데 인터넷주소위원회

7) 학술전산망협의회(ANC)는 자신의 활동 범위를 "네이밍 및 어드레싱의 조정, 관련 프로젝트들의 조정, 해외 전산망과의 연결 조정, CCIRN[1])의 한국대표, 국내 Internet Society 활동"으로 설정했다(ANC-91-012).

(NNC)는 2단계도메인 소멸원칙에 부합하지 않는다는 점을 들어 변경거부를 결정했다(전응휘, 2012-10-05). 당시 인터넷주소위원회(NNC) 위원들은 해당 2단계 도메인레벨을 신청한 3단계 도메인 수가 “0”이 되지 않는 한, 그 도메인에 대한 “이해관계 커뮤니티(community of interest)”가 존재하는 것으로 간주하여 소멸 결정할 수 없도록 하고(RFC-KR-131) 있었다. 오랜 논쟁을 거쳐서 2001년 기존의 영문 지역명과 병존하여 새로운 영문 지역명을 할당하는 것으로 결론지어졌다. 그럼에도 불구하고 여전히 기존의 영문 지역명을 폐기하고 새로운 영문 지역명으로 완전히 이전되어야 한다는 주장과 기존 영문 지역명 사용자가 자발적으로 전환할 때까지 기다려야 한다는 주장이 대립했다.

이 상황은 인터넷주소위원회(NNC)가 자신들의 기술문서(RFC-KR)를 사실상 '법'으로 간주했기 때문에 발생한 것이었다.[8] SDN-NNC 커뮤니티는 1992년부터 2단계 공공도메인으로 지역명 도입을 논의해왔고, 오랜 논쟁을 거쳐서 ".KR 지역 도메인 이름 체계(RFC-KR-009)"와 같은 기술문서를 정착시켜왔다. 이것을 수정하거나 변경하려면 다시 논의과정을 거쳐야만 했다. 그런데 정부의 담당자들 관점에서 볼 때, 인터넷주소위원회(NNC)의 합의는 국내 인터넷 사용자 전체를 대변하기 보다는 여전히 작은 커뮤니티 차원의 것으로 보였다(김광수, 2012-11-21; 강장진, 2012-12-04). 두 체계는 충돌할 수밖에 없었고 두 체계 사이의 긴장은 다른 논제에서도 격렬한 의견 차이로 이어졌다. 이 과정에서 .KR도메인 거버넌스 권한에 대한 한국인터넷정보센터(KRNIC)와 인터넷주소위원회(NNC) 사이의 오래전 합의는 희미해졌다. 인터넷주소위원회(NNC)는 정통부와 협력관계를 설정하지 못하면서 점점 활력을 잃기 시작했다(이수연, 2012-11-08).

3) 법률적 관리로 이행

.KR도메인 정책권한을 둘러싸고 벌어진 긴장은 2004년 "인터넷주소자원에 관한 법률"의 국회통과를 기점으로 일단락되었다. 당시 입법과정은 인터넷주소위원회(NNC)를 배제한 채, 정보통신부 주도로 진행되었다. 양자 사이의 타협은 거의 없었다(이동만, 2012-12-04). 한국인터넷진흥원(KRNIC)은 법률에 따라 해산절차를 진행했고, “한국인터넷진흥원(NIDA)”로 재편되어 정보통신부 산하 법정기구가 되었다. 이제 SDN-NNC 커뮤니티는 공식적인 역할을 잃고 흩어졌다. 그로써 RFC-KR이 수행했던 역할은 법률의 영역으로 넘어갔고, 정책권한은 정보통신부장관에게 이전되었다.

	운영관리	정책	
		개발	결정

8) RFC-KR 기술문서는 IETF의 RFC전통에 따라 1999년 .KR DNS 관련한 정보제공을 목적으로 체계적으로 작성되기 시작되었다. SDN 커뮤니티 시절 "지역 도메인의 실험적 시행(RFC-KR-008)"과 ".KR 지역 도메인 이름 체계(RFC-KR-009)"라는 근거 문서에 의해 2단계 지역도메인네임을 지정, 관리해왔었다.

1986-	KAIST/SALab	SDN 커뮤니티	
1991-		학술전산망협의회(ANC)	
1993-	KAIST/한국망정보센터(KRNIC)		
1994-	[법정법인]한국전산원/한국망정보센터(KRNIC)	한국전산망협의회(KNC)	
1998-		NIC위원회	
1999-	[재]한국인터넷진흥원(KRNIC)	인터넷주소위원회(NNC)	한국인터넷진흥원 이사회와 NNC의 공동 승인
2004-	[법정법인]한국인터넷진흥원(NIDA)	NNC 커뮤니티[실무위원회]	정보통신부장관(인터넷주소정책심의위원회)
2009-	[법정법인]한국인터넷진흥원(KISA)/인터넷주소관리센터	NNC 커뮤니티[인터넷발전협의회/주소분과]	방송통신위원회(인터넷주소정책심의위원회)

표 1 KR도메인 거버넌스의 변이

이제 .KR도메인은 정보통신부 단독의 관리아래 놓이는 것으로 보였다. 정보통신부 장관은 인터넷주소정책심의위원회를 구성하고 “학계, 산업계, 시민단체, 공공기관 등을 대표하는 학식과 경험이 풍부한 자”를 위촉하고 의사결정을 위임했다. 그런데 이 위원회는 정책을 ‘의결’할 수는 있으나 관련 정책을 개발하거나 깊이 논의할 수는 없었다. 한국인터넷진흥원(NIDA) 담당자들은 이를 보완하기 위해 이 위원회 산하에 "실무위원회"를 꾸리고, NNC 커뮤니티를 다시 초빙했다. 인터넷주소정책심의위원회 회의는 안건이 있을 때마다 부정기적으로 소집되었던 반면에 실무위원회는 NNC 커뮤니티가 해오던 방식대로 매달 정기 회의를 가졌다. 이 실무위원회가 구체적인 기술정책 사항에 대한 제안 문서를 작성하고, 한국인터넷진흥원(NIDA) 담당자들이 그 문서를 인터넷주소정책심의위원회에 상정하는 방식을 취했다.

이 당시 주요 논제 중 하나는 .KR 2단계도메인 개방문제였다. .KR도메인 등록이 100만개를 넘어서면서 정체상태를 보였던 시기였다. 한국인터넷진흥원(NIDA)과 정통부는 2단계도메인을 개방할 경우 사용자들이 편리성이 높아져서 도메인 신청이 증가할 것을 기대했다. 그러나 NNC 커뮤니티는 2단계도메인 개방에 신중한 태도를 보였다. 특정 2단계도메인이 악의적으로 선점되거나, 그런 선점을 우려하여 추가 신청을 함으로써 비용부담을 발생시킬 우려가 있다고 보았기 때문이다. 이 문제 역시 정부 담당자와 NNC 커뮤니티 사이에 긴장을 낳았고, 실무위원회는 1기 이후 재임명되지 않았다.

2009년, 정부조직 통폐합으로 정통부는 방송통신위원회가 되었고 한국인터넷진흥원(NIDA)은 다른 2개의 기구와 통합되어 한국인터넷진흥원(KISA)이 되었다. 한국인터넷진흥원(KISA)내 .KR도메인 담당자들은 방송통신위원회의 승인을 얻어, "인터넷발전협의회"라는 명칭으로 NNC 커뮤니티를 다시 초대했다. 인터넷발전협의회는 한글도메인 신청을 위한 제

안문서 작업을 주도하는데 기여했고, 그 성과로 2011년 ".한국" 도메인 도입이 순조롭게 이루어졌다(진충희, 2012-11-27; 오병일, 2012-11-27).

	RFC-KR	도메인네임관리준칙
1	도메인 이름 할당 원칙(RFC-KR-011) 1. 도메인 이름 신청기관은 한국내 적을 두어야 한다.	제4조(등록 조건) ①신청인 및 등록인은 대한민국에 주소지가 있어야 한다.
2	도메인네임 생성 규칙(RFC-KR-116, 145) 2. 도메인네임 생성 규칙 2.1 도메인네임의 구성요소는 레이블(label)과 '.' 이다. 2.2 레이블에 쓸 수 있는 글자 ·영어 알파벳 ([A-Z], [a-z]) ·숫자 ([0-9]) ·하이픈 ([-]) ·한글 ([한글 글자마디 11,172자]) 2.3 레이블은 하이픈으로 시작하거나 끝날 수 없으며, 영어 알파벳의 대소문자 구별은 없다. 2.4.레이블의 길이는 2자 이상, 63자 이하이며, 한글이 포함된 레이블은 17자 이하이어야 한다.	제5조(등록 기준) ① 3단계 도메인네임 등록 기준은 다음 각호와 같다. 1. 도메인네임은 영문자[A-Z][a-z], 숫자[0-9], 하이픈[-]으로 구성되어야 한다. 2. 도메인네임 길이는 2자 이상 63자 이하이어야 한다. 3. 도메인네임은 하이픈으로 시작하거나 끝나지 않아야 한다.
3	선접수 선처리 원칙(RFC-KR-112) KRNIC은 도메인네임 등록 신청서의 접수 순서에 따라 도메인네임을 처리한다. 즉, 선접수 선처리(First Come, First Served)원칙으로 처리한다.	제9조(등록) ①진흥원은 제8조의 규정에 의한 신청서가 진흥원에 도달한 순서대로 도메인네임을 데이터베이스에 등록하여야 한다.

표 2 도메인이름관리준칙(법률)의 RFC-KR 승계내용 중 일부

이상에서 볼 수 있듯이, 2004년 인터넷주소자원법 통과 이후에도 정부기구는 .KR도메인 관리에 있어서 NNC 커뮤니티를 완전히 대체할 수 없었다. 즉 .KR 도메인관리를 법률적 지배아래에 두는데 성공했으면서도, .KR도메인 거버넌스가 온전히 정부의 독자적 영역이 되지 못했다. 다만 거버넌스의 내용이 정책개발과 정책결정으로 분화되는 결과를 낳았다. 정책개발은 여전히 NNC 커뮤니티가 수행했고 최종적인 정책결정은 정부적 절차가 된 것이다.

이런 현상은 이미 예견된 것이기도 했다. 인터넷주소자원법은 세부적인 도메인관리에 대한 내용을 “도메인이름관리준칙”에 규정하고 있는데, 그 대부분의 내용은 SDN-NNC 커뮤니티가 오랫동안 수립해온 RFC-KR의 내용을 포함하고 있다. DNS의 관리가 법률적 절차가

되었지만 기술적 작동은 승계된 것이었다. 그러므로 사실상 NNC 커뮤니티가 도메인 관련 기술정책 문서 작업을 할 수 있는 유일한 집단이었다. NNC 커뮤니티는 인터넷 규약과 질서 체계에 대해서 가장 잘 알고 있는 전문가집단이었고, 반면에 정부 또는 정부가 지명한 심의위원들은 작성된 문서를 보고 의사결정을 할 수는 있었지만 관련 프로토콜에 관한 독자적 비전을 도출할 수는 없었다. 한편 NNC 커뮤니티는 한국인터넷진흥원(KISA)의 재정 및 실무지원이 없이는 지속적으로 유지되기 어려웠다.

4) .KR도메인 거버넌스; 이종교배 시스템

.KR도메인 거버넌스는 NNC 커뮤니티와 한국정부라는 이질적인 집단 사이의 긴장과 경합의 과정에서 변이했다. 인터넷 거버넌스와 국가시스템은 역사가 다르고 통치형식이나 통치의 대상도 달랐다. 그런데 이 두 시스템은 .KR 도메인이라는 기호적인 명칭을 두고 조우할 수밖에 없었다. 존 포스텔이 작성한 “RFC 1591(Domain Name System Structure and Delegation)”에 의하면, 국가코드최상위레벨도메인(ccTLD)은 ISO-3166이 지정하는 두문자 국가명을 참조하여 할당된다. ISO는 정부기반 대표들이 참여하는 ITU의 기술문서였다. 결과적으로 RFC문서가 ISO문서를 참조함으로써 지리적 경계가 없는 인터넷 세계에 전통적인 국가들 사이의 합의에 의한 정치적이고 지리적인 경계를 DNS 내부로 끌어들였다.

	전통적 국가시스템	인터넷 거버넌스
지리적	인터넷주소자원법	RFC-1592 RFC-KR-011 ANC-92-037R2
기호적	ISO-3166	ccTLD

표 3 .KR도메인; 이종교배적 시스템

그것이 무엇이든지간에 "국가"라는 라벨이 붙는 순간 해당 정부는 자신의 권한을 따지지 않을 수 없었다. NNC 커뮤니티 역시 .KR 도메인이 인터넷 도메인 체계에서의 한국을 대표한다고 여기고 있었다(RFC-KR-010). “.KR”이라는 문자는 기호에 불과했지만 DNS 내에서 그 자체로 '국가'가 되었다. 이는 한국정부로서는 양보할 수 없는 권한이었다. 그런데 경합의 과정에서 NNC 커뮤니티와 한국정부는 서로를 완전히 배제하는데 성공하기 보다는 서로에게 혼합되어 갔다. 그들은 자신도 모르게 서로를 계승하고 있었다.

2004년 제정된 법률에 의하여 "도메인이름관리준칙" 제4조(등록조건)는 "신청인 및 등록인은 대한민국에 주소지가 있어야 한다"고 규정하고 있다. 이것은 SDN 커뮤니티 시절부터 있어왔던 "도메인 이름 신청기관은 한국 내 적을 두어야"(RFC-KR-011) 한다는 규정을 승

계한 것이었다. 이 거주지 제한 요건은 인터넷 초기로 거슬러 올라가, SDN 커뮤니티에 의해 암묵적으로 수립된 것이었다. ICANN이나 RFC 차원에서 이러한 지리적 제한조건을 명시적으로 규정한 적은 없었다. RFC 1591은 다만 국가코드관리자에 대해서만 해당 국가 내에서 거주할 것을 조건으로 하고 있을 뿐, 국가도메인 일반신청자의 거주지 제한 규정을 두지는 않았다. 따라서 일반신청자의 거주지 제한 여부는 해당 국가코드도메인 관리주체의 해석에 달려 있었다.

RFC-1591은 국가코드최상위레벨도메인 관리자에게 “지역 인터넷 커뮤니티(local internet community)”를 대변할 의무와 책임을 부여하고 있으므로, 자연히 SDN 커뮤니티는 자신의 지역 커뮤니티를 특정해야 했다. 이 문제는 RFC문서가 지칭하고 있는 "지역(local)"을 무엇으로 해석하느냐는 문제이기도 할 뿐만 아니라, "각 국가코드도메인의 통치대상이 어디까지인가"를 규정하는 문제이기도 했다. SDN 커뮤니티는 "지역 커뮤니티"를 '지리적인 것'으로 해석했다(이동만, 2012-12-14). 이는 .KR도메인 관리 초기, 아직 한국 내에서 도메인에 대한 인식이 일반화되지 않았기 때문에 잠재적인 사용자의 도메인네임 사용권리가 누군가에 의해 선점될 것을 우려했던 점도 작용했다(오익균, 2012-12-12; 박태하, 2012-11-30).

2004년 법률이 제정될 때 정통부는 이 거주지 규정을 별 문제없이 수용했다. 그 규정에 의식적으로 동의했다기보다는 특별히 문제삼을만한 주제가 아니기 때문이다. 도메인네임 신청자의 거주지 제한조건은 한편으로는 도메인네임의 고의적 선점으로 인한 분쟁을 해소하는데 도움이 되기는 했지만 다른 한편으로는 전통적 국가시스템과 인터넷 거버넌스라는 이질적 시스템의 혼합이 일어나는 지점이기도 했다. 지리적 영토개념은 전통적으로 국가시스템의 통치대상이기 때문이다. 이는 정부관료 및 한국인터넷진흥원 담당자들과 NNC 커뮤니티가 서로 공유하는 인식의 지대가 있었음을 함축한다. 따라서 .KR 도메인신청자의 신원을 확인하기 위해 주민등록번호를 기입하는 항목도 자연스럽게 수용되었다. 거주지를 확인해야 한다면 주민등록번호나 외국인등록번호 같은 전통적인 통치시스템을 참조해야 했기 때문이다.

결과적으로 .KR도메인 거버넌스의 통치대상은 '프로토콜 사용자'와 '언어-기호적 사용자' 그리고 '지리적 거주자'가 중첩되는 영역에 놓이게 되었다. .KR도메인이라는 ‘경계’지역의 통치대상은 인터넷 거버넌스의 '중심'이 설정하고 있는 통치대상을 전제할 뿐만 아니라, 자신의 지역 커뮤니티 규정을 동시에 만족해야 하기 때문이다. 이로서 .KR도메인 거버넌스는 인터넷 거버넌스가 구축한 중심의 질서만이 아니라 지리적이고 전통적인 통치시스템이 구축한 이질적인 질서도 동시에 참조함으로써 '경계'로서의 특질을 드러내었다.

인터넷 거버넌스의 고유한 통치맥락을 본다면, 지리적 경계 또는 지리적 거주자 개념은 이질적인 요소였다. 그럼에도 불구하고 인터넷기술 커뮤니티와 한국의 SDN 커뮤니티는 '지리적 거주자' 개념을 쉽게 수용했다. 이 외재적 요소는 이후 복잡한 문제의 기원이 되었지만 그다지 잘 드러나지 않았다. 좀 더 엄밀하게 말해서, 이 현상은 ‘경계’의 특질이기도 하지만 ‘중심’으로부터 파생된 것이기도 하다. 그동안 인터넷 거버넌스 내에서는 너무나 잘 알고 있기 때문에 오히려 눈에 잘 띄지 않았던 사실이 있다.

그것은 인터넷 거버넌스가 기반하고 있는 언어-기호적 질서가 가지는 한계였다. 이 체계

내에서 ‘언어-기호적 질서’란 다름 아닌 영어만을 의미했다. DNS의 결핍을 고려하여 재해석해보면 즉각적으로 .KR도메인 거버넌스가 '지리적 거주자'라고 표지했던 것은 사실은 '한글 사용자'를 대변하는 것이었다는 것을 알 수 있다. 영어를 유일한 언어-기호적 질서로 하는 체계에서 지리적 경계 개념만이 다른 지역문화를 표지할 수 있는 범주로 남게 되었을 것이다. 종합해보자면, .KR 도메인이 대표해야하는 지역 커뮤니티가 한글사용자와 인터넷프로토콜사용자의 중첩지대에 형성되어야 함을 강하게 지시하고 있다. DNS가 숫자기호를 언어기호로 번역하는 임무를 수행한다는 점을 상기한다면 직관적으로 이해할 수 있다.

4. 결론

인터넷 거버넌스는 인터넷 작동의 근간이 되는 새로운 통치형식과 통치대상을 발명해냈다. 인터넷 프로토콜들은 인터넷 사용에 필요한 형식과 절차에 관한 기술적 질서이며, 이들 프로토콜들을 통해서만 이질적인 네트워크들은 하나의 네트워크인 것처럼 연결될 수 있다. 이 새로운 통치의 ‘경계’지역에 해당하는 KR도메인은 SDN 커뮤니티의 거버넌스와 한국정부라는 이질적인 시스템 사이의 긴장과 경합을 통하여 이종교배적 시스템으로 진화했다. 그들의 조우는 초기 인터넷기술 커뮤니티의 RFC 기술문서가 국가코드최상위레벨도메인(ccTLD)을 생성할 때부터 예견된 것이었다. "국가"라는 라벨이 붙는 순간 해당 정부는 자신의 권한을 따지지 않을 수 없었기 때문이다. 게다가 SDN 커뮤니티가 자신의 지역 커뮤니티를 '지리적인 거주자'로 규정함으로써 더욱 강화되었다.

이런 현상은 이종교배적 시스템으로 변이하는 ‘경계’의 특질이기도 하지만, 인터넷 거버넌스 ‘중심’의 질서체계로 부터 기원한 것이다. 초기 인터넷기술 커뮤니티는 대체로 영어사용자였기 때문에 그 외의 언어를 고려할 필요가 없었다. 그들에게 너무나 익숙한 것이었기 때문에 달리 규칙을 제정할 필요도 없이 영어사용은 자연스럽게 이 체제의 배경이 되어버렸다. 이것은 ICANN 체제가 수립된 이후에도 승계되었고, 도메인네임이 국제적으로 널리 사용된 연후에야 “다국어 도메인”과 같은 논제들이 부상할 수 있었다. 인터넷 거버넌스가 기반하고 있는 ‘언어-기호적 질서’가 내포하고 있는 이러한 제한을 인식하는 것은 중요하다. 그것을 고려하는 것만으로도 즉각적으로 .KR도메인 거버넌스가 '지리적 거주자'라고 표지했던 것은 사실은 '한글 사용자'를 대변하는 것이었다는 점이 드러난다. .

.KR도메인의 '지리적 거주자' 규정은 인터넷 거버넌스 ‘중심’ 체제가 영어 이외에 다른 언어의 존재를 고려하지 않음으로써 발생한 결핍의 일면이다. 한글학습자들은 "아리랑"이라는 단어의 의미를 공유한다. 의미의 공유는 언어-기호적 질서를 구성할 수 있고, 그런 점에서 DNS의 중요한 내적 요소이다. 인터넷 거버넌스의 결핍에 의해서 결과적으로 영어사용자가 아닌 프로토콜 사용자는 의미의 공유에서 배제되고 있다고 추론할 수 있다. 이런 점에서 한국정부와 .KR도메인 거버넌스 담당자들은 '지리적 거주자' 보다는 한글이라는 언어-기호적 영역을 새로운 전략적 연결점으로 고려해 볼 수 있다. 아마도 SDN 커뮤니티가 '우리말 언어 공동체'라는 개념을 제기한 것(RFC-KR-140)도 그런 결핍을 감지했기 때문일 것이다. 그러나 이 논의는 인터넷주소자원법 제정 이후 해당 커뮤니티가 위축되면서 더 이상 진화되지 못했다.

이상의 논점과 더불어 .KR도메인 거버넌스의 역사에서 여러 관련 논제들이 일반 사용자

들에게 깊이 있게 전달되지 못한 점도 제기될 필요가 있다. 정부관료와 기술커뮤니티는 모두 일반 사용자들의 이해를 대변하겠다고 주장하면서 경합했었다. 그러나 여전히 일반 사용자들은 인터넷 거버넌스 주제로부터 멀리 놓여있다. 인터넷 기술을 둘러싼 논쟁들은 전문적이며 오랜 노력을 요구한다. 그래서 일반 사용자들은 그러한 논의를 따라가기도 어렵고 그 결정에 참여하기도 어렵다. 이는 인터넷 거버넌스와 정부시스템 양쪽 모두 공히 "전문성의 정치(the Politics of Expertise)"가 작동했다고 할 것이다. SDN 커뮤니티는 기술공동체로서 훌륭했지만, 거의 전 국민이 인터넷사용자가 된 상황에서 .KR지역 커뮤니티 전체를 대변하는 형식과 절차를 구현해내지 못했다. 이점에서 한국정부의 비판은 적절했다. 그러나 한국정부가 .KR관리의 직접 주체가 되는 것은 무리가 있다는 것 또한 확인할 수 있다. 이는 최근 .KR거버넌스의 투명성이 더욱 악화되고 있는 것과 연관이 있다. 이런 상황이 계속된다면 인터넷주소자원법 제정의 정당성은 사라질 것이다. 일반 사용자들의 이해를 널리 구하기 위해, 그리고 SDN 커뮤니티와 한국정부의 협력을 강화할 수 있는 새로운 참여적 거버넌스 방식을 개발할 필요가 있다.

[참고문헌]

김지연. 2013. 「인터넷거버넌스와 전문성의 정치: 도메인네임시스템(DNS)의 '중심'과 '경계'」. 《경제와 사회》, 2013년 여름호(제98호), 304-340쪽.

이항우. 2010. 「신자유주의 글로벌 인터넷 거버넌스와 정당성 문제: 인터넷주소자원관리기구의 사례(1998~2009)」. 《경제와 사회》, 2010년 가을호(제87호), 172-203쪽.

한국전산원. 1997. 『한국인터넷정보센터 기반기술에 관한 연구』. NCAVIII-RER-97067.

Antonava, Slavka. 2007. "Power and Multistakeholderism in Internet Global Governance: Towards a Synergetic Theoretical Framework". Department of Management and International Business Research Working Paper Series 2007, No. 10. Massey University.

Fischer, Frank. 2009. Democracy and Expertise : Reorienting Policy Inquiry. Oxford University Press.

GAO. 2000. "Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers". official report(B-284206) to the House of Representatives. URL: www.gao.gov

Klein, Hans. 2002. "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy", The Information Society. 18:193-207.

McLaughlin, Lisa and Pickard, Victor. 2005. "What is bottom-up about global internet governance?". Global Media and Communication. Vol. 1, No. 3. pp. 357-373.

Mueller, Milton. 1999. "ICANN and Internet Governance: Sorting through the Debris of 'Self-regulation'", The Journal of Policy, Regulation and Strategy for Telecommunications Information and Media. Vol. 1, No. 6. pp. 497-520.

NTIA. 1998. "Improvement of Technical Management of Internet Names and Addresses. Green Paper. Federal Register 63:8825.

Park, Youn Jung. 2008. The Political Economy of Country Code Top Level Domains. Dissertation submitted in partial fulfillment of the requirements for the Degree of Doctor of Information Science and Technology at School of Information Studies of Syracuse University.

Schewick, Barbara van. 2010. Internet Architecture and Innovation. The MIT Press: Cambridge, Massachusetts, London, England.

Wilson Ⅲ, Ernest J. 2005. "What Is Internet Governance and Where Does It Come From?", Journal of Public Policy. Vol. 25, No. 1. pp. 29-50.

[RFC-KR-011] "도메인 이름 할당 원칙". KRNIC. 1998년 3월.

[RFC-KR-129] "한글 도메인 체계에 관한 고찰". 강경란, 고양우, 이수복, 김경석. 2001년 6월.

[RFC 1557] "Korean Character Encoding for Internet Messages". U. Choi, K. Chon, & H. Park. December, 1993.

[RFC 1591] "Domain Name System Structure and Delegation". J. Postel. ISI. March, 1994.

ABSTRACT

Internet Governance & Politics of Expertise

Kim, Ji-Yeon[9)]

ICANN has been governing the Domain Name System(DNS) "technically" since 1998. The architecture is called Internet Governance, and it brings about many different discourses; “What does that govern?”, “Who delegate its role to ICANN?”, “How could the regime ensure fairness?” etc. This article will analyze on Internet Governance by applying the government approach of Foucault, and try to compare two parts, the 'core' and the 'edge' of Internet Governance for method. Whereas the 'core' of it refers the site that be governed by the formal contract directly, the 'edge' as the rest of it means informal friendly relations with ICANN. The 'core' rule was stemmed from technological community such as IAB or IETF historically. They had invented new world and its population to integrate the technical order as protocol and the semiotic order as language, that be based on new government mode. On the other hand, ".KR" domain, one of the 'edges', has been evolved into more heterogeneous system, through contest and conflict between traditional state and Internet Governance. The governed object of ".KR" domain is situated in the crossing of each other the 'protocol user', the 'language-semiotic user' and the ‘geographical resident’. Here the ‘geographical resident’ rule was weird for DNS, so that shows the internal lack of Internet Governance. It needs to move to the concept of 'Hangeul(Korean-language) user' rather than the ‘geographical resident’.

9) Ph.D, Science & Technology Studies, Korea University, Lecturer of Seoul National University of Science & Technology

인터넷 거버넌스 모델로서의 멀티스테이크홀더

이영음[10]

1. 인터넷 거버넌스와 멀티스테이크 홀더 모델의 개념

인터넷이 글로벌 시대에 사회 전반에 영향을 주는 중요한 하나의 기본 커뮤니케이션 수단의 역할을 하게 되면서 인터넷 거버넌스(Internet governance), 즉 인터넷을 어떻게 관리할 것인가가 주요 이슈로 떠오르고 있다. 특히 2012년 12월에 개최되었던 국제전기통신연합(ITU)의 국제전기통신세계회의(World Conference on International Telecommunications, WCIT)와 2013년 5월에 개최되었던 세계전기통신정책회의(World Telecommunication/ICT Policy Forum, WTPF)에서 인터넷 거버넌스가 중심 이슈로 떠오르면서 2014년 10월에 한국에서 개최되는 ITU의 전권회의가 주목을 받고 있기 때문에, 인터넷 거버넌스에 대한 국내의 관심이 높아지고 있는 상황이다. 이런 와중에 2013년 5월에 터진 미국의 정보기관에 의한 광범위한 불법 정보수집의 폭로 사태로 인터넷을 관리하는 권한의 중요성이 더욱 부각되었고, 이제까지 미국의 영향력 하에 있는 인터넷주소관리기구(Internet Corporation for Assigned Names and Numbers, ICANN)의 관리 구조를 더욱 국제적인 거버넌스 구조로 개조해야 한다는 의견이 강하게 제기되면서, 2014년 5월에 브라질에서 인터넷 거버넌스 관련 회의가 새롭게 계획되기도 하는 등 인터넷 거버넌스는 전 세계적으로 주목을 받고 있는 화두가 되었다. 인터넷 거버넌스를 이해하는데 2013년 현재 가장 많이 이용되는 용어는 멀티스테이크홀더(multistakeholder)라는 개념인데 본 글에서는 인터넷 거버넌스와 멀티스테이크홀더 개념의 발전에 대한 이해를 통해 향후 인터넷 거버넌스의 발전 방향에 대한 지표를 제시하고자 한다.

“거버넌스(governance)"는 공식적인 기구에 의한 통치(government) 형태의 관리체계와 구분되는 개념으로 관련 주체들이 공동의 목적을 위해 일정 정도의 협력에 의해 행해지는 관리체계를 의미한다.[11] 이런 의미에서 인터넷 거버넌스에 대한 가장 일반적인 정의로 채택되고 있는 것은 튀니스에서 열린 정보사회세계정상회의(World Summit on Information

10) 한국방송통신대학교 미디어영상학과, yesunny@knou.ac.kr

11) Rosenau, J; Czempiel, E. (Ed.). Governace without government: order and change in world politics. Cambridge: Cambridge University Press, 1992; Maciel, M. and Pereira de Souza, C. A. (APC), (2011) "Multi-stakeholder participation on internet governance: An analysis from a developing country, civil society perspective" http://www.apc.org/en/node/12965 참조

Society, WSIS)의 2005년 의제 문건[12]에 나온 정의이다. 2003년 제네바 회의에서 구성된 인터넷 거버넌스 워킹그룹(Working Group on Internet Governance, WGIG)에 의해 제안되어 2005년 채택된 인터넷 거버넌스의 정의는 다음과 같다.

> 34. 인터넷 거버넌스는 정부, 민간, 시민사회가 맡은 역할을 통해 인터넷의 발전 및 이용과 관련하여 공유하는 원칙, 규범, 규칙, 의사결정 절차, 그리고 프로그램을 개발하고 응용하는 것이다.[13]

이와 더불어 35번 문단에서는 각 국의 정부, 기업, 시민사회, 그리고 국제기구 및 정부간 기구가 각각 역할을 해야 한다고 명시한 후 36번 문단에는 이러한 집단들을 "이해당사자(stakeholder)"라는 이름으로 표현하기 시작하면서 이들 그룹들을 자연스럽게 "다양한 이해당사자(multistakeholder)로 부르기 시작하였다. 다시 말해 멀티스테이크홀더(multistakeholder)의 개념은 어떤 사안을 관리하는데 있어서 그 사안에 이해관계가 있는 다양한 집단들이 참여하여 서로간의 어느 정도의 협의를 통해 관리의 원칙, 규범, 및 의사결정 절차 등을 정하는 것을 의미하는 것이다.

하지만 인터넷 거버넌스의 개념은 그 대상이나 인터넷 발전 시기에 따라 다양한 의미를 지니고 있었는데 본 글에서는 2005년 튀니지 WSIS 회의의 의제 문건에서 언급되기 시작한 멀티스테이크홀더의 모델이 가장 보편적인 개념으로 받아들여지게 된 이유 및 과정을 살펴봄으로써 인터넷 거버넌스의 바람직한 모델에 대한 이해를 돕고자 한다.

2. 인터넷 거버넌스 개념 분석

인터넷 거버넌스의 개념을 제대로 이해하기 위해서는 무엇을(what) 관리하는 것인가, 관리의 주체는 누구인가 (who), 그리고 관리가 어떻게 되어야 할 것인가 (how)에 대한 이해가 있어야 한다.

1) 인터넷 거버넌스의 대상

위에서 언급된 인터넷 거버넌스의 정의에서는 거버넌스의 대상을 "인터넷의 발전 및 이용과 관련하여 공유하는 원칙, 규범, 규칙, 의사결정 절차, 그리고 프로그램"으로 명시하고 있지만 대체적으로 인터넷 거버넌스의 대상이 되는 내용은 세 부류로 나눌 수 있다. 우선 기본적인 접속을 가능하게 해 주는 물리적 인프라인 네트워크 망 및 접속 기술에 관한 표준들이 그 관리의 대상이 될 수 있고, 한정적 자원으로 누군가 관리해야 하는 논리 계층인 도메인 네임과 IP 주소 등이 그 관리의 대상이 될 수 있고, 이렇게 구성된 네트워크를 통해 전송되는 내용이 그 관리의 대상이 될 수 있다(그림 1). 인터넷은 기본적으로 어떤 국제적 합의에 의해서 라기 보다는 필요에 의해 자발적으로, 혹은 소수의 주도에 의해 발전되어온 역

12) ITU, "Tunis Agenda for the Information Society," WSIS-05/TUNIS/DOC/6(Rev. 1)-E http://www.itu.int/wsis/outcome/booklet.pdf

13) 이 정의는 34번 문단에 명시되어 있는데 이에 대한 영어 원문은 다음과 같다. "A working defi nition of Internet governance is the development and applicationby governments, the private sector and civil society, in their respective roles, of shared principles, = norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

사가 있기 때문에 인프라층, 논리층, 콘텐츠층의 발전에 있어서 각각 다른 거버넌스의 모델이 적용되어 왔다는 역사가 있다.

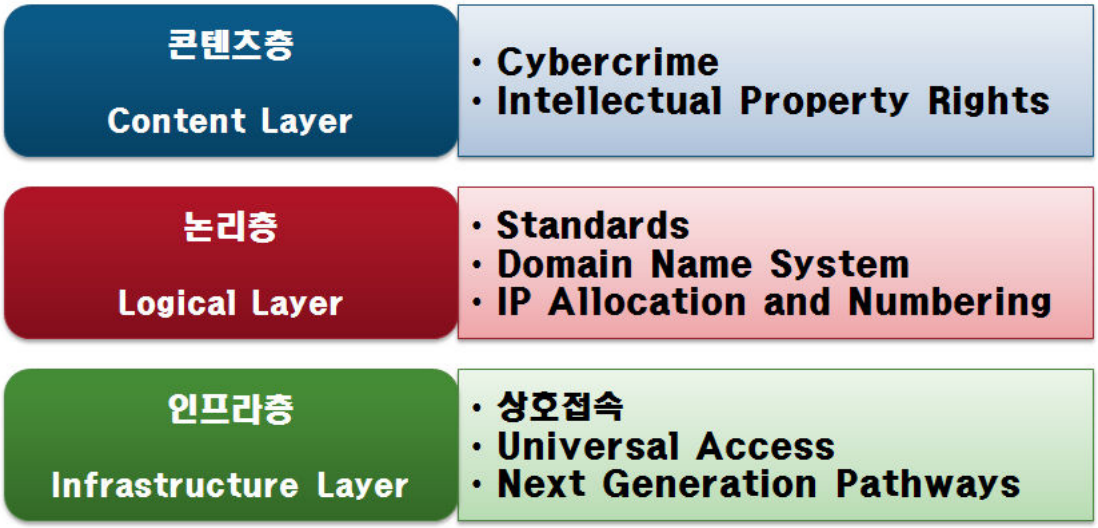

그림 1 인터넷 거버넌스의 대상

전화, 위성, 전파 등과 관련된 국제적인 통신기술은 기본적으로 ITU 내에서 각 국가간의 협의에 의해 관리되어 왔지만, 인터넷이 세계적인 네트워크로 발전하는 과정은 다양한 이해당사자들의 자발적인 참여가 주도해 왔기 때문에 인터넷은 국가간 협의가 없이 발전했다는 특징이 있다. 예를 들어 인터넷의 인프라층에 대한 표준은 기술발전을 주도하는 IETF (Internet Engineering Task Force)나 W3C(World Wide Web Consortium) 등의 커뮤니티에서 학계, 기술 개발자, 기업체, 정부인사 등의 자발적 협의를 통해 정해졌고, 채택에 대한 강제성이 없었음에도 중요한 이해당사자들의 협의였기 때문에 자연스럽게 채택되어 왔고, 이렇게 마련된 표준들이 인터넷의 표준으로 자리 잡아왔다.

인터넷망을 통해 통용되는 내용 부분에 대한 관리는 각 국가마다 다른 도덕적, 윤리적 및 법적 기준을 적용했기 때문에 대부분의 경우 국제적인 합의에 의한 관리의 필요성은 없었다. 내용과 관련해서 국제적인 협의가 필요했던 부분은 지적재산권에 대한 내용으로 이것은 기존의 지적재산권 문제를 관장했던 1994년의 지적재산권 협정 (Trade Related Aspects of Intellectual Property Rights, TRIPs)이나 세계지적재산권기구(World Intellectual Property Organization, WIPO)의 저작권 조약이나 실연 음반조약 등에 근거하여 각 국의 디지털 저작권법을 제정하고 서로간 조절함으로써 해결해 왔다.

하지만 인터넷 접속에 필수적인 도메인 네임이나 IP 주소는 기본적으로 미국 주도에 의해 개발되었기 때문에 미국 중심으로 관리되어 왔고, 이는 인터넷의 소통을 통제할 수 있는 막강한 권력을 의미하기 때문에 인터넷 이용이 세계적으로 증가함에 따라 중국, 러시아 등의 국가들이 통신규약을 관장하는 ITU를 중심으로 미국 중심의 체제에 지속적인 이의를 제기하게 되었고, 이에 따라 2000년대 중반부터 ITU 주도의 WSIS 개최 시부터 현재까지 특히 인터넷 주소체계와 인터넷 보안 분야에서의 인터넷 거버넌스의 주체에 대한 논란이 커지고 있다.

2) 인터넷 거버넌스의 주체

인터넷 발달 초기에는 인터넷 이용 주체들이 인터넷의 표준을 자발적으로 채택함에 따라 발전했기 때문에 인터넷 거버넌스의 개념이 크게 문제가 되지 않았지만 1990년대 말부터 인터넷 이용자가 확산되면서 유럽을 비롯해 중국, 러시아 등의 국가들이 미국 주도의 주소 체계에 대한 문제 제기를 시작하면서 인터넷 거버넌스에 대한 논의가 본격적으로 시작되었다. 인터넷 주소 체계를 주도적으로 개발하고 관장하고 있던 미국 정부에서는 주소 체계 관리의 정당성을 확보하기 위해 '거버넌스'의 개념을 적용시킨 ICANN이라는 조직을 1998년에 출범시켰고, 각 국의 정식 협정 없이 구성되었다는 약점을 지닌 이 조직이 전 세계 인터넷의 주요 자원인 인터넷의 주소체계를 관장하고 있는 것에 대한 정당성을 확보하기 위해 바람직한 인터넷 거버넌스의 모델을 지속적으로 추구해 왔다.[14]

하지만 ICANN의 가장 큰 약점은 거버넌스 모델이 기능적인 전문성에 따른 다양한 주체들을 중심으로 구성되었다는 것이었다.[15] 물론 지역적 다양성을 추구했기 때문에 구성 초기부터 각 대륙을 대표할 수 있는 인사들로 이사회를 조직하려는 노력을 기울였지만, 각 국가의 입장이 제대로 대변될 수 있는 체제가 없다는 비판을 수용하여 2004년에는 각 국가의 도메인을 관장하는 ccNSO(country code Names Supporting Organization)를 주요 보조기구(Supporting Organization, SO)의 하나로 격상시켰으며, 그 이후에는 정부자문위원회(Governmental Advisory Committee, GAC)의 의견을 점점 더 존중하는 형태로 국제적인 정당성 확대를 위한 노력을 기울였다. 즉, ICANN에서의 인터넷 주소 체계에 대한 거버넌스 모델은 초기에는 전문적인 이해당사자들이 주도하여 표준을 정했던 IETF나 W3C의 의사결정 모델을 추구했지만, 2005년에 튀니스 WSIS 의제 문건에서 인터넷 거버넌스에 대한 정의가 정해진 이후에는 특히 정부의 역할이 증대되는 멀티스테이크홀더(multistakeholder) 모델로 점차 그 운영 방향을 변화해 감에 따라 각 국가의 의견을 반영하려는 노력을 기울이고 있는 것이다. 이 정의는 2003년 제네바 WSIS에서 구성된 인터넷 거버넌스 워킹 그룹(WGIG)에 참여했던 다양한 인터넷 거버넌스 전문가들의 의견을 종합한 것으로, 그 이후 인터넷 거버넌스를 논하는 다양한 포럼에서 중요 개념으로 받아들여지고 있다.

위에서 언급된 인터넷 거버넌스의 정의에서는 인터넷 거버넌스의 주체를 "정부, 민간, 시민사회"의 세 부류로 나누고 있다. 최근에는 "이해당사자"들을 이렇게 단순화 하는 것에 대한 논란이 일고 있지만, 최근 인터넷 거버넌스 논의에서 크게 이슈가 되는 것은 각 국 정부의 참여와 시민사회의 참여 문제라는 점에서 일단 그 '주체'를 다음의 세 부류로 나누어 본다.(그림 2)

---

14) ICANN은 미국의 상무성과 ICANN간의 상호협약서에 의해 사단법인의 형태로 설립된 조직이다. Mueller, Milton L. 2002. Ruling the Root: Internet Governance and the Taming of Cyberspace. Cambridge: The MIT Press 참고.

15) 초기의 ICANN 조직을 보면 크게 기능에 따른 세 개의 주요 보조기구인 도메인 네임 보조기구 (Domain Name Supporting Organization; DNSO), IP 주소 보조기구 (Address Supporting Organization; ASO), 그리고 표준 보조기구 (Protocol Supporting Organization; PSO)로 구성되어 있는 것을 볼 수 있으며, 이외에 이사회에 대표를 보낼 수 있는 '이용자 (At Large)' 그룹이 있었고 정부자문기구는 결정 권한이 없는 자문 역할만 하도록 되어 있었다.

그림 2 인터넷 거버넌스의 주체

인터넷 거버넌스의 주체와 관련해서 가장 논란의 대상이 되는 것은 정부 주도의 거버넌스와 시민사회가 참여하는 거버넌스 모델간의 충돌이다. 인터넷 발전 이전의 국제 통신 관련 규약은 ITU와 같은 국제기구를 통한 국가 간의 협약에 의해 설정되었고, 이 모델은 국가 및 정부가 주도하는 거버넌스의 모델이었고 이에 대해 시민사회에서는 자신들의 의견이 제대로 반영되지 않고 있다는 불만을 제기해 왔다. 하지만 인터넷은 기본적으로 정부의 개입 없이 기술 개발 전문가들과 시민사회 전문가들 간의 협의 및 합의를 통해 발전되어 왔었기 때문에 ICANN의 초기 모델은 각 국의 정부가 '자문기구'에서 의견을 제시할 수 있을 뿐, 의사 결정을 하는 이사회에서는 정식 멤버가 아닌 구조로 되어 있었고 이에 대한 각 국의 불만을 수용하여 ICANN은 지속적으로 정부의 역할을 강화하는 방향으로의 멀티스테이크홀더 모델을 구축하려는 움직임을 보이고 있다.

반면에 인터넷 거버넌스 영역에 일정한 역할을 맡기를 원하는 ITU는 기본적으로 각 국가 간의 협약을 목적으로 하는 기구이기 때문에 최종 결정권은 각 국 정부의 대표가 가지고 있다. 민간 기업이 회원사로 참여하고 있기도 하고 ITU의 회의에서 시민사회의 의견을 듣기도 하지만 이들의 권한은 정부 대표의 권한에 자문 역할을 하는 것일 뿐이기 때문에 인터넷 거버넌스의 멀티스테이크홀더 모델을 제대로 반영하고 있지 못하다는 비판을 받았고 이에 따라 ITU에서도 2010년 이후 부터는 시민사회의 의견이 더욱 중요하게 반영될 수 있는 다양한 방법을 모색하고 있다.[16)]

이에 따라 바람직한 인터넷 거버넌스 모델은 위의 세 주체들이 서로의 역할에 따라 일정 정도의 균형적인 권한을 가지면서 협의를 하고 이를 통해 이해당사자들 간의 합의를 이끌어 내는 것이라는 의견이 힘을 얻어가고 있다. 하지만 거버넌스의 "이해당사자들"을 구체적으

16) 예를 들어, 2013년 5월에 열린 WTPF (World Telecommunication/ICT Policy Forum)에서 제안된 6개의 의견은 2012년 6월, 10월, 그리고 2013년 2월에 약 100여명의 전문가들이 참여한 회의를 통해 도출해 낸 의견들이었다는 점에서, 이전의 정부 위주의 의견 제시 모델에 비해 다양한 의견 청취를 하는 멀티스테이크홀더 모델의 특성을 지니고 있다고 볼 수 있다.

로 선정하려 할 때에 어떤 그룹이 포함되는지에 대한 구체적인 합의안이 없기 때문에 향후 거버넌스 모델을 수립해 나가는 과정에서는 어려움이 따를 것으로 예상된다.

3) 인터넷 거버넌스의 방법

인터넷 거버넌스에 관한 정의에서 거버넌스의 '방법'은 각 주체가 "맡은 역할을 통해 인터넷의 발전 및 이용과 관련하여 공유"하는 것으로 서술되어 있다. 즉, 각 주체가 맡은 역할이 있을 것이고 그 역할을 각자 하면서 서로가 공유할 수 있는 인터넷 발전 방향과 인터넷 이용 환경을 조성하는 것이라 할 수 있다. 서로가 공유할 수 있는 방안을 도출해 내는 방법으로는 서로 협의할 수 있는 시스템을 만들어서 당사자들 간의 의견을 교환하고 이를 바탕으로 각 주체들이 합의할 수 있는 결과를 도출해 내는 방법이다.

인터넷 거버넌스의 대상에서 언급 되었듯이 이제까지는 인터넷 거버넌스의 대상에 따라 관리 방법도 달랐다. 인터넷 관련 기술 표준의 경우에는 IETF나 W3C 등의 전문가들의 모임에서 특정 이슈에 관심 있는 전문가들이 자발적으로 모여 서로 치열한 토론을 통한 협의 끝에 기술 표준을 제안하는 합의문을 도출해 내는 방안으로 거버넌스가 진행되어 왔다.[17]

하지만 ICANN의 거버넌스 모델이나 ITU의 거버넌스 모델은 정부의 역할 또는 시민사회의 역할과 의견이 제대로 반영되지 못한다는 비판을 받아왔고 이 두 조직은 최근 이러한 비판에 대응하기 위한 다양한 노력을 기울이고 있다. ICANN에서는 정부의 역할을 증대시키고 더욱 국제화된 관리체계로의 변환을 도모하고 있고 ITU에서도 시민사회의 목소리를 더욱 많이 반영시키기 위한 여러 가지 노력을 기울이고 있다.[18]

위에서 언급된 인터넷 거버넌스의 멀티스테이크홀더 모델의 의의 및 발전 과정을 살펴보기 위해 WSIS, ICANN, 그리고 ITU를 통해 진행된 거버넌스 모델 정립 과정에 대한 논의를 간단히 정리해 본다.

3. WSIS에서의 멀티스테이크홀더 개념

ICANN의 설립과 함께 인터넷이 미국 주도의 관리체계로 변환이 됨에 따라 ITU에서는

---

17) IETF에서는 어떤 이슈에 대한 표준을 정할 때 우선 관심 있는 전문가들이 모이는 BoF(Boys of a Feather) 모임을 1~2회 개최한다. 여기서 여러 전문가들의 충분한 관심이 확인 되면 그 이슈에 관한 워킹그룹(WG)을 구성하게 되고 이 그룹 내에서 전문가들의 치열한 논쟁을 거쳐 그 이슈에 대한 가안(Internet Draft)을 만들어 발표하여 공개적으로 의견을 받은 후 이를 토대로 대부분의 인원이 동의할 수 있는 합의문이 RFC (Request for Comments) 형태로 발표된다. RFC의 채택 여부는 강제가 아니지만 주요 전문가들의 논의를 거친 합리적인 방안으로 간주되어 대부분 채택된다.

18) ITU에서는 WTPF 회의에서 활용했던 3차례의 전문가 회의뿐만 아니라 "강화된 협력 (enhanced cooperation)" 모델을 지향하는 새로운 형태의 거버넌스 모델을 논의하기 위해 UN의 개발을위한과학기술위원회(Commission on Science and Technology for Developmentl CSTD) 산하에 구성된 강화된 협력을 위한 워킹 그룹 (Working Group on Enhanced Cooperation)에서도 민간인 및 전문가들을 참여시키고 있다. "Final composition of the CSTD Working Group on Enhanced Cooperation" 28 March 2013 참조 http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=442&Sitemap_x0020_Taxonomy=Commission%20on%20Science%20and%20Technology%20for%20Development

통신 분야에 자신의 영향력을 증대시키기 위하여 인터넷 거버넌스 구조에서 일정한 역할을 담당하려는 노력을 지속적으로 기울여 왔다. 특히 중국이나 러시아 등 미국과 세계적 영향력을 놓고 경쟁하는 국가들의 경우, ITU를 적극적으로 활용하려는 움직임을 보이기도 했다.

ITU의 인터넷 거버넌스에 대한 관심은 1998년 전권 회의의 결과문에서 IP 분야의 중요성을 언급하기 시작한 이래(Resolution 101), 2002에 도메인 네임(Resolution 102)과 다국어도메인(Resolution 133)에 대한 조항을 추가함으로써 2002년 당시 ICANN의 조직 개편이 논의되던 시기에 ITU의 역할을 만들어 보려는 적극적인 노력을 기울였던 것에서 볼 수 있다.[19] 뿐만 아니라 2003년과 2004년에는 당시 ICANN에서 국가 도메인의 위상이 낮은 것에 대한 불만을 표현했던 ccTLD(country code Top Level Domain)들과 공동으로 ccTLD 문제와 관련된 워크샵을 2회 개최하기도 하였다.[20]

ITU의 이러한 노력들은 2003년 제네바와 2005년 튀니지에서 개최된 WSIS로 그 성과가 나타났고 여기서 인터넷의 발전 및 거버넌스와 관련된 다양한 논의가 전개되었다. 인터넷 거버넌스가 국제적인 이슈로 떠오르기 시작한 것은 2003년의 제네바 회의에서였는데, 이 때 가장 이슈가 되었던 것은 인터넷에 대한 관리의 주체로 "국제적(international) 협의체"를 포함시킬 것인가 하는 것이었다. 즉, 당시에 통신 관련 국가간 협약을 주도했던 "국가간(intergovernmental) 협의체"였던 ITU와 같은 조직의 권위만을 인정하려 했던 중국, 러시아 등의 의견에 대항하여 미국 및 서방 국가들은 좀 더 자율적으로 운영하는 것이 가능했던 "국제적 조직"인 ICANN을 포함시켜야 한다는 의견을 강력하게 피력했고 이에 대한 추가 논의를 위해 2003년 WSIS 이후에 WGIG(Working Grouop on Internet Governance)가 구성되어 1년 여의 논의 과정을 거쳤다.[21] 2005년의 WSIS 회의에 결과물을 제출하였고[22] 이 그룹에서 제안한 인터넷 거버넌스의 정의가 2005년 튀니지 WSIS 회의의 의제 문건의 일부로 채택되는 한편, 2003년의 문건에 등장했던 이해당사자(stakeholder)라는 용어가 WGIG 보고서에서 자연스럽게 이용되기 시작하였다.[23]

2005년의 WSIS 의제 문건에서는 미국의 강력한 의지 표명에 따라[24] "국제적 협의체"도

---

19) 2002년 4월, ITU-T의 의장인 Huolin Zhao가 ICANN이 겪고 있는 어려움을 해소하는데 ITU가 각 국 정부와의 관계 문제에 있어서 도움을 줄 수 있을 것이라는 의견서를 공개함. "ITU-T and ICANN Reform," http://www.itu.int/ITU-T/tsb-director/itut-icann/ICANNreform.html "In our opinion, it would not be easy either to replace ICANN with some other organization, or for ICANN to establish quickly the reporting and financial links with governments that Mr. Lynn has called for. Thus, we propose that ITU could provide support for ICANN and help it to overcome its current difficulties."

20) 2003년에는 각 국 정부와 ccTLD의 현황 점검 (http://www.itu.int/itudoc/itu-t/workshop/cctld/index.html), 2004년에는 ICANN 회의 직후 ICANN과 협력 (http://www.itu.int/dms_pub/itu-t/md/01/tsb/cir/T01-TSB-CIR-0234!!MSW-E.doc)

21) 이 때 WGIG에 제출된 거버넌스 관련 의견서의 사례로는 "A Framework Convention:An Institutional Option for Internet Governance: Concept Paper by the Internet Governance Project," (www.internetgovernance.org); Internet Governance Project (Mueller, Mathiason, McKnight), "Making Sense of 'Internet Governance': Defining Principles and Norms in a Policy Context," V 2.0, April 26, 2004 ()

22) deBossey, C., "Report of the Working Group on Internet Governance" June 2005, (www.wgig.org/docs/WGIGREPORT.pdf)

23) 멀티스테이크홀더 개념의 발전에 대한 설명은 Kummer, M, "Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation," Posted on 14 May 2013 (http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international) 참조

인터넷 거버넌스의 주체로 인정되었고 2005년의 WSIS 회의 이후에는 멀티스테이크홀더 모델이라는 개념이 널리 이용되기 시작하였다.[25]

결론적으로 2005년의 WSIS 회의에서는 미국 중심의 도메인 관리 체제에 대한 변화를 불러일으키는 것에는 실패를 했지만 미국 중심의 관리체제에 대한 비판의 목소리를 높이는 효과를 가져왔고, 이에 대한 논의를 하기 위해 ICANN이라는 논의의 장 외에, 인터넷거버넌스 포럼(Internet Governence Forum)이 매년 대규모로 개최되어 인터넷 거버넌스 관련 논의를 지속했을 뿐만 아니라 지역별 IGF 포럼이 만들어 지는 등 전 세계적으로 인터넷 거버넌스 관련 이슈에 대한 관심을 높이는데 기여하였다.[26]

WSIS의 결과로 구성된 멀티스테이크홀더 자문그룹(Multistakeholder Advisory Group, MAG)의 주관에 의해 개최되고 있는 IGF는 인터넷 거버넌스 이슈가 전 세계적 관심 이슈로 떠오르면서 매년 성공적으로 개최되고 있고, 2015년에는 WSIS 이후 10년을 평가하는 WSIS+10 회의가 계획되고 있지만[27], 이 회의를 통해서 어떤 정책이 수립되거나 국가 간의 협약이 이루어지지는 않기 때문에 ITU에서는 WSIS 이후 실질적인 정책 변화를 이끌 수 있는 국가간 협약기구인 ITU라는 장을 통한 변화를 모색하고 있고 특히 2014년의 ITU 전권회의가 주목을 받고 있다.

4. ICANN과 멀티스테이크 홀더 개념

1998년에 미국의 법인으로 설립되어 미국 상무성의 인가를 받은 ICANN은 인터넷 주소 관련 거버넌스의 문제를 관리하는 실질적인 주체로서의 역할을 해 오고 있다. ICANN은 설립 당시부터 비국가행위자들의 연합과 밑으로부터의 합의에 의해서 형성된 조직의 성격을 지닌 것으로 알려지기를 원했지만, 기본적으로 ICANN은 1990년대 말 설립 당시 도메인 네임 관리를 다른 비국가 행위자 세력에게 뺏기지 않기 위하여 미국이 선택한 민간 자율규제 조직이라 할 수 있다. 당시 IAHC(International Ad Hoc Committee) 세력으로 불리는 비국가 행위자들은 Internet Society를 중심으로 한 기술전문가 세력, 상표권(trademark) 세력 그리고 ITU를 위시한 정부간 기구들로 이루어져 있었으며 이들 나름의 자율규제안인 gTLD-MoU를 제시하고 있었다.[28] 미 정부는 무엇보다도 IAHC의 gTLD-MoU 안이 일국

---

24) 2005년 6월 30일, 미국의 NTIA에서는 DNS의 관리 권한을 포기할 의사가 없다는 것을 명확히 하였다. “The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS). Given the Internet's importance to the world's economy, it is essential that the underlying DNS of the Internet remain stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file.” http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system

25) ITU, “WSIS Outcome," Dec. 2005, (http://www.itu.int/wsis/outcome/booklet.pdf)

26) http://www.intgovforum.org/

27)http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/homepage/

28) 당시 기술전문가들을 대표하여 Internet Society(ISOC), Internet Assigned Numbers Authority(IANA), Internet Architecture Board(IAB), 상표권은 International Trademark Association(INTA)와 World Intellectual Property Organization(WIPO), 그리고 ITU와 미 정부기관인 Federal Networking Council(FNC)이 주된

일표를 원칙으로 하는 정부간 기구인 ITU에 의하여 주도되는 것을 원치 않았으며[29] 대신 미 정부 주도의 자율규제안을 담은 소위 Green Paper와 White Paper에 기초하여 ICANN이 탄생하게 된다. 초기 ICANN의 구조에는 시민사회의 요구를 수용하여 일반 네티즌을 대표하는 9명의 일반 이사(At Large directors)를 두는 등의 다양한 이해 집단의 요구를 수용하려는 노력이 보인다.[30]

하지만 인터넷의 중요성이 증대되면서 유럽을 비롯한 전 세계의 각 국가들이 미국 주도의 ICANN 체제에 반감을 갖게 되었고, 앞에서 언급했듯이 ITU의 인터넷 거버넌스에의 개입 노력이 가시화 되면서 2003년에 ICANN 조직의 개편이 이루어져서 ccTLD들이 하나의 주요 보조기구(ccNSO)로서의 위상을 갖게 되었을 뿐 아니라 정부 자문기구의 의견에 답변을 제공할 의무를 포함시킴으로써 각 국가들의 역할 증대 구조를 만들어 내었고, 이에 따라 서방 국가들로부터 ICANN 체제에 대한 동의를 이끌어내는데 성공한다.[31]

이와 더불어 ICANN에서는 2003년 WSIS 회의 결과문에서 언급된 “이해당사자들”(stakeholder)이라는 개념을 자신의 거버넌스 모델에 적용하기 시작하여 ICANN의 회의에서는 멀티스테이크홀더 개념이 주요 개념의 하나로 언급되기 시작하였고 ICANN에서는 자신의 조직 구조를 통해 멀티스테이크홀더 모델이 큰 문제없이 작동하고 있다는 것을 강조하였다.(그림 3)

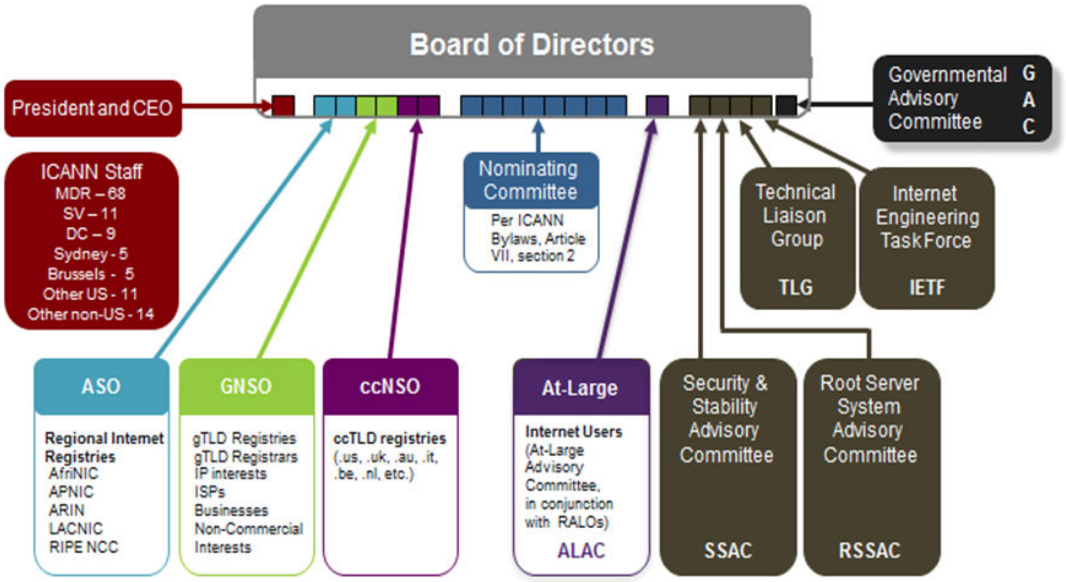

그림 3 ICANN의 멀티스테이크 홀더 모델 구성도

세력이었다. Mueller(2002) ch. 7 참고.

29) 당시 올브라이트(Madeline Albright) 국무장관은 gTLD-MoU 회의가 ITU 주관으로 제네바에서 열리는 것에 정식으로 항의하는 서한을 보내었으며 특히 ITU와 WIPO 등 국제기구들이 DNS를 관리하는 것에 대하여 문제를 제기한 바 있다. 또한 당시 미 정부의 안을 준비하고 있던 Interagency Working Group(IWG)도 국제기구, 특히 ITU의 역할을 반박하는 의견을 제시하였다. Mueller(2002), p. 157.

30) 그러나 일반 이사직은 초기 ICANN 구조에서 부분적으로만 실현되었으며 이후 ICANN 조직 개혁 과정에서 완전히 폐지되게 된다. 김의영(2002) 참고.

31) 김의영.이영음. (2008). "인터넷과 거버넌스: ICANN의 ccNSO 형성과정에서 ccTLD 세력의 역할을 중심으로." 『국제정치논총』, 48집 2호. 173-196쪽 참조.

<그림 3>의 ICANN 조직도에서 ICANN의 주요 정책을 최종 결정하는 이사회에는 다양한 "이해당사자" 그룹이 참여하고 있는데 우선 일반최상위 도메인 관리 관련 그룹(GNSO), 국가최상위 도메인 관련 관리그룹(ccNSO), 그리고 IP 주소 할당을 담당하는 각 지역의 RIR (Regional Internet Registries)로 구성된 주소보조기구(Address Supporting Organization; ASO)가 각각 2인씩 선정하는 6명의 이사, 지역 대표성 및 분야별 대표성을 담보하기 위해 각 계를 대표하는 추천위원회(Nominating Committee)가 선정하는 8 명의 이사, 그리고 일반 이용자를 대표하는 이사(At-Large) 등이 참여하게 되어있다. 기술이나 보안 관련 전문가와 정부 인사들은 이사회의 일원으로 참여할 수 있는 대표들을 보낼 수 있지만 최종 투표권한은 없는 구조이다. 하지만 2002년부터 ICANN에서는 특히 정부자문위원회(GAC)의 의견에 더욱 더 많은 신경을 쓰고 귀를 기울임으로써 글로벌 대표성을 증진시키기 위한 노력을 지속적으로 기울여 왔다.

뿐만 아니라 2012년부터 새로 부임한 ICANN의 사장인 파디 쉐하디(Fadi Chehadi)는 점점 더 글로벌화 되어가는 인터넷에 대한 정확한 인식을 바탕으로 ITU의 개입 노력에 대응하기 위한 다양한 정책을 도입하여 멀티스테이크홀더 모델을 가장 이상적으로 수행하는 조직으로 ICANN을 소개하고 있으며 이에 대해 대체적으로 긍정적인 평가를 받고 있다. ICANN은 현재 국제적인 인터넷 거버넌스 기구로서의 ICANN의 정당성을 높이기 위해 5개년 전략 수립을 위한 패널을 구성하였고[32], 해외에 ICANN의 주요 지부를 설립하는 등의 국제화 노력을 기울이고 있으며, 기업인, 시민사회, 그리고 특히 정부들과의 관계 개선을 위해 각 국의 정부들과의 접촉 기회를 넓히고 있다. 특히 브라질과 같이 정부 인사들이 인터넷 거버넌스 정책 결정 기구에 대거 참여하는 사례를 바람직한 사례로 소개하기도 하였고[33], 심지어 ITU의 2012년 12월의 WCIT 회의와[34] 2013년 5월의 WTPF 회의에도 참석하여 ICANN의 멀티스테이크 홀더 모델을 열심히 홍보하는 등의 노력을 기울이고 있다. 물론 인터넷 거버넌스에 대한 각 국가의 입장은 다양하고 또한 멀티스테이크홀더 개념도 다양하게 적용되고 있지만 ICANN의 멀티스테이크홀더 모델은 대체적으로 서방 세계의 지지를 얻고 있는 편이다.

ICANN의 거버넌스 모델이 가장 훌륭한 멀티스테이크홀더 모델로 항상 평가되는 것은 아니지만 적어도 ITU 중심의 모델 보다는 시민사회의 목소리를 더욱 많이 반영하고 있다는 평가를 받고 있는 것은 사실이다. 실제로 ICANN은 공모 등의 방법을 통해 다양한 이해관계 집단들이 의사결정 과정에 참여할 수 있는 기회를 열어놓고 있기도 하고 개인들이 자신들의 의견을 개진할 수 있는 "열린 의견란" 등의 다양한 체제를 마련해 놓고 있다.

5. ITU와 멀티스테이크 홀더 개념

ITU는 기본적으로 국가간의 협약에 의한 의사 결정을 하는 조직이다. 따라서 ITU에서 맺

32) ICANN, "ICANN Strategy Panels Launched," http://www.icann.org/en/news/announcements/announcement-15jul13-en.htm

33) 브라질은 cgi.br이라는 인터넷 거버넌스 기구를 통해 인터넷 정책 결정을 하는데 21명으로 구성된 이 기구의 구성원 중 9명이 정부의 각 부처의 인사들이다.

34) "Chehadé, Crocker Accept ITU Invitations to WCIT Opening Ceremony in Dubai, http://www.icann.org/en/news/announcements/announcement-28nov12-en.htm"

어진 협약은 국제법적인 지위까지도 지닐 수 있게 된다. 인터넷 발달 이전의 통신 관련 규약은 모두 ITU에서 관리하였으나 자발적 참여자에 의해 발달된 인터넷의 경우에는 ITU에 관리 권한이 주어질 수가 없었다. 따라서 1990년대 후반부터 ITU에서는 인터넷 관리에 일정한 역할을 갖기 위한 많은 노력을 기울여 왔고 WSIS를 통해 세계의 정상들을 모으는 것까지는 성공하였으나 그 회의를 통해 실질적인 변화를 이끌지 못하였기 때문에 그 이후 각 회원국들을 설득하기 위한 지속적인 노력을 기울여 왔다.

그 노력의 결실 중 하나가 2012년 12월 개최되었던 WCIT 회의이다. 이 회의에서는 이전의 전권회의의 결정사항 중 인터넷과 관련된 Resolution 101, 102, 133이 언급되었고 이러한 움직임에 서방 세계의 시민단체들이 심각한 우려를 표명하면서 많은 문제를 제기하였다. 기본적인 시민사회의 의견은 자발적으로 발달하여 큰 문제없이 운영되어 온 인터넷 관리 권한이 경직된 국가간 협약으로 넘어갈 경우 인터넷 발달을 저해할 우려가 있고, 특히 그러한 움직임을 주도하는 중국이나 러시아와 같은 비민주적인 국가들이 인터넷 장악을 시도할 우려가 있다는 의견을 표명하였다. ITU에서는 최종 권한이 공식적인 국가 대표에게만 있기 때문에 진정한 의미에서의 멀티스테이크홀더 모델이 불가능하다는 의견을 표명했던 시민사회들은, 물론 ICANN의 운영에도 많은 문제가 있지만 ITU 주도의 인터넷 거버넌스에는 적극 반대의사를 표명하였고, “ITU의 인터넷 장악” 가능성을 제기하면서 이에 대항하기 위해 WCITLeaks라는 사이트를 운영하여 정보를 교환하기도 하였다.[35]

2012년의 WCIT 회의에서의 중요한 화두는 멀티스테이크홀더와 국가 권력이 인터넷에 개입하는 문제였다. 이러한 문제는 특히 서방 세계의 시민사회뿐만 아니라 정부 인사들도 동조하여 “민주적인 절차”가 강조되는 멀티스테이크홀더의 모델과 “각 국가의 권리”가 강조되는 ITU 중심의 국제 관계 논리가 상충되었고, ITU에서 인터넷 통제 관련 논의가 이루어지는 것에 강한 반대를 표명한 미국 대표단의 입장에 동조하여 서방 세계의 국가들은 WCIT의 결론에 최종 서명을 하지 않은 바 있다. (<그림 4>)[36]

WCIT 회의는 ITU가 멀티스테이크홀더 개념의 중요성이 부각된 계기가 되었다는 비판을 받기도 한다. 특히 중국이나 러시아 등의 국가들이 논의를 중심적으로 이끌어가는 것에 대한 반감을 가진 미국이 지나치게 ‘국가의 개입’이라는 개념을 강조했기 때문에 실제보다 과장된 문제 제기가 이루어졌다고 보는 입장도 있다.[37] 뿐만 아니라 ITU 못지않게 ICANN에서도 미국이라는 국가의 권력이 지나치게 강하다는 비판적인 입장도 있다.[38]

---

35) http://wcitleaks.org/

36) World Socialist Web Site, "Global split over telecom treaty," http://www.wsws.org/en/articles/2012/12/28/wcit-d28.html; ITU, "Signatories of the Final Acts: 89" http://www.itu.int/osg/wcit-12/highlights/signatories.html

37) Milton Mueller, “ITU PHOBIA: WHY WCIT WAS DERAILED,” DECEMBER 18, 2012, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/; Milton Mueller, “How ARIN and U.S. Commerce Department were duped by the ITU,” 참조

38) 자세한 내용은 아르헨티나의 Enrique A. Chaparro가 쓴 3편의 WCIT 분석문 참조.
"WCIT and Its Relationship to the Internet," 27 December 2012, http://globalvoicesonline.org/2012/12/27/wcit-and-its-relationship-to-the-internet/
"WCIT and its Relationship to the Internet: Issues and Challenges," http://globalvoicesonline.org/2012/12/31/wcit-and-its-relationship-to-the-internet-issues-and-challenges/
"WCIT and its Relationship to the Internet: What Lies Ahead," 2 January 2013, http://globalvoicesonline.org/2013/01/02/wcit-and-its-relationship-to-the-internet-what-lies-ahead/

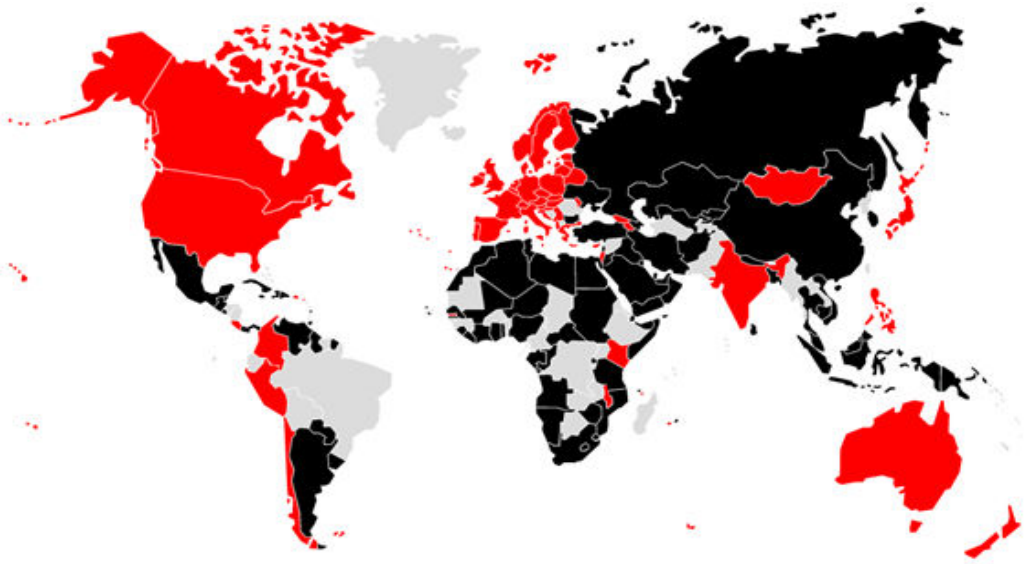

그림 4 WCIT 회의 서명국과 비서명국 비교 (검정: 서명국 빨강: 비서명국)

하지만 실질적으로 그 회의에 참석했던 시민사회 구성원들이 의사결정 과정에 참여할 수 없었음은 물론 자신들의 의견을 발표할 수 있는 기회조차 거의 없었다는 문제 제기를 하면서 인터넷 거버넌스의 문제에서는 각 이해당사자들의 입장이 제대로 반영될 수 있는 구조가 필요하다는 것을 ITU에게 뚜렷하게 인식시킬 수 있는 계기가 되기도 하였다. 따라서 야심차게 전 세계 국가들이 인터넷을 포함한 새로운 통신 관련 협의를 할 수 있는 기반을 마련하려던 ITU의 계획은 성사되지 않았다.[39]

하지만 WCIT의 회의는 ITU가 인터넷 거버넌스에 일정한 역할을 하고자 하는 다양한 노력의 하나이다. 이러한 노력은 2013년 5월의 WTPF 회의에서도 이루어졌는데, 이 회의에서 주목할 점은 제안된 안건들이 다양한 주체들이 1년 정도에 걸친 3번의 회의에서 논의하고 제안했던 내용들이 제시되었다는 것이다. 즉, 제시된 의견을 채택하는 최종 권한은 각 국가의 대표들에게 있었지만 의견 도출 과정에서는 시민사회와 일반 기업들을 비롯한 다양한 이해당사자들의 의견이 포함될 수 있었다는 것이다. 특히 제시된 의견 중 하나는 인터넷 거버넌스에 있어서의 멀티스테이크 홀더의 개념을 지지하는 것이라고 뚜렷하게 명시하였는데, 참석한 모든 국가들이 이 의견 채택에 동의를 함으로써 ITU 내에서도 인터넷 거버넌스를 논의할 수 있는 근거를 마련하기도 하였다.[40]

ITU는 2014년 10월 한국에서 개최되는 ITU 전권회의 이전에 이러한 여러 가지 노력을 통해 멀티스테이크홀더라는 개념에 대한 지지를 표명하면서 글로벌 인터넷 거버넌스에서 자신의 역할을 증대시키기 위한 노력을 지속적으로 기울이고 있다.

---

39) 인터넷 거버넌스 이슈에 대한 분석 사이트를 운영하고 있는 Kieren McCarthy는 2012년 12월 13일 "Internet humbles UN telecoms agency"라는 제목의 분석 기사에서 ITU가 WSIS에서 "창피스러운 실패(humiliating failure)"를 했고 ITU의 "심각한 명예실추"(severe embarrassment)가 있었다고 평했다. http://news.dot-nxt.com/2012/12/14/internet-humbles-un-telecoms-a

40) "Report by the Chairman of the 5th World Telecommunication Policy/ICT Forum" http://www.itu.int/md/S13-WTPF13-C-0016/en

6. 인터넷 거버넌스 모델의 미래

위에서 살펴보았듯이, 멀티스테이크홀더 모델은 인터넷 거버넌스의 기본 원칙을 구현할 수 있는 하나의 모델이다.[41] 현재 다양한 국가 및 국제단체들이 인터넷 거버넌스에 있어서 멀티스테이크홀더 모델의 중요성을 강조하고 있다. 하지만 ITU에서 생각하는 멀티스테이크홀더의 모델은 ICANN에서 현재 실시하고 있는 멀티스테이크홀더 모델과는 각 주체의 참여 정도에 있어서 상당한 차이가 있다.

이제까지는 인터넷 주소자원에 대한 실질적인 통제는 인터넷 도메인 정보의 근원을 제공하는 A 루트 서버의 권한을 지니고 있는 미국 정부가 하고 있었고, ICANN이라는 비정부조직을 통해 비교적 글로벌하고 민주적인 모습을 지닌 인터넷 거버넌스 모델이 대체적으로 인정을 받고 있었다. 하지만 2013년 5월 미국 정보기관의 불법 정보수집을 폭로했던 스노든 (Snowden) 사태가 일어남에 따라, 인터넷에 대한 미국 정부의 지나친 권력에 대해 서방국가들 조차도 강한 이의를 제기하기 시작하였고, 이에 따라 인터넷 거버넌스의 관리 체계에 대한 변화의 조짐이 보이고 있다.

바람직한 인터넷 거버넌스 모델을 구현하기 위한 방안으로 미국이라는 하나의 국가 주도의 모델이나 ITU라는 국가 주도의 국제기구 모두 그 폐해가 있다는 것이 드러난 시점이다. 하지만 인터넷의 발전에는 전문가들과 이해당사자들의 자발적인 참여가 있었다는 기본적인 논리에 근거한 인터넷 거버넌스 모델이 발전하는 것은 중요하다.

멀티스테이크홀더 모델이라는 개념도 문제가 없는 것은 아니다. 가장 큰 문제로 '이해당사자'를 어떻게 선정할 것인가 하는 것이 최근 큰 논란거리가 되고 있다. 뿐만 아니라 '참여'의 방법을 어떻게 정할 것인가 하는 것에 대한 의견도 다양하다. 즉, 논의에 참여하여 의견을 표현하는 것이 참여인지, 아니면 최종 결정 권한까지 주어지는 것이 참여인지에 대하여 합의된 의견이 아직 없는 실정이다.

이러한 이슈에 대한 논의는 앞으로 2014년 ITU 전권회의를 비롯해, 그 이전에 개최되는 브라질의 인터넷 거버넌스 관련 회의, 그리고 그 사이의 다양한 준비 회의에서 지속적으로 논의될 것이다.

인터넷 이용 환경이 변화함에 따라 인터넷 거버넌스에 대한 개념을 비롯해 인터넷 거버넌스의 방법 등에 변화가 있는 것은 당연한 이치이다. 하지만 이런 모든 논의에 있어서 관련 당사자들이 공유할 수 있는 원칙이 강조되는 인터넷 거버넌스의 근본정신이 강조되어야 할 것이다.

41) 인터넷 거버넌스 원리로 최근 유엔을 통해 강조되기 시작한 개념 하나는 '강화된 협력' (enhanced cooperation)이다.

ABSTRACT

The Multistakeholder Model of Internet Governance

Young-eum Lee[42)]

The multistakeholder model of Internet governance is based on the belief that the stakeholder groups should be able to agree on the rules and principles in governing the Internet space. The global expansion of the sweeping influence of the Internet has heightened the awareness of international governments on the importance of Internet governance, but since the Internet has developed mostly through voluntary participation by various groups, the organization with the greatest ability to manage the Internet space currently is ICANN(Internet Corporation for Assigned Names and Numbers), the U.S. based organization that manages the assignment of Internet domain names and IP addresses. Although ICANN has attempted to globalize its operation, governments in some nations are voicing dissatisfaction over the fact that the voice of the governments are not adequately represented within ICANN. This paper examines how the concept of multistakeholderissm has been used in WSIS(World Summit on Information Society), ICANN(Internet Corporation for Assigned Names and Numbers) and the ITU(International Telecommunication Union) as an important principle in emphasizing their roles in Internet governance.

42) Professor, Department of Media Arts and Sciences, Korea National Open University (KNOU), ICANN ccNSO council, Member of Internet Address Policy Review Board, Member of Korea Internet Governance Association

디지털 냉전론과 인터넷 거버넌스

김재연[43]

최근 미국의 외교가를 중심으로 디지털 냉전론이 대두되고 있다. 미국 정부, 기업이 현실 세계 및 사이버 공간에서 갖고 있는 권력과 지위를 감안했을 때 이러한 변화는 미국의 외교, 군사 정책상 변화로서 뿐 아니라 글로벌 인터넷의 운영, 인터넷 거버넌스의 행방에도 중요한 영향을 미칠 것으로 보인다. 이에 따라 본고는 디지털 냉전론이 발흥한 배경 및 이론적 타당성을 검증한다. 특별히 해당 논의에 따라 디지털 냉전에서 미국의 주요 경쟁 국가로 거론되는 중국의 인터넷 거버넌스 관련 정치적 역학 및 인터넷 거버넌스에 대해 취하는 태도에 대해 분석한다. 중국의 행동은 디지털 냉전론이 주장하는 것과 같은 수정주의적 국가로서 태도를 보이기보다는 자신들의 국내적 안정 유지를 획책하는 것에 가까우므로 디지털 냉전론은 이론적으로 타당하지 않으나 과거 냉전의 경험은 이들 강대국들의 경쟁 관계가 사이버 공간의 질서에 미칠 여파를 이해하는데 시사하는 바가 있다.

디지털 냉전 혹은 신(新)냉전론의 부상

2013년 현재, 외교평의회(Council on Foreign Relations, CFR), 브루킹스 연구소(Brookings Institute), 헤리티지 재단(Heritage Foundation)을 비롯한 다수의 미국 국제관계 관련 싱크탱크들은 보수, 진보의 이념적 스펙트럼을 초월해 사이버 안보(cyber security) 문제를 미국의 주요 국정 아젠다로 주목한다. 이들은 해외의, 특별히 중국의 해커들이 자국 정부, 기업 사이트뿐 아니라 전력망, 금융망과 같은 치명적인 국가 인프라(critical national infrastructure)를 그들의 공격 대상으로 삼고 있다고 주장하며 경계의 목소리를 높이고 있고, 미국 정부를 향해 개방적이고 자유로운 인터넷 환경 유지를 위해 사이버 안보를 미국 정부의 새로운 외교적, 군사적 목표로 삼아야 한다고 요구하고 있다.

또한, 비슷한 맥락에서 일명 '디지털 냉전'(digital Cold War) 혹은 '신냉전'(new Cold War)에 관한 논의 역시 미국 외교가에서 주목을 받고 있다. 일례로 오바마 행정부에서 국무부 정책기획실장을 역임한 바 있으며 현재는 뉴아메리카 재단(New America

43) 전세계 풀뿌리 언론가 네트워크인 Global Voices Online 활동가이며, 국제 인터넷 검열 비판 조직인 Global Voices Advocacy 회원이다. 본문과 관련하여 질문 사항 등이 있으면 jaeykim2@gmail.com을 통해 의사소통할 수 있다.

Foundation)의 회장이자 CEO를 맡고 있는 프린스턴 정치학과의 앤마리에 슬러터(Anne-Marie Slaughter) 교수는 2012년 8월 21일에 프로젝트 신디케이트(Project Syndicate)에 기고한 글에서 정보 전쟁의 서막을 예고한다. 그녀는 정보의 자유로운 흐름, 접근, 그리고 그와 관련된 인권의 해석을 둘러싸고 전 세계가 규범적, 현실적 입장을 달리하는 두 진영으로 나뉘고 있다고 주장한다. 특별히, 2010년 1월 당시 미국 국무부 장관이었던 힐러리 클린턴이 발표한 인터넷 자유 선언을 언급하며 미국이 정보와 접근에 관한 동등한 접근권과 국경으로 분열되지 않은 인터넷을 지지한다는 것을 강조한다. 이전에는 베를리 장벽이 동서를 나눴다면 이제는 정보 장벽이 미국이 속한 자유진영과 러시아, 시리아, 사우디아라비아 등과 같은 정보 통제 진영으로 나눈다는 것이 그녀의 주장의 골자다. 그리고 이런 시각에서 본다면 지난 2012년 12월에 두바이에서 개최된 국제전기통신세계회의(World Conference on International Telecommunication, WCIT, 이하 'WCIT-12')과 같은 회의는 이런 진영 간 의견차가 제도화되는 과정의 일부다.[44)]

물론, 이런 디지털 냉전론이 대두하는 배경에는 1980년대에 종결된 냉전 경험만 있는 건 아니다. 9.11 테러 사건 이후 미국 사회, 특별히 안보 측면에서 중심축인 테러리스트를 포함한 비국가조직(non-state actor)에 대한 위협론이 배후 변수로 작용한다. 일례로 네온 E. 퍼네타(Leon E. Panetta) 당시 미국 국방부 장관은 2012년 10월 11일 뉴욕시에서 행한 연설에서 미국의 사이버 인프라가 해외 국가뿐 아니라 테러리스트와 같은 비국가 조직(non-state actors)의 공격에 약점을 노출하고 있으며 과거 미국이 일본에 기습적으로 진주만을 습격당한 것과 같은 위험성이 미국의 사이버 인프라에 내재해 있다고 강조했다.[45)]

미국의 국력 및 미국 정부와 기업이 사이버 공간에 미치는 영향력을 감안할 때 이런 미국 사회 내에서의 신냉전론의 부상은 미국의 외교, 군사 정책상으로서 변화뿐 아니라 글로벌 인터넷의 운영, 인터넷 거버넌스 상에도 갖는 함의가 크다. 이에 따라 본고에서는 이러한 냉전론 발흥의 구체적 배경 및 이 냉전론 성립의 주요 전제가 되는 미국의 경쟁 국가로서의 중국의 성격을 분석하고 이런 분석 내용을 바탕으로 디지털 냉전론이 향후 인터넷 거버넌스 관련 논의에 시사하는 바를 설명한다.

강대국 간의 경쟁과 인터넷 거버넌스

디지털 냉전론이 주장하는 바인 미국 정부의 적극적 사이버 공간 개입은 얼핏 그간 우리가 이해해왔던 미국과는 다르게 느껴진다. 미국에 있어서 국가(state)란 국가가 독재하는 과거 동구권 국가나 국가가 시장을 통제하는 경향을 보여 온 동아시아 국가들에 비해 소극적으로 사회와 시장에 개입하는 것으로 인식돼왔기 때문이다. 또한, 미국은 헌법상 수정헌법 1조(First Amendment)를 통해 표현의 자유를 규정하고 있으며 오바마 행정부 내에서 우리로 따지면 외교부에 준하는 국무부(Department of State)가 주요 국정 목표로 인터넷 자유

44) Slaughter, A.-M. (2012). The Media Cold War by Anne-Marie Slaughter - Project Syndicate. Retrieved October 21, 2013, from http://www.project-syndicate.org/commentary/the-media-cold-war-by-anne-marie-slaughter

45) Panetta, L. E. (2012). Defense.gov News Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City. Retrieved October 21, 2013, from http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

를 제시하고 있다.[46] 그리고 미국은 국내외적으로 기업 이익 보호를 위해 정부 개입을 통한 인터넷 규제 신설에 대해 지속적으로 반대 입장을 취해왔기 때문에 인터넷에 대한 '적극적인 국가 개입'이란 미국의 기존의 입장과 상치되는 혹은 이질적인 주장으로 느껴질 수 있다.

그러나 이런 시각은 미국 국가는 '약한 국가'(weak state)라는 편견을 수용한 결과다.[47] 미국은 공화주의와 연방주의 전통에 따라 강압적이고, 수직적인 국가 구조(state structure)는 헌정 질서 아래에서 상대적으로 취약할 수 있다. 그러나 역사적인 맥락에서 볼 때 미국은 위기 대응을 명분으로 지속적으로 국가 능력(state capacity)을 강화해왔다. 건국 과정에서 영국과 대항하기 위해 연방정부를 신설했다. 루즈벨트 시절에는 대공항과 싸우기 위해 케인즈주의의 기치 아래 뉴딜국가(New Deal state)를 건설했고, 2차 대전에 참전하면서 급격히 미국의 군사화가 진행됐다. 현재 미국 정치계에서도 얼핏 국가 능력 강화에 대해 보수와 진보, 공화당과 민주당간 의견이 갈리는 것처럼 보이지만 깊이 들여다보면 실상은 다르다. 보수측은 지난 부시 행정부 이래 대(對)테러능력을 향상시키기 위해 행정부 권한 강화에 힘을 기울이고 있다. 진보측도 오바마 행정부 내에서 의료, 보건 영역 등에서 국가 활동 내용을 확장하는 데 초점을 맞추고 있다. 미국은 공화국으로서, 그리고 연방국가로서 중앙권력을 견제해온 전통을 갖고 있지만 그와 동시에 위기 대응을 위해 국가 능력을 꾸준히 강화해온 이력도 갖고 있다.

이런 미국 국가의 성격에 대한 좀 더 균형잡힌 시각은 미국의 인터넷 거버넌스에 관한 외교적 접근의 이해에 대해서도 현실적 분석을 가능하게 한다. 일례로 왜 미국은 인터넷 거버넌스의 현상 유지를 원하는 것일까?

미국이 WCIT-12를 위해 2012년 8월 최초 제출한 제안서의 핵심은 국제전기통신규약(International Telecommunication Regulations, ITR)이 관할하는 규제 영역의 현상 유지다. 구체적으로 해당 제안서는 ITR 전문(preamble) 변경의 최소화를 요구하고 있으며 '통신'(telecommunications)', '국제 통신 서비스'(international telecommunication service) 등 주요 용어의 의미가 확장돼 UN의 규제 권한에 인터넷이 포함되는 것을 우려한다. 그리하여 설사 규제 확장안이 통과된다 할지라도 그를 실행하는 것은 각국이 자발적으로 결정할 것을 주장한다. 명분상으로 이런 주장은 자국의 인터넷 자유 독트린에 따라 인터넷상 자유로운 정보의 흐름과 접근에 위해가 될 수 있는 과도한 국가 개입을 제지하기 위해서다.[48] 달리 말하면 미국이 지향하는 국가의 역할과 국가의 적극적 개입이 허용되는 새로운 인터넷 거버넌스 질서가 부합하지 않기 때문에 기존 질서의 유지를 지지한다는 것이다.

하지만 이미 과거 미국 역사에서 찾아볼 수 있듯 새로운 시대적 위기를 명분으로 한 미국의 국가 권한의 강화는 계속돼 왔다. 그리고 사이버 안보를 근거로 미국 국가의 사이버 공간에 대한 개입 정도를 확대하려는 시도는 이미 이루어지고 있다. 권력의 이기적 속성을 인

46) Clinton, H. R. (2010, January 21). Remarks on Internet Freedom. U.S. Department of State. Retrieved October 23, 2013, from http://www.state.gov/secretary/rm/2010/01/135519.htm

47) Novak, W. J. (2008). The Myth of the "Weak" American State. The American Historical Review, 113(3), 752-772. doi:10.1086/ahr.113.3.752

48) Kramer, T. (2012). Fast Facts on United States Submitting Initial Proposals to World Telecom Conference. U.S. Department of State. Retrieved October 21, 2013, from http://www.state.gov/e/eb/rls/fs/2012/195921.htm

정하면 그리고 국제 사회의 무정부 질서 아래에서 국가가 생존을 목표로 한다는 국제정치의 현실주의의 가정을 수용하면 현상유지를 획책하는 미국의 의도는 '국가의 개입 반대'을 토대로 한 이념에 기초했다고 판단하는 것만으로는 부족하다. 거기에서 나아가 미국이 이러한 입장 유지를 통해 '경쟁 국가'의 인터넷 거버넌스의 개입을 저지하여 어떻게 자신들의 국익을 추구하려 하는 지를 파악하는 것이 중요하다.

나아가 이러한 현실주의적 관점에서 미국 국가가 과거의 외교, 군사적 정책의 연장선상에서 인터넷 거버넌스를 어떻게 접근하고 있는 지를 이해하고자 한다면, 인터넷 자체는 새로운 기술이며, 인터넷 거버넌스 역시 전문가 집단, 시민사회 영역에서 발달해 온 사적 규제 네트워크의 속성을 갖고 있으나, 여전히 미국과 미국의 주요 경쟁국가 간의 관계가 주요 분석 대상으로 떠오르게 된다. 단적으로 국가가 기술적인 문제를 넘어서 안보를 포함한 광범위한 정책 영역에서 가장 강력한 경쟁 대상으로 여기는 건 국가, 특별히 자신들의 생존에 위협을 끼칠 수 있는 능력과 의도를 갖고 있는 국가이기 때문이다.

그렇다면, 디지털 냉전이 부각되는 현재 미국 외교가의 분위기를 감안할 때, 냉전 시대 소련에 이어 이러한 신냉전 시대 미국의 주적으로 부상하는 대상은 누구인가? 동시에 냉전과 함께 9.11 테러가 이러한 신냉전론의 배경 변수로 감안하는 것을 고려할 때, 어느 국가가 테러리스트의 온상으로 지적되고 있는가? 이런 점에서 러시아 등 다른 권위주의 국가와 함께 직간접적으로 미국의 사이버 공간상 주요 경쟁 국가로 손꼽히고 있는 것은 중국이다. 한 가지 예로 2010년 10월 미국 오바마 대통령이 중국을 방문하였을 때, 오바마는 인터넷을 통해 타운 홀(town hall) 미팅을 진행했고, 이 기회를 활용해 인터넷 자유를 홍보했다. 구체적으로 그는 정보 접근권이 향상됐을 때 시민들이 자신의 정부 책임성을 향상시킬 수 있고 새로운 아이디어를 창출할 수 있으며 창조성과 기업가 정신이 강화된다고 주장했다. 규범적인 측면에서 오바마의 이러한 인터넷 자유에 대한 주장이 얼마나 타당한 지는 차치하고, 이런 국빈 방문의 정치적 맥락을 생각할 때, 오바마의 발언은 미국의 인터넷 자유 독트린을 선포하고 중국을 인터넷 자유상 잠정적 위협 국가로 인지하고 있음을 보여준다.[49]

또한, 최근 미국 외교가의 주요 이슈 중 하나가 중국의 사이버 스파이 행위를 다룬 맨드리안트(Mandriant) 보고서였던 것도 주지할 만한 사실이다. 미국의 방위 컨설팅 업체 맨드리안트는 그들이 2013년 2월에 공개한 보고서에서 미국을 향한 지능형 지속 해킹(Advanced Persistent Threat, APT)의 출처가 중국 인민해방군 61398부대이며 2006년 이후 이들이 적어도 141개의 기관에서 테라바이트 단위의 데이터를 훔쳤고 이들이 과거 1,905회에 가깝게 행한 공격 중 97%가 국가의 중대한 기간 시설을 대상으로 했다고 주장한다. 또한, 맨드리안트는 이러한 부대가 중국이 운영하는 20개 부대 중 1개 부대일 뿐이라고 지목하면서 실제로 중국이 미국의 사이버 안보에 미치는 위협은 더 심각할 수 있음을 강조한다.[50]

그렇다면 왜 미국은 중국을 미국의 사이버 안보상 주요한 경쟁 국가로 주목하고 있는가? 그 이유는 무엇보다 중국의 고속 경제 성장과 동시에 존재하는 이념적 이질성 때문이다. 중

49) Clinton, H. R. (2010, January 21). Remarks on Internet Freedom. U.S. Department of State. Retrieved October 23, 2013, from http://www.state.gov/secretary/rm/2010/01/135519.htm

50) Mandiant Intelligence Center Report. (2012). Mandiant. Retrieved October 21, 2013, from http://intelreport.mandiant.com/

국은 1979년 개혁개방 이후 최근 금융위기 전까지 연평균 경제 성장률 10%에 가까운 경이적인 경제 성장을 기록해 왔다. 그리고 그와 동시에 지구상에 몇 안 되는 공산주의 이념을 채택한 국가로서 공산당에 의한 일당 독재 체제를 유지하고 있다. 이런 경제적 자유와 정치적 통제의 공존, 그리고 후기 미국 국제사회에서의 잠재적 초강대국으로서의 부상은 미국에게 심각한 부담으로 다가온다. 미국이 갖고 있는 자유 민주주의 이념과 민주주의를 확산하겠다는 외교 정책상 목표에 비춰보았을 때 중국은 위협적인 존재이기 때문이다. 미국의 입장에서 봤을 땐 중국의 정치체제 안정을 통한 점진적 시장개혁 모델인 베이징 콘센서스(Beijing Consensus)는 미국의 충격 요법을 통한 자유 시장, 자유 민주주의 확산 모델인 일명 워싱톤 콘센서스(Washington Consensus)의 안티테제이다.

나아가 중국의 과거 행적 역시 미국의 의심을 초래할 수 있는 부분이 있다. 미국은 그간 정보 자유권, 접근권과 같은 인권을 명분으로 기존의 인터넷표준화기구(Internet Engineering Task Force, IETF), 인터넷주소관리기구(Internet Corporation for Assigned Names and Numbers) 등의 국제기구를 통한 일명 '다자간 협력주의'(multi-stakeholderlism)에 따른 현상유지적 운영 방식을 옹호해왔다. 이는 현실주의적 관점에서 봤을 때 IETF, ICANN 등의 기구들이 기업, 전문가 집단, 그리고 일부 시민사회의 참여를 통해 다자간 협력방식을 취하고 있으나 이들이 또한 미국이 현재 사이버 공간에서 갖고 있는 우월한 지위에 대해 특별히 위협적이지도 않기 때문이다.

하지만 중국을 비롯한 권위주의 국가, 아시아, 아프리카 등지의 신흥국가는 이런 기존 질서에 만족하지 않았다. 중국은 2011년 러시아, 타자흐스탄, 그리고 우즈베키스탄과 함께 UN 총회에서 다자간 협력주의나 시민사회의 역할에 대한 논의를 배제한 '정보 안보를 위한 국제 행위 규약'(International Code of Conduct for Information Security)을 제출한 바 있다.[51] 특기할만한 점은 이 문서에서 중국 등의 국가가 공식적으로 정보통신기술의 발달이 국제안정과 국가안보에 위해가 될 수 있다고 주장함과 동시에 이를 방지하기 위해 국가간 공조가 필요함을 제시하고, 나아가 인터넷 관련 정책영역은 국가의 주권(the sovereign right of the States)임을 명시하고 있다는 점이다. 또한, 같은 문서는 양자간, 지역간, 국제적 공조를 이끌기 위해서 UN의 역할이 강화돼 국제 규범의 창설, 국제 분쟁의 해결, 정보안보 영역의 국제 협력의 증대가 필요하다고 역설하고 있다. 이런 맥락에서 보면 미국이 WCIT-12에서 UN의 인터넷 규제 권한 확대에 대해 민감하게 반응한 것은 이러한 변화가 중국 등 권위주의 국가, 신흥 국가 중심으로 새로운 인터넷 거버넌스 질서를 형성하고자 하는 노력의 일부로 보고 이를 저지하기 위함이다.

그리고 이런 추세는 쉽게 바뀔 것처럼 보이지도 않는다. 2013년 시진핑(習近平) 정부 출범 이래 중국은 본격적으로 강대국 외교를 표방하고 있다. 이 맥락에서 사이버 안보를 외교의 주요 아젠다로 설정했으며 이전의 저자세 수비 위주 외교에서 좀 더 공격적 외교로 전환될 것이 예상되고 이에 대한 미국의 반응 역시 더욱 강해질 것으로 보인다. 특별히 같은 해, 미국의 국가안보국(National Security Agency, NSA)의 자국 인터넷 기업의 서비스를 통한 불법 개인 정보 수집 논란이 불거진 후, 밖으로는 인터넷 자유를 주장하면서 안으로는 자국의 국가 이익 증대를 추구하는 미국의 이중적 태도에 대한 중국의 의심 역시 한층 더

51) International Code of Conduct for Information Security. (2011, September 14). United Natiions General Assembly. Retrieved from http://www.citizenlab.org/cybernorms/letter.pdf

가중됐고, 유럽 등 다른 국가들의 불만을 이용해 인터넷 거버넌스와 관련된 의제를 놓고 미국과 충돌할 가능성, 인터넷 거버넌스의 국제정치화 역시 가속될 것으로 여겨진다.[52]

그러나 인터넷 거버넌스상 강대국 간의 경쟁관계의 존재 자체가 디지털 냉전론의 이론적 타당성을 입증하지 않는다. 디지털 냉전론이 성립하기 위해서는 그 핵심 가정인 중국이 기존 체제를 전복하고자 하는 수정주의적 국가(revisionist state)임이 성립되어야 한다. 과거 소련이 공산주의의 전 세계적 확대를 노렸던 것처럼 중국이 자신들의 인터넷 거버넌스 모델로 기존의 인터넷 거버넌스 모델을 대체하고자 노력할 것인가? 이 질문에 대답하고, 중국 부상론이 인터넷 거버넌스상에서 어떻게 해석될 수 있는 지를 검증하기 위해 아래에서는 1) 중국이 사이버 공간에서 국가 주권에 대해 어떠한 해석을 내리고 있으며, 2) 실제 중국의 인터넷 검열, 통제 사례를 놓고 보았을 때 중국이 이러한 주권 해석을 정보 통제 정당화에 어떻게 사용하고 있는 지, 3) 나아가 이런 주권해석, 정보통제에 기초했을 때 그들의 인터넷 거버넌스에 대한 접근법은 어떠한 지를 살펴보고자 한다.

중국식 인터넷의 실체: 네트워크 권위주의와 취약한 강대국

1989년 천안문 사태 직후인 1990년대만 해도 중국의 인터넷 발전을 바라보는 시각의 초점은 꺼진 민주화의 불씨를 다시 살리는 데 있어 인터넷의 역할이었다. 최근 아랍의 봄 이후 다시 각광을 받고 있는 이런 인터넷 민주화론의 전제는 MIT 미디어랩 소장을 역임한 바 있는 니콜라스 네그로폰테(Nicholas Negroponte) 등 사이버 이상주의자들이 주장한 초국가적 인터넷은 물리적 영토에 기초한 국가 주권이 통제할 수가 없다는 '믿음'이었다.[53] 그로부터 20년 가까운 시간이 흘렀고 중국이 중국식 자본주의(capitalism with Chinese characteristics)[54]뿐 아니라 통제를 통한 발전이란 중국식 인터넷(the Internet with Chinese characteristics)에 대해서도 어느 정도 성공을 거둔 것이 가시화됐다. 그리고 그런 흐름에 따라 현재의 중국 인터넷에 대한 실증적 연구의 초점은 이런 인터넷의 급속한 발전과 공존하는 체제 안전성에 대한, 중국의 인터넷 통제 메커니즘에 대한 이해로 옮겨가고 있다.

그렇다면 중국의 인터넷 통제는 무엇이 특별한가? 먼저, 국가가 인터넷을 통제한다는 '사실' 자체는 그렇게 특별한 사실이 못 된다. 중국뿐 아니라 미국을 포함한 다른 고도 산업화가 이뤄진 민주국가(advanced industrial democracies)에서도 산업 발달, 시장 규제, 사회 보호 등을 명분으로 국가가 사이버 공간을 일부 통제하는 행위는 일반화됐다. 문제는 통제가 아니라 '어느 정도 수준'의 통제가 '어느 정도의 범위'로 행해지는 것이 통용되는 지, 그리고 그것이 해당 국가의 정치적 정당성(political legitimacy)과 경제적 효율성(economic efficiency)에 어떠한 영향을 미치는 가이다.[55] 그리고 이 점에서 중국이 다른 국가에 비해

52) Gupta, P. (2013, June 8). Barack Obama and Xi Jinping discuss cybersecurity as tension over privacy increases in U.S. - Salon.com. Salon. Retrieved October 23, 2013, from http://www.salon.com/2013/06/08/barack_obama_and_xi_jinping_discuss_cybersecurity_as_tension_over_privacy_increases_in_u_s/

53) Negroponte, N. (1996). Being digital. New York: Vintage Books.

54) Huang, Y. (2008). Capitalism with Chinese characteristics: entrepreneurship and the state. Cambridge ; New York: Cambridge University Press.

55) Goldsmith, J. L., & Wu, T. (2008). Who controls the Internet?: illusions of a borderless world. New

특이점을 갖고 있다고 한다면, 그것은 중국의 인터넷 통제가 그들의 4억 인터넷 인구를 대상으로 인터넷 통제 역사상, 기실 정보 통제 역사상 가장 광범한 규모로 이루어지고 있다는 점이다.

구체적으로 트위터, 페이스북 등 일부 사이트에 집중된 미국과 달리 중국은 다양한 사이트에 트래픽이 나뉘어져 있는데 정부 가이드라인에 따라 이런 사이트들 대부분이 자발적으로 인터넷 검열을 행하고 있다. 이런 사이트들은 최대 1,000명에 달하는 모니터링 요원을 동원하고 있고, 2만 명에서 5만 명에 달하는 인터넷 경찰(網絡警察)이 활동하고 있다. 그리고 25만에서 30만 명으로 추정되는 친(親)정부 인터넷 평론원들(五毛黨)이 존재하여 반(反)정부여론에 맞서 정부에 우호적인 온라인 여론을 주도한다.[56]

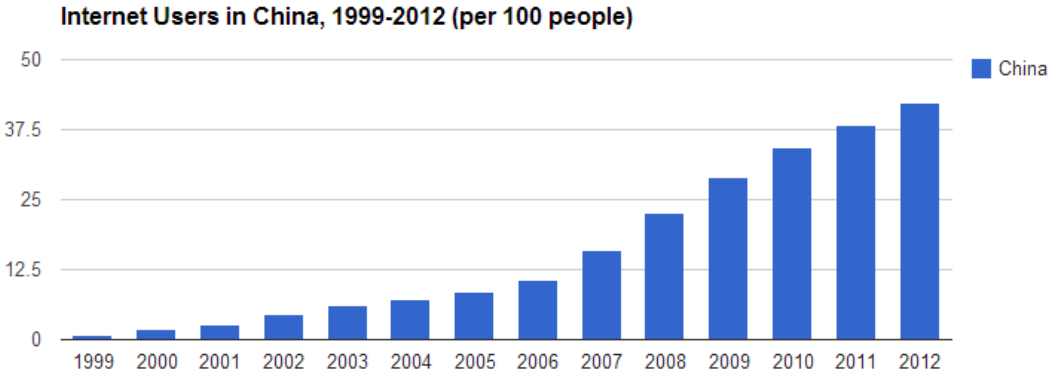

그림 5 중국의 인터넷 인구 성장, 출처: World Bank (2012)

나아가 더욱 주목할 만한 부분은 중국의 이런 인터넷 통제 시스템이 위의 <그림 5>에서 보듯 중국 인터넷 인구가 폭발적으로 성장해 왔음에도 불구하고 건재해 왔다는 부분이다. 일례로 2012년에 중국의 인터넷 이용자는 전체 인구의 37.5%, 약 4억 3천만을 넘어섰다. 어떻게 급증하는 인터넷 인구와 그에 따른 인터넷 트래픽의 증가에도 이런 통제 시스템이 유지될 수가 있는가?

중국의 인터넷 검열 시스템의 안정성(resilience)의 열쇠는 균형이다. 하버드 정치학과의 게리 킹(Gary King) 교수팀이 중국의 300개 이상의 소셜 미디어의 검열 데이터를 전수 조사하고, 계량 분석해 2013년에 발표한 논문에 따르면 이런 중국의 인터넷 통제 원칙은 '개인의 표현의 자유는 허용하되 집단적 행동은 차단한다'이다. 개인이 정부를 비방하는 내용 등을 일부 허용할 경우 정부에 대한 비판적 여론이 형성될 수 있으나 선거를 통해 공직자가 선출되지 않는 중국의 정치체제상 그러한 부정적 여론이 체제 유지에 본질적 위협이 되지 않는다. 또한, 중국 공산당은 이런 제한된 자유를 통해서 반대 여론이 지나치게 강해지는 것을 억지할 수 있으며 시민들의 불만이 표현을 통해 일부 해소돼 적극적 행동으로 나서지 않게 된다는 걸 인지하고 있다. 이는 반대로 중국 정부가 개인들이 온라인을 통해 조직화하

York: Oxford University Press.

56) King, G., Pan, J., & Roberts, M. E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. American Political Science Review, 107(02), 326-343. doi:10.1017/S0003055413000014

여 지난 2012년의 아랍 민주화 운동에서처럼 인터넷에 기반해 집단행동을 개시하는 것은 용인하지 않는다는 걸 뜻한다.

즉, 중국의 인터넷 통제는 북한처럼 인터넷 접근을 체제 안정을 위해 애초에 전면적으로 차단하는 극단주의와는 차별성이 있다. 같은 체제 안정을 목적으로 하지만 경제 발달에 기초해 정치적 정당성을 얻고 있는 그들의 경우, 개인의 표현의 자유는 일부 허용하되 집단행동의 가능성에 대해서는 적극적 제지를 가하는 방식으로 균형을 유지해 인터넷 검열 시스템의 안정성을 유지하고 있다. 그런 점에서 중국은 CNN 베이징 지국장 출신 인터넷 정책 전문가 레베카 매키넌(Rebecca MacKinnon)이 지적한 것처럼 중국은 중국식 인터넷, 네트워크 권위주의(networked authoritarianism)을 표방한다.[57] 이러한 권위주의 국가의 인터넷 통제의 변이성(variation)은 인터넷 검열 제도가 왜 중국뿐 아니라 대다수의 국가에서 유지되고 발전될 수 있을 지를 이해하는 데 핵심적이다.

동시에 이런 중국 내부의 미묘한 정치적 역학은 중국의 인터넷 거버넌스에 대한 입장에도 영향을 미친다. 중국은 글로벌 네트워크인 인터넷을 수용했지만 체제 안정을 통한 경제 발달을 지속하기 위해 인터넷에 대해 국경의 구분에 기반한 자신의 전통적 주권을 행사하기를 원한다. 중국의 검열 만리장성(The Great Firewall)은 이러한 주권 행사를 침해할 수 있는 요소에 대해서 자국을 보호하기 위함이며 중국은 이러한 입장을 국가의 정당한 권리 행사로 정의한다. 일례로 중국이 2010년에 발표한 백서에 따르면 중국 정부는 인터넷을 중국의 중요 인프라로 간주하고 있으며 인터넷이 중국 국경 안에 있는 한은 중국의 주권이 적용된다고 밝히고 있다. 그리고 그에 따라 중국의 인터넷 주권(the Internet sovereignty of China)은 국제 사회에서 반드시 존중되고 보호되어야 하고 중국 국경 안에 있는 한 중국인이든 외국인이든 자신들의 개인의 자유에 따라 인터넷을 사용할 권리는 있으나 그 권리의 경계는 중국 법과 규제이며 중국의 인터넷 안보를 위협하지 않는 선에서 이뤄져야 한다는 점을 강조한다.

이러한 중국의 체제 안정성에 대한 불안에 따른, 국경에 기반을 둔 국가 주권 개념에 대한 지지는 국가 중심 인터넷 거버넌스 질서에 대한 선호로 연결된다. 그들의 시각에서 볼 때 기존의 ICANN 등의 민간 기구를 통해 이뤄지는 인터넷 거버넌스는 자신들이 받아들이기엔 지나치게 초국가적이고 지나치게 자본주의적이다. 이에 반대해 중국은 좀 더 '민주적인' 인터넷 거버넌스를 지지하는데, 시라큐스 대학의 인터넷 거버넌스 전문가인 밀턴 뮬러 교수(Milton L. Muller) 교수에 따르면 여기서 중국이 '민주적' 인터넷 거버넌스라 말할 때 이 '민주주의'는 개인의 권리가 아니라 국가간의 평등한 관계에 더 가깝다. 예를 들어 중국이 UN이 국제 인터넷 행정에 전적인 권한을 행사해야 하고, 인터넷 행정 조직에 대해서 '민주적' 절차를 도입해야 한다고 주장할 때, 이 '민주주의'는 시민 차원의 권리가 아니라, 국가 차원의 평등 원칙이다.[58]

---

57) MacKinnon, R. (2010, October 11). Networked Authoritarianismin China and Beyond: Implications for global Internet freedom. Presented at the Liberation Technology in Authoritarian Regimes, sponsored by the Hoover Institution & the Center on Democracy, Development and the Rule of Law (CDDRL), Stanford University.

58) Mueller, M. L. China and Global Internet Governance: A Tiger by the Tail. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds.) Access Contested: Security, Identity and Resistance in Asian Cyberspace. Cambridge, Mass: MIT Press (2011). pp. 180-181.

인터넷 거버넌스와 관련해 중국과 미국이 갖는 입장의 중대한 차이점은 수직적 관계 측면에서 국가 통제의 개입 여부에 대한 찬성과 반대에 있지 않다. 이에 대해서는 실제 행동의 측면에서 보면 양 국가 모두 '개입'으로 나타나고 있다. 그보다는 이러한 개입의 범위와 수준을 정하는 문제가 어떻게 정해지느냐가 중국과 미국 사이의 국내적 인터넷 거버넌스 질서에 대한 본질적 차이를 드러낸다. 예를 들어 중국식 인터넷의 경우에는 국가 이외의 행위자가 '게임의 법칙'으로서 제도에 적극적으로 간여할 수 있는 권리가 인정되지 않는다. 즉, 두 국가 사이에 존재하는 차이는 수직적보다는 수평적 관계 측면에서 국가 외 이용자 네트워크와 같은 시민사회 영역의 새로운 행위자들이 수용되는 정도의 차이, 그리고 그 차이가 만들어내는 그들 간의 인터넷 거버넌스에 대한 선호(preference)의 차이다. 중국의 내부 정치체제와 인터넷 검열 시스템 역학은 수직적 권위와 통제에 의존하는 국가 공조 중심 인터넷 거버넌스에 대한 선호를 이끌고 있다. 최근 중국이 그들의 국제 안보 협력 기구인 상하이 협력 조직(上海協力機構) 프레임워크에 따라 중국-러시아간 정보 안보 협력 체계를 구축하고 비슷한 방식으로 영국, 미국, 프랑스, 일본, 한국, 파키스탄 등과의 정보 안보 협력 관계를 확장해나가는 것도 이런 그들의 선호도를 잘 보여준다.[59]

그러나 이러한 중국의 네트워크 권위주의적 입장이 기존 인터넷 거버넌스 질서를 전복하는 수정주의적 국가 형태로 발현될 것이라는 주장에는 다소 무리한 감이 있다. 밀러 교수는 그의 중국의 인터넷 거버넌스 관련된 논문의 결론부에서 매키넌이 제안한 '네트워크 권위주의'가 중국식 인터넷을 설명하기에 가장 적절한 표현인 지에 대해서는 동의하지 않는다고 밝혔다. 그 이유는 개방과 통제가 지속적으로 반복되고, 교차되는 중국식 인터넷의 역학을 설명하기에는 '네트워크 권위주의'는 너무 정적인 개념이고, 수평적 네트워크와 수직적 권위주의가 '상호 모순'되는 개념이기 때문이다.[60] 하지만 이러한 '상호 모순'이야말로 중국정치 권위자인 수잔 셔크(Susan Shirk) 교수가 명명한 취약한 강대국(fragile superpower)으로서 중국의 자화상을 인식하는 데 적절한 시각일 수도 있다. 셔크 교수에 따르면 천안문 사태 이후 중국 정부는 자국의 시민들이 집단적으로 항거할 수 있는 잠재력을 경계하고 있다. 그리고 이런 중국 정부의 불안감이 중국이 자국 시민들의 민족주의를 자극해 정부에 대한 비판의 화살을 외국으로 돌리려는 행동으로도 나타난다고 주장한다. 즉, 서구에서는 이러한 중국의 공격적 외교 행태가 중국의 새로운 패권 도전 국가의 증거로 여겨지지만 정작 중국 내부에서는 이런 공격성 자체가 그들의 취약한 내부적 정치 구조를 입증하는 증거로 받아들여진다.[61]

외부에서 중국 인터넷을 볼 때는 중국의 인터넷 검열 시스템의 안정성, 지속성이 더 깊은 인상을 줄 수 있으나 중국인들 자신은 상대적으로 자신들의 정보 안보 '취약성'을 더 강조한다. 중국의 공공 그리고 민간 영역 리더들은 중국의 컴퓨터와 웹사이트에 대한 공격이 매해 80% 이상 증가하고 있으며 대략 계산했을 때도 중국이 전 세계에서 가장 많은 사이

59) Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway. (2010). East West Institute.

60) Mueller, M. L. China and Global Internet Governance: A Tiger by the Tail. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds.) Access Contested: Security, Identity and Resistance in Asian Cyberspace. Cambridge, Mass: MIT Press (2011). p.191.

61) Shirk, S. L. (2008). China: fragile superpower : [how China's internal politics could derail its peaceful rise]. New York; Oxford: Oxford University Press.

버 공격을 받고 있다고 주장한다. 실제로 2011년 12월에 12개 이상의 중국 유명 온라인 쇼핑몰, 마이크로 블로그, SNS, 게임 사이트가 해킹을 당했으며 1억 명 이상의 중국 인터넷 이용자의 이름, 비밀번호, 이메일이 유출됐다. 또한, 지적재산권이 정착하지 않은 중국에서는 대부분 컴퓨터의 보안 관련 업데이트가 취약해 1천만 대 이상의 컴퓨터가 사이버 범죄에 사용되는 봇넷(botnet)과 연관된 것으로 알려져 있다.[62]

미국은 중국의 '패권국가'(superpower)로서의 지위 강화에 신경을 기울이고 있지만, 중국이 상대적으로 더 신경을 쓰고 있는 건 자국의 '취약성'(fragility)이다. 그리고 이런 관점에서 보면 중국이 수직적 인터넷 거버넌스 질서를 찬성하는 까닭이 기존 질서를 대체하려는 야심이라 보는 건 무리한 해석일 수 있다. 그보다는 중국이 수평적 측면이 강조되는 기존의 인터넷 거버넌스 질서가 자국 내의 정치적 제도에 침투해 들어왔을 경우 이에 저항할 수 있는 근거와 기제를 마련하기 위해 현재와 같은 인터넷 거버넌스 전략을 진행하고 있다고 보는 것이 더 적절하다. 중국은 인터넷 거버넌스에서도 역시 취약한 강대국이다.

디지털 냉전론의 한계와 시사점

사이버 공간, 인터넷 거버넌스상에서 강대국 간의 경쟁 관계를 냉전의 연장선에서 취급하는 데는 한계가 있다. 미국의 일부 학계, 정치권에서 인식하고 있는 바와 달리 주적으로 간주되는 중국의 인터넷 거버넌스상 국가 행위는 내부 정치 역학에 기인한 바가 많으며, 따라서 그들이 체제 전복을 꿈꾸는 수정주의적 국가로 보기에는 한계가 있기 때문이다. 과거 소련은 전 세계 공산화의 야심이 있었다. 그러나 중국의 야심은 적어도 현재까지는 중국의 국가 주권 기반 인터넷 거버넌스를 존중받고 보호하는 것에 더 가깝다. 이런 중국의 입장에서 본다면 수정주의적 국가는 자신보다 자신들의 체제에 위협적인 미국이 더 가까울 것이며 미국이 자신의 이념적 입장을 강조하면 강조할수록 중국은 더 공격적인 자세로 나올 가능성이 크다. 이는 달리 말하면 디지털 냉전론 자체는 이론적인 타당성을 입증하기 어려우나 이런 논의가 지속된다면 이것이 사이버 군비 경쟁을 통해 자기예언적 효과(self-fulfilling prophecy)를 가질 수 있다는 걸 뜻한다.

그리고 이와 같은 관점에서 이러한 강대국 간의 사이버 공간상 경쟁이 과거 소련과 미국 간의 양극 체계를 답습하진 않으나 냉전이 야기했던 것과 유사한 국내외적 효과를 일으킬 수 있다. 대표적으로 과거 냉전 시기 두 초강대국 간의 군사적 긴장 관계는 군산복합체(military-industry complex) 발달과 언론 통제 등 기본권 침해로 나타난 바 있다. 마찬가지 맥락에서 디지털 냉전론을 통한 냉전 이데올로기의 부활은 이번 PRISM 사건에서 보듯 미국의 인터넷, 통신 기업과 정부간 유착을 정당화하고, 정보통신 인프라에 대한 정부의 통제, 검열, 도청 등의 문제를 야기할 가능성이 크다. 이미 냉전적 사고에 따라 미국은 자국의 통신, 인터넷 인프라의 보안 강화를 위해 미국의 국토안보부(Department of Home Land Security)의 관련 권한을 확대했다. 즉, 디지털 냉전 자체는 성립하지 않더라도, 냉전론의 수용만으로도 새로운 정치적 변화가 나타날 수 있다.[63] 새로운 아이디어의 수용은 새로운

62) Lieberthal, K. & Singer, P. W. (February 2012). Cyber Security and U.S.-China Relations. John L. Thorton Center at Brookings. pp.4-5.

63) Ignatius, D. (2010). Cold War Feeling on Cybersecurity | RealClearPolitics. Retrieved October 28, 2013, from

제도가 탄생할 수 있는 촉매 작용을 할 수 있기 때문이다. 냉전론이란 아이디어만 수용할지라도 이를 통해 이득을 볼 수 있는 정치적 행위자들이 자신들의 이익을 극대화할 수 있는 제도를 생성하고 유지하기 위해 노력할 것이다. 전쟁은 과학•기술 발달에 중요한 기여를 하기도 하지만 적절한 견제와 균형 없는 국가 권력의 강화와 남용을 통해서 자유주의와 민주주의 발달에 위협이 되기도 한다. 따라서 민주주의와 인권의 관점에서 볼 때 냉전론 자체는 이론적 근거가 취약하다 할지라도 냉전론의 미국 그리고 정책적 학습을 통한 미국 외 타국가 내에서의 수용과 그 효과에 대해서는 관심을 가질 필요가 있다.

과거 냉전의 경험에 기초해 디지털 냉전론의 함의에 대해 생각해볼 수 있는 또 한 가지는 기존의 인터넷 거버넌스 제도의 근간으로 인정돼왔던 다자간 협력주의(multi-stakeholderism)의 한계다. 역설적으로 다자간 협력주의는 그들이 견제하고 있는 UN의 한계와 닮았다.

UN은 1945년 제2차 세계대전 종전 이후 세계 평화와 국제 경제, 사회, 인도적 문제의 해결을 돕기 위해 창설됐다. 하지만 UN에서 유일하게 결의안이 권고에 그치지 않고 구속력을 갖고 있어 권력의 중추에 해당되는 안전보장이사회(Security Council, 일명 '안보리')의 경우 제2차 세계대전 승전국인 미국, 영국, 러시아, 프랑스, 중국(1971년까지 대만 혹은 중화민국이었으나 이후 중국 혹은 중화인민공화국이 대체했다.)만이 안보리의 상임 이사국이다. 나머지 국가들은 10개 국가만이 2년 임기의 비상임 이사국으로 임명될 수 있다. 또한, 미국과 소련간의 촉발과 진화의 과정에서 보듯 UN의 존재에도 불구하고 주도적인 강대국간의 불화가 심화되면 UN에서는 이를 저지할 수 있는 메커니즘이 취약하다.

강대국의 이익을 일부 반영하고 이들 간의 합의에 따라 제도의 지속성이 보장되며 따라서 강대국 간의 이익이 충돌할 경우 이를 저지할 수 있는 내부적 메커니즘이 부족하다는 문제점은 다자간 협력주의에서도 발견된다. 비록 ICANN 등의 운영이 미국의 일방주의 원칙에 따라 운영된다고 보는 것은 무리가 있으나 상대적으로 미국의 입장이 더 강력히 반영되는 것은 사실이다. 중국, 러시아 같은 국가에서는 따라서 인터넷 수용에 따라 자국 내에 서방국가, 특별히 미국의 간섭이 확대되는 걸 바라지 않는 바, 기존 다자간 협력주의를 그대로 수용하는 데 무리가 있다. 이럴 경우 현재하고 있는 것처럼 중국, 러시아 같은 국가들이 기존 체제를 전복하진 않더라도 이에 이탈해 UN 등을 이용해 새로운 인터넷 거버넌스 질서를 창설해 그들의 기존 인터넷 통제를 지속하고자 할 때 다자간 협력주의가 이를 견제할 수 있는 내부적 메커니즘은 취약하다.

일부에서는 비록 공식적으로는 그러한 메커니즘이 존재하지 않더라도 비공식적으로 이런 사이버 공간의 제도적 전쟁에 대해 이용자 네트워크의 연대가 저항군으로서 역할을 할 수 있다는 의견도 제시되긴 했다.[64] 그리고 실제로 지난 2012년 미국 상•하원의 지적재산권법 개정안(SOPA/PIPA)에 대해서 초국가적 활동가들이 연대하여 저항하기도 했다.[65] 이론적으

---

http://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html

64) Benkler, Y. (2006). The wealth of networks : how social production transforms markets and freedom. New Haven: Yale University Press.

65) Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A., & Etling, B. (2013). Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate. SSRN Electronic Journal. doi:10.2139/ssrn.2295953

로도 사이버 공간의 익명성, 연결성이 집단행동(collective action)의 거래 비용(transaction cost)을 낮춘다는 점에서 볼 때 일견 이 주장은 일리가 있어 보인다. 그러나 이러한 사이버 공간을 통한 초국가적 활동가 연대의 한계는 그래도 여전히 높은 참여 비용, 그리고 이 비용이 특별히 개발도상국의 활동가들에게는 크다는 점을 감안했을 때 이러한 저항이 얼마나 지속적으로 일어날 수 있을지, 그리고 얼마나 다양한 활동가들의 의견과 이익을 반영하고 있을 지에 대해 의문을 제시하게 된다. 또한, 미국 정부가 인터넷 자유 선언 전후로 민주화의 새로운 기수로서 이른바 해커 활동가들에 대해 관심을 기울이고 이들에 대해 제도적 지원을 하고 있는 바 이들이 UN이 표방하려고 하는 것처럼 중립적인 기구로서 역할을 할 수 있을 지에 대해서도 한계점이 지적된다.

또한, 무역에서 WTO와 같은 다자간 무역과 함께 FTA와 같은 양자간 무역 협의가 진행되고 있는 것처럼 인터넷 거버넌스에 관련된 국제회의의 양과 종류도 갈수록 늘어나고 있는 추세다. 인터넷 거버넌스만 따로 취급하는 국제회의도 있지만, G8과 같은 기존의 강대국 간의 협의체나 혹은 정상회담의 아젠다의 일부로 인터넷 거버넌스가 삽입되는 경향도 보인다. 이건 달리 말하자면 국가 행위자들이 그들의 인터넷 거버넌스에 대한 권한 확대를 위해서 상대적으로 저항이 덜한 국제회의를 통해 그들간 이해관계의 공조를 추구할 가능성이 커졌다는 걸 뜻한다. 즉, 시민사회가 이러한 인터넷 거버넌스를 놓고 벌어지고 있는 새로운 경쟁 양상에 대해서 적절한 전략적 대응책을 만들어내지 못할 경우 다자간 협력주의에서 이탈하거나 혹은 그 구색만 갖추는 국제회의가 늘어날 것이며 그를 통해서 자기 이익을 관철하려고 하는 국가 행위자들의 성향도 더 두드러질 것이다.

물론, 다자간 협력주의의 한계점을 일부 인정하고 이를 보완하려는 노력이 그간 없었던 것도 아니다. 예를 들어 레베카 매키넌 같은 경우는 영국의 정치철학자 존 로크(John Locke)의 자유주의 정치철학을 원용해 이용자에 의한 동의(the consent of the networked)가 다자간 협력주의의 정당성의 기초이자 구속력의 원천으로서 활용되어야 한다고 주장한다. 그녀의 관점에 따르면 인터넷은 대표적 공유지(commons)이며 이 공유지를 개방과 통제 사이에서 적절하게 관리하는 방식은 국가와 시장 외에도 이용자들에 의한 자발적 거버넌스로서 이뤄져 왔다. 따라서 이용자의 동의라는 내부적 기제는 전통에 따라서도 그리고 공리적 관점에 의해서도 긍정된다. 그러나 최근 인터넷의 권력화, 상업화, 그리고 국가와 기업 간의 연대 강화에 따라 기존에 존재해왔던 암묵적인 행위자들 간의 세력 균형이 무너지고 있는 상황이다. 이에 따라 이제 이용자의 권익을 보호하고 인터넷 거버넌스의 기본 틀을 유지하기 위해서는 이용자에 의한 동의가 새롭게 확장되는 인터넷 거버넌스의 규범적 기반으로 수용되어야 한다.[66]

하지만 매키넌의 대안 역시 기존의 다자간 협력주의에 대한 비판에서 크게 자유롭지 못한다. 만일 중국과 같이 국력 상승에 따라 인터넷 거버넌스상에서도 영향력을 확대해가고 있는 국가가 '인터넷이 공유지'란 시각에 공감하지 않는다면? 그리고 그들이 '이용자의 동의'보다는 '국가 주권'이 더 중요하다고 강조한다면? 또한, 이들이 그러한 자신들의 선호를 보다 효과적으로 반영하기 위해 자신들만의 인터넷 거버넌스 레짐(regime)을 구축한다고 했을 때, 다자간 협력주의는 혹은 기존의 인터넷 거버넌스 관련 단체들은 과연 어떤 조건 하에서

66) MacKinnon, R. (2013). Consent of the networked: the world-wide struggle for Internet freedom. New York: Basic Books.

얼마만큼의 견제를 가할 수 있는가? 물론 이러한 주장은 다자간 협력주의에가 무용하다는 것도 무효하다는 것도 아니다. 여기서 강조하고자 하는 것은 강대국 간의 경쟁관계가 인터넷 거버넌스에도 확장되고 있으며 이 관점에서 봤을 때 기존의 인터넷 거버넌스상에는 심각한 취약점이 존재한다는 것이다.

나아가 구성주의적 관점에서 봐도 매키넌의 인터넷 거버넌스론은 통치 권력이 시민의 자발적 동의에 기초했다는 서양 정치사상의 홉스 이래 자유주의적 정치 이론에 기초한 바, 이와 같은 규범적 가치, 정치적 이론에 동의하지 않는 국가 행위자들에게는 수용되기 어렵다. '개방, 공유, 협업'을 강조하는 기존 인터넷 거버넌스는 '서구' 혹은 '자유 민주주의적' 가치에 근접하는데, 이것은 이러한 가치가 본질적으로 다른 가치보다 우월하기 때문이 아니라 인터넷의 태동 및 발달 과정에서 미국 및 서구 국가의 영향력과 개입 정도가 컸기 때문이다. 따라서 인터넷 인구가 미국과 유럽 외의 타 지역에도 지속적으로 증가하고 있으며, 경제적으로도 세계 경제의 중심이 대서양에서 태평양으로 옮겨간 바, 매키넌이 과거 전통에 의거해 인터넷 거버넌스에 관한 암묵적 사회적 합의라 간주한 '네트워크 이용자의 동의'는 오늘날, 그리고 앞으로의 인터넷 거버넌스에 관한 국제적 논쟁에서 주요 아젠다가 될 가능성이 크다.

즉, 국가 권력의 견제와 균형에 대한 문제를 핵심 쟁점으로 삼지 않고 논의의 형식이나 내용에 대해서만 다룬다면 향후 인터넷 거버넌스에 대한 현실적, 규범적 대안을 만들기란 쉽지 않다. 오히려 강대국의 인터넷 거버넌스 개입이 기정사실이 된 현실 하에서는 인터넷 거버넌스에 등장하는 새로운 문제들을 해결하기 위해 국가 개입 찬성, 반대와 같은 극단적 입장을 취하기보다는 '어떤 국가의 역할'이 필요한가에 대한 논의로 기존의 논의를 확장하는 것이 더 바람직할 수 있다. 이를 통해 대내외적으로 인터넷 거버넌스상 국가 역할에 대해 새로운 현실적, 규범적 인센티브를 제공할 수도 있기 때문이다.

예를 들어 현재의 인터넷 거버넌스상 국가 역할에 대한 논의는 국가가 대외의 적으로부터 대내의 국민을 보호하는 안보 위주로 이뤄지고 있다. 그러나 국가의 기원은 홉스식의 개인의 생명 혹은 로크식의 개인의 재산의 보호일지 모르나 선진 사회에서 현대 국가는 그 이상의 경제적, 사회적 책임을 지고 있다. 국가는 일정 시기 발전 국가(developmental state)의 형태를 띠고, 산업화의 주체로서 역할을 하며 이런 산업화의 부작용과 병폐가 드러나고 사회적 갈등이 심화될 경우 이를 무마하기 위해 복지국가(welfare state)의 몫을 수행하기도 한다. 또한, 시장에서 독과점 기업의 횡포를 막고 시장 진입과 경쟁의 정도를 촉진하기 위해 규제 국가(regulatory state)로서 활동하기도 한다. 이러한 다양한 국가의 역할은 그 국가의 발전 단계와 대내외적 현실에 따라 주어진 국가 능력과 국가 구조를 통해 발현된다. 기존의 인터넷 거버넌스론에서는 이러한 다채로운 국가 역할 중 극히 일부에 대해서만 강조하고 있다. 그리고 실제로 이런 다채로운 역할이 발현되기 위해 어떠한 국가 능력이 어떻게 계발될 수 있을지(capacity-building)에 대한 논의, 그리고 이런 국가 능력이 발현되기 위해서는 어떠한 국가 구조가 필요한 지에 대한 논의는 상대적으로 취약하다. 특별히 디지털 냉전론의 경우 이 중 안보적 책임에만 집중해 논의가 진행돼 왔는데 이럴 경우 국가의 다른 중대한 책임에 대한 논의를 단순화, 간소화하는 오류를 범할 수 있으며, 앞서 설명하였듯 그 과정에서 민주주의를 위축시킬 수도 있다.

이런 비판을 고려해 향후 인터넷 거버넌스론에서는 안보적 문제를 도외시하진 않으나 디지털 냉전론에서, 그리고 기존의 이분법적인 인터넷 거버넌스 진행에서도 벗어날 필요성이 있다. 국가 행위자의 안보 영역에서 기존 역할은 인정해야 하지만 그 외 산업화, 공정 규제, 권리 보호와 복지 증진의 영역에서도 국가가 해야 할 책임을 균형있게 다하여 국제 번영, 안정, 인권의 향상에 기여할 수 있도록 대내외적 기제를 증설하는 데 초점을 맞추는 것이 더 이상적인, 그리고 현실적인 목표가 될 것이다.

결 론

미국이 중심적인 위치를 차지해 왔던 인터넷 거버넌스를 중국 혹은 다른 강대국이 전복하고자 한다는 시나리오에 기초한 디지털 냉전론의 이론적 타당성은 취약하다. 그러나 이런 논의 자체가 무의미한 것은 아니다. 디지털 냉전론 자체는 실체가 없을 지라도 냉전론의 수용 자체만으로 강대국 간의 갈등을 심화시킬 수 있다. 또한, UN의 창설에도 불구하고 냉전이 촉발했듯 다자간 협력주의와 기존 인터넷 거버넌스 관련 기구들이 존재함에도 불구하고 새로운 논의와 국제회의들이 증가하고 있는 건 기존 인터넷 거버넌스 질서가 국가 행위자들의 이해관계를 수용하는 데 한계가 있다는 걸 보여준다. 다자간 협력주의를 통한 인터넷 거버넌스에서 이탈해 새로운 거버넌스 질서를 형성하고자 하는 이러한 국가 행위자들의 활동을 저지하거나 제한할 수 있는 기제가 등장하지 않는 이상, 이런 흐름은 기존의 인터넷 거버넌스 질서에 큰 변화를 야기할 수 있다. 본고는 이에 대응해 향후 인터넷 거버넌스상에서는 국가 행위자의 역할은 인정하되 그 역할을 논의하는 폭을 넓힐 것을 제의한다.

ABSTRACT

The Digital Cold War Argument and the Internet Governance

Jae Yeon Kim[67)]

The Digital Cold War argument has become one of the heatedly discussed foreign policy agendas in the U.S. Considering the authority and power of the U.S. government and Internet companies in the cyberspace, this shift is not negligible in understanding not only the changes in the U.S. foreign and military policies but also that in the operations of the global Internet governance. Given these circumstances, I seek to explain the origins of and test the theoretical validity of the Digital Cold War argument. In particular, I analyze how the political concerns of the Chinese authorities shaped the characteristics of their control of the domestic Internet and their approach to the global Internet governance. The findings indicate that the Chinese way of the Internet governance is more concerned of their domestic political stability than overthrowing the current Internet governance regime, which many supporters of the Digital Cold War argument cited as the key evidence of such political contentions. Though the Digital Cold War argument is theoretically unwarranted, its growing popularity and the historical lessons of the Cold War have broad implications to the understanding of the impacts of the great power rivalries on the future Internet governance.

67) digital activist for Creative Commons Korea and Global Voices Online, member of Global Voices Advocacy

인권적 관점에서 본 인터넷 거버넌스

박성훈[68]

거버넌스의 구조와 민주주의 원리

인터넷 거버넌스(Internet Governance)란 인터넷 정책과 관련된 다양한 이슈를 정부, 민간, 시민단체 등 다양한 이해당사자가 참여해 인터넷 발전과 이용 활성화를 위한 원칙, 규범, 의사결정 절차 등을 개발하고 적용하는 것을 말한다. 여기서 가장 핵심이 되는 거버넌스의 개념과 원리 그리고 국제적 논의로의 확장을 고민해 볼 필요가 있다.

유엔개발계획(Unoted NAtions Development Programme, UNDP)은 거버넌스를 정의하면서 한 국가의 여러 업무를 관리하기 위하여 정치, 경제 및 행정적 권한을 행사하는 것으로 정의하였고, 거버넌스는 시민들과 여러 집단이 자신들의 이해관계를 밝히고 그들의 권리를 행사하며 자신들의 의무를 다하고 그들 간의 견해 차이를 조정할 수 있는 복잡한 기구와 과정 등의 제도로서 구성된다고 설명하고 있다.

그리고 거버넌스(Governance)의 의사소통 방식은 수평적 관계 속에서 정부, NGO, 기업 등 다양한 이해당사자들의 의견수렴 절차를 거치는 상향식(Bottom-Up) 논의 구조를 지니고 있으며, 이는 국가·정부의 통치기구(Government)의 지시와 명령에 의한 하향식(Top-Down)의 의사소통과는 본질적으로 다르다.

거버넌스 구조에서의 정책결정은 정책에 대한 여러 이해당사자들의 참여 속에 끊임없는 토론과 논의를 통하여 방향을 결정하는 민주주의 원리가 내재되어 있다고 할 수 있다. 이는 헌법 제1조 “대한민국은 민주공화국이다. 대한민국의 주권은 국민에게 있고, 모든 권력은 국민으로부터 나온다”에서도 그 근거를 찾을 수 있다.

하지만 무어(Moore)에 의하면 거버넌스는 정부(government)를 의미하는 것도 아니며, 통치행위 자체를 의미하는 것도 아니다. 거버넌스는 조직 및 사회가 스스로 바람직한 방향을 찾아나가는 과정을 의미한다고 주장하였으며, 거버넌스 이론을 수립하는데 기여한 로즈(Rhodes)는 참여와 협력을 바탕으로 각 행위자 사이의 상호의존적인 네트워크 관계 형성을 통한 정책 의사결정 과정이라고 주장했다.

---

68) 국가인권위원회 인권정책과 정보인권 담당, cyber152@humanrights.go.kr

즉, 통치자와 소수의 정책결정자의 생각에 의하여 정책이 결정되고 집행되는 구조가 아닌 정책과 사회적 이슈에 대하여 각각의 이해당사자가 끊임없는 토론과 논의를 바탕으로 합의된 기준을 만들어 가는 것이 거버넌스인 것이다.

UN과 거버넌스

오늘날 UN은 서로 관련된 이슈들을 종합적으로 접근하는 연구, 국제적 합의도출, 인권보호 및 목표설정의 역할, 국제조약 혹은 협의 준비와 협상을 위한 포럼 개최, 기술적 조정과 기준의 설정 및 정보의 수집과 배포, 국제기관 사이의 행동의 조정 등을 하고 있다.

대규모 세계적 회의를 조직하고 이를 통해 주요 사회·경제적인 문제들에 있어서 국가 간의 합의를 도출하고 있으며, 인권과 관련된 UN의 광범한 규약들과 기제들은 인권의 표준을 설정하고 준수 여부에 대한 감시를 시행하여 국가들에게 하나의 압력으로 작용하고 있다.

최근에는 UN의 논의가 정치적, 시민적 권리뿐만 아니라 환경권, 생존권으로 확대되고 있고, 정보통신기술의 발달에 따라 정보사회에 대한 논의로 확대되고 있으며, 이러한 권리들의 증진을 위하여 국제기구가 관여해야 한다는 지지가 확대되고 있다.

따라서 정보통신기술 및 인터넷과 관련한 제반 문제는 이제 UN 차원의 글로벌 거버넌스로 해결해야 할 문제로 인식되고 있으며, 특히 인터넷의 접속과 활용은 인류의 보편적 기본권으로서 인권적 측면에서 다루어야 할 필요성이 제기됨으로써 인터넷 거버넌스 포럼의 중요성이 부각되고 있다고 할 것이다.

기본적 인권으로서의 인터넷 접속권 그리고 인터넷 주소자원 관리

새로운 기술은 언제나 인간의 권리에 대한 새로운 도전을 제기해 왔다. 하지만 지금까지 어떠한 기술적 혁신도 인터넷과 정보통신기술과 같이 인간이 자신을 표현하고, 소통하며 토론하고, 인적 네트워크를 만들면서 자신을 드러내며, 놀이와 쇼핑하는 방식을 급격하게 변화시킨 것은 없었다. 이로 인하여 인터넷이 인간 활동에 미치는 영향은 대단하며, 모든 기존의 인권 문제와 관련해서도 인터넷과 정보통신기술의 변화에 따라 수많은 도전과제가 부상하게 되었다.

따라서 인터넷에 대한 접속은 사회를 살아가는데 있어 없어서는 안 될 보편적 인권으로 보장되어야 한다. 이는 UN을 비롯하여 EU, ASEM 회원국 등 전 세계 회의에서 법률 및 권고사항으로 구체화되고 있다.

UN은 인터넷에의 보편적 접근권을 보장하는 것이 모든 국가의 우선과제가 되어야 한다고 권고 하고 있으며, EU 의회도 인터넷 접속권을 표현의 자유와 동등한 기본권으로 규정하였다. 또한 각 국가별로 에스토니아 국회는 2000년도에 인터넷 접속을 기본적인 인권으로 선언하는 법안을 통과시켰고, 프랑스 헌법 위원회는 2009년 인터넷 접속이 기본권이라고 실질적 선언을 한 바 있다. 정보인권을 주제로 한 제12차 ASEM 인권세미나에서도 모든

인간의 권리로써 정보통신기술의 접근을 논의하고 회원국들에게 권고사항으로 정보통신기술에 접근하고 이를 효율적으로 사용할 수 있는 능력은 다양한 인권 및 기타 기본권을 점진적으로 실현시키기 위한 필수조건으로 진화하였다는 점을 분명히 하고 있으며, 국가인권위원회 정보인권 보고서에서도 국가의 인터넷 접속권 보장 확대와 관련한 정책적 제안을 제시하고 있다.

이처럼 정보사회에서 인터넷 접속이 기본적 인권으로 보장되어야 한다는 주장이 대두되면서 자연스럽게 인터넷 접속과 관련한 국제적 표준과 기준을 다루는 문제는 한 국가가 아닌 국제적 인권을 다루는 문제로 확대되었다는 점이다.

기본적으로 인터넷 접속권 보장은 인터넷 주소자원의 관리에 관한 문제와 직결된다. 하지만 인터넷 주소자원 관리는 기술적 차원을 넘어 도메인 네임과 관련한 개인정보 보호 등 프라이버시 문제, 인터넷 검열과 같은 내용규제, 정보격차, 지적재산권 및 전자상거래 등 사이버 공간에서 일어나는 활동 전반에 관한 정책과 연결된다고 할 수 있다.

인터넷 거버넌스를 다루는 국제적 기구는 ICANN 이외에도 ISOC, IETF, IEEE, ITU 등이 있다. 하지만 ICANN이 수행하는 역할은 단순한 기술 문제를 넘어서 개별 국가 도메인 명칭 등록 환경을 포함하여 글로벌 인터넷 정책과 관련한 많은 이슈와 관련되며, 인터넷 기반의 정보통신기술이 발달하면 할수록 그 영향력은 커지고 있는 상황이다.

하지만 현재 ICANN은 미국의 한 기업이 운영하고 있으며, 2000년대에 들어서 인터넷 접속과 관련한 보편적 기본권이 한 국가의 기업에 의해 결정될 수 있다는 점에 우려를 표하며, 많은 국가에서 국제적 논의를 의제화 했고, 결국 인터넷과 관련한 거버넌스 논의 구조를 구성하게 되었다.

인터넷 주소자원 관리를 둘러싼 정책결정 구조의 논쟁과 프레임워크의 전환

인터넷 거버넌스 포럼은 결국 90년대 중반 신자유주의 과정에서 나타난 민영화로 인하여 국적을 초월한 국제기구 성격을 지녀야 할 인터넷주소자원관리기구가 한 국가의 주법에 적용을 받는 민간법인 기관으로 구성되면서, 기구의 정당성과 대표성뿐만 아니라 민주적 원리에 의한 의사결정 구조를 갖지 못한 한계에 대한 반발로 만들어지게 되었다.

결국엔 정보통신기술의 발달과 정보사회의 핵심인 인터넷에 대한 정책과 주소자원의 관리가 전 세계의 관심 이슈로 떠오르면서, 미국 중심의 의사결정 구조와 통제에 위협을 느낀 국제사회가 UN이 주최하는 정보사회세계정상회의(WSIS)를 통하여 인터넷 거버넌스 문제를 제기하였고 지속적인 논의를 위해 유엔 차원의 인터넷 거버넌스 포럼(Internet Governance Forum)이 구성되게 되었다.

인터넷 거버넌스 포럼의 가장 큰 이슈는 인터넷 주소자원에 대한 관리를 어떤 논의 구조로 가져갈 것인가와 2015년까지 제출하기로 한 상설 국제기구화 운영방안에 관한 논의이다.

하지만 인터넷 거버넌스 포럼은 정보사회의 다양하고 중요한 이슈를 논의하는 자리가 변화해 왔고, 더 나아가 해가 거듭할수록 주소자원관리에 대한 논의 이외에도 정부, 기업, NGO, 국제기구, 전문가 등 다양한 이해당사자가 모여 정보사회와 관련한 수많은 이슈를 논의하는 거대 담론의 장이 되었다. 2013년 제8차 회의에서는 인터넷 거버넌스의 원칙, 다자간 협의 모델의 원칙과 정부의 역할, 사이버 보안, 성장과 지속발전을 위한 엔진으로서의 인터넷, 인터넷에서의 인권, 표현의 자유, 그리고 정보의 자유 흐름, 정보 격차 등의 주요 주제에 대한 120여개의 패널토의가 열렸다.

정보통신기술과 인권(정보인권)

앞서 이야기한 것처럼 인터넷은 우리의 삶의 질을 변화시키는 필수 요소가 됐지만 고도의 기술 발전은 국가와 기업 등 타인에 의해 개인정보가 수집되고 유통되며, 고도화된 기술을 통해 감시와 통제가 발달했으며, 정보에 대한 접근성에 따라 사회적 불평등 현상을 초래한 것도 사실이다.

최근 미국의 국가안보국(National Security Agency)이 전 세계 인터넷과 통신을 감청해 왔던 사실이 드러나면서, 국가의 인터넷과 통신 감청, 글로벌 정보통신 기업들의 국가와의 협조 문제는 모든 것이 디지털화되고, 인터넷으로 전송 및 공유되는 현실에서 통신비밀, 개인정보 보호, 검열에 의한 표현의 자유 등의 문제를 다시 생각하게끔 한다.

세계 인권선언문 제12조는 사생활 보호 및 통신의 자유를, 제19조는 표현의 자유를 규정하고 있으며, 이를 보다 구체화한 국제규약인 시민적 및 정치적 권리에 관한 규약(자유권 규약)은 제17조와 제19조에 이를 규정하고 있다. 최근 유엔 표현의 자유 특별보고관은 정보통신기술에 의한 사생활과 표현의 자유의 제약에 관한 보고서(A/HRC/23/40)를 제출하였다.

정보통신기술의 발달과 삶의 변화는 프라이버시권과 표현의 자유에 관한 문제를 넘어서 세계 인권선언문 제6조 평등권(자유권 규약 제2조), 제27조 문화 향유권(사회권 규약 제15조) 영역으로 확대되고 있다.

이에 국가인권위원회는 2013년 정보통신기술의 발달에 따른 인권 문제를 종합적으로 조망한 정보인권 보고서를 발간하고, 정보인권(Information Communication Technologies & Human rights)이란 “정보통신기술에 의하여 디지털화된 정보가 수집·가공·유통·활용되는 과정과 그 결과로 얻어진 정보가치에 따라 인간의 존엄성이 훼손되지 않고 자유롭고 차별 없이 이용할 수 있는 기본적 권리”라고 정의하고 있다.

따라서 정보인권 보호를 위해서는 국가가 정보통신기술과 인터넷에 보편적이고 차별 없는 접근권을 보장함으로써 정보사회에서의 인간의 존엄과 가치를 위한 기본적 인권 보장의 틀을 마련하여야 하며, 개인의 사생활과 통신의 자유를 위한 정보프라이버시권의 보호하고 누구나 인터넷에 자신의 의견을 자유롭게 표현하고 이를 공유하고 향유할 수 있도록 해야 한다는 것이다.

정보인권 보호를 위한 논의의 장으로서의 인터넷 거버넌스

정보사회가 고도화되면 될수록 정보는 단순한 데이터나 지식이 아니라 그 자체가 지배 혹은 권력의 중요한 요소로 작용한다. 따라서 사회공동체 내에서 정보를 누가 얼마만큼 장악하고 지배하느냐는 그 공동체의 권력구조와 국민 개개인의 자유를 결정하는 핵심조건이 된다.

따라서 정보인권 보호를 위한 모든 국가, 각 국가 내 정책결정에 있어서 인터넷 거버넌스는 핵심이다. 이미 NSA의 전 세계 인터넷과 통신 감시로 인하여 인터넷 관련한 독점 문제는 얼마나 큰 병폐를 불러올 수 있는지 검증되었다. 그리고 모든 정책결정은 민주주의 원칙에 따라 상향식 논의 구조에 의해 투명하게 결정되어야 한다.

이미 글로벌 국제 거버넌스로 UN이 존재하며, 정보사회에서 정보통신기술과 인터넷의 접속이 보편적 기본권으로 인식되고 있는 만큼 인터넷 주소자원 관리와 정보통신기술에 따른 여러 제반 문제에 대하여 수많은 이해당사자가 거대 담론의 장을 형성하고 있는 인터넷 거버넌스 포럼은 그 중요성이 크다 할 것이다.

[참고 문헌]

국가인권위원회(2013), 정보인권 보고서

박민정(2013), “ITU와 글로벌 인터넷 논의의 추이와 현황”, KISDI 방송통신정책 제25권 제10호

문상현(2012), “SNS와 인터넷 거버넌스”, 제38대 한국언론학회 제1차 기획연구 <한국사회의 정치적 소통과 SNS> 세미나

이항우(2010), “신자유주의 글로벌 인터넷 거버넌스와 정당성 문제”, 경제와 사회 통권 제87호

이항우(2009), “지구화, 인터넷 거버넌스, 그리고 ICANN”, 경제와 사회 통권 제82호

장용석외(2011), “융합사회와 거버넌스”, 사회이론 통권 제18집

장우영외(2005), “인터넷 규제의 거버넌스: EU와 한국의 비교”, 한국거버넌스학회보 제12권

최현실(2005), “글로벌 거버넌스로서의 유엔과 한국의 의사결정과정에 여성참여 정책”, 여성학 연구 제14·15권

ASEM(2012), 제12차 ASEM 인권세미나 최종 보고서

A/HRC/17/27

A/HC/23/40

ABSTRACT

Internet Governance in the light of Human Rights

Park, Seong Hoon[69)]

Information and Communication Technologies(ICTs) have substantially enlarged both the opportunities to realize one's human rights but have also resulted in the emergence of new challenges.[70)]

ICTs are so deeply embedded and cental to almost all aspects of human activity. And ICTs are assuming an increasingly central role in all aspects of human and societal development across the world. But this is especially true of the right to privacy, which faces challenges such as profiling and data mining for public(including national security) and private purposes.

ICTs access is a fundamental right for all humans in the information age. So we have need for regulation based on human rights in the digital age. And governments have a responsibility to protect individuals against violations of human rights and data protection by public authorities, but also by private entities.

In addition, internet governance and multi-stakeholder principle have to be stressed on all of the internet issues because internet governance is included in the principle of democracy which have bottom-up communication and equality. So it is very importance that Internet Governance Forum is the space for a meaningful discussion on public policy issues relating to the internet.

---

69) National Human Rights commission of Korea Policy Division, Advisory Expert on the ICTs and Human Rights

70) NHRCK(National Human Rights of Korea) have commented that ICTs and Human Rights is related to the right to privacy, freedom of expression, access to knowledge(including digital divide) and right to cultural enjoyment of the internet.

▮ 제2부

인터넷 거버넌스, 무엇이 문제인가

글로벌 거버넌스 공론장으로서 IGF의 의미

박지환[71]

1. 서론 : IGF, 다양한 이해당사자들의 광범한 참여로 운영되는 공론장

인터넷 거버넌스(internet governance)의 논의 대상은 인터넷 주소자원의 할당과 관련된 의사결정에 한정되지 않고 프라이버시, 망중립성, 보편적 인터넷 접근권 등 정보인권이 다루고 있는 제 영역까지 확대되어가고 있다. 2013년에는 인터넷 거버넌스를 주제로 다양한 이해당사자들이 참여하는 공론장을 표방한 국제회의가 다수 개최되었다. 그 중 대표적인 것으로 2013년 10월 22일~25일 인도네시아 발리에서 개최된 제8회 인터넷 거버넌스 포럼(Internet Governance Forum, 이하 "IGF")과 이보다 앞서 2013년 10월 17일~18일에 대한민국 서울에서 개최된 사이버스페이스 총회(Seoul Conference on Cyberspace)를 들 수 있다. 이들 국제회의는 모두 정보인권을 포함한 다양한 주제가 국제적 수준에서 논의되는 공론장이라고 볼 수 있는데, 최근 연일 화제가 되고 있는 미국 국가안보국(NSA)의 대규모 도청, 감청 문제도 이번 IGF에서 중요한 이슈 중 하나로 다루어진 바 있으며,[72] 서울 사이버스페이스 총회에서는 인터넷 접근권의 보편적인 보장을 위한 저개발국의 역량강화 등의 이슈까지 다루어지기도 하였다.

본 보고서에서는 필자가 인도네시아 발리에서 개최된 제8회 IGF에 패널리스트로 참가한 경험을 바탕으로 IGF의 멀티스테이크홀더리즘(multistakeholdersim) 구현 방식 중 특히 시민사회의 참여를 어떤 식으로 보장했는지를 살펴보고, IGF에서 각 분야의 논의가 진행되는 과정을 분석하여 글로벌 거버넌스 공론장으로서 IGF의 의미에 대해 검토해보도록 한다. 또한 보고서 말미에서는 역시 다양한 이해당사자의 참여를 강조했던 서울 사이버스페이스 총회에 대해서도 함께 검토해보기로 한다.

2. IGF 참여절차 및 회의 운영방식

IGF는 이른바 멀티스테이크홀더리즘(multistakeholdersim)을 추구하는 것을 기치로 정보사회세계정상회의(World Summit on the Information Society, WSIS)의 튀니스 어젠다

71) 법률사무소 혜윰, 사단법인 오픈넷 자문 변호사, 망중립성이용자포럼 소속, bobpark925@gmail.com
72) https://www.accessnow.org/blog/2013/11/07/igf-2013-in-review

(Tunis Agenda)에 따라 2006년부터 매년 열리고 있는 국제회의이다. 2013년까지 모두 8회 개최되었으며 제8회 IGF는 인도네시아 발리에서 개최되었다. IGF는 국가주권 단위의 의사결정과정방식인 다자주의(multilateralism)에 기반한 기존 국제기구 회의와는 달리 국가도 IGF에 이해당사자의 하나로 참여하게 되며, 시민사회 등 모든 이해당사자들의 보편적인 참여를 보장하고 이들의 발언권을 보장하기 위하여 IGF 내에 다양한 참여 방식을 제공하고 있다.

(1) 등록

IGF는 참석을 희망하는 모든 사람들에게 개방되어 있으며, 인터넷 사전 등록 또는 현장등록을 통해 본 회의에 손쉽게 참여할 수 있었다. IGF에 처음 참여했던 필자 역시 인터넷을 통한 간단한 등록만으로 참가 신청을 완료할 수 있었고, 신청에 대하여 별도의 심사를 거치거나 PIN 번호를 부여 받는 등의 실질적인 심사 절차는 부재하였다.[73] 다만 정보인권 시민단체인 APC(Association of Progressive Communication)는 IGF의 등록과정에 대하여 보안에 취약하고 필요 이상으로 지나치게 개인정보를 많이 요구한다는 비판을 제기하기도 하였다.[74]

(2) 멀티스테이크홀더 자문 그룹(Multistakeholder Advisory Group, MAG)

IGF는 멀티스테이크홀더 자문그룹(이하 "MAG")을 운영하고 있으며, MAG은 정부와 시민사회, 학계 및 기술 분야의 전문가 집단을 아우르는 이해당사자들이 모두 참여하고 있으며 2013년 현재 56명이 MAG에 속해있다. MAG은 IGF 회의의 프로그램이나 회의 일정 등에 대하여 실질적인 자문을 제공하고 있는데, 이들은 주로 메일링리스트로 의사결정을 하고 있으며 메일링리스트 상에서 논의된 내용은 IGF 홈페이지를 통해 정리되어 전문이 공개되어 있다. 2013년 11월 현재 2014년에 활동할 새로운 MAG 구성원을 선발하는 중이며, 이 과정에도 시민사회는 스스로 조직한 Civil Society Internet Governance Caucus(IGC, 홈페이지는 http://igcaucus.org)를 통하여 MAG에서 활동할 인사를 추천하고 있다. 다만 MAG이 가진 중요성에도 불구하고, MAG 선발과정이 다분히 불투명하게 운영되고 있다는 지적도 제기되고 있어 선발과정에 대한 개선이 요구된다.

(3) 워크샵 및 원격 참가

① 워크샵(workshop)

IGF의 대부분의 일정은 다양한 이해당사자들이 자발적으로 조직하여 진행하는 워크샵(workshop)으로 구성된다. 워크샵은 인터넷 거버넌스와 관련된 다양한 이슈를 다루고 있으며, IGF 사무국은 제한된 시간과 장소를 고려하여 사무국에 제출된 워크샵 기획안들 중 비슷한 주제들을 선별하여 통합, 조정하는 역할을 하며, 워크샵의 내용 및 구성 자체에는 관

73) 반면 서울에서 개최된 제3회 사이버스페이스 총회의 경우 본 회의에 참석하기 위해서는 사전 심사를 거쳐 PIN 번호를 발급하였고, PIN 번호를 받은 사람에 한하여 본 회의에 입장할 수 있었다

74) http://www.apc.org/en/news/security-vulnerabilities-igf-registration-process

여하지 않는다. IGF의 워크샵 관련 프로그램 구성과 일정 결정에 앞서 설명한 MAG이 적극적으로 참여하여 자문을 제공하고 있다. IGF는 이처럼 일련의 워크샵으로만 진행되며 별도의 공식적인 결과물을 발표하지 않고 있다. 다만 각 워크샵에서 논의된 모든 내용은 인터넷으로 생중계되고, 녹화된 파일은 유투브(youtube)를 통하여 게시되어 있으므로 누구나 IGF의 모든 워크샵 내용에 직접 접근할 수 있다. 그리고 각 워크샵에서 참가자들이 한 발언 내용은 속기록(transcript) 방식으로 정리되어, 어떤 이해당사자가 어떤 발언을 하였는지를 손쉽게 확인할 수 있다.[75]

제8회 IGF에서 한국 시민사회에서는 '온라인 상 익명성(anonymity)'과 '망중립성(net neutrality)' 이라는 두 가지 분야에서 워크샵을 기획하고 진행하였다. 사단법인 오픈넷[76](이하 "오픈넷")은 영국의 BCS(British Computer Society, The Chartered Institute for IT)와 함께 온라인 상 익명성 문제에 대한 워크샵[77]을 함께 기획하고 진행하였으며, 국내 시민단체의 연합인 망중립성 이용자포럼[78]은 망중립성 관련 워크샵[79]에 참여하여 한국의 망중립성 정책에 대하여 발표한 바 있다.

그림 6 제8회 IGF 워크샵 사진

② 워크샵 진행 및 원격 참가(remote participation)

발리에서 개최된 제8회 IGF에서는 각 워크샵 별로 90분의 시간이 주어졌고 대부분의 워크샵은 패널리스트의 주제 발표와 현장 및 원격참가자가 참여하는 토론으로 구성되었다. 인

75) 2013년 제8회 IGF의 각 워크샵 속기록은 http://www.intgovforum.org/cms/igf-2013-transcripts 에서 확인할 수 있다.
76) 인터넷을 자유, 개방, 공유의 터전으로 만들기 위한 바람직한 인터넷 정책 및 환경을 논의하는 공론장을 추구하며 창설된 시민단체로 2013년 2월에 개소하여 활발하게 활동 중에 있다. (홈페이지 : http://opennet.or.kr)
77) "Security and Governance of Identity on the Internet"
78) 11개 시민단체가 공동으로 참여하고 있는 망중립성 정책 관련 시민단체 연합체이며, 2012년에는 주로 망중립성 정책에 대한 시민사회의 입장을 대변하였고 2013년에는 인터넷 거버넌스 분야로 그 활동 영역을 확대하여 제8회 IGF에 적극적으로 참여하였다. (홈페이지 : http://nnforum.kr)
79) "Network Neutrality: From Architecture To Norms" 및 "Could OTT Enterprises and Telecom Operators be Win-Win"

터넷 거버넌스를 논하는 자리답게 IGF는 인터넷을 통한 질의응답 과정인 원격참가(Remote Participation)를 통해 시간적, 지리적, 경제적 이유로 참석하지 못하는 이해당사자들의 참여까지 보장하고 있다.[80] IGF 사무국은 원격참가 사이트를 통해서 인터넷 이용자들에게 워크샵 현장에서 제공되는 프리젠테이션 파일 등을 제공하였는데, IGF 사무국 직원은 워크샵에 패널리스트로 참석한 필자에게 발표에 사용될 프리젠테이션 파일을 원격참가자들에게 제공해도 되는지 여부에 대해 동의를 구했고, 필자의 동의하에 원격참가 사이트를 통하여 해당 프리젠테이션 파일이 공유되었다. 또한 워크샵 진행자는 수시로 원격참가 사이트에 실시간으로 게시되는 질문들을 확인하도록 되어있기 때문에 원격참가 사이트를 이용해서도 워크샵 논의에 실제적으로 참여하는 것이 가능하였다. 더욱이 현장에 참석하지 못한 패널리스트가 자국에서 인터넷을 통한 영상통화 장비를 이용하여 원격으로 프리젠테이션을 진행하는 경우도 다수 있었다.

(4) 다이나믹 코얼리션(Dynamic Coalition) 및 오픈 포럼(Open Forum)

① 다이나믹 코얼리션

다이나믹 코얼리션(Dynamic Coalition, 이하 "DC")은 IGF회의를 통하여 자발적으로 조직된 집단이며 인터넷 분야 외에 기후변화(climate change)에 이르기까지 다양한 분야와 주제를 바탕으로 활동하고 있다. 이들 DC는 공식적인 실체나 별도의 법인격을 가지고 있지는 않으나, 메일링리스트 등을 통해 활발하게 의견을 공유, 수렴하고 있으며, 매년 개최되는 IGF 회의를 통하여 논의된 결과물을 발표하거나 해당 주제에 관심 있는 여러 이해당사자들과 교류하며 참여를 독려하고 있다. 현재 IGF 홈페이지에 소개되고 있는 DC는 모두 11개로, DC on Net Neutrality, DC on Climate Change, DC on Child Online Safety 등 이들이 다루고 있는 주제도 매우 광범하다. IGF 회의 내에서 활동방식 역시 다양한데, 일례로 DC on Net Neutrality는 제8회 IGF를 통하여 각국의 망중립성 법안이나 정책의 기본 자료로 활용할 수 있는 망중립성 모델프레임워크(Model Framework on Net Neutrality)를 발표하기도 하였다.

② 오픈 포럼

한편 IGF는 인터넷 거버넌스 관련 이슈를 다루는 주요 단체들에게 단체 명의로 오픈 포럼(Open Forum)을 개최할 수 있도록 하고 있다. ICANN이나 UNESCO, IETF, OECD 등 인터넷 거버넌스와 관련하여 국제적으로 명성을 가지고 있는 단체 또는 국제기구들이 주로 오픈 포럼을 진행하고 있다. 오픈 포럼은 해당 단체들이 지난 1년 동안 인터넷 거버넌스와 관련되어 활동해온 구체적인 성과를 정리 발표하고, 이에 대해 참가자들과 토론을 하는 방식으로 진행된다. IGF 사무국은 IGF에 처음 참여하는 한국의 시민단체인 오픈넷에게도 오픈넷 명의로 오픈 포럼을 개최하도록 허용하였고, 오픈넷은 망중립성 이용자포럼과 함께 오픈 포럼을 함께 개최하여 한국의 망중립성 정책 및 IT 정책에 대한 한국 시민사회의의 활동을 폭넓게 다룰 수 있었다.[81]

---

80) 물론 인터넷 기반 시설이 갖추어지지 않은 저개발국의 이해당사자인 경우 인터넷을 통한 원격참가마저도 어렵다는 한계가 존재한다.

81) 오픈포럼의 내용은 http://www.intgovforum.org/cms/open-forums/list-of-open-fora 에서

(5) 기타 : 오픈 마이크로폰(Open Microphone)

IGF에서는 회의 마지막 날에 오픈 마이크로폰(Open Microphone)이라는 세션을 진행한다. 본 세션에서는 IGF에 참석한 참가자 누구나 원하는 발언을 자유롭게 할 수 있다. 오픈 마이크로폰은 IGF가 다양한 이해당사자들의 참여에 기반하여 진행된다는 점을 가장 잘 드러내는 세션이라고 할 수 있다.

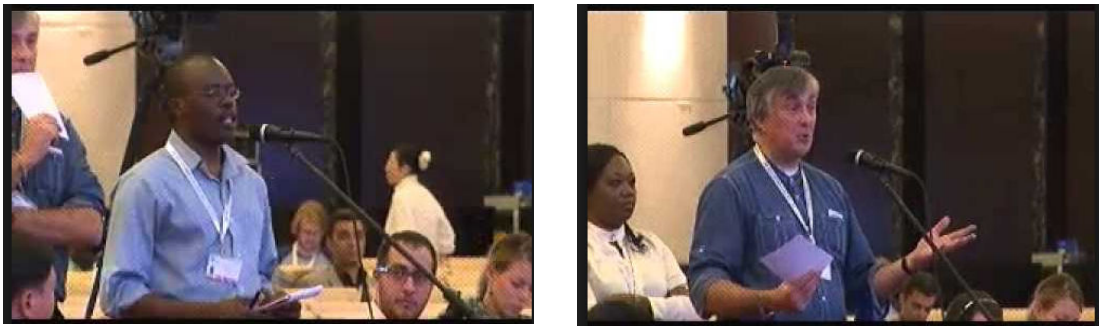

그림 7 IGF 오픈마이크로폰 장면 (출처: youtube 화면 캡쳐)

3. IGF 공론장의 특성

이하에서는 정보인권을 포함한 인터넷 거버넌스를 논의하는 글로벌 거버넌스 공론장으로서 IGF가 어떠한 의미를 가지는지를 간략하게 분석하도록 한다.

(1) 튀니스 어젠다(Tunis Agenda)의 IGF 기획

앞서 언급한 바 있듯이 튀니스 어젠다(Tunis Agenda)에서 IGF가 지향하는 지점은 다양한 이해당사자들의 광범한 참여를 통하여 탈 국가중심적인 멀티스테이크홀더리즘(multistakeholderism)에 기반한 공론장을 구축하는 것이었다. 앞서 IGF의 운영방식의 특징은 아래 표5의 튀니스 어젠다에서 IGF의 목표 및 운영방식을 구체화한 결과물에 해당한다. 다만 현재 IGF가 운영되는 방식이 튀니스 어젠다의 기획을 제대로 반영하고 있는지, 그리고 튀니스 어젠다 자체가 이해당사자의 광범한 참여를 전제로 하는 멀티스테이크홀더리즘을 제대로 지향하고 있는지 여부는 별도의 연구를 통하여 구체적인 평가가 필요할 것이다.[82]

확인할 수 있다.

82) 번역은 <인터넷거버넌스 정보보호 논의방향> , 한국인터넷진흥원 (2006. 3.) 참조.

72. a) 인터넷의 안정성, 지속성, 개발 등을 위한 인터넷 거버넌스 관련 중요 요인들과 관련된 공공정책 논의 b) 인터넷과 관련된 상이하고 대조적인 국제 공공정책이나 현재 어떤 기구에서도 논의되고 있지 않은 인터넷 관련 이슈 토론 c) 적절한 국가간 기구와 자기영역내의 문제해결을 추구하는 타 학술기관과의 상호교류 d) 정보와 프랙티스 교류 활성화와 이와 관련한 학술적, 과학적 기술적 커뮤니티 활용 e) 개도국의 인터넷 활용을 높이기 위한 방법을 이해당사자에 제공 f) 인터넷 거버넌스 매커니즘에 개도국의 이해당사자 참여 독려 g) 떠오르는 이슈를 정의하고 이와 관련된 기구와 협의체에 적절한 대응책 격려 h) 지역별 노하우, 지식을 활용하여 개도국에서의 인터넷 거버넌스 능력제고 i) 현재 상태에서 인터넷 거버넌스 절차에서 WSIS 원칙 구체화 j) 주요 인터넷 요소 관련 문제 토론 k) 인터넷 활용 및 악용 관련 특히 매일 사용자의 관심과 관련된 이슈 해결방안 모색 l) 프로시딩 공개
73. a) 정부, 기업, 시민단체, 국제기구들이 참여한 모든 이해당사자들간 상호보완을 강조한 인터넷 거버넌스의 구조 구축 b) 정기적 리뷰가 가능하도록 가볍고 탈중심적인 구조로 운영 c) 관련 주요 UN 회의와 함께 개최하여 정기적인 회의 개최를 통해 효율성 제고

표 5 튀니스 어젠다 중 IGF의 목표 및 운영방식

(2) IGF, 독특한 글로벌 거버넌스의 한 형태

IGF는 지난 8회에 걸쳐 다양한 이해당사자들의 참여 하에 인터넷을 중심으로 정보인권에서 기후변화에 이르기까지 다양한 현안을 두고 IGF 회의 기간을 이용해 집중적으로 논의를 진행하는 독특한 방식의 공론장을 형성해 왔다. 이는 1 국가 1 의결권이라는 전통적 의사결정방식과는 다른 것이며, 글로벌 거버넌스의 실험적인 운영 방식이라고 평가할 수 있다. 사실 IGF가 추구하는 멀티스테이크홀더리즘이란 용어는 그 의미상 반드시 인터넷 거버넌스 분야에만 한정되어 사용될 필요는 없으나 엄밀한 의미의 멀티스테이크홀더리즘이 구현되는 영역은 현재로서는 인터넷 거버넌스 분야가 거의 유일하다고 볼 수 있다.

예컨대 글로벌 환경 거버넌스의 주요 의제인 '온실가스 감축'의 경우만 해도 온실가스 감축의 실질적 의무자인 온실가스 다배출 기업과 시민사회 등 비 국가행위자들의 적극적인 참여가 요구되고 있고, CAN(Climate Action Network, CAN)과 같은 시민사회의 전문성과 지식이 협상의 주도적인 역할을 하고 있다.[83] 그러나 기후변화와 관련한 글로벌 환경 거버넌스의 경우 기본적으로 유엔의 '기후변화에 관한 유엔기본협약(United Nations

Framework Convention on Climate Change, 이하 "UNFCCC")'이 주도적인 역할을 하고 있다고 보아야 한다. 각 국가들은 국가별 온실가스 감축량을 설정하고, 할당된 온실가스를 국가단위로 감축해야하기 때문에 온실가스 감축 의제의 일차적인 의사결정 주체는 여전히 개별 주권 국가인 것이다. 결국 글로벌 환경 거버넌스의 경우와 같이 시민사회, 전문가 집단 등과 국가가 협력적인 거버넌스 체제를 구축하는 분야는 많지만 멀티스테이크홀더리즘에서처럼 국가가 시민사회와 동등한 이해당사자의 하나로서 참여하는 국제적 공론장은 전체 글로벌 거버넌스 체제에서 매우 독특한 지위를 획득하고 있다고 하겠다.

물론 IGF의 경우 IGF라는 명의로 공식적인 결과물이 도출되거나, 별도의 정책 보고서를 발간하는 절차가 존재하지 않고 일련의 워크샵들로만 진행되어 이른바 '말 잔치'나 '덕담'(happy talk)을 나누는 곳에 불과하다는 지적에서 자유로울 수 없다. 반면 국가 간 공식적인 의사결정 과정에서 발생하는 의사결정의 경직성이나 국가 간 이해관계의 극명한 대립에 따른 논의의 고착(deadlock)에서 다분히 자유롭다는 점은 IGF 공론장이 가진 장점에 해당한다. IGF가 추구하는 멀티스테이크홀더리즘(multistakeholderism)은 국가간 다자주의적 의사결정방식(multilateralism)보다 다양하고 유연한 관점에서 구체적인 논의가 가능하고, 경우에 따라서는 이를 반영한 자발적인 결과물이 도출될 가능성도 함께 배태하고 있다. 실제로 IGF에 참여하고 있는 DC on Net Neutrality의 경우 유럽 평의회(Council of Europe) 담당자를 포함한 각 국의 이해당사자들이 망중립성 법안 등에 활용할 수 있는 망중립성 모델 프레임워크(Model Framework on Net Neutrality)를 도출하여 제8회 IGF에서 발표하였고, 이러한 과정은 별도의 보고서[84]를 통하여 정리, 발간되었다. 이처럼 다양한 이해당사자의 참여가 전제된 IGF에서 특정 주제의 논의과정 및 결과물이 정책 보고서의 형태로 정리되는 경우, 일국 차원의 정책형성 과정에서도 구체적인 근거 자료로 활용될 수 있다고 판단된다.

(3) 다자주의(multilateralism)와 멀티스테이크홀더리즘(multistakeholdersim)의 간극 : 서울 사이버스페이스 총회

다자주의 의사결정방식이 가진 경직성이나 시민사회 등 이해당사자들의 제한된 참여를 극복하기 위하여 다자주의적 의사결정 방식과 시민사회와의 광범한 협력을 동시에 추구하려는 시도도 나타나고 있다. 그 대표적인 사례가 본 보고서의 서두에서 언급한 바 있는 사이버스페이스 총회이다. 2011년부터 진행된 사이버스페이스 총회는 장관급 회의의 성격이 짙어, 다분히 다자주의적인 의사결정 방식을 채택하고 있었으나, 2013년에 개최된 제3회 서울 사이버스페이스 총회의 경우 아래 그림 8의 제3항에서 보듯 기획 단계에서부터 시민사회와의 협력 강화(strengthening public-private partnership)를 특히 강조하였다.

---

83) <법적 측면에서 본 글로벌 환경거버넌스 - 기후변화협약체제를 중심으로>, 차경은, 법학연구(연세대학교 법학연구원) (2012).

84) <A discourse-Principle Approach to Network Neutrality: A Model Framework and its Application>, Luca Belli and Matthijs van Bergen (2013).

그림 8 서울 사이버스페이스 총회의 지향 (출처: 서울 사이버스페이스 총회 공식 홈페이지)

그러나 결론부터 이야기 하자면 서울 사이버스페이스 총회는 다자주의적 의사결정 방식에서 크게 벗어나지 못하였으며, 본 총회의 결과물로 제시된 서울프레임워크 (Seoul Framework for and Commitment to Open and Secure Cyberspace, 이하 "서울프레임워크") 역시 시민사회에 폭넓은 참여기회가 제공되지 않은 채 도출되었다.[85] 서울 프레임워크의 초안이 사전에 시민사회에 공개되지도 않았으며, 서울 프레임워크에 대하여 시민사회에서 의견을 제시할 수 있는 의견수렴과정 역시 존재하지 않았다.[86] 결국 서울 프레임워크의 도출 과정에 대해서는 총회 의장 요약(Chair's Summary)에서 간단하게 언급되는 수준으로 공개되었고, 그마저도 시민사회와의 협력에 대한 언급보다는 '국가' 단위의 논의와 참여가 중심이 되었던 것으로 정리하고 있다.[87]

이는 사이버스페이스 총회가 기본적으로 장관급 회의의 성격을 띠고, '사이버 보안(Cyber Security)' 이슈가 중심이 되는 회의라는 점에서 어느 정도 예견된 결과이기도 하다. 그러나 시민사회와의 협력을 강화하겠다는 당초의 목표에 비추어 평가해보면, 제3회 서울 사이버스페이스 총회가 당초 계획했던 목표 수준을 충분히 달성하였다고 보기는 어렵다. 오히려 서울 사이버스페이스 총회 사례는 다자주의와 멀티스테이크홀더리즘의 간극은 매우 크며 두 가지 의사결정 방식을 단순히 물리적으로 결합하는 기획이 생각만큼 용이하지 않다는 점을

85) 실제로 한국에 인터넷을 도입하는 역할을 한 인터넷 분야 전문가 및 인터넷 거버넌스 분야에서 오랫동안 활동해온 시민사회 활동가 모두 서울 사이버스페이스 총회 참석에 요구되는 PIN 번호를 받지 못하여 총회에 참석하지 못할 처지에 놓여있다가, 사무국에 강력하게 항의를 한 활동가에게만 PIN 번호가 뒤늦게 발급되는 해프닝이 발생하였다. 결국 해당 인터넷 전문가는 PIN 번호가 없어 총회에 참석할 수 없었다고 한다.

86) 물론 이 과정에서 학계 등 전문가들이 자문 위원으로 참여했다고 하지만, 이를 시민사회의 광범한 참여라고 평가하거나, 서울 사이버스페이스 총회가 추구했던 강화된 협력모델(public-private partnership)의 모범적인 사례로 보기에는 무리가 있다.
(http://www.mofa.go.kr/webmodule/htsboard/template/read/korboardread.jsp?boardid=235&seqno=346286&typeID=6)

87) We have been pleased to welcome a wide range of stakeholders from governments, industry, civil society and the youth. Delegates from 87 countries, including 43 ministers and vice-ministers, attended. We are especially pleased to have welcomed many more delegates from developing countries this year.Together, we identified a number of the key policies, actions, and best practices necessary to realize the economic and social benefits of cyberspace, and to ensure that they are made available for all.

We found areas of common ground on the elements that promote an open and secure cyberspace, and reflected them in the Seoul Framework for and Commitment to Open and Secure Cyberspace. We believe this document represents the summary of where international consensus among governments has been achieved. (서울 사이버스페이스 총회 Chair's Summary 중 관련부분 발췌)

방증하고 있다고 하겠다.

4. 결론 : IGF 논의체제의 장점을 활용한 의사결정 전략 필요

인터넷이 가지는 개방성과 최종 이용자(end-user)가 중심이 되는 특성을 고려한다면, 인터넷 거버넌스를 논의하기 위해서는 그 기본 전제로 최종 이용자가 논의과정에 반드시 포함되어야 한다. IGF는 이를 위하여 이해당사자의 광범한 참여와 자발적인 노력으로 구현되는 글로벌 거버넌스 체제를 구축해왔고, 멀티스테이크홀더리즘이 구현된 대표적 인터넷 거버넌스 공론장의 하나로 평가받고 있다. 한편 IGF에는 특정 주제에 대한 심도 있는 정책 논의를 위한 기구나 의사결정 기제가 부재하고, 회의를 통하여 구체적인 보고서도 생산되지도 않아 다분히 현상유지(Status Quo)적 성격이 크다는 비판을 듣고 있다. 즉, IGF에 구현되고 있는 멀티스테이크홀더리즘이 ICANN 등 다른 인터넷 거버넌스 공론장들이 구현하는 그것에 비해 반드시 우월한 것이라고 단정 짓기는 어려운 것이다.

하지만 IGF는 다자주의적 논의 체제 하에서는 구현하기 어려운 자유롭고 참여 촉진적인 성격의 공론장을 제공하고 있는 것은 분명하다. 이는 앞서 언급한 사이버스페이스 총회의 사례에서도 잘 드러난 바 있다. IGF는 회의의 기획단계 부터 운영에 이르기까지 다양한 이해당사자들이 참여할 수 있는 기회를 열어두고 있으며, 회의에서 제시된 이해당사자들의 다양한 의견들은 빠짐없이 기록되고 인터넷을 통하여 투명하게 공개되고 있다. 또한 IGF 사무국은 개발도상국이나 저개발국 이해당사자의 참여를 보장하기 위하여 원격 참가에도 역시 많은 공을 들이고 있는 것이다. 따라서 시민사회를 포함한 각 이해당사자들에게는 인터넷 거버넌스 공론장으로서 IGF가 가지는 장점을 최대한 활용하고 향후 IGF의 발전 방향을 설정하는데 적극적으로 참여하는 등 전략적인 접근방식이 요구된다.

요컨대 IGF 논의에 참여가 활발한 서방 선진국 등 일부의 이해관계가 과대 대표된다는 지적은 유효하나, 반대로 이는 그동안 IGF에 참여하지 않았던 이해당사자들이 적극적으로 참여해야 하는 필요성을 역설하고 있기도 하다. 한국의 최종 이용자를 대변하는 시민사회가 적극적으로 제8회 IGF에 참여했던 것도 이와 맥이 닿아있다. 향후에는 IGF 뿐 아니라 예컨대 2014년 개최 예정인 인터넷 거버넌스에 대한 브라질 회의(Global Multistakeholder Meeting on Internet Governance, GMMIG) 등 인터넷 거버넌스의 새로운 틀을 짜기 위한 기획 과정까지 그 참여의 폭을 넓혀나가야 할 것이다. 한편 전략적인 접근 측면에서 평가한다면, 한국의 국가인권위원회가 2013년 제8회 IGF에서 다양한 워크샵 등 제반 행사 일정에 직접 참여했다는 것은 큰 의미를 가진다고 할 것이다. 국가인권위원회는 IGF 참여를 통해 시민사회를 포함한 세계의 다양한 이해당사자들과 교류하고, 정보인권을 다루는 다양한 논의 과정에 참여할 수 있었기 때문이다. 이러한 경험은 국가인권위원회가 정보인권 분야의 국제적인 흐름을 파악하고 정보인권 정책을 형성하는 데에 매우 적확한 자산으로 기능할 것이다. 향후에는 국가인권위원회가 IGF 내에서 직접 워크샵이나 오픈 포럼을 주재하여 아시아 지역뿐 아니라 국제 정보인권정책 논의를 선도해나가기를 기대해본다.

ABSTRACT

The meaning of IGF in the context of global governance model

Jihwan Park[88)]

An essential prerequisite for negotiating governance of 'internet,' a world of 'end to end' nature, is to guarantee end-users' participation. Internet Governance Forum (IGF), the outcome of World Summit on the Information Society(WSIS) Tunis Agenda, has played an important role as a representative mulitistakeholder - based governance model, which puts emphasis on wide range participation of stakeholders. Notwithstanding multistakeholderism materialized in IGF has been challenged, IGF itself is a unique place for participation to broad internet governance discourse, as all voices get hearing grounded on openness, inclusion, and transparency, quite distinct from the multilateral negotiation based model such as 'Conference on Cyberspace.' Therefore civil society which represents end-users' interest, as a crucial stakeholder of internet governance, should establish more strategic and coordinated approach to IGF itself as well as reformation discourse of internet governance. In this regard, civil society groups of Korea, began with hosting workshops and Open Forum at the 2013 IGF in Bali, Indonesia. This report also describes the detailed activities of Korean civil society group in 2013 IGF.

88) Attorney at Law, Heyum Law Office Advisory Lawyer of OpenNet Korea

한국 내 인터넷 거버넌스 형성과 인터넷주소에 관한 법률

윤복남[89]

1. 들어가며

최근 '인터넷 거버넌스'라는 주제에 대해 많은 논의가 전개되고 있다. 국제적으로는 ITU 등에서 도메인이름을 더 이상 민간기구에서 관리하는 것이 아니라 국가간 기구나 국제기구에서 이를 관리해야 한다는 것에서부터, 국내에서는 정보통신부, 방송통신위원회에 이어서 미래창조과학부에서 인터넷 분야를 관장하면서 국내 인터넷 거버넌스를 어떻게 운영할 것인지에 대해 논의가 다양하다.

그런데, 하나 주목할 것이 있다. 한국 내에서의 인터넷 거버넌스에 관한 다양한 의견에도 불구하고 한국에서는 꽤 일찍 이에 대한 법률적 정비가 이뤄졌다는 점이다. 즉, 인터넷 거버넌스에서 민간참여의 폭에 대해 일부 논의가 되더라도 이미 법률에서 정해진 범위 내에서 한계가 있다는 점이다.[90]

그렇다면, 한국 내에서 바람직한 인터넷 거버넌스를 형성하기 위해서는 이미 만들어진 '법률'이라는 제도적 틀에 대한 변경에 대해 구체적으로 검토하지 않을 수 없다.

이 글에서는 먼저 인터넷 거버넌스에서 자주 논의되는 멀티스테이크홀더 모델(multi stakeholder model)[91] 원칙에 대해 살펴보고, 이러한 관점에서 한국 인터넷 거버넌스는 어떻게 운영되고 있는지를 구체적으로 검토해 보고자 한다. 특히 인터넷 주소에 관한 법률로 어떻게 제도화되었는지에 초점을 맞춘다. 이러한 검토 이후에 바람직한 한국 인터넷 거버넌스 형성을 위한 향후 발전방향을 스케치해 보고자 한다.

---

89) 법무법인(유) 한결 변호사, 한국인터넷거버넌스협의회 주소인프라분과위원, bnyun@hklaw.co.kr

90) 본고에서는 '인터넷 거버넌스'라는 일반적 용어를 사용함에도 불구하고, 일단 '인터넷주소' 관련 정책에 국한하여 다루기로 한다. 원래의 인터넷 거버넌스는 넓은 의미에서는 인터넷 관련 정책 전반을 대상으로 하나, 본고에서는 일단 좁은 의미에서 인터넷주소 관련 정책으로 국한시키고, 이를 확대적용하는 방식을 채택하려고 한다. 현재의 세계적 논의에서도 인터넷 공공정책에 관련하여서 이와 같이 인터넷 주소를 매개로 하되, 그 영역을 넓히는 예는 많이 볼 수 있다.

91) 이를 "다자간 협의모델"이나 "다중이해당사자 모델"로 번역하곤 하는데, 원어와 그 의미가 같지 않게 보여지므로 부득이 외국어 그대로를 사용하고자 한다.

2. 분석의 기준 – 멀티스테이크홀더 모델 구현여부

멀티스테이크홀더 모델은 인터넷주소에 관한 논의에서 매우 중요한 위상을 차지하고 있다. 다양한 이해당사자들이 참여하여 의사결정을 하는 구조는 이제 ICANN 이외에도 IGF(인터넷거버넌스포럼)이나 WGEC(Enhanced Cooperation 워킹그룹) 등 여러 차원에서도 많은 원칙으로 채택되었다. 대표적으로 정부간 회의결과인 튀니스 아젠다에서 결의된 내용 역시 이러한 멀티스테이크홀더 모델에 입각하여 각 이해당사자의 역할을 명기하는 방식이다.

그런데, 이러한 멀티스테이크홀더 모델에서의 가장 중요한 점은 의사결정구조에 있다고 본다. 즉 의사결정 방식이 bottom up 프로세스인가, 의사합치(consensus) 방식이 얼마나 중시되는가가 매우 중요하다. 그렇다면 한국 인터넷 거버넌스가 얼마나 이러한 멀티스테이크홀더 모델 원칙에 입각해서 잘 조직되어 있고, 운영되고 있는가를 살펴보는 것은 의미있는 일일 것이다.

구체적인 법제도적 분석을 위하여 위와 같은 멀티스테이크홀더 모델의 구현기준을 아래와 같이 좀 더 세부적으로 나누어서 주제별로 더 상세히 살펴보고자 한다.

(1) 의사결정과정이 bottom up 프로세스 및 의사합치(consensus) 방식을 구현하고 있는가? 아니면, top down 방식인가?

(2) 누가 최종적 의사결정권을 행사하고 있는가? 주도적인 의사결정권자가 누가인가?

(3) 논의과정에 참여하는 다른 참여자는 누가 있는가?

(4) 정책자문위원회의 구성방식이 bottom up인가? 아니면, top down인가?

(5) 민간활동에 대한 정부의 지원은 활발한가?

3. 한국 내 인터넷 거버넌스 현황 요약

현재의 한국 내에서 인터넷 거버넌스에 관한 한 정부(구체적으로는 미래창조과학부)가 주도하는 top down 방식의 프로세스라는 점에 대해 누구도 부정하기는 어렵다고 본다. 2004년 제정된 인터넷 주소자원에 관한 법률(이하, '인터넷주소법')이 시행된 이후 확고부동하게 정부는 인터넷 주소를 포함한 인터넷 정책 전반에 관한 주도권을 행사해 오면서 이와 같이 의사결정을 해 왔기 때문이다. 이는 법률상 인터넷 주소관리기관으로서 별도의 '한국인터넷진흥원'(이하, '인터넷진흥원')이 있어도 마찬가지이고, 정책자문기구로서 민간으로 구성된 인터넷주소정책심의위원회가 있어도 마찬가지이다. 이는 법령상의 권한을 넘어서는 실제 정책결정 및 집행 프로세스 하나하나에서 정부(구체적으로는 미래창조과학부 인터넷정책과)가 거의 전적으로 정책에 관한 최종적인 의사결정권을 행사하고 있기 때문이다.

따라서 법령을 구체적으로 검토하기 전에 우선 실제 어떤 프로세스로 정부의 인터넷(주소)에 관한 정책이 결정되는지 그 메커니즘을 구체적으로 살펴보기로 한다.

먼저 정책의 제안은 주로 인터넷진흥원 인터넷주소센터에서 이뤄진다. ICANN 회의 의제에 대한 검토, 이에 대한 의견 및 참여범위, 국내 인터넷주소 정책에 대한 새로운 제안 등에 대해서 정책제안을 한다. 또는 미래창조과학부 담당공무원의 지시에 의하여 정책제안 자체를 연구하기도 한다.

이러한 제안을 받은 정부(미래창조과학부)는 구체적으로 이에 대한 검토를 통하여 의사결정을 하되, 필요하면 민간자문을 받기도 한다.[92]

원래 1년에 몇 차례 열리는 인터넷주소정책심의위원회가 있으나, 여기에서는 주요한 정책과제만을 심의할 뿐, 구체적으로 쟁점이 되고 있는 현안문제에 대한 자문, 심의를 진행하지는 못하고 있다. 또한, 심의위원 일부는 인터넷정책 분야의 전문성이나 다양성을 갖고 있지 못한다. 더구나 통상 분기에 1회 개최되는 회의 여부도 정부 관계자가 재량으로 정하므로 회의 개최가 생략되기도 한다.

정책을 집행하는 단위는 다시 인터넷진흥원 인터넷주소센터이다. 국제회의에 참여하거나, 국내에서 세미나를 개최하거나, 일정한 정책을 집행하는 일 모두 인터넷진흥원의 몫이다. 인터넷진흥원 인터넷주소센터에서는 비공식적으로 인터넷거버넌스협의회 주소인프라분과위원회의 자문을 받는다. '비공식적'이라는 의미는 구체적으로 어떤 공식적 자문관계를 맺지 않고 사실상 자문을 한다는 의미에서 비공식적이다. 대신 인터넷진흥원 인터넷주소센터에서 필요한 사항이 있으면 자문안건으로 제기하여 회의에 부쳐진다는 의미에서 자문을 받기는 한다는 이중적 의미를 갖는다. 그러나 비공식적 자문이다 보니, 이 회의에는 인터넷진흥원 인터넷주소 책임자나 정부 정책담당자가 지속적으로 참여하지는 않는다.[93]

결국 특정한 의사결정이 필요할 때 정부 담당공무원의 재량에 따라 일부 민간전문가를 초청하여 자문을 구하는 경우는 있으나, 공식적으로는 인터넷주소정책심의위원회의 일정한 범위의 제한된 심의 외에는 거의 모든 이슈에 대해 미래창조과학부의 업무분장에 따른 담당공무원에 의하여 한국 인터넷주소에 관한 정책이 결정되고 있고, 이를 한국인터넷진흥원 인터넷주소센터에서 보좌하고 집행하고 있다고 요약된다.

4. 한국 인터넷 거버넌스를 뒷받침하는 현재의 법률체계 – 인터넷주소법 등

앞서 한국에서의 인터넷주소에 관한 정책이 어떻게 결정되고 있는지의 현황을 묘사한 바, 이를 뒷받침하는 법률이 인터넷주소법이다. 그런데, 한 가지 주목할 것은 인터넷주소법이나 다른 법령에서 명시적으로 정부의 의사결정권을 언급하고 있는 것은 아니라는 점이다. 이하

92) 2012년 신규 gTLD의 도입을 앞두고 비정기적인 자문회의가 개최된 바 있다. 필자는 2차례의 자문회의에 참여한 바 있는데, 이 회의는 정부 담당자의 일방적 지명에 의하여 누가 참석할지 정해지고, 주제 및 토의도 회의 당일에야 알 수 있다. 따라서 사전에 의안을 검토하거나, 지속적인 회의로 진행되지는 못하였다.

93) 이는 과거 2003년 이전의 인터넷주소위원회와 확연하게 구별된다. 당시 인터넷주소정책기구로서의 인터넷주소위원회는 정부관계자 및 한국인터넷정보센터(당시 재단법인) 도메인이름 팀장이 꼬박꼬박 참석하여 보고 및 안건토의를 진행하였다. 이는 당시 인터넷주소위원회는 인터넷주소에 관한 정책에서 일정한 '공식적' 지위를 갖고 있었기에 가능하였다.

에서 구체적으로 살펴보겠다. 아래의 분석은 앞서 검토한 멀티스테이크홀더 모델의 구현여부를 소주제별로 구체적으로 검토하기로 한다.

(1) 정책결정권

인터넷주소 정책에 관한 최종적인 의사결정권에 대해 인터넷주소법에 명시되어 있는 것은 아니다. 즉, 인터넷주소법에서 명시적으로 국가가 모든 인터넷정책을 관장한다고 언급되어 있는 것은 아니다. 국가는 인터넷 주소에 관한 기본계획을 수립, 시행할 의무가 있다고만 명시되어 있다. 따라서 기본계획의 수립과 시행 이외에 구체적인 인터넷정책 모두가 정부의 권한인 것은 아니다. 그러나 이 법이 시행된 이후 사실상 국가의 권리이자 의무인 것으로 해석하여 운용되고 있고, 여기에 어떤 이의도 제기되지 않고 있다.[94]

제3조(국가의 책무)
① 국가는 인터넷주소자원의 개발과 이용을 촉진하고 인터넷주소가 공정하고 적절하게 사용될 수 있도록 노력하여야 한다.
② 국가는 인터넷주소자원 관련 정책이 투명하고 민주적으로 수립·시행되도록 노력하여야 한다.
제5조(기본계획의 수립·시행)
① 미래창조과학부장관은 인터넷주소자원의 개발과 이용촉진 및 관리에 관한 기본계획(이하 "기본계획"이라 한다)을 수립·시행하여야 한다.
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 인터넷주소자원의 개발·이용촉진 및 관리를 위한 기본목표
2. 인터넷주소자원의 현황과 수급에 관한 사항
3. 인터넷주소자원의 개발과 표준화에 관한 사항
4. 인터넷주소의 사용자 보호와 분쟁해결에 관한 사항
5. 인터넷주소자원과 관련한 국가·지방자치단체 및 민간의 협력에 관한 사항
6. 인터넷주소자원과 관련된 국제협력에 관한 사항
7. 인터넷주소자원의 개발과 이용촉진 및 관리를 위한 재원의 조달 및 운용에 관한 사항
8. 그 밖에 인터넷주소자원의 개발과 이용촉진 및 관리에 관한 사항

한편, 미래창조과학부의 직제규정에서는 아래와 같이 정해져 있다.

미래창조과학부와 그 소속기관 직제(대통령령)
제18조(정보화전략국)
③ 국장은 다음 사항을 분장한다.
42. 인터넷 관련 법·제도 운영, 전문지원기관의 육성·지원 및 인터넷서비스에 대한 규제 선진화
43. 인터넷주소자원 확산을 위한 정책의 수립·추진
44. 인터넷주소자원 이용 촉진을 위한 기술개발, 표준화, 인력양성, 시범서비스에 관한

94) 이러한 관점에서 인터넷주소법 자체가 문제가 아니라, 이를 운용하고 있는 메커니즘이 문제라는 견해도 있다.

사항
45. 차세대 인터넷주소자원의 개발, 이용촉진 환경 조성 및 지원에 관한 사항

미래창조과학부와 그 소속기관 직제 시행규칙(미래창조과학부령)
제14조(정보화전략국)
⑦ 인터넷정책과장은 다음 사항을 분장한다.
1. 인터넷 이용기반의 확충, 이용활성화 및 국제협력
2. 인터넷 이용환경 개선 및 이용자 보호
3. 인터넷 관련 법·제도의 정비
4. 인터넷 정책 관련 전문지원기관의 육성·지원
5. 인터넷서비스에 대한 규제선진화 정책의 수립·시행
6. 인터넷 사업자 자율규제 및 사업자간 협력 지원
7. 인터넷주소자원 확산 기본계획의 수립·추진
8. 인터넷주소자원 이용 촉진을 위한 기술개발, 표준화, 인력양성, 시범서비스에 관한 사항
9. 인터넷주소 분쟁조정 및 주소자원 사용자 보호
10. 차세대 인터넷주소자원의 개발 및 이용 촉진

그런데, 이러한 직제규정이 곧바로 해당 업무의 의사결정권을 의미하는 것은 아니다. 즉, 말 그대로의 업무분장으로서 각 주제별로 담당공무원이 누구인지를 정하는 의미만 있고, 해당 주제의 의사결정권을 정하는 취지는 아니다. 그러나 한 가지 유의할 것은 현실에서는 앞서 살펴본 바와 같이 해당 업무에 대한 정책결정권을 실제 갖고 있는 것으로 운용되고 있다는 점이다.

(2) 정책심의위원회 – 구성과 역할

한편, 인터넷주소법 제3조 제2항에서 정한 투명하고 민주적인 정책수립을 위하여 아래와 같이 민간위원회의 정책심의를 받도록 정해져 있다.

제5조(기본계획의 수립·시행)
③ 미래창조과학부장관은 기본계획을 수립하는 때에는 제6조에 따른 인터넷주소정책심의위원회의 심의를 거쳐야 한다.
제6조(인터넷주소정책심의위원회)
① 인터넷주소자원에 관한 정책 등을 심의하기 위하여 미래창조과학부 소속으로 인터넷주소정책심의위원회(이하 "심의위원회"라 한다)를 둔다.
② 심의위원회는 다음 각 호의 사항을 심의한다.
1. 기본계획의 수립·시행에 관한 사항
2. 제9조에 따른 인터넷주소관리기관 업무위탁의 승인에 관한 사항
3. 제13조에 따른 인터넷주소관리준칙의 승인에 관한 사항

4. 인터넷주소와 관련된 분쟁의 해결을 위한 주요 정책에 관한 사항
5. 인터넷주소자원과 관련된 주요 국제협력에 관한 사항
6. 그 밖에 인터넷주소자원과 관련된 주요 정책사항으로서 위원장이 부의하는 사항
④ 심의위원회의 위원은 인터넷주소자원에 관한 학식과 경험이 풍부한 자로서 다음 각 호의 어느 하나에 해당하는 자 중에서 미래창조과학부장관이 위촉 또는 지명한다.
1. 3급 이상의 공무원 또는 이에 상당하는 공공기관의 직에 있거나 있었던 자
2. 판사·검사·변호사 또는 변리사의 직에 10년 이상 있거나 있었던 자
3. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 5년 이상 있거나 있었던 자로서 정보통신분야를 전공한 자
4. 정보통신관련 기업의 임원의 직에 5년 이상 있거나 있었던 자
5. 정보통신관련 단체 또는 기관의 대표자의 직에 있거나 있었던 자
6. 그 밖에 위와 동등한 자격이 있다고 미래창조과학부장관이 인정하는 자

그런데, 민간위원회의 구성 측면을 보면, 미래창조과학부장관이 일방적으로 위촉 또는 지명하도록 되어 있다(위 법 제6조 제4항). 따라서 다양한 의견을 수렴하여 민주적으로 구성하는 절차를 거치지 않는다면, 미래창조과학부 장관이 일방적으로 구성하여 실질적인 민간부문의 목소리를 제대로 반영하지 못하는 방식으로 구성될 수 있는 한계가 있다. 또한 운영측면을 살펴보면, 앞서 지적한 바와 같이 실질적인 운영이 정부에 맡겨져 있으면서 그 횟수나 운영방식 등에서도 충분한 정책심의는 이루어지지 않고 있다고 본다.

(3) 정책집행기관(인터넷주소관리기관)

인터넷 관련 정책의 집행은 한국인터넷진흥원이 맡고 있다. 이는 2004년 인터넷주소법이 신설되기 이전에 재단법인 한국인터넷정보센터의 재산, 권리, 의무를 모두 승계하여 설립된 조직이다.[95]

인터넷주소법 부칙 제2조 (재단법인 한국인터넷정보센터에 관한 경과조치)
①이 법 시행 당시 재단법인 한국인터넷정보센터(이하 "정보센터"라 한다)는 이사회의 의결을 거쳐 그의 모든 권리 및 의무를 제9조의 규정에 의하여 설립되는 한국인터넷진흥원이 승계할 수 있도록 정보통신부장관에게 이에 관한 승인을 신청할 수 있다.
②제1항의 규정에 의한 신청에 의하여 승인을 얻은 정보센터는 이 법에 의한 진흥원의 설립과 동시에 민법 중 재단법인의 해산 및 청산에 관한 규정에 불구하고 해산된 것으로 보며, 정보센터에 속하였던 모든 재산·권리 및 의무는 이 법에 의하여 설립되는 진흥원이 이를 승계한다.
③이 법 시행 당시 정보센터의 직원은 제1항의 규정에 의한 정보통신부장관의 승인을 얻은 날부터 진흥원의 직원으로 본다.

95) 부칙 제2조에 의한 규정을 일종의 수용으로 보는 견해가 있다. 즉, 민간조직을 정부에서 공적 목적으로 수용한 경우라고 해석하는 견해이다. 다만, 부칙 제2조 제1항에 의하여 재단법인 이사회에서 스스로 의결하여 승계를 요청한다는 내용이 있어서 법에 의해 강제적으로 수용당하는 경우와는 구별된다. 그러나, 이러한

이와 같이 신설된 한국인터넷진흥원은 다른 기능과 함께 통합되면서 여러 차례 조직 확대를 꾀하게 된다. 현재의 한국인터넷진흥원은 다음 법률에 의해 설립된 특수법인이다.

> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제52조 (한국인터넷진흥원)
> ① 정부는 정보통신망의 고도화(정보통신망의 구축·개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)을 설립한다.
> ③ 인터넷진흥원은 다음 각 호의 사업을 한다.
> 5. 정보통신망의 정보보호 및 인터넷주소자원 관련 기술 개발 및 표준화
> 17. 「인터넷주소자원에 관한 법률」에 따른 인터넷주소자원의 관리에 관한 업무
>
> 인터넷주소법 제2조(정의)
> 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> 3. "인터넷주소관리기관"이란 인터넷주소의 할당·등록 등과 관련된 업무를 수행하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)과 인터넷진흥원으로부터 인터넷주소 관리업무를 위탁받은 법인 및 단체를 말한다.[96]

결국 인터넷진흥원은 인터넷정책에 관한 모든 영역에 대한 '관리'업무를 맡고 있다. 그런데, 이는 정부산하기관이자 특수법인으로서 정부가 설립자이고, 실질적으로 정부의 감독을 받을 수밖에 없는 기관이다. 따라서 대내외적으로 이를 비정부조직이라고 말하기는 어렵다. 즉, 독립성 있는 조직에 의하여 정책이 집행된다고 말하기는 어렵다.

(4) 민간활동에 대한 지원

인터넷주소법에서는 민간활동에 대한 지원을 국제협력의 범위로 한정하여 아래와 같이 정하고 있다.

> 제8조(인터넷주소자원에 관한 국제협력)
> ② 미래창조과학부장관은 인터넷주소자원에 관한 민간부문의 국제협력활동을 지원할 수

절차를 거쳤다고 하더라도 실질적으로는 재단법인의 재산을 국가 산하기관(특수법인)으로 흡수한 것은 분명한 만큼 충분한 행정법적 검토가 필요할 수 있다. 특히 재정적으로 도메인이름 등록자들로부터 받은 수수료로 운영되던 민간조직의 재산 모두를 승계하게 된 결과, 해당 재산의 사용권한이 명시적으로 정부산하기관에 귀속되어 운영되고, 도메인이름과 직접 관련되지 않는 활동에 대한 예산으로 전용되는 점에 대해서는 비판적인 문제제기가 많다.

96) 인터넷주소법 제9조(인터넷주소관리기관의 업무위탁)에서는 다음과 같이 정하고 있다.
"인터넷진흥원은 인터넷주소관리기관의 업무를 인터넷주소별로 구분하여 미래창조과학부장관의 승인을 받아 대통령령으로 정하는 법인 및 단체에 위탁할 수 있다."
그러나, 현재 한국에서 인터넷주소 관리 업무를 위탁받은 다른 인터넷주소관리기관은 없다.

있다.

시행령 제9조(민간부문 국제협력활동의 지원)
미래창조과학부장관은 법 제8조제2항에 따라 다음 각 호의 사항과 관련된 민간부문의 국제협력활동을 지원할 수 있다.
1. 인터넷주소자원과 관련된 정보·기술·인력의 교류
2. 인터넷주소자원에 관한 공동연구, 기술협력 및 국제표준화의 추진
3. 인터넷주소 관련 국제기구에 대한 참여 및 대응전략의 수립
4. 인터넷주소 관련 국제회의의 국내 유치
5. 그 밖에 인터넷주소자원의 안정적 운영과 확충을 위하여 필요한 국제협력의 증진

5. 바람직한 한국 인터넷 거버넌스 형성방향

정부가 인터넷 거버넌스에서 일정한 역할을 맡고 있음은 부인할 수 없다. 특히 공공정책에 관련한 이슈에서 정부는 적극적으로 개입하여 의견을 개진하고, 최대한 '공공적으로' 귀결되도록 최선의 노력을 경주해야 할 것이다.

그러나 반면 민간부문의 참여가 배제된 상태에서 정부가 일방적으로 결정하는 방식의 폐해는 그 동안 꽤 지적되어 왔다. 정부만의 독단적 결정으로는 변화하고 복잡다단한 인터넷 세계의 정책을 제대로 다루기에는 한계가 있을 수밖에 없다. 따라서 민주주의의 일반 원칙에 의하여 투명하고, 공개적으로 의사결정을 하자는 것이고, 다양한 민간부분 이해당사자들이 정책결정과정에 직접 참여할 경우 정책 내용도 충실해지고, 사회적 합의를 이끌어 내기에도 적합하다고 본다.

이러한 관점에서 보았을 때 현재 한국 인터넷 거버넌스의 운영현황에서는 민간부문의 정책결정과정 참여와 의견수렴절차 마련이 초미의 과제라고 본다. 특히 그 동안의 정책결정이 사실상 정부에 의해 주도되었다는 반성을 하면서 적극적인 민간참여 의사결정 구조를 만들 필요가 있다. 이를 구체적인 제도로 구현하려면 독립적인 정책위원회의 도입을 검토하여야 한다고 본다. 이러한 정책위원회는 인터넷 주소정책 수립(혹은 인터넷 정책 일반으로 넓힐 수도 있음)에 관한 최고 의사결정기구로서 정부관계자도 해당 위원회의 멤버로 참여하고, 민간부문에서도 NGO, 이용자, 업계, 기술전문가, 정책전문가 등의 다양한 이해당사자가 참여하여 정책형성과정에서 의견수렴을 하고, 동시에 이에 의해 결정된 정책에 대해서는 일정한 구속력을 부여하여 실질적으로도 최고 의사결정 기구의 역할을 하게 하는 것이다.[97]

원칙적인 의미에서 이는 인터넷 거버넌스의 민간이양의 관점에서 이뤄져야 한다. 즉, 정

97) 한편, 독립적이고 제도화된 정책위원회는 현 단계에서 적절하지 않다는 견해도 있다. 정부 부문에서는 이러한 법제도화된 위원회가 부담이 되고, 민간부문에서도 참여하기 부담이 있으므로 느슨한 형태의 포럼(예컨대 한국인터넷거버넌스포럼)을 분기별로 개최한다든가 하는 방안이 검토될 수도 있다. 혹은 이와 달리 기존의 인터넷주소정책심의위원회를 그대로 활용하여 실질화하거나, 2004년 도입된 바 있는 인터넷주소정책실무위원회를 도입하여 멀티스테이크홀더 모델을 구현해 보자는 견해도 있다. 후자의 견해는 제도화된 방식이 갖는 장점을 고려한 것이므로 향후 여러 방향에서 열린 논의가 필요하다고 본다.

부가 주도하는 인터넷 거버넌스가 아니라, 정부와 민간이 협력하는 협치(協治)의 관점으로 변화가 이뤄져야 할 것이다.

아울러 정책집행에 있어서도 인터넷주소관리기관의 독립성이 강조되어야 한다. 현재의 한국인터넷진흥원은 정부산하기관으로 지나치게 정부의 구체적 지휘, 감독 하에서 운영되어 있어서 형식적, 실질적 독립성이 거의 없다. 따라서 이를 실질적으로 독립적으로 운영하기 위한 조치가 연구되고 실행되어야 한다. 당장에 이를 성취하기 어렵다면, 인터넷주소법 제9조를 적용한 업무위탁을 통하여 민간조직(예컨대 도메인 관련 회사)에서 특정 인터넷주소의 관리를 수행하게 하는 방식도 검토할 필요가 있다.

이러한 방향에서 몇 가지 실무적 과제를 제안하면 다음과 같다.

첫째, 독립정책위원회의 법제도화에 대해 구체적으로 연구해야 한다. 즉, 멀티스테이크홀더 모델을 구현하는 방식의 정책단위를 독립정책위원회로 할지, 인터넷거버넌스포럼으로 할지, 아니면 기존 인터넷주소정책심의위원회를 실질화 할지의 방향을 먼저 정하고, 아울러 법제도화 여부에 대해 검토하여야 할 것이다. 또한 넓은 의미의 인터넷정책과의 연계성을 고려하여 인터넷주소 이외에도 프라이버시 보호, 사이버 보안, 망중립성 등 다양한 인터넷 이슈를 포괄하는 광의의 "인터넷거버넌스(정책)위원회"로 주제를 확대하는 것도 충분히 고려되어야 할 것이다.

둘째, 정책위원회의 민간위원 선임에 관련하여 bottom-up 프로세스에 의한 추천절차 및 다양성 보장방안에 관한 연구가 필요하다. 그 동안의 정부관련 위원회에서는 관례적으로 민간위원을 일방적으로 top-down 방식으로 위촉하거나 지명하는 방식으로 진행된 바, 이러한 방식으로는 민주적 구성이나 다양성 어느 측면에서도 문제가 많다고 본다.[98] 따라서 어떤 방식으로 민간위원을 추천받거나 선임할지에 대한 현실적이고 구체적인 방법 연구가 필요하다.[99] 이런 면에서 좀더 느슨한 형식의 인터넷거버넌스포럼이 민간참여를 독려하기에 부담이 적고 자유롭다는 장점이 있다고 본다. 다만, 포럼의 경우 어떤 의사결정을 할 수 있을지, 혹은 제도화가 안 될 경우 조직적 안정성이 보장될지 등의 문제가 검토되어야 할 것이다.

셋째, 민간활동 지원에 대한 일관적, 장기적 정책마련이 필요하다. 특히 국제활동 분야에서는 지속적 활동을 하지 않는 한 인터넷 거버넌스에 관한 민간전문가가 양성되기 어렵다. 그렇다면 민간전문가를 양성하기 위한 장기적 정책을 마련하여 이를 일관적으로 추진할 필요가 있다. 아울러 국내활동에서도 민간분야가 활성화되도록 여러 방면의 지원을 할 필요가 있다고 본다.

---

98) 위원 구성의 다양성에 관련하여 참고할만한 케이스가 브라질 Internet Steering Committee 이다. 이 위원회는 인터넷정책에 관한 논의를 하는 위원회인데, 정부 관련부처 9명, 기업체 4명, 제3섹터 4명, 과학기술 커뮤니티 3명, 인터넷전문가 1명으로 합계 21명으로 구성되어 있다(www.cgi.br 참조).

99) 과거 2004년 이전 인터넷주소위원회를 선임하기 위해서 인터넷이용자들 중 투표권을 신청한 자를 대상으로 투표를 통하여 위원을 선임한 예가 있다. 각 분야별로 추천절차나 투표절차 등을 구체적으로 마련할 수 있을 것이다.

6. 맺음말

인터넷 거버넌스에 관한 논의가 세계적으로 급박하게 진행하고 있는 상황에서 한국 내에서도 바람직한 인터넷 거버넌스를 형성하기 위하여 다양한 논의가 필요하다고 본다. 이미 2004년 인터넷주소법이 제정된 지 10년이 지난 상태에서 그 성과와 한계를 정확히 진단해 보고, 어떻게 하면 다양한 이해당사자를 적극적으로 참여하게 하여 잘 된 의사결정을 할 것인지를 짚어보는 것은 국제적 인터넷 거버너스 논의에 참여하기 위한 필요조건이기도 하다.

ABSTRACT

Suggestion on Korean Internet governance system by multi stakeholder approach and Introduction of Korean Internet address law

Boknam Yun[100)]

This article consists of 3 parts. Part I is multi stakeholder approach on Internet governance system. Part II is analysis of the Korean Internet governance system. In this part, I explain relevant laws in Korea, including Korean Internet Address Resources Act. Part III is my suggestion on Korean Internet governance system using a multi stakeholder approach.

First of all, the keyword of the Internet governance system is decision making process: that is, consensus based versus top-down approach. Then who are major players in Internet governance in national level? Government, or Private sectors such as business and civil society.

Korean legal system for Internet governance shows a top-down decision making process. Major players are the government (that is, Ministry of Science, ICT and Future Planning) and KISA affiliated with the government. Other players include Internet Address Policy Committee, Korea Internet Governance Alliance, and NGOs.

The key statute for Internet governance in Korea is Internet Address Resources Act of 2004. Articles 3 and 5 require the Ministry of Science, ICT and Future Planning to take a proactive role in Internet governance. The government shall consult with the Internet Address Policy Deliberation Committee for Internet governance. Yet this Committee is established under the control of the Ministry of Science, ICT and Future Planning. All members of this Committee are also commissioned or nominated by the Chairman of the Ministry. Meanwhile, there are also non-official organizations, including Sub-committee on Address & Infrastructure of Korea Internet Governance Alliance.

I suggest to reform decision making process of Korean Internet governance system based on BOTTOM-UP process for CONSENSUS BASED DECISION. My suggested system includes the following: (1) The government hands over a major role in Internet governance to INDEPENDENT Internet policy organization. And the government participates in such organization as ONE of the players. (2) Nomination

---

100) Attorney at law, Hankyul Law Firm(2000 - present), Member, Sub-committee on Address & Infrastructure of Korea Internet Governance Alliance / Internet Numbers and Names Policy Forum (2009 - present), Member, Numbers and Names Commitee(2001 - 2004)

of this committee member must be bottom-up process for a genuine multi-stakeholder model including civil society, commercial organization, end-users and experts. (3) The government should establish plan for supporting the private sector's international activity on the long-term basis.

미국/영국 정보기관의 무차별 정보수집행위: 인터넷과 법치주의의 위기

김기창[101]

1. 인터넷의 기술적 기초에 대한 오해: 인터넷의 '익명성'?

인터넷은 익명성이 보장되는 매체가 아니다. 고안 단계에서부터도 인터넷은 교신의 확실성과 공격에 대한 저항능력(질긴 생명력, robustness)을 확보하는데 주안점을 둔 설계 원칙(end-to-end 원칙)에 기반한 것이었을 뿐, 교신 당사자의 프라이버시나 익명성 보장이 인터넷의 기술적 특징은 아니었으며, 지금도 그렇지 않다.[102]

인터넷의 기술적 기반을 이해하지 못하는 자들은 마치 인터넷이 '익명성'을 제공하는 교신수단인 것처럼 전제하고 이런 저런 주장을 펴고 있지만, 웹서버나 메일서버의 로그파일을 한번이라도 들여다 본 적이 있는 사람이라면 인터넷은 교신 당사자의 행적을 이때까지의 어떠한 오프라인 교신 수단보다도 더 철저히 매순간 기록하고 있음을 쉽게 이해할 것이다. IP 주소 역시, '익명성'을 보장하려는 것이 아니라, 해당 교신을 수행하는 node를 네트워크상에서 '특정'하기 위한 것이다.

암호화 기술 역시 익명성이나 개인의 프라이버시를 보장해 줄 수 있는 것이 아니다. 암호화에 사용되는 암호키를 상대방이 제3자에게 제공하거나, 제3자가 당사자들 모르게 암호키를 입수하거나, 암호 프로그램에 허점이 있거나(의도한 허점이건 의도하지 않은 허점이건), 교신내용이 거쳐 가는 여러 node 들이 모두 정직하게 자신의 임무를 수행한다는 전제가 충족되지 않는다면 암호화는 무의미하게 될 경우가 많다. 인터넷 '기술'이나 암호화 '기술'이 인간의 신뢰나 기대를 보장하거나 충족해 주는 것이 아니다. 교신 과정에 직접 간접으로 개입된 여러 당사자, 즉 '기술'이 아니라 '인간'이 자신의 임무나 약속을 지키는지가 신뢰의 핵심을 이룬다.

---

101) 변호사, 법학박사, 고려대학교 법학전문대학원 교수, 사단법인 오픈넷 비상임 이사, keechang.kim@gmail.com

102) RFC1958 ("Architectural Principles of the Internet") http://www.ietf.org/rfc/rfc1958.txt RFC3724 ("The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture") http://www.ietf.org/rfc/rfc3724.txt 참조.

신뢰는 기계나 기술에 근거하는 것이 아니라, 인간의 행위와 노력에서 생겨나고 인간의 행위에 좌우되는 것이며, 기술이나 기계는 이렇게 생겨난 신뢰를 - 인간이 원하는 경우, 그리고 원하는 동안에만 - 겨우 '유지'해 줄 수 있는데 그친다는 평범한 진리는 현대 정보통신 기술의 현란한 복잡성에 가려서 잊혀지는 경우가 잦다. 미국과 영국의 정보기관들에 의하여 자행된 대량 정보수집행위의 일단이 조금씩 드러나면서 우리는 그동안 잊고 있었던 바로 이 평범한 진리를 다시 마주하게 된 것이다.

2. 미국/영국 정보기관의 대규모 정보수집행위

2013년 여름부터 영국 가디언 신문사는 미국 정보기관(NSA; 국가안보국)과 영국 정보기관(GCHQ; 교신정보총국)이 사람들이 흔히 상상하는 수준을 훨씬 넘어서는 규모로 인터넷 통신망, 통신관련 업체 등을 통하여 정보를 수집, 저장하고 있다는 내용의 보도를 하기 시작하였다. 같은 내용을 확인하고, 그 전모를 더 상세히 밝히는 후속보도는 가디언뿐 아니라 뉴욕타임즈, 워싱턴 포스트 등 여타의 언론 매체들에서도 이어졌다. 이들 보도는 미국 국가안보국 협력업체 직원이었던 에드워드 스노든이 확보하여 언론사와 공유한 자료에 기초한 것이다.

지금까지 드러난 정보 수집행위의 방대한 규모와 대담한 방법을 지극히 간단하게 소개하자면 다음과 같다.

1) 광케이블을 통한 정보 수집(Upstream collection): 미국의 국가안보국은 대량 데이터를 처리하는 광케이블망을 관리하는 업체들로부터 데이터를 확보하는 프로그램을 가동하고 있었다(Blarney, Fairview, Oakstar 그리고 Stormbrew 라는 코드네임으로 비밀리에 운영해 온 프로그램). 영국의 교신정보총국 역시 이와 유사한 대량정보 수집프로그램을 Tempora 라는 코드네임으로 운영해 오고 있었다. 미국과 영국의 정보기관들은 이렇게 각각 수집한 정보들을 서로 공유하는 관계였다.

2) 인터넷 사업자를 통한 정보 수집(Downstream collection): 미국 국가안보국은 마이크로소프트, 구글, 페이스북, 애플, 야후, 스카이프 등 미국의 인터넷 기업들로부터 이메일, 사진, 사회관계망, 접속이력, 인터넷음성통화내용, 파일 등을 입수하는 프로그램을 Prism 이라는 코드네임으로 운영하고 있다.[103]

103) http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3 참조.

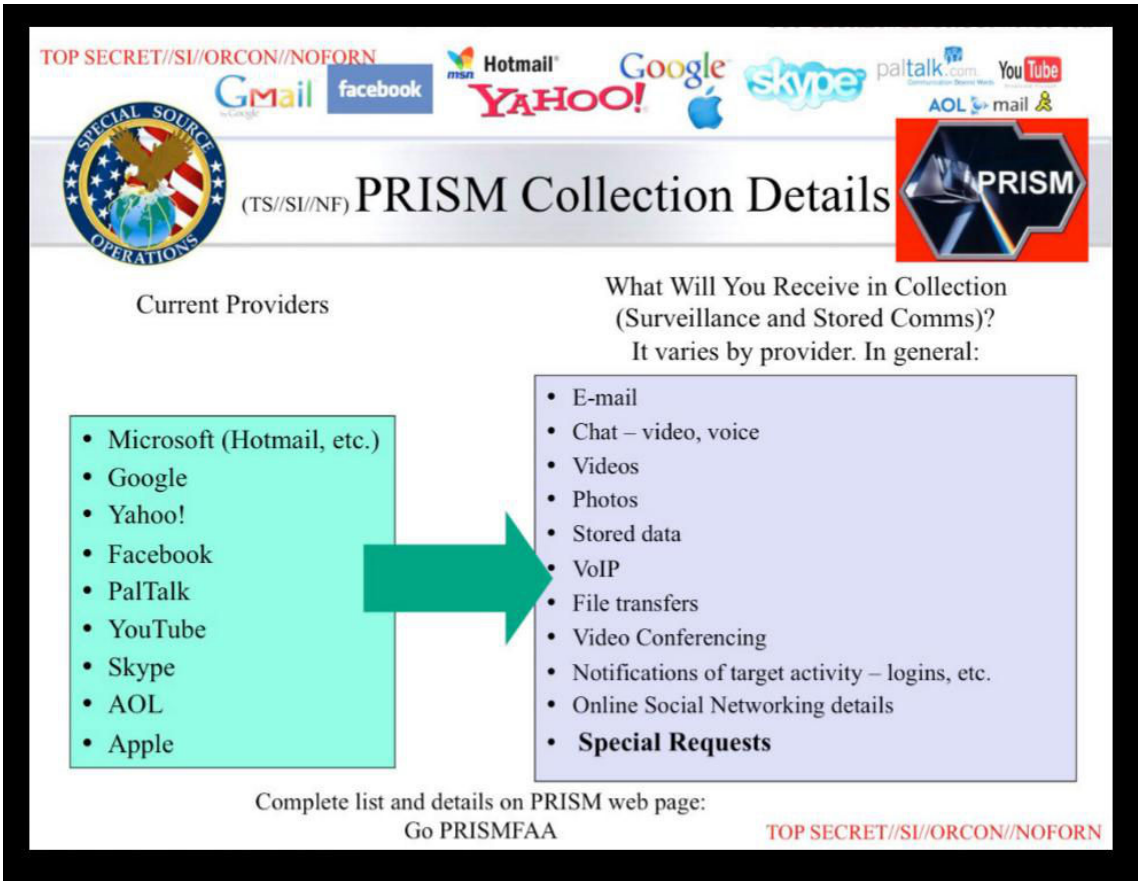

그림 9 미국 NSA가 운영한 PRISM 프로그램

3) 암호화기술 무력화를 위한 활동: 미국과 영국의 정보기관은 막대한 예산을 투입하여 현재 광범하게 사용되는 암호화 알고리즘이나, 암호화 프로그램의 취약점을 공략하는 기술적 가능성을 연구, 개발하여 이미 일부 확보하고 있는 것으로 보인다. 암호화 기술의 허점을 연구하는 행위 자체는 전적으로 정당하고 바람직한 것이지만, 그 성과를 비밀에 붙이고 기존의 암호화 기술을 은밀하게 무력화하는 행위는 - 그 행위가 어떤 용도에 사용되는지 여부에 따라서 - 부도덕하고 파렴치한 것으로 평가될 수 있다. 강력한 암호화 제품이 아예 시장에 나오지 못하도록 하는 행위도 정보당국에 의하여 자행되었다. 미국 국가안보국은 보안기술업체들이 개발, 판매하는 제품들이 "허술하게 되도록 몰래 영향력을 행사"하기 위한 목적으로 연간 2억5천만 달러를 쓰고 있는 것으로 드러났다. 널리 사용되는 상용 암호프로그램에 은밀한 허점(백도어)이 포함되도록 하는 것도 바로 이 예산이 지출되는 이유 중 하나이다.[104]

대서양 횡단 광케이블이나 태평양 횡단 광케이블 등을 포함한 망 자체에 대한 접근을 통하여 입수한 데이터(암호화된 형태)에 대하여 은밀히 확보한 복호화 기술을 적용하여 그 내용까지를 파악하는 것이 가능한 수준에 도달해 있으므로, 미국과 영국의 정보기관이 원하기만 하면 지구상의 거의 모든 교신 내용을 파악할 수 있다는 결론도 무리한 것이 아니다. 일

104) http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security 참조.

부 보도에 따르면, 지금까지 드러난 도청, 감청 행위는 적대국은 물론이고, 우호국의 수반, 주요 국제기구의 수장 등의 교신 내용까지를 대상으로 이루어졌음을 알 수 있다.[105]

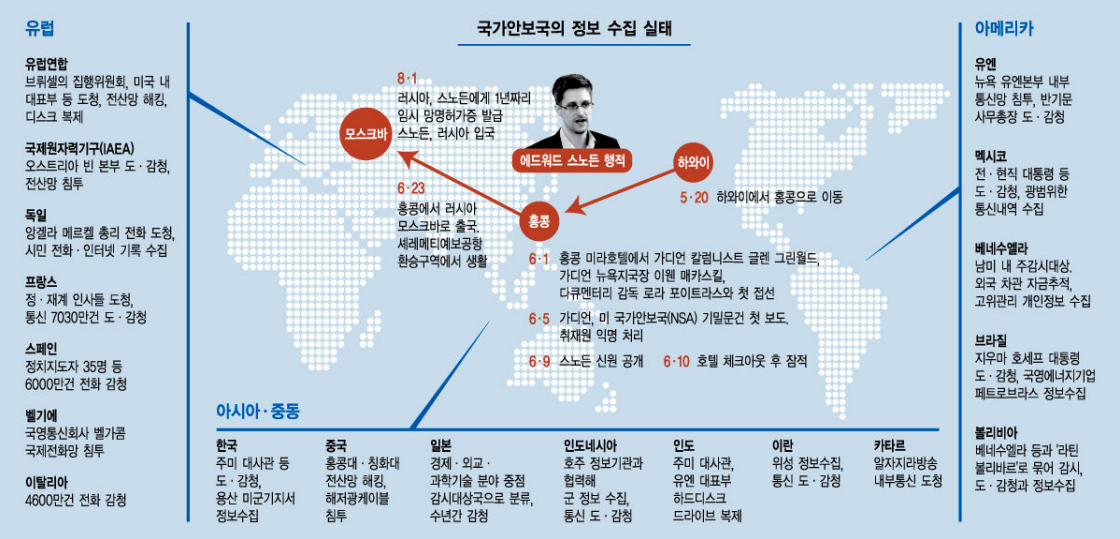

그림 10 미국 NSA의 정보 수집 실태

3. 유명무실한 '사법적' 통제

광케이블을 통한 정보수집이나 인터넷 사업자를 통한 정보 수집은 흔히 해외정보감시법(Foreign Intelligence Surveillance Act; FISA)이 정한 절차에 따라서 발부된 정보수집허가서에 기하여 이루어진 것으로 보인다. 이 절차는 전통적인 영장주의를 배제하고 해외정보감시법정(FISA court)이라는 곳에서 일방주의, 비밀주의에 근거한 매우 간단한 '심사'를 거쳐서 이루어지는 것이다. 즉, 감시 대상이 될 당사자는 정보 수집이 자신에 대하여 이루어지는지 자체를 알 수도 없고, 모든 절차는 비밀리에 진행되며, 정보수집허가가 발부되었는지 여부조차도 비밀에 붙이도록 되어 있다. 이러한 내용의 법 개정은 9.11 테러 사건의 여파로 도입된 것이다.

물론 해외정보감시법에 따른 정보의 수집은 주로 외국인을 상대로 하는 것이긴 하지만, 미국 국가안보국은 영국 정보기관이 수집한 정보(미국 국민에 대한 정보까지 포함)를 공유하는 처지였으므로 내국인/외국인 구분에 따른 적법절차의 차등적 적용이라는 원칙도 사실은 무의미하게 된 경우가 많다. 해외정보감시법정의 심사 절차 자체도 지극히 형식적이고 기계적인 것이어서 사실상 어떠한 실효성도 없다는 것이 일반적인 인식이다.

사생활에 대한 광범한 침투를 쉽게 허용하는 내용의 법 개정은 9.11사태 이후에 부각된 이른바 '테러와의 전쟁'이라는 시대적 분위기에서 도입된 것이다. 테러에 대한 '공포'와 테러 방지 수단을 확보할 '필요'를 내세워 도입된 이러한 느슨한 사법적 통제를 이용하여 대규모로 이루어진 정보 수집 행위가 테러 시도를 사전에 포착하고 방지하는데 과연 어느 정도 기

105) http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201311102314415

여했는지는 대단히 불분명하다. 반면에 시민들에 대한 무차별적인 감시체제가 이러한 제도적 변화를 계기로 확고히 자리잡게 되었다는 점은 의문의 여지가 없이 명백하다.

테러행위가 공동체 구성원들의 자유와 생존을 위협하는 것이라는 점은 의문의 여지가 없다. 그러나 테러 대응, 국가 안보 등을 빌미로 도입되는 여러 제도들이 공동체 구성원의 자유를 심각하게 박탈한다면 그러한 제도는 그것으로 지키려는 소중한 것을 스스로 파괴하는 모순을 저지르는 것이라고 할 수 밖에 없다. 국가 안보를 내세우는 이들이 늘상 내세우는 "Salus populi est suprema lex (인민의 안녕이 지상의 법이다)"라는 키케로의 말에 대하여 영국의 빙험 대법관은 그 오용과 남용을 경계하면서, "안보를 자유보다 우선하는 자는 어느 것도 누릴 자격이 없다"(Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety)는 벤자민 프랭클린의 말에 분명히 힘을 실어주고 있다.[106]

9.11 사태 이후, 테러와의 전쟁이라는 명분으로 도입된 '대폭 완화된 사법적 심사를 통한 사적 통신에 대한 접근'이 지금껏 과연 실효성이 있었는지를 냉정히 재평가해야 할 시점에 도달하였다고 생각한다. 만일 이러한 대량 정보 수집 및 감시행위가 실제로는 별 실효성이 없었다면 우리 모두는 득보다는 실이 많은 제도 변화의 피해자가 될 것이다. 특히 기술적 진보에 근거하여 이러한 정보입수행위가 이루어지고 있으므로, 정작 테러를 기획하는 세력들은 이러한 기술적 정보입수행위를 '우회'하는 손쉬운 다른 교신 방법이나 기법을 이미 채택하고 있을 가능성 또한 심각하게 고민해야 한다. 정작 제어, 감시되어야 할 자들에 대해서는 별 실효성도 없고, 나머지 절대 다수의 선량한 시민들은 무차별적인 사적 정보 노출을 감수하며 살아가야 한다면 지금의 상황은 개선이 필요하다.

4. 교훈 및 대처방향

(1) 기술적 가능성과 규범적 금지의 상관관계

종래의 교신 기술 상황에서 사생활의 자유나 통신의 비밀이 유지되었던 이유는 타인의 교신이나 활동에 대한 접근이 '기술적으로 불가능'해서가 아니다. 예를 들어, 편지봉투에 밀봉되어 배달되는 편지의 내용을 당사자 몰래 파악하는 것이 '기술적으로 어려워서' 편지봉투를 열지 못한 것이 아니다. 유선 전화의 내용을 도청하는 것이 기술적 어려움을 제기하였던 것도 아니다. 기술적으로 가능하다고 해서, 규범적으로 그 행위를 해도 무방한 것은 아니다. 사생활의 비밀이나 프라이버시는 애초부터 기술적으로 방어되고 유지되어 왔던 것이 아니라, 규범적 금지를 준수함으로써 유지, 보호될 수 있었던 것이다.

이러한 원리는 현대의 교신 기술 상황에서도 변함없이 관철되어야 한다. 중요한 차이점은 종래의 교신 기술 상황에서는 광범한 대상(당사자들)에 대하여 그들의 교신 내용에 접근하려면 훨씬 많은 인적, 물적 자원이 소유되었던 것에 반하여, 현재의 교신 기술 속성상 무수한 사람들의 교신이 집중되어 처리되고 있으므로 그 내용에 접근하는 것이 기술적으로 오히려 쉬워졌다는 점이다. 바로 이러한 '기술적 용이함'이 존재하는 현재에는 사적 교신에 대한

106) 톰 빙험, 법의 지배 (김기창 옮김), 역자 후기 참조.

무단 접근을 규범적으로 통제해야 할 더욱 큰 필요성이 생겨났다는 점을 분명히 이해할 필요가 있다. 9.11 사태 이후에 이루어진 일은 정반대 방향으로 제도가 수정된 것이고, 그 결과를 이제 우리들이 접하게 된 것이다.

(2) 인터넷의 기술적 속성에 대한 이해 및 계몽의 필요성

인터넷이 교신의 비밀이나 익명성을 기술적으로 보장해 줄 수는 없다는 너무나 당연하고 초보적인 사실을 더욱 널리 계몽하고, 바람직한 이용 행태를 교육하는 것이 필요하다. 인터넷 망을 통하여 이루어지는 이메일, SNS, 전화 등 대부분의 의사소통 행위들이 기술적으로는 제3자에게 투명하게 그리고 완전하게 노출될 수 있음을 모든 유저들이 보다 명확하게 이해하는 것이 필요하다. 자신이 사용하는 매체의 기술적 속성을 보다 정확하게 이해하는 것이 자신의 사생활이나 프라이버시가 부당하게 침해될 가능성을 그나마 조금이라도 줄이거나 일부라도 회피하는데 도움이 된다.

그리고 소스가 공개되지 않은 상용 소프트웨어(소스가 공개되지 않으므로, 어떤 취약점이 은밀히 내재하는지를 누구도 확인할 수 없는 소프트웨어)는 가급적 사용을 피하고, 소스가 투명하게 공개된 소프트웨어를 사용하는 것이 자신의 안전과 이익에 도움이 된다는 점도 보다 널리 알릴 필요가 있다. 정보당국이 은밀히 심어 놓은 숨은 취약점은 악의적인 공격자 역시도 발견하여 이를 은밀히 이용할 수 있다. 정보당국은 자신의 정보수집 필요성만을 고려에 두고 취약점을 은밀히 심어두는 결정을 할 뿐, 유저가 그러한 취약점 때문에 제3자에 의하여 공격을 당할 가능성에 대해서는 어떠한 고려나 고민, 보호도 제공하지 않는다.

(3) 사적 교신의 비밀 보장과 공권력 행사의 투명성

상상을 초월한 규모의 대량 정보수집 행위에 직면하고, 인터넷의 속성 자체가 애초부터 이러한 정보수집행위를 기술적으로 가능하게 한다는 점을 비로소 인식할 경우, 사생활의 자유, 교신의 비밀, 프라이버시 보호는 변화된 기술 환경에서 현실적으로 아예 '기대할 수 없는 것'으로 치부하고 패배주의에 빠질 우려가 없지 않다. 그러나 이러한 시각은 잘못된 것이다. 교신의 비밀 보장, 프라이버시 보호 등은 기술적 가능성에 좌우 되는 것이 아니라, 인간의 행위에 대한 규범적 통제에 달려있다는 점을 상기할 필요가 있다. 정부의 권한 행사가 보다 투명하게 되고, 정보기관의 정보수집 신청에 대한 실효성 있는 사법적 심사가 이루어진다면, 대규모 정보수집이 비록 '기술적으로는 가능'하더라도, 실제로 지금처럼 광범하게 자행될 수는 없게 될 것으로 기대할 수 있다.

(4) 국제적 대응의 필요

인터넷을 통한 교신, 그리고 그 교신에 대한 은밀한 접근 및 정보 수집은 어느 한 국가의 법제도만의 문제가 아니라 국제적 대응이 필요한 사안이다. 미국의 정보기관이 영국의 정보기관과 협정을 체결하고 정보 수집 행위의 결과를 공유해 온 사례에서 보듯이 정보수집 단계의 '국제 공조'가 이루어져 왔는바, 이러한 행위가 가능한 것과 마찬가지로 정보수집에 대한 사법적 통제나 감시 메커니즘 역시 국제적 공조가 가능할 뿐 아니라 필요한 분야임이 분

명해졌다. 따라서 각국 정부는 정보수집의 원칙, 정보수집 시도에 대한 사법적 통제의 원칙 등에 대해서 구체적인 내용과 절차에 대한 합의점을 도출하고 향후 이러한 일이 재발하지 않도록 하는데 필요한 국제적 공조 체제를 수립할 필요가 있다.

사생활의 자유, 통신의 비밀, 프라이버시 보호 등은 문명사회를 지탱하는 중요한 초석이다. 스노든의 폭로행위로 드러난 미국과 영국 정보기관의 다양한 정보수집 행위는 이러한 근본 가치들에 대한 심각한 도전으로 받아들여질 여지도 많다. 이 사태를 계기로 위와 같은 논점들에 대한 더욱 활발한 논의가 이루어 질 수 있기를 바란다.

ABSTRACT

Massive Surveillance by US-UK intelligence services : Crisis of the Internet and the Rule of Law

Keechang Kim[107)]

The revelations made possible by Edward Snowden, a contractor of the US intelligence service NSA, are a sobering reminder that the Internet is not an 'anonymous' means of communication. In fact, the Internet has never been conceived with anonymity in mind. If anything, the Internet and networking technologies provide far more detailed and traceable information about where, when, with whom we communicate. The content of the communication can also be made available to third parties who obtain encryption keys or have the means of exploiting vulnerabilities (either by design or by oversight) of encryption software. Irrebuttable evidence has emerged that the US and the UK intelligence services have had an indiscriminate access to the meta-data of communications and, in some cases, the content of the communications in the name of security and protection of the public. The conventional means of judicial scrutiny of such an access turned out to be ineffectual.

The most alarming attitude of the public and some politicians is "If you have nothing to hide, you need not be concerned." Where individuals have nothing to hide, intelligence services have no business in the first place to have a peek. If the public espouses the groundless assumption that State organs are benevolent ("they will have a look only to find out whether there are probable grounds to form a reasonable suspicion"), then the achievements of several hundred years of struggle to have the constitutional guarantees against invasion into privacy and liberty will quickly evaporate.

This is an opportune moment to review some of the basic points about the protection of privacy and freedom of individuals. First, if one should hold a view that security can override liberty, one is most likely to lose both liberty and security. Civilized societies have developed the rule of law as the least damaging and most practicable arrangement to strike a balance between security and liberty. Whether we wish to give up the rule of law in the name of security requires a thorough scrutiny and an informed decision of the body politic. It is not a decision which can secretly be made in a closed chamber. Second, protection of privacy has always depended on human being's compliance with the rules rather than technical

107) Professor at Korea University Law School, Director (non-executive), OpenNet Korea

guarantees or robustness of technical means. It is easy to tear apart an envelope and have a look inside. It was, and still is, the normative prohibition (and our compliance) which provided us with protection of privacy. The same applies to electronic communications. With sufficient resources, surreptitiously undermining technical means of protecting privacy (such as encryption) is certainly 'possible'. But that does not mean that it is permissible. Third, although the Internet is clearly not an 'anonymous' means of communication, many users have a 'false sense of anonymity' which make them more vulnerable to prying eyes. More effort should be made to educate the general public about the technical nature of the Internet and encourage them to adopt user behaviour which is mindful of the possibilities of unwanted surveillance. Fourth, the US and the UK intelligence services have demonstrated that an international cooperation is possible and worked well in running the mechanism of massive surveillance and infiltration into data which travels globally. If that is possible, it should equally be possible to put in place a global mechanism of judicial scrutiny over a global attempt at surveillance.

망중립성 거버넌스

- 기원, 내용과 동향에 대한 개요 -

필자 매티스 반 베르겐 (Matthijs van Bergen)[108]
번역 신하영[109], 김보라미[110]

망중립성은 오늘날 인터넷 정책에 있어서 가장 논쟁적인 주제 중 하나이다. 이 글은 미국과 유럽을 중심으로 하지만, 다른 국가들과 지역의 경우도 훑어봄으로써, 망중립성 거버넌스의 기원, 내용, 그리고 그 동향에 대하여 간략하게 분석해 보았다.

1. 망중립성 논쟁의 기원

인터넷은 사상과 정보를 취득하고 전달할 개인의 자유를 대단히 증진시켜 왔다.[111] 그러나 최근 십년 전부터 학계와 공공정책 관계자들은, 그동안 인터넷과 그 기술설계에 대한 디자인 원칙들의 본성이라고 인식했던 자유와 민주주의가, 정부와 민간 영역 두 곳으로부터 위협받고 있는 것에 대하여 지속적인 경고를 제기했다. 초창기의 경고는 대부분 미국에서 나타났으며, 그 시기는 1994년까지 거슬러 올라갈 수 있다.[112]

---

108) Matthijs van Bergen works as a legal advisor at ICTRecht, and is simultaneously developing his PhD thesis concerning net neutrality and the protection of freedom of speech and privacy in information societies at Leiden University. Matthijs has advised the Dutch NGO Bits of Freedom concerning net neutrality from 2010 to 2012, on an entirely voluntary ('pro bono') basis. Currently Matthijs is also serving as a network neutrality expert for the Council of Europe

109) 육아정책연구소 전문원(Managing Editor at Korea Institute of Child Care and Education), 숙명여대 박사수료(Ph.D candidate of Sookmyung Women's University, ABD), 크리에이티브커먼즈 코리아 활동가(Volunteer of Creative Commons Korea)

110) 망중립성 이용자포럼 코디네이터

111) The importance of the free and open Internet for the freedom of expression has been stressed in countless publications. A few prominent ones: F. La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', report of 16 May 2011, no. A/HRC/17/27; Council of the European Union, 'Council conclusions on the open Internet and net neutrality in Europe', 13 December 2011; Council of Europe, 'Declaration of the Committee of Ministers on network neutrality', 29 September 2010.

112) See i.a. Noam 1994, Lemley & Lessig 1999, Lessig 1999, CBUI 2002, Lessig & Wu 2003, Privacy International & GreenNet 2003, Zittrain 2008, Nunziato 2009, Bendrath & Mueller 2010, and Van Schewick 2010.

‘망중립성’이라는 용어는 2002년 컬럼비아 대학 교수인 팀 우에 의하여 탄생했다. 팀 우는 ‘망중립성을 위한 제안’이라는 논문을 발표하면서, 이 논문을 통해 “광대역 서비스 사업자에게는 대역폭 사용과 로컬(local)의 다른 문제들을 관리하는 것에 대하여는 자유가 있는 반면에, 광대역 서비스 사업자가 손해(harm)의 입증 없이, 인터넷 연결을 통하여 이용자가 하는 행위를 제한하는 것은 금지되어야 한다”는 제안을 하였다.[113] 그 해 11월, 광대역 서비스 이용자들과 혁신가들- 여기에는 아마존닷컴, 애플 컴퓨터, 마이크로소프트, 소비자 전기 협회(the Consumer Electronics Association) 등이 포함됨- 의 임시적인 연합체인 CBUI(the Coalition of Broadband Users and Innovators)가 연방통신위원회(FCC)에 진정서를 제출했다. 그들은 소비자들과 인터넷 이용자들이 적법한 콘텐츠와 서비스에 접속할 수 있는 제한 없는 권리를 누리고, 서로 간에 커뮤니케이션하고 상호작용하며, 전송망 사업자(transmission network provider)들에 의한 방해 없이 원하는 인터넷 주소지에 송신하는 행위를 앞으로도 계속할 수 있도록 FCC가 이를 보장하는 조치를 취해야 한다고 주장했다. 그러자 ‘전미 케이블 & 방송통신 연합(NCTA: The National Cable & Telecommunications Association)’, 콤캐스트(Comcast), 그리고 다른 광대역 사업자들은 뒤이은 진정서에서 규제는 불필요하며 바람직하지 않을 뿐 아니라, FCC가 이러한 규칙을 제정할 권한이 있는지에 대하여 문제제기를 하였다.[114]

이는 미국에서 법과 정책을 통해서 망중립성을 보장해야 하는지, 그 방법은 무엇인지에 대하여 이루어진 지난하고 격렬하게 이루어진 망중립성 논쟁의 시작이었다. 이 논쟁은 곧 전 세계의 다른 지역으로도 퍼져나갔고, 현재는 망중립성보호취지가 규정된 규칙(Regulation)[115]이 제안된, EU의 상황에서도 특별히 중요한 사회적 이슈이기도 하다.[116]

이 논쟁의 중요성은 아무리 강조해도 지나치지 않다. 이 결과는 향후 인터넷, 즉 오늘날 정보사회가 형성되어 온 기술적, 사회적 플랫폼이 발전할 방향과, 근본적인 권력구조와 권력분배 형성을 중요한 수준으로 결정할 것이다.

2. 망중립성의 내용

램리(Lemley) 교수와 레식(Lessig) 교수는 인터넷의 특별한 성장과 성공은 근본적으로 인터넷 설계 원칙에 있음을 설득력 있게 주장해 왔다.[117] 정책과 기술은 많은 측면에서 비슷하고 자주 서로 영향을 준다. 과학과 기술 모두, 사람들의 문제를 해결하거나, 생활을 증진시키는 의도가 있거나, 또는 적어도 그래야만 한다. 또한 어떤 기술이나 정책을 만들 때, 다양하고 경쟁적인 이해관계들 사이에서 이루어지는 타협-이 타협안에는 서로 합쳐지기 어려울 정도로 멀리 떨어져 있는 사회적 의미들이 있기는 하다-이 항상 존재한다. 정책 원칙들과 기술적 설계 원칙들은 특정한 구체적 사안에 대한 타협을 만들어 나가는 방법에서 공

113) Wu, 2002
114) National Cable & Telecommunications Association Ex Parte Letter, December 10, 2002.
115) EU의 규제방법 중 하나로, 각 국에 대하여 직접적인 구속력을 가지는 방법으로 우리나라 규칙의 의미와는 다르다.
116) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, 2013/0309 (COD).
117) Lemley & Lessig 1999

통점이 있다.

인터넷 분야에서 정책과 기술은 깊은 수준으로 상호작용을 하고 있으며, 인터넷의 기본 디자인 원칙들 중에는 특정 민주주의 원칙들과 상당한 수준으로 유사성을 가지는 부분이 있다.

망중립성은 그 용어가 의미하는 것처럼, 본질적으로 인터넷 트래픽 전송 과정에 적용되는 비차별적 원칙을 의미한다.[118] 망중립성은, 원칙적으로 모든 인터넷 트래픽이 동등하게 전송되거나, 그렇지 않을 경우 최소한 특정 응용프로그램, 콘텐츠, 서비스, 기기나 이용에 대하여 특혜를 부여하지 않는 방법으로, 특히, 불이익을 주지 않는 방법으로 전송되어야 한다고 규정한다.[119]

이 원칙은 단대단 원칙(end-to-end principle)과 긴밀하게 연결 되어 있고, 실제로 단대단원칙의 결과물이기도 하다. 단대단 원칙이란, 망의 기능(정보처리기능intelligence)이 끝단(호스트)에 있어야 하고, 중앙(라우터)에서의 기능은 필요할 때에만 가능한 것을 의미한다.[120] 이렇게 단대단 원칙은 민주주의의 보완성(subsidiarity) 원칙을 상기시킨다. 보완성 원칙이란 권력과 자치는 가능한 한 분권화되어야 하며, 오직 정당한 (공공적) 목적을 위하여 필요한 경우에만 중앙집중화 되어야 한다는 것이다. 이러한 유사성을 인지하는 것은 망중립성의 중요성을 이해하고, 망중립성이 근대 (유럽) 정보 사회의 헌법적 원칙으로 간주될 수 있는 이유를 설명하는데 도움이 된다. 또한, 이는 삼권분립(trias politica)과 같이, 민주적 사회조직들을 이끌어 온 다른 기본원칙들처럼 유사하게 중요한 것을 이해하는 데에도 잠재적으로 도움이 될 것이다. 보완성의 원칙은 유럽 인권법과 연관은 있지만, 다소간의 차이를 가진다. 즉, 유럽인권법에서는 예를 들어 표현의 자유와 같은 기본권과 관련되어서는 어떠한 (중앙집중화된) 국가의 개입이나 규제는, 그 개입이 필요하고, 좁게 특정하게 제한된 정당한 목적을 달성하는데 비례하는 범위 내에서만 정당화될 수 있으며, 여전히 명백히 효과적이면서도 가장 최소한도로 제한적인 수단이 사용되어야 한다. 유사하게, 인터넷 트래픽 전송에 대한 어떠한 제약과 차별, 혹은 인터넷 서비스 제공자에 의한 다른 종류의 (중앙집중화된) 조치는, 그 조치가 필요하고, 좁게 제한된 특정한 정당한 목적, 예를 들어, 네트워크와 이를 통해 제공되는 서비스들, 또는 이에 연결되어 있는 기기들 간의 통합성(integrity)과 보안(security)을 보호하기 위한 목적(즉, 디도스(DDoS)공격 등 유해 소프트웨어 등을 차단하기 위해)을 달성하기 위하여 비례적으로 필요한 범위 내에서만 허용되어야 할 것이다.

모듈(module), 계층화(layering)와 단대단과 같은 기술적 디자인 원칙들이 결합되어, 네트

118) Wu may have better called it Internet neutrality instead of network neutrality, because the principle is commonly understood to apply only to Internet traffic and not necessarily to traffic which may flow through specialized services offered on closed digital networks utilizing the Internet Protocol.

119) For further explanation of the concept of application-agnosticism, see Van Schewick 2012.

120) The “broad version” of the end-to-end principle is defined by Barbara van Schewick as follows: “a function or service should be carried out within network layer [i.e., available to all clients of the network] only if it is needed by all clients of that layer.” Art. 5(3) of the Treaty on the EU states: “Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

워크 내부의 계층과 기능들을 통합하고, 특정 응용프로그램을 위하여 네트워크를 최적화함으로써 얻을 수 있는 종류의 효율성을 버리고, 인터넷을 전체적으로 개방적이고 다목적이며, 유연하고, 활발하게 만들게 되었다.[121] 이 디자인은 인터넷 서비스 제공자의 허가나 계약관계 없이도, 자연스럽게 이용자들이 선택한 어떠한 온라인 콘텐츠, 응용 프로그램, 서비스든지, 선택한 기기로 송수신할 수 있고, 다른 원하는 인터넷 이용자와 커뮤니케이션할 수 있게 하여, 자연스럽게 개인적인 혹은 인터넷 이용자들의 집단적인 자기결정을 촉진시켰다.

민주주의 사회는 개인과 집단의 자기결정이라는 이상에 기반하고 있으며, 거버넌스 시스템으로써의 민주주의는 전체주의 사회보다 활발하고 유연하며 개방적인 것으로 설명할 수 있다. 이러한 특성들은 삶의 모든 영역이 중앙집중적으로 통제되고 모든 반대주장들을 잠재워 얻을 수 있는 그런 종류의 효율성을 포기함으로써 얻게 되는 것이다. 또 다른 특기할 만한 인터넷 설계에 있어서의 민주주의적 요소는 인터넷을 작동시키는 기술 프로토콜(protocol)이 하버마스의 실천적 담론(practical discourse)을 구성하는 것 같은 개방적이고, 투명하며, 참여적인 절차로 만들어졌다는 것이다.[122]

인터넷 프로토콜을 만들어 가는 이러한 실천적이고, 개방적이며, 투명하고, 철저히 민주적인 접근방식은 오늘날 인터넷과 관련된 정책을 발전시키는 과정과 계획에 계속적으로 반영되고 있다. 예를 들어, 유럽연합 집행위원회(European Commission)는 규칙(Regulation) 초안[123]을 다듬어 가기 전에, 망중립성에 관한 다양한 (복수의) 인터넷 협의체들을 조직해 왔다. 그리고 (인터넷거버넌스포럼 내의) 망중립성 역동적 연합(the Dynamic Coalition on Net Neutrality)[124]은 망중립성 문제를 다루는 데에 있어서 인터넷 공공 서비스와 기본권의 가치를 극대화시키는 것을 지향하면서 동시에 몇몇 소수의 인터넷 서비스 사업자들에게 혁신을 위한 권력을 집중시키기보다는 모든 인터넷 사용자들에게 혁신을 위한 권력을 나누어 주는 것과 관련된 법적 체계를 정교하게 발전시키는 개방적이고 참여적인 절차를 활용했다. 인터넷 거버넌스의 이러한 참여적이면서 멀티스테이크홀더(multi-stakeholder)적인 절차들은, 인터넷이 가지는 속성 자체, 또는 그러한 속성에 따라 가능했다. 위 절차들은 인터넷 설계에 이미 내재되어 있는 민주적 가치들을 보호하려는 의도가 있으며, 이는 앨 고어(Al Gore)가 1994년에 한 연설에서 제안한 '새로운 민주주의의 아테네 시대'(New Athenian Age of Democracy)[125]를 만들어 나가는 데 인터넷을 이용하자는 이상이기도 하다.

근대 국가(nation states)의 존재, 조직, 권력이 지배 엘리트의 변덕이나 욕망이 아니라 시민들, 그리고 일반 대중들의 필요와 요구에 따라 정당화된다는 민주주의 이상과 유사하게, 모든 정보통신망의 존재는 궁극적으로는 서비스 제공자가 네트워크 활용을 통해 얻을 수 있는 이익보다는, 이용자들의 커뮤니케이션을 할 의사에 따라 합법화된다. 시장의 힘이 인터넷 접근을 제공하는 자와 그러한 이용을 이용하는 자들 간의 이해관계의 균형과 조율을

121) For a much more detailed and complete analysis and description of the principles of modularity, layering and end-to-end, see Van Schewick 2010

122) See: Belli & Van Bergen 2013.

123) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, 2013/0309 (COD).

124) http://www.intgovforum.org/cms/dynamic-coalitions/1330-dc-on-network-neutrality.

125) Al Gore, Information Superhighways Speech International Telecommunications Union Monday March 21, 1994, available at http://vlib.iue.it/history/internet/algorespeech.html.

담보할 수 없게 되는 범위 내에서, 민주적으로 채택된 교정이 요구된다.

3. 법체계의 발전과 동향

지난 몇 년간, 망중립성에 관한 법체계는 다음과 같이 발전해 왔다.

▪ 2009년 11월 경 유럽입법자들은 텔레커뮤니케이션에 대한 신 규제체제(New Regulatory Framework : NRF)를 채택했다. 이 신 규제체제에서는 전자 커뮤니케이션 회사들에 대한 투명성 요건과 함께, 유럽연합 집행위원회(European Commission)가 "각 국의 규제기구들에 의하여 촉진되어 온 정책목적과 규제원칙으로서의 망중립성을 보장하려는 공동규제자들의 의지를 모두 고려하여, 인터넷의 개방적이고 중립적인 성격을 보존하는 것을 우선 순위에 둔다"고 선언하였던 망중립성에 대한 집행위원회 선언(Commission Declaration on Net Neutrality)이 포함되어 있다. 2009/136/EC 지침(directive)의 28조에서 구체적으로 "2002/21/EC 지침 (directive) 제8조에서 규정된 것처럼, 국가 규제기관은 이용자들의 정보에 접근하고 배포할 권리, 그들의 선택에 따른 어플리케이션과 서비스를 이용할 권리를 증진시켜야한다"고 규정하고 있다.

▪ 2010년 7월 경 칠레는 전 세계 최초로 망중립성 보호를 목적으로 하는 법을 채택한 국가가 되었다. 칠레의 이 법은 인터넷 서비스 사업자들이 망을 통하여 이루어지는 적법한 활동에 대하여 임의적으로 차단 또는 차별하는 것을 금지하고 있다.[126)]

▪ 2010년 11월 경, 유럽연합 집행위원회(European Commision)는 6월 말부터 9월 말까지 이루어진, 318개의 의견이 첨부된, 공공 협의과정을 끝내고, "유럽에서의 오픈 인터넷과 망중립성에 대한 정상회의"를 개최했다. 공공 협의에 대한 유럽연합 집행위원회의 보고서에 따르면, "대다수의 의견들은 일반적으로 EU 텔레콤 프레임워크(telecommunication framework)가 인식된 이슈들(질문 3)을 다룰 수 있다고 보고 있고, 몇몇 소수가 이 지점에서 추가적인 규제를 주장하고 있다"라고 기술되어 있다.[127)]

▪ 2010년 12월 경 FCC는 합리적인 네트워크 관리에 따라, 망 사업자들이 적법한 콘텐츠, 어플리케이션, 서비스, 또는 유해하지 않은 기기를 차단하는 것을 금지하는 규칙을 채택했다. 이 규칙에는 미국의 인권 용어들, 예를 들면 "엄격히 특정하게 제한된(narrowly tailored)"과 같은 용어들이 사용되었다.

▪ 2010년 12월 이스라엘 의회는 무선 통신 사업자가 인터넷을 통하여 전송되는 서비스나 어플리케이션의 이용을 제한하거나 차단하는 것을 금지하는 법을 채택하였다. (인터넷전화 포함)[128)]

---

126) Technollama.co.uk, 28 January 2012, 'Chile enforces net neutrality for the first time, sort of', <http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of>.

127) This may be considered surprising, given the fact that submissions made by civil society organizations such as European Digital Rights, Bits of Freedom and La Quadrature du net, the Free Knowledge Institute, The International Telecommunications Users Group, Universities such as the Essex University, as wel as prominent application providers such as Skype had (often loudly) cried for additional regulatory measures to ensure end users' ability to access and distribute the information or run the applications and use the services of their choice on the Internet.

▪ 2011년 7월 경 벨기에 의회에서는 같은 해 6월에 네덜란드 의회 하원에서 채택한 것과 같은 법안이 제안되었다.

▪ 2011년 11월 경, 유럽의회는 유럽연합 집행위원회에 대하여 인터넷의 개방성과 중립성 원칙을 수호하고 이용자들의 정보에 접근하고, 배포할 권리, 그들이 선택한 어플리케이션과 서비스를 이용할 수 있는 권리를 증진시킬 것을 요구하는 것이 포함된 결의를 채택했다.[129]

▪ 2012년 5월 네덜란드 의회 상원에서 망중립성을 보호하는 법 제안이 통과되었다. 네덜란드 법은 인터넷 서비스 사업자가 정당한 목적에 필요한 경우(예, 혼잡 완화, 망과 기기의 안전 보호)가 아니라면, 온라인 어플리케이션을 차단하거나 방해하여서는 안 된다는 것을 법에 규정하였다. 이 법의 구성은 ECnHR(유럽인권협약) 제10조에 영향을 받았다. 디지털 어젠다(Digital Agenda)에 대한 유럽연합 집행위원회 위원인 크로스(Kroes)는 시기상조라고 하면서 공식적으로 몇 차례나 네덜란드 법에 대한 명시적인 반대를 하였다.[130]

▪ 2012년 5월 경, 베렉(BEREC, 유럽전자통신규제기관)은 P2P에 대한 계약상 제한이 90%의 사업자들에 의하여 강요되고 있으며, 인터넷전화에 대한 계약상 제한은 56%의 모바일 사업자들에 의하여 기술적으로 이루어지고 있는 상황에서, 적어도 인터넷 이용자들의 20%와 잠재적으로는 모바일 인터넷 이용자들의 절반가까이가 인터넷 전화나 P2P와 같은 서비스 제한을 허용하는 계약을 맺고 있다는 사실을 보여주는 트래픽 관리에 대한 보고서를 발표했다.

▪ 2012년 8월 경, 이스라엘 통신부는 망중립성 원칙을 모바일에서 모든 통신 사업자에게 확대하는 제안을 제출하였다.

▪ 2012년 12월 경, ITU는 두바이에서 국제통신규약(ITRs)을 위한 회의를 열었다. 인터넷 트래픽에 대한 다른 요금부과모델에 대한 몇몇 주장들, 예를 들면 발신자비용부담(SPNP , Sending party network pays) 모델 같은 것들이 제안되었으나 이 제안들에 대한 다수의 비판이 제기된 이후 채택되지 않았다.[131] ETNO는 추가적으로 “개발될 차별화된 서비스 전송 품질과 관련된 상업적 약정을 배제하지 않는다”라는, ITU 회원 국가들이 망중립성 규제를 더 이상 할 수 없도록 하는 것을 보장하는 것으로 해석될 수 있는 규정이 포함된 제안을 하였으나, 이 규정도 채택되지 않았다.

---

128) Broadband Traffic Management, 7 December 2010, 'Net Neutrality [Israel] - Parliament Approved Wireless Neutrality' <http://broabandtrafficmanagement.blogspot.be/2010/12/net-neutrality-israel-parliament.html>.

129) European Parliament 7 November 2011, 'European Parliament resolution on the open internet and net neutrality in

130)ZDNet 3 October 2011, 'Kroes attacks Dutch net-neutrality rules', <http://www.zdnet.com/kroes-attacks-dutch-net-neutrality-rules-3040094084/>(l.c.o.3February2013);Telecompaper14June2011,'KroessaysDutchnetneutralityrulespremature'<http://www.telecompaper.com/news/kroes-says-dutch-net-neutrality-rules-premature--809381>.

131) E.g. Forbes 8 September 2012, 'Why is the UN Trying to Take over the Internet?' <http://www.forbes.com/sites/larrydownes/2012/08/09/why-the-un-is-trying-to-take-over-the-internet/3/>(l.c.o.18March2013);seealsoBEREC14November2012,'BEREC'scommentsontheETNOproposalforITU/WCITorsimilarinitiativesalongtheselines'<http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines>.

▪ 2012년 12월에 슬로베니아 의회는 망중립성 법안에 대하여 찬성하였다. 이 법안은, 제한된 정당한 목적 사유에 필요한 경우가 아니라면, 인터넷 트래픽을 차단, 지연시키거나 기타 방해하는 것을 금지하는 점에서 네덜란드 법과 유사하다.

▪ 2012년 11월 경 BEREC은 망중립성에 대한 활동 방향과 위치에 대한 보고서를 발표했다. 이 문서에서 BEREC은 "개방적 인터넷을 위하여 노력하고 있으며, 현재의 규제 수단들이 충분히 적용될 때, 국내규제기관(NRAs)이 망중립성 관련 문제들을 다룰 수 있어야만 한다"고 입장을 발표했다.[132)]

▪ 2013년 1월 네덜란드 망중립성 법이 발효되었다.

▪ 2013년 3월에 프랑스 정부의 요청으로 프랑스 전국 디지털 위원회가 정부에 대하여 법에 망중립성 의무조항을 포함하는 것을 권고하는 의견서를 발표하였다. 이 제안서는 너무 모호하고, 구체성이 결여되어 있다고 몇몇 비판을 받았다.[133)]

▪ 2013년 9월 경 유럽연합 집행위원회는 연결된 유럽(the Connected Europe)을 실현하기 위하여 유럽 전자 커뮤니케이션 단일 시장 규칙(Regulation) 초안을 발표하였다. 제23조에 따르면, 좁게 제한된 정당한 목적에 대하여 규정한 제한적 사항을 위하여 필요하거나 비례적인 예외적인 경우가 아니라면, 특정 콘텐츠와 어플리케이션의 차단과 속도제한은 금지된다.

앞에서 본 것처럼, 우리는 망중립성의 원칙을 법과 정책에 규정하려고 하는 명백한 경향이 있다는 결론에 이를 수 있다. 인권에 대한 고려는 망중립성 논쟁에 있어서 점차적으로 중요한 역할을 하고 있으며, 이것은 망중립성과 관련된 법적 규정을 채택하거나 제안한 몇몇 용어들에 반영되어 있다.

현재 유럽의 망중립성 논의에서 가장 중요한 이슈들로는, 규칙(Regulation) 초안에서 애매하게 여지를 남겨 둔 특별 서비스(Specialized Service)의 정의와 경계, 그리고 망중립성의 진정한 보호에 있어서 필수적인 "우선순위 선점에 따른 대가지불(pay-for-priority) 사업 모델의 금지" 등이 있으나, 위 초안의 표현만으로는 명백하지 않다.

참고문헌

Belli & Van Bergen 2013: Belli, L and Van Bergen, M., A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application, in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet

132) BEREC November 2012, 'BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines' <http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines

133) BEREC November 2012, 'BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines' <http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines

of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, 2013, available at http://nebula.wsimg.com/a0d2191d5788b8177915108786bfba7a?AccessKeyId=B45063449B96D27B8F85&disposition=0.

Bendrath & Mueller 2010: Bendrath, R. & Mueller, M. The End of the Net as we know it? Deep Packet Inspection and Internet Governance, available at http://ssrn.com/abstract=1653259.

CBUI 2002: Ex Parte Letter from CBUI to Michael K. Powell, FCC Chairman, CC Docket Nos. 02-33, 98-10 & 95-20, CS Docket No. 02-52, and GN Docket No. 00-186 (November 18, 2002).

Lemley & Lessig 1999: Lemley, M.A., Lessig, L., Ex parte declaration of Professor Mark A. Lemley and Professor Lawrence Lessig in the matter of: Application for consent to the transfer of control of licenses of Mediaone Group, Inc. to AT&T Corp, CS Docket No. 99-251, before the Federal Communications Commission.

Lessig 1999: Lessig, L., Code and other laws of cyberspace. New York: Basic Books.

Lessig & Wu 2003: Lessig, L. and Wu, T., A Proposal for Network Neutrality, Ex Parte Submission in CS Docket No. 02-52 (August 23, 2003).

Noam 1994: Noam, E. M., Beyond Liberalization II: The Impending Doom of Common Carriage, Telecommunications Policy Volume 18, Issue 6, August 1994, Pages 435?452.

Nunziato 2009: Nunziato D., Virtual Freedom, Net Neutrality and Free Speech in the Internet Age. Palo Alto, Stanford University Press 2009.

Privacy International & GreenNet 2003: Banisar, D. et al, Silenced: an international report on censorship and control of the internet. Stanford, Privacy International & GreenNet Educational Trust 2003, available at http://www.privacyinternational.org/survey/censorship/silenced.pdf.

Van Schewick 2010: Van Schewick, B., Internet Architecture and Innovation. Londen, The MIT Press 2010.

Van Schewick 2012: Van Schewick, B., Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like, The Center for Internet and Society, June 2012.

Wu 2002: Wu, T., A Proposal for Network Neutrality, available at http://www.timwu.org/OriginalNNProposal.pdf.

Zittrain 2008: Zittrain, J., The Future of the Internet and How to Stop It. New Haven, Yale University Press 2008.

Net neutrality governance

A Brief View on Origin, Substance and Trend

Matthijs van Bergen[134)]

Net(work) neutrality is one of the most hotly debated topics of Internet policy today. This article briefly analyses the origin, substance and trend of network neutrality governance, focusing on Europe and the United States, with a glance at other countries and regions as well.

1 Origin of the net neutrality debate

The Internet is widely held to greatly enhance the freedom of individuals to receive and impart ideas and information.[135)] However, since more than a decade now, persistent warnings have emerged from academic and public policy circles that the perceived free and democratic nature of the Internet and the fundamental design principles of its technological architecture are under threat, both from governments and the private sector. The earlier warnings have mostly originated from the US and can be traced back as far as 1994.[136)]

---

134) Matthijs van Bergen works as a legal advisor at ICTRecht, and is simultaneously developing his PhD thesis concerning net neutrality and the protection of freedom of speech and privacy in information societies at Leiden University. Matthijs has advised the Dutch NGO Bits of Freedom concerning net neutrality from 2010 to 2012, on an entirely voluntary ('pro bono') basis. Currently Matthijs is also serving as a network neutrality expert for the Council of Europe.

135) The importance of the free and open Internet for the freedom of expression has been stressed in countless publications. A few prominent ones: F. La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', report of 16 May 2011, no. A/HRC/17/27; Council of the European Union, 'Council conclusions on the open Internet and net neutrality in Europe', 13 December 2011; Council of Europe, 'Declaration of the Committee of Ministers on network neutrality', 29 September 2010.

136) See i.a. Noam 1994, Lemley & Lessig 1999, Lessig 1999, CBUI 2002, Lessig & Wu 2003, Privacy International & GreenNet 2003, Zittrain 2008, Nunziato 2009, Bendrath & Mueller 2010, and Van Schewick 2010.

The term 'net(work) neutrality appears to be coined in 2002 by Tim Wu (professor at Columbia University), who published an article entitled 'a proposal for network neutrality' in which he proposed to “forbid broadband operators, absent a showing of harm, from restricting what users do with their Internet connection, while giving the operator general freedom to manage bandwidth consumption and other matters of local concern.”[137] In November of the same year an ad hoc group called the Coalition of Broadband Users and Innovators (“CBUI”), with among its members companies like Amazon.com, Apple Computers, Microsoft Corporation and the Consumer Electronics Association[138], filed an ex parte letter with the FCC, urging the FCC to take measures to assure that “consumers and other Internet users continue to enjoy the unfettered ability to reach lawful content and services, and to communicate and interact with each other and reach desired Internet destinations without impediments imposed by transmission network providers.” Subsequent ex parte submissions from The National Cable & Telecommunications Association (“NCTA”), Comcast and other broadband operators argued that regulation was unnecessary and undesirable and questioned the FCC's authority to issue such rules.[139]

This marked the start of a long and fierce debate in the United States about whether and how to protect network neutrality through law and policy. This debate soon started to spread to other parts of the globe, and now is particularly topical in the EU context, where a Regulation has been proposed with the intention of protecting net neutrality.[140]

The importance of this debate is difficult to overstate. The outcome is likely to determine to a significant extent in which direction the Internet, the technological and social platform on which today's information societies are built, can develop further and which fundamental structures and divisions of power will apply.

2 The substance of net neutrality

As professors Lemley and Lessig have eloquently argued, the extraordinary growth and success of the Internet rests fundamentally on its design principles.[141] Policy and technology are similar in many ways and they often intertwine. Both are, or at least should be, intended to fix people's problems and make their lives better. Also, when people create either technologies or policies, there are always

137) Wu 2002.
138) See CBUI 2002 for a complete (as may be assumed) list of members.
139) National Cable & Telecommunications Association Ex Parte Letter, December 10, 2002.
140) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, 2013/0309 (COD).
141) Lemley & Lessig 1999.

trade-offs involved between different competing interests, while such trade-offs regularly have far-reaching societal implications. Policy principles and technical design principles have in common that they can help provide guidance as to how to best make such trade-offs in concrete cases.

The interplay between policy and technology in the Internet is profound, and so are the similarities between some fundamental design principles of the Internet and certain fundamental democratic principles.

As the name suggests, net neutrality is essentially a non-discrimination principle which applies to the transmission of Internet traffic.[142] Net neutrality prescribes that in principle, all Internet traffic must be transmitted equally, or at least in a manner that does not favour or, in particular, disfavour specific applications, content, services, devices and uses.[143]

This principle is closely related to, and follows from, the end-to-end principle, which prescribes that the functionalities (and therefore the 'intelligence') of a network should be placed at the edges (hosts) when possible and at the core (routers) only when necessary.[144] As such, the end-to-end principle recalls the democratic principle of subsidiarity, which prescribes that power and autonomy should be decentralized as much as possible and centralized only to the extent this is necessary for a legitimate (public) purpose. Recognizing this similarity helps to understand the importance of net neutrality and explains why net neutrality can be regarded as a constitutional principle of modern (European) information societies, potentially of similar importance as other fundamental principles which guide the democratic organisation of society, such as trias politica.

The principle of subsidiarity has a related but slightly different meaning in European human rights law, in the sense that any (centralized) state interference or restriction with respect to a fundamental right, such as the freedom of speech, can only be justified to the extent that such interference is necessary and proportionate to achieve a narrowly circumscribed legitimate aim, and only the least restrictive measure that is still sufficiently effective may be used. In a similar fashion, it can be argued that any restriction, discrimination or other kind of (centralized)

---

142) Wu may have better called it Internet neutrality instead of network neutrality, because the principle is commonly understood to apply only to Internet traffic and not necessarily to traffic which may flow through specialized services offered on closed digital networks utilizing the Internet Protocol.

143) For further explanation of the concept of application-agnosticism, see Van Schewick 2012.

144) The “broad version” of the end-to-end principle is defined by Barbara van Schewick as follows: “a function or service should be carried out within network layer [i.e., available to all clients of the network] only if it is needed by all clients of that layer.” Art. 5(3) of the Treaty on the EU states: “Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

interference by Internet providers with respect to the transmission of Internet traffic, should only be allowed to the extent that such interference is necessary and proportionate to achieve a narrowly circumscribed legitimate aim, such as protecting the integrity and security of the network, the services delivered through it, or the devices connected to it (e.g. blocking malware, (D)DoS attacks, etc).

The combined technical design principles of modularity, layering and end-to-end help to make the Internet as a whole open, versatile, flexible and robust, at the cost of some efficiency that could be achieved by integrating layers and implementing functionalities within the network, thus optimising the network for specific applications.[145] This design simultaneously facilitates the individual and collective self-determination of Internet users, by giving them the ability to receive and impart any online content, applications and services of their choice, through any Internet-connected device of their choice, and communicate with any other willing Internet user, without having to obtain permission from any Internet provider, nor requiring a contractual relationship with any Internet provider other than their own.

Democratic societies are (also) based on the ideal of individual and collective self-determination and as a system of governance, a democracy can be argued to be more robust, flexible and open than a totalitarian society, be it at the cost of some efficiency that could be achieved if all aspects of life could be centrally controlled and all opposing voices silenced.

Another remarkably democratic element of the Internet's architecture is that the technological protocols that make things work, are created through open, transparent and participatory processes, which appear to embody the Habermassian ideal of a practical discourse.[146] This practical, open, transparent and quintessentially democratic approach to the creation of Internet protocols is now increasingly mirrored in processes and initiatives to develop Internet-related policy. For example, multiple Internet consultations about net neutrality have been organised by the European Commission before it elaborated its draft Regulation[147] and the Dynamic Coalition on Net Neutrality[148] has deployed an open, participatory process to elaborate a model legal framework on net neutrality, aiming to maximize the Internet's public-service and fundamental rights value, while spreading out the power to innovate to all Internet users, rather than consolidating such power with only a few Internet providers. Such participatory and multi-stakeholder processes of

145) For a much more detailed and complete analysis and description of the principles of modularity, layering and end-to-end, see Van Schewick 2010.
146) See: Belli & Van Bergen 2013.
147) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, 2013/0309 (COD).
148) http://www.intgovforum.org/cms/dynamic-coalitions/1330-dc-on-network-neutrality.

Internet governance, enabled by and through the Internet itself and intended to protect the democratic values embedded in the Internet's architecture, speak to the ideal formulated by Al Gore in 1994, to use the Internet to create a 'New Athenian Age of Democracy'.[149)]

Analogous to the democratic ideal that the existence, organisation and power of nation states is legitimized by the needs and wants of the citizens and population at large rather than the whims and desires of a ruling elite, the existence of any telecommunications network is ultimately legitimized by the users' wish to communicate rather than the profit that can be made from the exploitation of the network by a provider. To the extent that market forces fail to correctly balance and align the interests of those who provide access to the Internet and those who use such access, a democratically adopted correction is in order.

3 Legislative developments and trend

Over the last years, the following legislative developments have taken place with respect to net neutrality.

▪ In November 2009 the New Regulatory Framework (“NRF”) on telecommunications was adopted by the European legislator. This NRF contained transparency requirements for electronic communications companies and the “Commission Declaration on Net Neutrality”, in which the European Commission declared to “attach high importance to preserving the open and neutral character of the Internet, taking full account of the will of the co-legislators now to enshrine net neutrality as a policy objective and regulatory principle to be promoted by national regulatory authorities.” Recital 28 of Directive 2009/136/EC states that “National regulatory authorities should promote users’ ability to access and distribute information and to run applications and services of their choice, as provided for in Article 8 of Directive 2002/21/EC (Framework Directive)”

▪ In July 2010 Chili became the first country in the world to adopt legislation aimed at protecting net neutrality. The Chilean law forbids Internet providers from arbitrarily blocking or discriminating against legal activity conducted through the network (paraphrased from an unofficial translation).[150)]

▪ In November 2010 the European Commission held a “Summit on 'The open Internet and net neutrality in Europe'”, following a public consultation phase from

149) Al Gore, Information Superhighways Speech International Telecommunications Union Monday March 21, 1994, available at http://vlib.iue.it/history/internet/algorespeech.html.

150) Technollama.co.uk, 28 January 2012, 'Chile enforces net neutrality for the first time, sort of', <http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of>.

the end of June till the end of September, which attracted 318 responses. The Commission's report on the consultation stated that “in general, respondents consider the EU telecoms framework to be capable of dealing with the issues identified (question 3) and only very few advocate additional regulation at this stage.”[151]

▪ In December 2010 the FCC adopted rules which forbid network operators to block lawful content, applications, services, or non-harmful devices, subject to reasonable network management. Some US human rights language was used, such as the term 'narrowly tailored'.

▪ In December 2010 the Parliament of Israel adopted a law to prevent wireless operators from blocking or limiting the use of services and applications delivered over the Internet (including VoIP).[152]

▪ In July 2011 a proposal was launched in the Belgian Parliament for the same law text as that which the Dutch Second Chamber of Parliament had adopted in June 2011.

▪ In November 2011 the European Parliament adopted a resolution, in which Parliament has “called on the Commission to safeguard the principles of the neutrality and openness of the internet and to promote end users’ ability to access and distribute information and run applications and services of their choice.”[153]

▪ In May 2012 the Dutch First Chamber approved a law proposal to protect net neutrality. The Dutch law holds that network and Internet providers may not block or hinder online applications unless necessary for a legitimate aim listed in the law (e.g. mitigate congestion, protect safety of network and devices). The format of the law was inspired on that of article 10 ECnHR. EU Commissioner Kroes of the Digital Agenda has publicly spoken out against the Dutch law on several occasions, calling it 'premature'.[154]

---

151) This may be considered surprising, given the fact that submissions made by civil society organizations such as European Digital Rights, Bits of Freedom and La Quadrature du net, the Free Knowledge Institute, The International Telecommunications Users Group, Universities such as the Essex University, as wel as prominent application providers such as Skype had (often loudly) cried for additional regulatory measures to ensure end users' ability to access and distribute the information or run the applications and use the services of their choice on the Internet.

152) Broadband Traffic Management, 7 December 2010, 'Net Neutrality [Israel] – Parliament Approved Wireless Neutrality' <http://broabandtrafficmanagement.blogspot.be/2010/12/net-neutrality-israel-parliament.html>.

153) European Parliament 7 November 2011, 'European Parliament resolution on the open internet and net neutrality in Europe'

154) ZDNet 3 October 2011, 'Kroes attacks Dutch net-neutrality rules', <http://www.zdnet.com/kroes-attacks-dutch-net-neutrality-rules-3040094084/> (l.c.o. 3 February 2013); Telecompaper 14 June 2011, 'Kroes says Dutch net neutrality rules premature' <http://www.telecompaper.com/news/kroes-says-dutch-net-neutrality-rules-premature--809381>.

▪ In May 2012 BEREC published its report on traffic management, showing that at least 20% of all Internet users and potentially up to half of all mobile Internet users, have contracts that allow restriction of services like VoIP or P2P, while contractual restrictions on P2P are enforced by 90% of operators and contractual restrictions on VoIP are technically enforced by 56% of the mobile operators.

▪ In August 2012 the Ministry of Communications of Israel submitted a proposal to extend net neutrality from mobile to all telecom operators.

▪ In December 2012 the ITU convened in Dubai for the International Telecommunication Regulations (ITRs). Some initiatives for alternative charging models regarding Internet traffic, such as the 'sending party network pays' (SPNP) model had been proposed, but were not adopted, after much criticism was voiced on these proposals.[155] ETNO had also proposed to include a provision holding that "Nothing shall preclude commercial agreements with differentiated quality of service delivery to develop", which could be interpreted to hold that ITU member states would no longer be allowed to adopt net neutrality regulations, and which provisions were not adopted.

▪ In December 2012 the Slovenian Parliament voted for net neutrality legislation which resembles the Dutch law in that it forbids blocking, throttling or otherwise hindering Internet traffic, unless necessary for a limited list of legitimate aims.

▪ In November 2012 BEREC published a summary of its positions and lines of action on net neutrality. In this document BEREC expressed that it "is committed to the open Internet, and believes that the existing regulatory tools, when fully implemented, should enable NRAs to address net neutrality-related concerns."[156]

▪ In January 2013 the Dutch law on net neutrality entered into force.

▪ In March 2013 the National Digital Council (Conseil national du num?rique or CNNum), on request of the French government, published an opinion recommending the government to include net neutrality obligations in the law. The proposal has been criticized by some for being too vague and not specific enough.[157]

---

155) E.g. Forbes 8 September 2012, 'Why is the UN Trying to Take over the Internet?' <http://www.forbes.com/sites/larrydownes/2012/08/09/why-the-un-is-trying-to-take-over-the-internet/3/> (l.c.o. 18 March 2013); see also BEREC 14 November 2012, 'BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines' <http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines>.

156) BEREC November 2012, 'BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines' <http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines>.

157) Arstechnica.com 13 March 2013, 'France could join the small club of countries that require net

▪ In September 2013 the European Commission issued its Draft Regulation on the European single market for electronic communications and to achieve a Connected Continent. Article 23 forbids blocking and throttling of specific content and applications, except when necessary and proportionate to an exhaustive list of narrowly circumscribed legitimate aims.

From the above we can conclude that there is a clear trend towards the enshrinement of net neutrality into law and policy. Human rights considerations play an increasingly important role in the net neutrality debate, which is also reflected in the language of several adopted and proposed legal statutes relating to net neutrality.

The most important issues in the net neutrality debate in Europe currently revolve around the definition and demarcation of specialized services, where the Draft Regulation arguably leaves something to be desired, and the prohibition of pay-for-priority business models on the Internet, which seems essential to any true protection of network neutrality, but does not appear to clearly follow from the language of the Draft Regulation.

References

Belli & Van Bergen 2013: Belli, L and Van Bergen, M., A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application, in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, 2013, available at http://nebula.wsimg.com/a0d2191d5788b8177915108786bfba7a?AccessKeyId=B45063449B96D27B8F85&disposition=0.

Bendrath & Mueller 2010: Bendrath, R. & Mueller, M. The End of the Net as we know it? Deep Packet Inspection and Internet Governance, available at http://ssrn.com/abstract=1653259.

CBUI 2002: Ex Parte Letter from CBUI to Michael K. Powell, FCC Chairman, CC Docket Nos. 02-33, 98-10 & 95-20, CS Docket No. 02-52, and GN Docket No. 00-186 (November 18, 2002).

Lemley & Lessig 1999: Lemley, M.A., Lessig, L., Ex parte declaration of Professor Mark A. Lemley and Professor Lawrence Lessig in the matter of: Application

---

neutrality'
<http://arstechnica.com/tech-policy/2013/03/france-could-become-worlds-third-net-neutrality-nation/>.

for consent to the transfer of control of licenses of Mediaone Group, Inc. to AT&T Corp, CS Docket No. 99-251, before the Federal Communications Commission.

Lessig 1999: Lessig, L., Code and other laws of cyberspace. New York: Basic Books.

Lessig & Wu 2003: Lessig, L. and Wu, T., A Proposal for Network Neutrality, Ex Parte Submission in CS Docket No. 02-52 (August 23, 2003).

Noam 1994: Noam, E. M., Beyond Liberalization II: The Impending Doom of Common Carriage, Telecommunications Policy Volume 18, Issue 6, August 1994, Pages 435?452.

Nunziato 2009: Nunziato D., Virtual Freedom, Net Neutrality and Free Speech in the Internet Age. Palo Alto, Stanford University Press 2009.

Privacy International & GreenNet 2003: Banisar, D. et al, Silenced: an international report on censorship and control of the internet. Stanford, Privacy International & GreenNet Educational Trust 2003, available at http://www.privacyinternational.org/survey/censorship/silenced.pdf.

Van Schewick 2010: Van Schewick, B., Internet Architecture and Innovation. Londen, The MIT Press 2010.

Van Schewick 2012: Van Schewick, B., Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like, The Center for Internet and Society, June 2012.

Wu 2002: Wu, T., A Proposal for Network Neutrality, available at http://www.timwu.org/OriginalNNProposal.pdf.

Zittrain 2008: Zittrain, J., The Future of the Internet and How to Stop It. New Haven, Yale University Press 2008.

인터넷 거버넌스와 이용자

김보라미[158)]

1. 망중립성 이용자 포럼과 인터넷 거버넌스

지난 2년간 “망중립성 이용자 포럼"은 망중립성의 국내정책결정에서 의견을 표명하고, 필요한 제안을 하는 등 관련활동을 해 왔다. 망중립성 이용자 포럼이 처음 망중립성 이슈를 문제 삼았던 가장 큰 이유는, 방송통신위원회가 모바일 인터넷 전화를 제한하는 이동통신사들의 약관을 현행 전기통신사업법의 규정들에 반하여 이용자의 권리를 침해하면서까지 승인해 준 것 때문이었다.

그러나 이 문제를 풀어가는 과정에서 광의의 망중립성 문제는 단지 통신사들이 인터넷 이용방법에 제한을 가하는 것만이 아니라는 점이 명확해졌고, 가장 본질적인 문제는 “인터넷이 더 이상 우리가 이용하던 인터넷”이 아니게 된다는 것에 있었다. 즉, 그동안 평등하고, 진입장벽이 없다고 생각해 왔던, 또는 가정해왔던 인터넷이, 우리가 생각하는 이상과는 다른 방향으로 발전할 수도 있는 징후들이 곳곳에서 나타나기 시작한 것이다. 망중립성에서 가장 큰 문제는, “DPI(Deep Packing Inspection)"의 활용으로 인터넷 망 이용환경이 실시간 감시체제로 변화되고 있다는 것인데 이런 감시기술의 발전은 이 징후들의 가장 대표적인 예이기도 하다. 그렇다! DPI나 그와 유사한 데이터 추적기술들은 이미 현재 우리의 현실에 존재할 뿐만 아니라 필수적이라고까지 평가되고 있다. 누군가는 어디에선가 망의 일시적 혼잡과 안정성 확보를 위한 명목으로, 또는 경제적으로 차별하려는 의도적인 명목으로 우리의 인터넷 패킷들과 인터넷 활동 내역들을 보고 있다. 결국 이 문제는 국내만의 문제라기보다는, 전 세계적으로 나타나고 있는 인터넷의 통제와 감시에 대한 국제적인 문제일 수밖에 없다.

더 이상 인터넷상의 문제들이 몇몇 주권국가들의 권한행사만으로, 또는 몇몇 주권국가들에 대한 통제만으로는 해결될 수 없는 상황에서 중요한 문제는 “누가, 어떻게” 문제를 해결해야 하는가라는 질문이 나올 수밖에 없게 된다. 결론적으로 이 문제는, 단대단 원칙이 최

158) 변호사, 망중립성 이용자 포럼 코디네이터, squ24n@gmail.com
망중립성 이용자 포럼 (http://www.nnforum.kr)은, 11개 시민단체가 망중립성에 대한 합리적이고 이용자 친화적인 논의를 위하여 창립한 수평적 포럼으로 통신요금과 통신정책 등 망중립성과 관련된 다양한 주제로 지속적인 포럼을 개최하며, 포럼에서 논의된 내용을 토대로 정책제안, 입법청원 등 이용자 중심의 망중립성 정책의 마련을 위한 다양한 활동 전개하고 있다. http://www.nnforum.kr/61

종 이용자(end-user)에게 망에 대한 선택권과 통제권을 줄 수밖에 없는 중요 근거가 된다는 것, 최종 이용자들의 선택권과 통제권이 망중립성의 중요원리로 이해되는 것과 유사하게 접근할 수밖에 없다. 즉, 망중립성 논의에서 주체로서 인식되는 최종 이용자들이, 국제적인 인터넷 정책에 있어서도 중요 주체로 인식되어야 하며 그들의 참여 방법 역시 사실상 그리다를 수 없게 될 것이다.

2. 인터넷의 구조와 설계 원칙

인터넷이 시작된 것은 냉전시대의 미소간의 분쟁이 극에 달하였을 때 미국에서 핵무기 발사와 관련된 미대통령의 명령이 소련의 공격에도 불구하고 시의 적절하게 전달되어야 한다는 요구에 대한 답변으로 분산형 네트워크를 개발하면서 시작되었다. 이후 이 분산형 네트워크는 레이어링, 모듈[159], 그리고 인터넷 프로토콜(IP)을 채택하면서 언뜻 보면 호환이 되지 않는 네트워크들 간에 인터넷 프로토콜을 통하여 커뮤니케이션을 할 수 있는 중요한 계기를 마련해 주었다. 그리고 이 네트워크는 민영화 과정에서 표현의 자유를 비즈니스의 측면에서, 또는 정치적 자유의 측면에서, 다양하고 적극적으로 체험하고 실감할 수 있게 해주었다. [160] 아래에서는 이의 이해를 위하여 인터넷 계층 이론, 모듈 이론, 인터넷 프로토콜에 대하여 간단하게 설명하도록 하겠다.

1) 인터넷 계층 이론(layering), 모듈 이론

인터넷 계층 이론이라 함은 "인터넷의 각 기능은 계층으로 구별되어 있다"라는 것이고, 모듈이론은 이 계층들이 독립적인 법칙으로 운영되고, 독립적인 역할을 하는 모듈로서 역할을 한다는 취지이다. 즉, 각 계층은 서로 독립적인 규칙으로 운용되지만 전체적으로는 인터넷이 작동할 수 있게 하는 원리로 설명되고 있다. 이 계층이론을 단대단 원칙 설명에 적합하게 도식화하자면, 가장 아래에는 물리계층(physical layer), 중간에는 논리계층 (logical layer) 중 인터넷 계층(internet layer), 가장 위에는 응용계층(application layer)이 존재한다.

물리계층이란 구리선이나 광섬유 등 눈으로 직접 볼 수 있는 매개체를 통해 전송되는 단계의 계층을 의미하는 것으로, 원칙적으로 망사업자가 직접적인 역할을 한다. 논리계층 중 인터넷 프로토콜이라 함은 각 끝단의 컴퓨터들, 또는 네트워크들 간에 커뮤니케이션이 가능하도록 하는 계층으로 모두 일반에게 공개된 범용규칙으로 누구든지 활용할 수 있으며 이 단계에서 필요한 정보는 인터넷 주소정보만 있으면 된다. 응용계층은 웹브라우저, 웹사이트들이 구동되게 하는 계층으로 이 응용계층은 망사업자가 아닌 끝단의 컴퓨터들이 그 내용과 형식을 결정하게 된다.[161]

위 각 계층들은 계층마다 필요한 역할과 규칙들을 가지고 있으며, 서로 간에 중복되지 않고 다른 계층의 역할에 관여하지 않으면서, 다만 계층들의 독립된 역할들이 서로 연결되어

159) 『Internet Architecture and Innovation』, Barbara van Schewick, The MIT Press, 2010, pp.83-90
160) 『디지털 크로스로드』, 조나단 넥터라인, 필립 와이저, 정영진 옮긴, 나남, 2005, pp.236-245
161) 『Internet Architecture and Innovation』, Barbara van Schewick, The MIT Press, 2010, pp.83-90

전체적인 커뮤니케이션이 가능하도록 하는 기능을 수행한다. 따라서 물리계층은 논리계층, 응용계층에 관여하지 않고, 응용계층은 논리계층에 관여하지 않는다. 즉, 망사업자가 물리적인 망을 깔고 나면, 그 위에서 벌어지는 커뮤니케이션에 허가 등의 행위를 하지 않더라도 인터넷 상에서의 커뮤니케이션에는 아무런 문제가 없는 것이다.

2) 인터넷 프로토콜

그런데 위 계층 중 인터넷 프로토콜은 더욱 독특하게 인터넷 상의 커뮤니케이션을 형성하는데 중요한 역할을 하고 있다. 즉, 인터넷 프로토콜은 전송되는 각 커뮤니케이션 대상 데이터 패킷의 주소정보(발신자와 수신자의 인터넷 주소정보)만으로도 다른 추가적인 정보 없이도 서로 다른 물리망의 커뮤니케이션이 가능하게 하고 호환되게 하는 기적을 인터넷상에서 보여주고 있다. 즉, 원칙적으로 주소정보만 있으면 커뮤니케이션이 될 수 있는 상황에서, 추가적으로 물리망 사업자가 인위적인 추가적 감시절차를 수행하지 않는다면, 인터넷 망 끝단의 이용자들의 커뮤니케이션을 차별, 차단하게 할 능력이 없다는 결론에 이르게 된다.

이렇듯 끝단의 이용자들의 커뮤니케이션에 대하여 이용자들이 자율적으로, 망사업자들의 허가나 승인 없이도 커뮤니케이션을 할 수 있는 자유를 누릴 수 있게 해 준 것, 원래 인터넷 설계에서는 망사업자가 이용자들의 커뮤니케이션 내용을 감시하는 것이 본래적 모습이 아니라는 것 등의 속성을 단대단 원칙(end-to-end)이라 한다.

3) 최종 이용자와 인터넷 거버넌스

인터넷 이용자 개념에서 가장 중요한 것은 끝단에서 자유로운 커뮤니케이션이 가능하다는 점이다. 즉, 재미있는 것은 인터넷 이용자는, 위에서 보듯 인터넷 주소만으로 서로 간에 커뮤니케이션할 수 있는 끝단의 자들로, 원칙적으로는 지역별, 성별, 사회적 계층적인 차별 없이 하나의 커뮤니티로 묶일 수가 있다. 즉, 원칙적으로 인터넷의 이용과 같은 룰을 인터넷 커뮤니티 안에서 정하는 과정에서 정부나, 각 주권국가의 고려가 적용될 이유는 없고 이용자들 간의 논의를 통하여 자유롭게 룰을 정하는 것이 원칙이 되어야 한다. 지금은 더 이상 현실적인 논의라고 보지 않으나, 과거 인터넷에 대한 규제에 대하여는 이런 인터넷 자유론이 힘을 얻기도 하였다.

그러나 주권국가는 스스로 이 문제에 대하여 주권국가의 힘을 확장하는 방법의 국내 인터넷 정책을 펴 왔다. 그리고 여러 가지 문제들이 있지만 가장 최근의 인터넷 정책과 관련된 논의들에는 망의 보안, 안정성 등과 관련된 망중립성 논의, 표현의 자유 등과 연관된 내용규제 논의, 그리고 감시와 관련된 프라이버시 논의 등을 대표적으로 꼽을 수 있다. 이러한 이슈들에 대하여 과연 몇몇 주권국가들에 의하여 파편화된 정책으로 존치하는 것이 바람직한 것인지 의문이 제기되고 있다.

결국 이런 여러 가지 모순적이지만 현실적인 상황들, 주권국가의 존재가 인터넷 정책 결정과정에서 고려되어야 한다는 점, 전세계 이용자들이 하나의 단일 이용자 커뮤니티의 구성원임에도 각 국의 규제에 따라 다른 인터넷 환경을 경험하게 된다는 점들이 모두 다 함께 존재하면서, 비록 끝단의 이용자들이 모두 참여하여 자유롭게 인터넷상의 논의를 형성하고

발전시킬 수 있는 가능성이 애시당초 상당 부분 혼란스럽게 되었다. 하지만, 이 끝단에서 발생하는 커뮤니케이션이 파생시키는 여러 문제들에 대하여 어떻게 해결하고, 우리가 디지털 디바이드의 문제를 해결하면서 우리 인류의 현재를 꽃피워나갈 수 있는가의 논의가 인터넷 거버넌스라는 형태로 논의되고 있다. 여기에서 중요한 것은 이 논의에서 주체가 누가, 어떤 방식으로 되어야 하느냐 하는 것이다.

3. 인터넷 이용자의 개념

그렇다면 인터넷 이용자란 무엇인가. 과거 인터넷 커뮤니티란 책 한권에 들어가는 수준의 한정된 인원으로 이해될 수도 있었고, 그렇다면 그 인터넷을 이용하는 커뮤니티가 그 룰을 결정하는 것으로도 충분히 의미있는 논의가 될 가능성도 있다. 그러나 지금은 그렇지 않다. ITU에 따르면, 2011년 현재 전 세계 인터넷 이용자의 전체 숫자는 20조가 넘어서고 있다고 하며, 인터넷 접속은 현실의 복지와 경제활동에 직접적인 영향을 주고 있는 현실 때문에, 인터넷 정책은 첨예한 권리, 즉 인권의 문제가 되고 있다. 물론, 현재 인터넷 접속권 자체가 인권으로서 모두가 찬성하는 상황은 아니지만, 다른 인권의 행사를 촉진시켜주는 플랫폼으로 이해되고 있어, 인터넷 이용자들은 실제 인터넷을 이용하는 자 이외에도 보편적 인간으로 이해되어야 할 필요가 커졌다. 따라서 인터넷 정책을 논의하는 인터넷 이용자 커뮤니티는, 단순히 현재 인터넷을 이용하는 그룹이 아닌 인터넷 가능 세계의 시민이라는 측면(citizens of an Internet-enabled world)에서의 논의[162]로 확장되어야 하고 그 절차와 과정에서 '인권'적인 접근이 수반될 수밖에 없다.

앞에서 본 것처럼 인터넷이 준 장점은, 인터넷 프로토콜을 통해서 인터넷 망의 통제권을 망사업자들이 아닌 전세계 최종이용자에게 준 데에서 시작한다. 그러나 이러한 형태의 디자인 원칙이 앞에서 본 것처럼 현실의 인터넷 현실과 반드시 동일한 것은 아니다.

현실과 이상이 다르다 하더라도, 인터넷이 가지고 있는 본래적 측면을 고려할 때, 인터넷 현실과 관련된 논의들의 시작은, 인터넷에 연결되어 있는 이용자들로부터 시작할 수밖에 없을 것이다. 실제로도 인터넷 정책결정은 인터넷의 이러한 특수한 측면이 감안되어, 다른 경우와 달리, 개방적이고, 투명하며, 참여적인 방법으로 이루어져야 한다는 논리들은 여러 주장들의 설득력 있는 논거로 활용되고 있다. 실제로 이러한 인터넷 거버넌스 논의를 위하여 만들어진 IGF나 ICANN과 같은 인터넷 정책 기구들은, 멀티스테이크홀더라는 취지에서 위에서 아래로의 의사형성과정보다는, 아래에서 위로의 의사형성과정, 이해당사자들이 대다수 포함되어 논의할 수 있는 플랫폼을 제공하려고 노력하고 있다. 물론 국내에서는 이러한 절차들이 현실화되지 않고 있으나, 최근 미래창조과학부는 인터넷 정책과 관련된 "트래픽 관리안'에 대한 의견들을 수렴하면서 이러한 절차를 형식적이나마 따라하려고 노력한 바 있다. 미래창조과학부에서 민간인들이 포함된 자문위원회를 운영하고, 초안에 대한 의견을 공개적으로 수렴하고, 관련 자료들을 모두 공개하는 방향으로 정책을 변화한 것에 대하여 우리나라에서의 정책결정과정에서의 새로운 노력으로 지켜볼 필요가 있다.

---

162) http://gurstein.wordpress.com/2013/11/27/internet-justice-a-meme-whose-time-has-come/

4. 결어

인터넷의 설계원칙은 인터넷에서 다른 제3자의 간섭이나 허가 없이도 끝단에 위치한 이용자들이, 사회적 지위나 지리적 위치와 무관하게 자유롭게 커뮤니케이션을 할 수 있는 가능성을 열어 주었다. 하지만 그 가능성이 바로 정책적 현실이 되는 것은 아니고 인터넷 정책형성과정의 문제 역시 문제로 대두되고 있다. 그러나 인터넷 이용자가 바로 하나의 커뮤니티가 되는 성격을 고려할 때 인터넷 정책 형성과정에서 누가 어떻게 대표되고, 누가 어떻게 참여할지에 대한 논란, 주권국가의 위치를 어떻게 이해할 것인가의 논란은 여전히 계속되고 있다.

그러나 적어도 이 문제에서 이 하나의 커뮤니티 그룹안의 이용자들은 현재의 이용자들뿐만 아니라 보편적 인간을 포함해야 한다는 것은 인정할 수밖에 없는 사실이다. 그리고 인터넷 이용이 오늘날 오프라인의 현실과 복지에 직접적인 영향관계가 있다는 측면에서 인터넷 거버넌스의 논의에서 인권적 기준이 반드시 적용되어야 할 것이다. 미국의 NSA를 통한 전세계 시민감시의 문제로 내년에 새로운 인터넷 거버넌스의 발전적 모델에 논의가 동시다발적으로 터져 나오고 있다. 이런 논의들에 대하여 인권적 접근을 통해 좋은 프레임을 만들 수 있도록 국내적인 논의가 함께 시작되어야 할 때라고 생각한다.

ABSTRACT

Internet Governance and Users

borami Kim[163)]

Having taken actions for 2 years, Net Neutrality User Forum has realized Net Neutrality as a international issue of future Internet. Although the Internet design principle (layering, module, IP protocol) has enabled the end users to communicate each other without any additional permission or interference, in the reality, the end users have been tracked by both companies and governments, and the communications could be blocked, or restricted by surveillance devices, such as DPI , which could change the whole Internet design principle. Given that the Internet is a large community of the equal end-users based on end-to-end principle, it's essentially the issues of the whole Internet users, rather than of one nation, and we should focus on developing the transparent and participatory ways in Internet governance. The current Internet governance discussion have taken placed in ICANN, IGF, etc., in bottom-up processes of multistakeholderism to reflect the views of end-users. However there have been the controversial issues in Internet Governance, such as the position of government as a stakeholder, global north-south problem, transparency, so we have faced the debate on the new or evolving frame of Internet governance.

163) Lawyer, Coordinator of Network Neutrality User Forum

▮ 3부

인터넷 거버넌스, 어디로 갈 것인가

ITU WCIT의 위협 분석

필자 밀튼 뮬러 (Milton Meuller)[164]
번역자 박지환, 황규상[165]

1. 역사적인 맥락

국제전기통신연합(ITU)의 국제전기통신세계회의(WCIT)와 인터넷 거버넌스의 연관성은 매우 논쟁적인 주제이다. 본 주제에 대하여 관심을 표명하기 위한 조직적인 활동이 전개되고 있으며, 미국 하원에서 본 주제로 청문회[166]가 예정되어 있기도 하다.

이러한 점이 의미하는 바는 이미 인터넷이 대중에게 공개된 지 20년, ICANN이 만들어진 지 13년, 정보사회세계정상회의(WSIS)의 결과가 도출된 지 7년이 지났음에도 현재 우리는 국가 주권과 인터넷 거버넌스와의 관계에 대하여 치열하게 논쟁 중이라는 점이다. 이러한 지점은 내가 최근 저서인 "네트워크와 국가(Networks and States)"[167]를 통해 깊이 있게 다루려고 했던 주제와 정확히 일치한다. 자랑처럼 보일지 모르지만, 최근 벌어지고 있는 논쟁에 다양하게 참여해 온 필자의 경험은 역사적 관점이나 경험에 기반한 이론적 분석 측면에서 도움이 될 것으로 판단한다.

먼저 러시아와 같은 국가들이 ITU가 ICANN이나 기타 민간 인터넷 관련 기관들을 대체하길 기대하고 있다는 점에 대해서는 의문의 여지가 없다. 그러나 대부분의 사람들이 간과하고 있는 것은 몇몇 정부들이 이러한 입장을 수십 년 간 지속적으로 옹호하여 왔다는 점이고, 그들의 시도는 반복적으로 실패하고 있었다는 점이다.

이러한 역사는 다시 반추해 볼 가치가 있다. 1996년으로 돌아가 보면, ITU는 당시 도메인네임 시스템(DNS)에 대한 통제권을 차지하려고 했었고, 매우 역설적이게도 ITU는 인터넷 소사이어티(Internet Society)[168]와 함께 DNS 루트서버에 대한 관리를 민영화

---

164) 시라큐스 대학 정보사회학 교수, mueller.syr.edu@gmail.com
인터넷 거버넌스 프로젝트 운영. http://www.internetgovernance.org/
165) 서울대학교 경영대학, 사단법인 오픈넷 인턴
166) http://thehill.com/blogs/hillicon-valley/technology/229231-house-to-hold-hearing-on-international-control-of-the-internet
167) http://www.amazon.com/Networks-States-Governance-Information-Revolution/dp/0262014599
168) http://www.isoc.org/

(privatize)하여 미국 정부의 손에서 DNS 관리권을 인수(take over)하려고 했다. 그러나 미국 정부는 이들의 이러한 노력을 철저하게 짓밟았고 ICANN의 출범을 주도하였다.

국민국가의 인터넷 거버넌스에 대한 도전이 절정기에 이르는 다음 일화는 바로 2002년에서 2005년 사이에서 개최된 WSIS[169]에서 펼쳐진다. WSIS에서 몇몇 국가들은 ICANN의 존재에 대하여 이해하면서도 인터넷에 대한 국가간 기구가 부재하다는 점에 대하여 의견을 같이 했다. 이들 국가들 간에는 정부의 강화된 역할을 주장하는 거대한 공감대가 형성되고 있었던 것이다. 프랑스가 주도적 역할을 했던 유럽연합 집행위원회(European Commission, EC)와 더불어 브라질, 아랍 국가들, 이란, 남아공, 그리고 수많은 아프리카 국가들, 중국, 러시아 등 국가들은 미국이 DNS 루트서버에 대하여 주도적인 역할을 하는 것에 대하여 비판적인 시각을 견지했고 국가단위에서 기획하는 '전 지구적으로 적용 가능한 공공 정책 원칙'을 주창하기에 이르렀다. 그러나 이들 국가의 노력은 기본적인 ICANN의 거버넌스 모델을 변경하거나 인터넷 거버넌스에 대한 기본적인 접근조차 실행하지 못한 채 실패하고 만다. WSIS는 간접적으로나마 ICANN 내에서 정부의 역할을 강화하는데 영향을 미치긴 했는데, 그마저도 미국이 .xxx (성인물) 도메인을 금지하기 위하여 ICANN 내의 정부자문위원회(GAC)[170]에서 정책 결정에 개입하려 했던 것이 더욱 결정적인 기여를 하였기 때문이다.

2009년과 2010년 사이 ITU는 IP 주소 관리[171]에 대한 스스로의 역할을 확대하기 위해 노력하였다. 최근 WCIT-12에서 표출되었던 많은 우려들은 2010년 과달라하라(Guadalajara)에서 개최된 ITU 전권회의[172]에서도 이미 표출된 바 있다. 2010년 전권회의의 결과에 대한 일련의 우리가 알고 있는 보고들[173]이 의미하는 바로는, 본 전권회의에서 드러난 결의안들은 위 관리 권한을 전혀 인수(take over)하지 못했을 뿐 아니라, ITU의 결의안으로는 최초로 ICANN을 언급하면서 오히려 그들에게 해당 권한을 양보하는 듯 보였다. 러시아와 같은 국가들은 ICANN의 GAC을 관리 권한을 가진 국가 간(intergovernmental) 기구로 변환하거나 ITU와 ICANN 사이의 발전적 협력에 대한 합의를 도출하고 정부의 참여를 증대하는 메커니즘을 정의하자고 제안하였으나, 이러한 제안은 문서에서 모두 삭제되었으며, 서서히 진행되어가고 있던 국가중심주의 기획은 일단 실패를 맛본 셈이다.

가장 최근으로 2011년에는 인도, 브라질, 남아공이 UN에 '인터넷 관련 정책위원회'(Committee on Internet Related Policies, CIRP)를 창설하자는 제안이 있었다.[174] 본 제안이 UN의 관리 권한 인수라는 측면에서 경종을 울리는 성격의 것이었지만, 본 제안은 사실상 UN 총회에서 검토될 제안서를 생산해내는 정책 개발 위원회(policy development committee)와 관련된 것이었다. CIRP는 비정부 이해당사자(non-governmental

169) http://www.itu.int/wsis/index.html
170) https://gacweb.icann.org/download/attachments/1540116/GAC_25_Wellington_Communique.pdf?version=1&modificationDate=1312543504000
171) http://www.itu.int/dms_pub/itu-t/oth/06/2C/T062C0000010001PDFE.pdf
172) http://www2.afrinic.net/news/ITU_mexico.htm
173) http://www.internetgovernance.org/2010/10/28/free-online-access-to-itu-resolutions/
174) http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html

stakeholder)를 대표하는 구조는 거의 가지고 있지 않았으나, 그 자체로 구속력이 있거나 규제 권한을 가지지 않았으며 오로지 제안서를 생산하는 능력만을 가지고 있었다. 정부들은 제안서를 바탕으로 협상을 하거나 이를 조약 비준의 단초로 삼을 수 있을 뿐이다. 필자의 생각으로는 이 같은 방식은 좋은 생각은 아니라고 판단되는데, EU나 미국과 같은 주요 인터넷-경제 국가들이 조약 비준을 거부한다면, 이러한 시도는 사실상 어떠한 영향도 미칠 수 없기 때문이다. 그럼에도 이들 국가의 제안은 강력한 반발에 부딪혔다. 브라질은 차후에 본 제안을 철회하였고, 인도는 여전히 이를 지지하고 있으나, 일부 보도된 것과는 다르게[175] 인도 정부의 지지 의사가 인도 내 인터넷 검열[176]로 이어질 것을 우려하는 의회[177] 및 제3세계의 시민사회 그룹으로부터 공개적으로 비판을 받고 있다.

CIRP 제안은 그 자체로 많은 정부들이 IGF에 불만을 가지고 있다는 점을 방증하며, 특히 제3세계(the global south) 내에 위치하고 있는 신흥 개발국의 불만을 잘 보여주고 있다. IGF는 WSIS의 주요 결과물이었으며, 인터넷 자원에 대한 미국의 영향력에 대한 해결되지 않은 논쟁을 공개적이고 멀티스테이크홀더 방식의 포럼을 통해 논의하는 장으로 기획되었다. 그러나 인터넷 거버넌스의 현상 유지(status quo)적 관점에 대하여 비판적인 논조를 가진 비평가들은 IGF에 대한 환멸을 보이기도 하였다. 몇몇 정부들은 다른 이해당사자 그룹과 동일한 지위에서 협력하는 것에 대해 소극적이었다. 시민사회의 비평가들은 기득권에 대해 현상유지를 원하는 참여자들이 IGF에서 논쟁적인 이슈가 논의되거나 권고안이 도출되는 것을 방해하고 있다고 지적하였다. 서구 기업부문 이해관계자들은 재해구조나 그린 IT(green IT) 등 글로벌 인터넷 거버넌스와 직접적 관련이 없는 이슈에 대한 의미 없는 덕담(happy talk)으로 일관하여 IGF에 대한 불만족에 기여하기도 하였다. 이 같은 양상은 유엔 차원의 IGF 개선을 시작하도록 하였는데, 여기서 개선이란 IGF를 보다 관료체제화(bureaucratization)하는 것을 포함하며, 이는 더욱 약화된 형태의 IGF(weaker IGF)를 지지하는 세력이 반대해온 것이기도 하다.

이하는 위 논의의 요약이다.

1. UN 혹은 ITU의 인터넷에 대한 영향력을 강화하려는 움직임은 갑작스러운 일이 아니다. 대신 네트워크와 국가 간의 국가적 수준과 지구적 수준에서의 긴 세월에 걸친 투쟁이 존재하였던 것이다. WCIT 논의는 가장 최근의 사례이고, WSIS와 비교하면 지엽적인 수준에 불과하다.

2. 국가와 ITU와 같은 국제기구에 대한 정치적 지지(political support)가 확대되고 있다는 증거를 찾기 어렵다. 기존처럼 같은 행위자들이 같은 역할을 수행하고 있는 것이다. 오히려 정부간 협력주의(intergovernmentalism)는 약화되는 양상이며, 브라질의 CIRP 포기가 그 예이다.

3. ITU는 그야말로 종이호랑이(paper tiger)다. ITU가 1996년부터 인터넷에 대한 통제권

175) http://www2.afrinic.net/news/ITU_mexico.htm
176) http://www.timesofassam.com/headlines/censorship-on-internet-another-dictatorship-of-congress/
177) http://indiatoday.intoday.in/story/mp-rajeev-chandrasekhar-global-internet-censorship-wsis/1/189131.html

을 잡으려는 노력을 해왔지만 이러한 점이 인정되거나 WSIS 또는 어떠한 국제 개발 차원에서도 강화되었다고 보기 어렵다.

4. 정부 간 협력주의는 쇠퇴하고 있는 이데올로기이다. 개발도상국과 브릭스 국가들은 여전히 미국의 경제적, 정치적 선도성에 대하여 분개하고 있고, 정부간 기구를 그러한 분개를 표현하는 수단으로 바라보고 있으나, 그들은 초국가적 기구들에 의한 국가 차원의 인터넷 통제권 주장에 대해 반복적으로 성공하고 있지 못하다. 이들 국가의 시민사회와 기업들은 양분되어 있는데, 그들이 그들 정부의 노력을 언제나 지지하고 있는 것은 아니다. 대부분의 인터넷 관련 활동가들은 멀티스테이크홀더 방식의 거버넌스 즉, 국가의 역할을 축소하는 방향에 서 있다.

5. 가장 강력한 위험요소는 각 국가 단위에 존재한다. 국가들(인도, 중국, 러시아 뿐 아니라 미국, 영국 그리고 다른 서방 민주주의 국가도 포함된다)은 그동안 국가 단위의 사법권 행사방식과 마찬가지로 인터넷에 대해서도 새로운 규제를 하기 위한 중요한 진전을 이루어 왔다. 이와 같이 세계의 각 정부들이 인터넷을 국가 단위로 제제하려고 한다면 결국 이들간 국제적인 통제에 대한 합의에 이르게 될 것이고, 이러한 움직임은 실제로 매우 위험한 것이다. 그러나 우리는 아직 그러한 합의와는 매우 먼 거리에 있다.

따라서 ITU와 ITU의 국제통신규칙(International Telecommunication Regulations, 이하, “ITR”)에 대한 사람들의 경고에 귀를 기울이기 보다는 현실적인 위협과 맥락에 대한 분석이 요구되며, 이에 다음 장에서 ITR 및 이를 통해 그들이 행하려고 하는 것에 대한 관심이 어떻게 실제로 초래되었는지에 대하여 보다 세부적으로 살펴볼 예정이다.

2. 전기통신 vs 인터넷

ITU의 WCIT에서 실제로 무슨 일이 일어나고 있는지 이해하기 위해서는, 우선 매우 오래된 질문으로 돌아가야 한다. 인터넷은 전기통신(telecommunication)인가 아니면 다른 무엇인가? 이와 같은 정의에 관련된 다분히 모호한 질문은 1960년대 중반부터 커뮤니케이션 및 정보 정책의 중심에 위치하고 있었으며, 단순히 UN이 인터넷을 장악하려 한다는 차원이 아니라, WCIT을 이해하는 출발점이 되어야 한다.

50년도 전에 미국의 연방통신위원회(FCC)는 ‘기본(basic)’적 전기통신(1960년대와 70년대에 전기통신은 AT&T 사에 의해 독점적으로 운영됨)은 엄격하게 규제되어야 하나, 반면 ‘응용(enhanced)' 서비스 (예컨대 전화 네트워크를 이용하여 시작된 네트워크 컴퓨터 서비스 등)에 대해서는 개방되어야 하며 규제도 완화되어야 한다고 결정한 바 있다. 이러한 정책 목표를 가능케 하기 위해서 FCC는 ‘기본’ 서비스와 ‘응용' 서비스에 대한 규제를 구분하였다. 전기통신의 경우 신호(signal)가 직접적으로 전송되는 것이라면, ‘응용' 서비스는 전기통신에 ‘정보처리(information processing)'가 부과되는 형태였다.

그 당시 PTT(postal, telephone and telegraph monopolies)로 알려진 전통적 전기통신(데이터 통신에 대한 OSI 모델[178]의 layer 1 물리계층 및 Layer 2 데이터링크 계층)은 매

178) http://support.microsoft.com/kb/103884

우 엄격하고 경쟁 보호적이며, 대체로 정부 소유 방식에 의해 독점적으로 제공되었다. 정보서비스(information services)가 별개의 규제/법체계 하에 놓이면서 정보서비스 제공자는 전기통신 기본설비(infrastructure)를 제한 없이 사용할 수 있었으며, 통신회사에 대해 정부가 세워둔 진입 장벽이나 게이트키핑(gatekeeping) 규제의 대상이 되지도 않았다. 1980년대와 1990년대에 이르는 기간 동안 많은 국가들은 그동안 외국 회사와의 경쟁에서 자국의 전기통신 사업을 계속 보호하는 것과 교환하여 정보서비스 시장을 개방하는 것을 마다하지 않았다.

이처럼 전기통신과 정보서비스의 구분은 개방적이고, 경제적으로나 정치적으로 자유로운 인터넷을 구축하는 주춧돌 역할을 하였다. 인터넷 프로토콜은 기본적으로 소프트웨어 성격이기 때문에 '정보처리'나 '응용(enhanced)' 서비스로 포섭될 수 있었다. 1990년 초반에 인터넷이 입소문을 탔을 때, 국제적으로 정보 서비스에 대한 탈규제 양상을 이용하여 리좀(rhizomes, '땅속 줄기'를 뜻함)과 같이 널리 확산될 수 있었다.

1980년대부터 layer 1-2 전기통신 서비스 역시 자유화(liberalize) 수순을 밟게 된다. 새로운 경쟁자들은 세계 시장에 진입하는 것이 가능해진 것이다. 공공 기반시설은 보다 다양해지게 되었으며, 정부가 소유하던 이른바 PTT 서비스도 민영화(privatize)되기 시작한다. 가격 및 상품에 대한 규제는 철폐되었고, 무선 네트워크는 유선 네트워크를 대체하기 시작했다. 산업이 보다 다변화되고 경쟁적으로 변모하면서, 분명하던 '전기통신'과 '정보서비스' 간의 구별이 복잡해지기 시작한다. 무어의 법칙(Moore's law)과 광대역 통신(bandwidth)이 결합되면서 전통적인 전기통신이나 방송망을 대체하는 over the top(OTT)서비스인, 예컨대 인터넷 전화(VoIP), 비디오 스트리밍, 또는 인스턴드 메시징(instant messaging) 등 어플리케이션 단에서의 서비스가 가능해졌다. 이에 따라 수천 개의 서비스를 호스팅하는 단일의 독점적인 플랫폼 대신 다양한 통신사의 플랫폼이 제공하는 다양한 서비스를 이용할 수 있게 되었다. 통신사의 플랫폼 밖에서 서비스 제공자들이 운영되는 것은 매우 어려웠고, 반대도 마찬가지였다.

이에 뒤이은 논쟁은 자유 시장, 그리고 계약 기반의, 탈규제적인 인터넷 모델을 옹호하는 측과 규제자로 하여금 ISP를 규제 대상인 기간통신 사업자(common carrier)와 같이 취급하여 1990년대의 인터넷을 보호하기를 희망하는 자들 간에 이루어진다. 이는 기존의 전기통신-정보서비스 이분법에 기반해 있는데 2005년에 이러한 구분은 다시 한 번 확정된다. 바로 Brand X 판결에서 미국 연방대법원이 파월(Powell)의 FCC가 케이블 모뎀 기반 인터넷을 '정보 서비스'로 구분한 것을 인정한 것[179]이 그것이다. 미국 내 망중립성(Net Neutrality) 옹호자들은 본 결정에 반대 입장을 표명했는데, ISP들을 '전기통신'이 아닌 '정보 서비스' 사업자로 구분하게 되면 기간통신 사업자에게 부여되는 규제가 적용되지 않기 때문이다. 그러나 망 사업자들은 잠재적으로 그들을 약화시킬 정치적, 규제적 개입으로부터 면제되었는데, 특히 상호접속에 대한 규정이 대표적인 사례였다.

그렇다면 이러한 점이 WCIT 및 ITR과 무슨 관련이 있는 것인가? 그것은 다음과 같다. ITU가 ITR을 개정 하려는 것은 전기통신과 정보서비스 사이의 경계에 대하여 논의하려는 새로운 시도인 것이다. 예컨대 어떤 서비스가 전기통신으로 정의되는 순간, 전통적인 전기

179) http://www.law.cornell.edu/supct/pdf/04-277P.ZO

통신을 지원하기 위해 디자인된 국제적 규제의 대상이 된다. 대부분의 ITR 개정은 ISP간 상호접속 규정을 목표로 하고 있다. 왜냐하면 Layer 4 이상에서 급증하고 있는 인터넷 경제로부터 소외된다고 느끼고 있는 해외의 전기통신 담당 책임자들과 특히 개발도상국의 관료에 의하여 많은 부분 이러한 노력이 가속화되고 있기 때문이다. 이러한 측면에서 개정 노력은 다분히 반응적(reactionary)이거나 위협적인 것이다.

그러나 이를 두고 ITU가 인터넷을 접수(take over)하려 한다고 해석하는 견해는 틀렸거나 순진한 것이다. ITU나 산하기관이 기반하고 있던 계약조건들(terms and conditions)의 점점 많은 부분들을 규정하며, *오히려 인터넷이 전기통신(telecommunication) 세계를 접수하고 있다.* 인터넷을 기반으로 하는 서비스의 수익 면에서의 성장은 전기통신 사업자들의 그것을 훨씬 능가하고 있다. 전기통신 플랫폼을 기반으로 새롭고도 멋진 경제 영역이 출현하고 있는 것이다.

이러한 이슈는 상호접속(interconnection) 경제 부문에서 주로 논의되는데, 예컨대 데이터 트래픽의 유입 및 유출과 관련된 수익의 배분에 대한 것이 대표적이다. 이러한 점은 IETF나 ICANN, 또는 IP 주소 등록 등에 대한 장악 시도와는 거의 무관하다. WCIT 역시 두 가지 체제 간의 충돌이다. 대체로 사적으로 협의된 계약에 기반하고 있으며, 세계적으로 교류가능하며, 거리에 민감하지 않은 인터넷 프로토콜에 의해 만들어진, 허가가 불필요한 서비스 제공에 기반한 초국가적(transnational) 체제가 그 하나이며, 다른 하나는 통신회사를 둘러싼 일련의 계층적인 규제(hierarchial regulation)와 국경 단위의 게이트키핑(gatekeeping)에 기반한 국민국가 시스템(nation-state system)이 그것이다. WCIT내의 가장 치열한 전장은 검열이나 보안문제가 아니다. 당신이 국가적 규제 당국이 ISP 일반에 대해 공동 규제(collective regutlation)하기를 원한다면, WCIT의 이 같은 노력을 지지해야 할 것이다.

ITU와 그 구성원들은 언제나 그래왔듯 한발 물러서서 반응하는 중이다. ITR은 1988년에 규정되었는데, 이때는 우리가 아는 공공 인터넷(public internet)이 존재하기도 이전이다. ITR은 오래된 대상들을 다수 포함하고 있는데, 예컨대 여전히 텔렉스(telex)를 다루고 있다. ITR이 존재해야 할 이유가 있다면 이를 개정하고 있지 않다는 점은 오히려 매우 이상한 일일 것이다. 그러나 이러한 지점은 아무도 묻고 있지 않지만 매우 흥미로운 질문으로 연결된다. “과연 ITR이 존재해야 하는가? 그리고 왜 우리는 ITR를 필요로 하는가?”

정부간 기구에 의하여 체결된 조약에 기반한 전기통신 규제들의 존재는 전기통신 서비스가 국영 독점 방식으로 제공되는 시점에는 의미를 가질 수 있다. 국가 통신당국을 가로지르는 전기통신 상호접속을 협의하는 것은 상호 여권/비자 인정 협약을 협의하는 것과 매우 유사하다. 또한 많은 정부들은 호환되지 않는 그들만의 기술 표준을 가지고 있었으며, 호환성 없는 국가 단위의 전기통신 표준 체제 역시 가지고 있었기 때문에, 국제기구를 통하여 각 국가표준 간 호환성을 논의하는 것은 의미가 있었던 것이다.

그러나 인터넷의 세계는 이와 매우 다르다. 인터넷은 서비스가 자유롭게 교역되는 곳이고, 초국가적 서비스와 기업 그리고 많은 사적 영역에서 자발적으로 구성된 기술표준 관련 포럼들, 더 이상 국영이 아닌 민간 영역에서 타사와 경쟁관계에 놓여있는 다양한 네트워크 운영 회사들, 그리고 인터넷을 기반으로 복수의 플랫폼 위에서 서비스가 제공되는 세계이

다. 그런데 왜 우리는 인터넷 분야에 대한 거버넌스를 조약 체결을 위한 정부간 협의 과정에서 발생하는 그 무엇으로 다루려고 하는가?

왜 우리는 일련의 국제 통신 규제를 필요로 하는 것인가? 각 국은 상호접속, 프라이버시, 반독점, 소비자보호 등에 대한 고유한 규제 체제를 가지고 있다. 플랫폼이나 서비스 간 호환성은 1930년대보다 기술적으로 매우 해결하기 쉬워졌으며, 시장에서 해결되는 경향을 가지고 있다. 국제적 차원의 전기통신은 결국 '서비스 무역'의 영역에 놓여있는 것이며, 해외 또는 다국적 서비스 사업자가 다른 규제를 가진 시장에 진입하거나 초국가적 서비스를 제공하는 것에 대해서는 이미 WTO가 충분한 규제 기반을 제공하고 있는 것이다.

또 한 가지 간과되고 있는 사실은 ITR과 ITU가 얼마나 취약한가에 대한 것이다. 만약 당신이 적법한 절차에 따라 제정된 FCC 규제를 위반한다면, 당신은 벌금을 내거나 당신의 라이선스를 더 이상 사업에 이용할 수 없게 될 수도 있다. 그러나 ITU는 그 자체로 어떠한 경찰력도 가지고 있지 않으며, ITR 역시 회원국가 간 어떠한 것을 하자는 동의에 대한 구두 합의사항을 모아놓은 것일 뿐이다. 어떠한 회원국가가 동의하지 않거나, 동의한 것을 강제하지 않기로 결정한다면 그 합의는 전혀 의미가 없다.

필자는 WCIT에 대한 새로운 프레임을 짜는 것이 독자들이 일반적인 맥락을 좀 더 잘 이해하는데 도움이 되길 희망한다. 다음 장에서는 ITR 개정안의 구체적인 내용을 통해 과연 어떠한 내용들이 인터넷 자유에 대해 위협을 미치는지, 혹은 그렇지 않은지에 대해 살펴볼 것이다.

3. 당신에게 과금(charging)하는, 나에게 과금하는

우리는 (TD-64[180]에 담겨 있는) ITR에 관해 제안된 수정 사항들은 물론, 최근 제안된 다른 사항들이나, WCIT[181] 준비 기간 동안의 ITU 발표 내용들을 면밀히 검토해보았다. 검토 결과, 인터넷에 대한 ITR의 잠재적인 영향력은 유선 네트워크로 된 국제 인터넷 연결처리(connectivity arrangements)을 바꾸고자 하는 ITR의 시도에서 주로 나올 것이라고 본다. '*관세 및 회계, 국제 모바일 로밍, 국제 인터넷 접속, 그리고 조세 이슈에 대한 ITU의 작업'(ITU work on tariff and accounting matters, international mobile roaming, international Internet connectivity, and taxation issues)*에 관하여 잘 요약된 내용을 보려면 2012년 2월, 방콕의 WCIT 준비 회의에서 있었던 이 발표[182]를 보기 바란다. 이 제안들의 동기는 우선 경제적인 것이다. 그들은 자금의 흐름을 처리해야 했고, 또한 업체들을 통제하고 통상 교섭을 해야 하는 각국의 규제자의 역할도 다뤄야 했다. 이런 문제들이 규제나 인터넷 자원을 '접수(taking over)'하는 일보다 우선시되었다.

우리는 검열과 ITR 사이의 분리와 관련하여, 선의의 시민단체(advocacy groups)와 논쟁을 하게 되었다. (이 글에 대한 댓글[183]을 보라.) ITR 수정 사항들이 자유로운 정보의 흐름

180) http://www.internetgovernance.org/2012/06/06/td-64-for-breakfast/
181) http://www.itu.int/en/wcit-12/Pages/default.aspx
182) http://www.itu.int/oth/T065B000010/en
183)http://www.internetgovernance.org/2012/06/07/threat-analysis-of-wcit-part-2-telecommunications-vs-internet/

을 규제하거나 통제하려는 것이라고 주장하는 것은 정치적으로 편리한 일일지 모르지만, 우리 학자들은 정확성에 대해, 그리고 관점과 맥락에 대해 주장을 해야 한다. 어떤 종류의 위협은 다른 것들보다 자신의 (지지)기반을 동원하기 쉽다는 것을 이해하지만, 우리 생각에 문제의 핵심을 오도하는 것은 장기적으로 아무에게도 도움이 되지 않는다. 실제로 그런 왜곡은 역효과를 낳을 수도 있다. 요금 체계나 경제 규제의 변화는 자유로운 정보의 흐름에 매우 중요한 영향력을 가할 수 있다. 우리가 위협을 제대로 이해하여 그들을 어떻게 다룰 것인지 알고자 한다면, 제안된 사항과 그들이 제안된 이유, 그리고 그들의 영향력이 무엇인지 정확히 파악해야 한다.

쟁점 요약

'인터넷'이라는 단어는 6개의 ITR 수정 제안 사항에 등장한다. 그리고 직접적으로 인터넷을 대상으로 삼지는 않지만, 그에 영향을 줄 수 있는 제안들도 몇 존재한다. 스팸이나 보안에 관련된 정의들(definitions)은 물론 어느 정도 영향을 줄 수 있겠지만, 직접적으로 언급된 사항들이 가장 중요한 것이며, 그리고 이들 대부분은 국제적 인터넷 연결의 경제학과 관련되어있다.

인터넷에 대한 첫 번째 언급은 국제 전기통신 서비스(international telecommunication service)를 정의하는 2.2에 대한 수정 제안에서 등장한다. 이는 정의를 확대하여 'Internet traffic termination'을 포함하도록 할 것이다. (2.2를 통째로 삭제하자는 반박 제안도 존재한다.) 4.2를 수정하고자 하는 비슷한 제안에서도 회원국들이 공급에 협조하기로 동의한 서비스들의 긴 목록에 'services for carrying Internet traffic and data transmission'을 추가하고자 하였다. 인터넷에 대한 직접적인 두 번째 언급은 3.7에 대한 새로운 제안에서 등장한다. 이에 따르면 ITR은 행정 관리자들로 하여금 다음을 수행하도록 요청할 것이다.

> 국제적 인터넷 접속에 관한 조항에 참여하고 있는 모든 당사자들 (국가가 공인한 운영기관 포함)이 다음과 같은 사항에 대해 협의하고 동의하기 위해 국내적인 적절한 조치를 취해야 한다. 각 구성요소의 가치들, 예컨대 트래픽 흐름, 라우트의 개수, 지리적 커버리지, 국제적 전송 비용, 상호간 네트워크 외부효과(network externalities) 적용 등에 대한 당사자들 사이의 가능한 보상의 필요성을 고려한 직접적인 국제 인터넷 연결을 가능하게 하는 양자 간 상업적인 방식, 혹은 행정부 사이의 대안적인 형태의 방식.

이는 ETNO의 요청에 따라 ITU에 의해 공개적으로 발표된 ETNO의 제안[184]과 유사한 점이 있다. ETNO의 제안은 다음과 같다.

- IP 상호접속을 ITRs에 완전히 규정함으로써 이를 ITU의 관장 영역에 포함시킬 것,

- 패킷 데이터 유닛(packet data units)의 전송을 위한 '최선형(best effort)' 및 '단 대 단 품질(end to end quaility)'에 대한 두 개의 새로운 정의를 만들 것, 즉, 패킷 스위칭을 ITR에 공식적으로 포함시킬 것.

184) http://files.wcitleaks.org/public/ETNO%20C109.pdf

이 기술들에 기초하여, ETNO의 제안은 두 가지를 시도한다.

첫째로 전반적으로 양질의 서비스를 제공하며 최선형 패킷 전송(best-effort packet forwarding)을 가능하게 하는 상호 접속 환경을 회원국이 허가하도록 보장하며, 둘째로 통상 협의가 통신 서비스에 대한 지속 가능한 보상 체계를 달성하도록 하고, 경우에 따라서는 타사 네트워크의 지불 원칙을 존중하도록 하여 결과적으로 높은 대역폭 인터넷 설비에 대한 투자가 적절한 보상을 받을 수 있도록 업체들이 협상에 참여하도록 보장하고자 하였다.

인터넷에 대한 다음의 직접적인 언급은 6.7에 대한 새로운 제안에서 등장한다. 가장 흥미로운 제안에는 다음과 같은 내용이 등장한다.

> 6.7 회원국들은, 인터넷 접속을 포함한 국제적 접속 문제와 관련되거나, 혹은 그것으로부터 발생하는 협상이나 협정의 각 당사국이 다른 당사국의 경쟁 당국에 호소할 수 있는 지위를 부여해야 한다.

보면 알 수 있듯이, 이는 동등접속(peering)이나 상호 접속(interconnection)에 관한 국제 협상에서 불만을 가진 측이 협상 상대 정부의 경쟁 당국을 협상에 끌어들일 수 있도록 허가한다는 의미이다. 이를 통해 왜 미국의 대기업들이 이를 싫어하는지 알 수 있으며, 동시에 미국이나 그 밖의 국가의 경쟁관계 기업들이 국가 소유의, 혹은 독점적으로 운영되는 민간 영역의 국제적 게이트웨이(international gateways)에 대하여 각 지역의 경쟁 당국에 이의 제기를 할 수 있다는 점을 알 수 있다. 다른 제안에서는 '별도의 분쟁 처리 구조에 대한 접근권'을 덧붙여 이상의 내용을 수정한다.

인터넷을 언급하는 마지막 제안은 새 8.A.4인데, 다음 내용을 담고 있다.

> 8.A.4 회원국들은, 세계인권선언에 포함되어 있는 프라이버시와 표현의 자유에 관련된 조항 내용을 보호하고 존중하면서도, 사이버범죄와 스팸에 대응하기 위해, 인터넷의 안정성이나 보안을 보장하는 수단들을 강구해야 한다.

좋다. 여기에 쓰인 말들은 그 자체로 받아들일 만하지만, 동시에 국제 협정에 흔히 등장하는 모호하고 실행하기 불가능한 말의 전형이다. 우리는 사이버 보안과 ITR의 접점에 관해 더 이야기할 것이 많으며, 이는 다음 장에서 언급될 것이다.

분명하게 인터넷을 겨냥하면서도 명시적으로 언급하지는 않은 다른 수정 제안은 3.1에 대한 것인데, 이는 업체들에게 다음을 요청한다.

> 만족할 만한 수준의 서비스 [그리고 관련 ITU-T 권고안에 따른 최저 수준을 상회하는 수준의 서비스]를 제공하기 위한 국제적인 네트워크를 설립, 운영, 유지하기 위해 협력한다.

괄호로 묶은 내용은 (이는 지원의 부족을 나타내는데) 완전히 보호 무역론자의 입장을 따르는 조치이다. 의무적인 최소 품질 기준은 많은 인터넷 기반 서비스나 응용 프로그램을 금지하는 효과를 낼 것인데, 이는 인터넷의 대부분이 최선형 패킷 전송(best-effort packet forwarding)에 의지하고 있기 때문이다. 예를 들어, VoIP 서비스는 상당한 경우에 규제 기준이 되는 품질 이하로 떨어질 것 수 있다. 소비자들은 종종 품질이 다소 낮더라도 그 대신

가격이 싼 것을 선호하기도 한다. (스카이프가 그 예이다.)

분석

이들 제안들이 정의 조항을 수정하여 인터넷, 특히 '국제 인터넷 연결'을 ITR의 사안으로 삼고자 한다는 것은 분명하다. 필자의 블로그에 서술된 것처럼[185], 이는 분명히 통신이 무엇인지, 그것이 인터넷을 포함하는지 다투어온 오래된 논쟁의 연장선상에 있다. 인터넷을 통신 서비스라고 정의하는 것은 우리가 원하는 것이 아니며, 그렇게 될 경우에 지금은 시장의 힘에 의해 사적인 협상과 계약에 근거해 형성되는 상호 접속 환경을 규제할 길을 닦아주는 꼴이 될 것이다.

이상에서 논의된 내용 분석해 보면 ITR 수정안들 중 많은 것들이 '인터넷을 접수'하려는 새로운 시도가 아니라 전통적인 통신 사업과 시장을 혼란에 빠뜨린 인터넷에 대한 오랜 전투의 연장이라는 것을 알 수 있다. 이러한 제안들은 네트워크 layer 1과 2를 운영하는 특정 회사들이 응용 프로그램 계층에서 급증하는 데이터 트래픽을 감당하는 대가를 더 많이 받고자 하는 이해관계, 또는 그것으로부터 보호를 받고자 하는 이해관계를 반영한다. 일부 (특히 국가나 독점 기업이 네트워크 사업을 하고 있는 개발도상국의) 행정 당국 관리자의 입장에서 그것은 과거처럼 비용을 분담하던 모델이 아니라 연결에 대해 자신이 비용을 지불하는 인터넷 모델에 대한 불만족과 정부의 규제를 받는 상호 접속에 반대되는 계약 협상에 대한 불만족을 반영하고 있는 것이다.

국제 인터넷 연결을 둘러싼 싸움은 새로운 것이 아니다. 1999년으로 거슬러 올라가면, 인터넷 콘텐트의 중심에서 멀리 떨어진 예컨대 호주를 포함한 다양한 국가들이 국제 인터넷 대역폭 비용을 해당 국가의 운영자들이 분담하는 것이 아니라 접속에 대해 과금하는 새 인터넷 모델과 관련해 ITU에게 항의한 바 있다. 그 결과 ITU-T 권고 D.50[186]이 만들어졌고, 이는 2000년에 통과된 후 몇 번 수정되었다. D.50은 그저 권고(recommendation)에 불과하다. 그리고 몇 수정 제안은 그것을 ITR로 가져와서 이를 필요 요건(requirement)으로 만들고자 하고 있다. 이는 보기보다 별 것 아닌 위협일 수도 있으나 지켜봐야 할 필요가 있는 것이다. ITU는 인터넷 트래픽을 측정하고 비용을 청구하는 방식과 관련해 끝없는 연구와 논쟁을 이어왔다. 그러나 이 문제에 대한 명확하고, 동의를 이끌어내는 제안을 결코 만들어 낼 수 없었다. 유튜브를 비롯한 다른 응용 프로그램 단의 업체들이 비용을 더 내도록 했던 AT&T의 초기 노력이 결코 사라지지 않은 것처럼[187] 통상 협정을 통해 통신 서비스를 위한 공정한 보상 체계를 구축해 지속 가능한 체계를 만들겠다는 ETNO의 생각이 어떻게 구체화될 것인지 전혀 명확하지 않다. ETNO는 또한 상호접속에 관한 단대단(end to end) 서비스 품질에 대한 협상을 위한 무임승차(free pass)를 요구하고 있다. 이는 망 중립성 지지자들에게 고민을 던져주겠지만, 각국의 규제는 그것이 차별적 효과를 내지 않도록 보장할 수 있다.

---

185)http://www.internetgovernance.org/2012/06/07/threat-analysis-of-wcit-part-2-telecommunications-vs-internet/

186) http://www.itu.int/rec/T-REC-D.50/e

187) http://arstechnica.com/uncategorized/2005/10/5498-2/

우리가 보기에는 이런 모든 노력은 폐기되어야 마땅하며, 이를 ITR에 중요하게 포함되도록 해서는 안 된다. ETNO의 회원들은 이미 그들의 파트너가 동의하는 어떠한 요금 체계에 관해 서도 협상할 수 있다. 만약 그들이 규제자들의 참여를 원한다면, 그것은 시장이 절대로 그들이 원하는 바가 이루어지게 두지 않을 것이기 때문이다. 접속 요금 체계가 사용시간(duration in minutes)이나 트래픽, 패킷의 수, 패킷 흐름의 방향 등과 같이 규제에 의해 분명히 통제되어야 한다는 생각은 시대착오이며, 그런 생각은 불균질성(heterogeneity)을 특성으로 하는 서비스와 다양한 시장(multi-sided market)이 만연하고 있는 상황을 반영하는 것이 아니다. 데이터는 음성이 아니며, 호시절을 그리워하는 통신 당국들은 잠에서 깨어나 인터넷 응용 프로그램이 작동하는 방식에 대한 진실을 마주할 필요가 있다.

모바일 로밍

우리는 지금까지 국제 모바일 로밍 요금에 대한 이야기를 피해왔는데, 이는 적어도 음성 통화가 포함되어 있던 과거에는 분명히 통신의 영역으로 이를 분류할 수 있었기 때문이다. 그러나 과거 이동 통신이 유선 통신의 역할을 대체한 것처럼 지금은 데이터 통신이 이동 통신의 역할을 대체하고 있다는 것을 우리는 모두 알고 있다. 또한, 역시 알고 있는 바와 같이, 국제 데이터 통신 로밍 요금은 음성 로밍 요금과 비교해도 과도하게 높게 책정되어 있다.

우리가 알기로, 제안된 ITR 개입은 일반 소비자 보호 문제에 초점을 맞추고 있으며, 그 예로는 가격 투명화, 고지, 소비자들이 추가 비용을 요구하는 로밍 서비스를 거절할 수 있도록 하는 것 등이 있다. 모바일 데이터 상호 접속 요금을 규제하거나 통제하려는 구체적인 노력은 없는 것 같다. 국가의 경계를 넘나드는 대부분의 모바일 데이터가 아마도 유선 네트워크를 거치므로, 살펴봐야 할 것은 아마도 유선 네트워크 요금 체계일 것이다. 새로운 4.6은 모바일 로밍 협정에 의한 서비스 품질을 규제하고자 한다. 그러나 이는 별로 지지를 받고 있지 않다. 가장 중요한 부분은 다음과 같다.

> 4.4 회원국들은 국제적인 전기통신 서비스 제공자, 특히 국제 로밍 부문의 사업자가 로밍 비용을 포함한 소매 비용에 대한 투명하고 최신의 정보를 제공하도록 보장해야 한다. [특히, 각 소비자들은 로밍 서비스가 필요 없다고 자국의 사업자에게 고지하지 않은 이상, 해외에 있을 때, 관련된 가격정책(price plan)에 관하여 정확하며 적절한 시기에 제공되는 가격(세금 포함된)에 대한 정보에 대하여 별도 비용 없이 용이하게 접근하거나 이를 제공받을 수 있어야 한다.]

결론

ITR에 통신 규제 당국의 표준 형식을 국제 인터넷 연결 환경으로 확장하려는 노력들이 있다. 이런 경제적 개입이 통과된다면, 새로운 서비스에 상대적으로 열린 공간이라는 인터넷의 지위에 타격이 가해질 수도 있으나, 그들이 얼마나 큰 지지를 받고 있는지 잘 모르겠다. 그나마 잠재적으로 가장 신경이 쓰이는 제안은 ETNO의 것이며, 이는 대다수 선진국의 통신 업체들이 국제 인터넷 연결을 ITR에 넣고 싶어 하기 때문이다. 그럼에도 불구하고 그

들의 영향력이 그리 크지는 않을 것인데, 그 이유는 제안된 새 요금 체계가 '지속 가능하고' '공정한' 보상이라는 모호함에 기초하고 있기 때문이다. 그러나 시장에 의한, 자유롭고 열린 인터넷을 믿는 이들에게 있어서, 이는 오랜 시간에 걸쳐 그런 것들을 ITR의 영향력 아래에 두는 좋지 않은 선례가 될 가능성이 있다.

4. ITU와 사이버 보안

이전 장에서는 ITR이 상호접속 합의의 중요성을 강조하고 있다는 점과 WCIT의 어젠다를 이끌고 있는 펀딩의 흐름에 대해서 살펴보았다. 이러한 내용은 맞는 내용이긴 하지만 어쩌면 사이버 보안(cyber security)가 ITR에 포함되는 것 역시 갈등과 협상의 대상이 되는 중심적인 문제라는 점에 대해서 과소평가하게 만들고 있는 것인지도 모르겠다.

필자는 그동안 인터넷에 대한 보안강화 행위(securitization)[188]는 인터넷 상의 자유에 대한 주요한 위험요소라는 점을 지적한 바 있다. 애국심에 호소하는 것은 일전에 "악당의 마지막 피신처(refuge of a scoundrel)"라고 언급될 정도이며, 이는[189] 표현의 자유를 제약하고, 프라이버시를 침해하며, 익명성을 파괴하고, 새로운 사업 기회를 제약하며 사이버 보안을 언급하는 국가의 힘을 더해주는 행위와 다름 아니다. 누가 디지털 서비스와 인터넷 기반 시설의 보안과 프라이버시를 개선하겠다는 노력에 대해 반대를 할 수 있겠는가? botnets, DDos공격, 횡횡하는 미승인된 감시, 사이버 간첩행위 및 국가의 지원을 받은 공격 등 사이버 범죄 문제가 존재한다는 점은 모두 사실이다. 따라서 사이버 보안에 관한 논의는 매우 신중하게 이루어져야 한다. 사이버 보안에 대한 논의는 사이버 범죄행위에 대하여 적법한 필요에 의해 이루어지고 있기도 하지만, 남용되고 조종되어 보안이라는 표지 하에 이루어지는 일종의 가장무도회일 수도 있다는 점을 명시해야 한다.

ITU가 사이버 보안 문제야말로 인터넷과의 관련성을 주장할 수 있는 지점[190]이라는 사실에 대하여 간파했다는 점은 이미 명백하다. 그러나 더 놀라운 것은 이 문제에 관심을 끌고, 참여하고, 펀딩을 받는 행위가 워싱턴 DC의 정책 연구기관[191]이나 다양한 미국 정부 기관들[192]이 하는 방식을 그대로 보여주고 있다는 점이다. 더욱이 ITU가 사이버 보안과 관련되어 하는 대부분의 것들은 기본적으로 교육과 역량강화[193]와 관련되어 있다. ITU 전권회의 결의안 130과 146[194]은 ITU가 일반적으로 취하는 접근방식을 보여주는데, 관료적인 방식으로 풀어갈 수 있다고 판단되면 그들은 개발도상국에게 도움을 주는 방식으로 이를 요청하고 있는 것이다.

많은 어플리케이션이 매우 유용하게 활용하고 있는 공개키 기반의 X.509 표준과는 별개

188) http://en.wikipedia.org/wiki/Securitization_%28international_relations%29
189) http://www.lexipedia.com/english/scoundrelly
190) http://www.itu.int/cybersecurity/
191) http://csis.org/program/commission-cybersecurity-44th-presidency
192) http://www.hstoday.us/briefings/today-s-news-analysis/single-article/house-dhs-budget-boosts-border-security-cybersecurity-nixes-revamp-of-fema-grants/b14ad3c596ea16bc58a2b9b2cac1b57d.html
193) http://www.itu.int/ITU-D/cyb/
194) http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf

로 ITU-T는 그 자체로 사이버 보안 이슈와 관련된 표준을 확립하는데 그다지 강력한 역할을 하지 못했다. ITU는 규제와 관련된 역량이 매우 작으며, 대부분의 구성원 국가들이 통과된 규칙을 해당 국가 스스로 규율하고 강제하는 것을 기대하는 수밖에 없다.

따라서 ITU를 컴퓨터와 인터넷 보안과 관련하여 강력하거나 독특한 참여자라고 보기는 어렵다. 강력한 힘을 가진 동시에 강력한 자금력을 가지고 있는 미국 정부의 경우에도 자국의 부처와 기관들의 네트워크 보안 관련 행태를 변경하는데 매우 어려움을 겪었기 때문이다.[195] ITU가 수천 개의 공적 기관들, 수만 개의 사적 네트워크들 그리고 세계의 수십억대의 디바이스에 대한 보안과 신원확인 행태에 관하여 명령하고 강력하게 틀을 잡을 수 있는 기관이라는 주장은 신뢰를 받기 어렵다.

실제로 인터넷 자유에 대한 가장 강력한 사이버 보안관련 위협은 ITR가 아닌 각 국가 정부로부터 발생한다. 국가주권과 국가 안보에 대한 주장은 이미 국가로 하여금 모든 형태의 국제적 또는 국내적 커뮤니케이션에 대하여 모든 형태의 탄압적이고 군사 행동과 같은 조치를 취할 수 있도록 하고 있는데, 콘텐츠에 대한 차단이나 필터링, 디바이스에 대한 사용금지나 사용규제 그리고 접속 차단 등이 그것이다. *ITU constitution*[196]*의 제34조 35조 및 37조*는 이미 각 주권국가 별로 국가의 보안을 증진하고 다양한 방식으로 커뮤니케이션을 차단할 수 있는 점을 인식하고 있다. 오래된 규율을 상정하지 않더라도 무정부적 국제 정세하에서 다른 국가가 주권을 침해하려고 하는 경우에는 일국 차원에서 국가 안보를 위하여 대응 행위를 할 수 있다는 사실상의(de facto)권리가 있다는 점은 분명하다. 따라서 ITR을 어떻게 개정하더라도 킬 스위치(kill switch)와 이와 관련한 위험이 극적으로 증가하리라 보기는 어렵다.

캐나다 학자인 드웨인 윈섹(Dwayne Winseck)은 현재의 ITU 조약은 주권 옹호(sovereigntist) 모델에 기반해 있다고 강조하고 있다. 그는 다소 과장된 표현이지만, ITU 조약은 "1850년대부터 있어 왔던 정보의 흐름에 대한 가로채기 행위, 중단 행위 및 차단 행위"를 정당화해 왔다고 평가한다. 다만 ITU 조약이 다분히 억압적인 행위를 가능하게 해왔지만, 통치권(sovereignty)은 동시에 그 자체로 견제와 균형 역할을 해왔다고 보고 있다. 각 국가는 그 자체로 매우 높은 수준의 자율성을 가지고 있으며, 이는 다른 국가들의 규제나 관행으로부터 각 국이 영향을 받는 것을 방지하고 있다. 즉, 국가의 다른 나라에 대한 이해관계에 따라 서로에게 주는 영향을 상쇄할 수 있는 것이다.

따라서 사이버 보안에 대한 법령과 정책의 가장 중요한 정치적 동인은 각 국가 수준에서 발견할 수 있다. (사적 영역에서는 이와 대조적으로 이러한 행위에 대한 시각은 초국적 성격을 띠고, 계약에 기반해 있으며, 운영과정에서 드러나게 된다.) 사실 TD-62의 관련 제안들을 살펴보면 이들의 사이버 보안과 관련된 제안이 얼마나 광범위하고, 초점도 없으며, 제공되는 정보도 없이 때로는 매우 순진하게(naive) 작성될 수 있는 지에 대하여 놀랄 것이다. 대부분의 내용은 구성원 국가들에게 포괄적인 언어로 "스팸을 방지하라" "데이터와 네트워크가 완전한 상태로 유지되도록 보호하라" 거나 "각 국가 내의 기업들의 운영을 관리감독하라"면서 그 목표로 "ICT를 합리적인 방법으로 사용하도록 하기 위함"을 들고 있다.

195) http://en.wikipedia.org/wiki/Einstein_%28US-CERT_program%29
196) http://www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx

필자가 가장 좋아하는 문구는 “인터넷의 보안과 안정성을 보장하라" 이다. 더욱이 아프리카 국가들이 제안한 보안과 관련된 새로운 조항은 2010년 3월 “사이버스페이스 정책 검토(Cyberspace Policy Review)”라는 이름으로 발표된 미국 대통령 선언(Presidential Declaration)의 내용을 문자화한 수준에 불과하다.

보다 심각한 것은, ITR 제안서는 각 국가의 내부 정세나, 주권, 국가 안보 또는 영토 보전을 방해하는 국제적 수준의 커뮤니케이션을 제한하려고 했다는 점이다. 이러한 제안은 “체제 전복적인 내용"에 초점을 맞추고 있는데, 인터넷을 통하여 정보가 국경을 초월하여 공유되면서 생성되는 현재의 국제적 공론장의 성격에 비추어보면 이는 매우 과도한 반응으로 판단된다. 그러나 이들이 각 국가 차원에서도 이미 할 수 없는 수준의 행위들을 어떤 방식으로 정당화하려 했는지를 알아내기는 어렵다. 우리는 이러한 제안들이 법적이나 규범적 차원에서의 ‘현상유지(status quo)’적 태도로부터 멀리 나아가려고 하지 않는다는 점을 종종 망각하곤 한다. 최근 커뮤니케이션 관련 국제 동향은 법적으로나 실질적 운영 측면으로나 모두 주권옹호/국가 안보(sovereigntist/national security) 강조 모델로부터 도출되었다. 이는 브래들리 매닝(Bradley Manning)이 수감된 이유와 위키리크스(Wikileaks)가 기소되게 된 이유에 해당한다. 또한 이러한 점은 왜 중국이 만리방화벽(Great Firewall)을 구축하려 하고, 한국 정부가 북한의 인터넷 접속을 검열하고, 북한 역시 마찬가지인지를 설명해준다. 또한 야후가 나치 기념품을 전시한 행위를 프랑스 정부가 왜 기소하였는지를 설명하는 이유이기도 하다.

그리고 이는 우리의 다음 논점으로 이끄는데, ITR의 사이버 안보 관련 규제에 대한 강력한 주장은 러시아가 주도하고 있다는 점이다. 러시아의 입장은 러시아가 미국이 관여하고 있는 사이버 보안 관련 조약에 대한 논의에서 아무런 역할을 하지 못하고 있다는 점을 방증한다. 1998년부터 러시아는 미국이 반대함에도 불구하고 사이버스페이스를 군사적 목적으로 사용하는 것을 금지하는 성격의 조약을 지지해왔다. 오바마 정권에 이르러 미국의 입장이 변경되었고, 새로운 협력 모델에 대한 논의가 진행 중에 있지만[197], 러시아는 여전히 사이버 전쟁 게임에서 스스로를 매우 취약한 당사자로 판단하고 화학무기 관련 조약과 같은 성격의 조약을 희망하고 있는 것이다. 플레임(Flame)과 스턱스넷(Stuxnet)[198]의 개발단계에서 미국의 역할에 대한 최근 폭로를 살펴보면 그동안 미국이 왜 그러한 제약에 스스로를 제약시키는 행위에 비협조적이었는지를 분명히 설명해주고 있다. 미국의 월등한 기술적 능력과 더불어 강력한 미국 인터넷 산업은 사이버 보안 측면에서 다른 국가들에게 분명한 위협이 되고 있는 실정이다. 마찬가지로 아랍 국가들이 러시아의 사이버 보안 관련 제안에 강력하게 찬성하고 있는 이유도, 많은 아랍 국가들의 독재자들이 정보의 자유로운 흐름을 불편해하고 있기도 하지만, 네트워크 검열과 감시기술 영역에서 이스라엘이 기술적 우위에 있기 때문에 미국과 함께 사이버 무기를 개발하는 것을 염려하고 있기 때문이기도 하다.

따라서 러시아와 이에 찬동하는 국가들은 사이버 보안과 사이버 주권을 가능한 한 최대로

197) 사이버보안 전문가 그룹과 미국, 벨라루스, 브라질, 영국, 중국, 에스토니아, 프랑스, 독일, 인도, 이스라엘, 이탈리아, 카타르, 러시아, 남아공, 한국 외교관들은 UN 사무총장에게 international computer security treaty에 대한 논의를 위한 일련의 제안을 하는데 합의하였다.
(NYT: http://www.nytimes.com/2010/07/17/world/17cyber.html)

198) 역주: 발전소・공항・철도 등 기간시설을 파괴할 목적으로 제작된 컴퓨터바이러스로, 2010년 6월 벨라루스에서 처음으로 발견됨, 네이버 사전 참조

보장하는 내용이 ITR에 들어가길 희망할 것으로 예측된다. 이는 타 국가들의 사이버 관련 역량에 의해 위협을 느끼고 있는 러시아를 비롯한 국가들에겐 가장 현실적인 수단으로 기능하는 것이다.

그러나 ITR에 의존하는 행위는 많은 측면에서 취약점을 드러내는 표시에 해당한다. ITR은 특정 국가가 자신을 국제적 정보의 흐름과 사이버 공격으로부터 방어하기에 매우 불완전한 수단이며, 컴퓨터와 인터넷 보안에 대한 종합적인 규제로서는 더욱 불안전하다. ITR은 기본적으로 공공 전기통신 네트워크 운영자들 간의 관계에 대한 것이다. 이에 대하여 ITR의 정의를 국제적인 인터넷 말단(termination)까지 포함하는 것으로 확대하려는 시도가 있지만, 앞서 언급한 바와 같이 이러한 정의 조정 시도는 강력한 국가들의 이의에 봉착했다. 설사 정의조항이 확대 해석된다고 하더라도, ITR이 사이버 보안 영역에서 중요한 역할을 할 것으로 보이지는 않는다. 인터넷은 수백 개의 공적인 기구에 의해서 운영되는 네트워크가 아니며, 수만 개의 사적 네트워크와 수백만 개의 어플리케이션 그리고 수십억 개의 다양한 디바이스로 구성되어 있는 네트워크이기 때문이다. 인터넷 상의 기술 표준은 자발적인 다양한 사적 연합체들에 의해 형성되며, 사이버 영토상의 가장 관련된 표준은 디바이스, 소프트웨어 및 어플리케이션 제공자들이 관여하게 되며 여기에 ITU는 거의 관여하지 못한다. ITU는 스스로의 관장 영역에서조차도 강제적인 표준을 제정하는 능력을 가지고 있지 않으며, 단지 ITU-T 권고안을 필요조건으로 하자는 몇몇 제안이 있었을 뿐이다.

요점은 ITR의 네트워크 보안 영역에 대한 진입 시도로 인한 가장 큰 위협은 정의 조항에 대한 이슈로 정리될 수 있다는 것이다. 만약 정의 조항이 ITR 소관인 전기통신 영역에 인터넷과 사이버 보안 영역이 포함된다고 해석된다면, 큰 문제에 봉착한다. 이러한 문제는 몇몇이 지적한 것처럼 장대한 서사를 가지고 있는 성격이거나 각국 정부의 일방적인 행위에 의하여 최종 이용자들이 겪는 문제처럼 중요한 것이 아닐 수 있다. 다만 이렇게 해석되는 한 이미 충분히 복잡한 생태계에, 통신 규제와 사이버 보안 그리고 인터넷 규제가 뒤섞이는 문제가 발생하는 것이다. 또한 다수 국가가 미국과 인터넷 기술 커뮤니티의 반대에도 불구하고 ITR의 정의를 변경하여 이를 통하여 사이버 보안을 규제하려고 시도한다면 충분히 심각한 문제라고 할 수 있는 것이다.

반면 정의조항이 확대되지 않는다면 ITR이 인터넷 보안 관련 거버넌스 영역에서 미칠 수 있는 악영향은 매우 미미할 것이다. 왜냐하면 시민사회는 다음과 같이 주장할 것이기 때문이다. a) ITU의 표준은 권고사항에 불과하지 필요적 요건은 아니며, b) ITR과 그 정의는 기반시설의 layer 1과 layer 2와 관련된 원래의 목적 달성과 밀접하게 운용되어야 한다.

필자는 알려진 WCIT 문서[199] 중 몇 가지 특정한 제안에 대하여 살펴보려고 한다. 제안된 수정안들은 스팸과 관련된 언급이 많이 포함되어 있고 그들 중 몇몇은 매우 형편없이 정의되어 있다. 몇몇은 이러한 언급들이 인터넷 내용규제에 대한 문을 열 수 있다고 주장하고 있다. 필자는 윈섹(Winseck)의 분석에 동의하는데, 스팸과 관련된 제안은 내용상 온건한 편이며, 단순히 국가로 하여금 '국가 차원의 입법'(많은 경우 법률을 가지고 있다)을 권고하는 내용과, 스팸에 대응하기 위한 조치를 취하기 위해 협력한다는 내용(이미 대부분 하고 있다), 그리고 각 국에서 스팸에 대응하면서 얻게 된 정보와 조치내용을 공유한다(무엇이 잘

199) http://www.wcitleaks.org/

못되었는가?)는 내용에 불과하다. 따라서 스팸에 대한 언급이 ITU의 관할권을 인터넷 내용 규제에까지 미치도록 구성될 것이라는 증거는 거의 희박하다. 물론 정의와 관련되어 딱 잘라 말하기 어려운 부분이 존재하지만, 필자는 ITR에서 스팸이 다루어지는 것을 보고 싶지 않은데, 이는 정보 서비스의 이슈이지 전기통신 이슈가 아니기 때문이다.

다른 제안은 이렇게 언급하고 있다.

> 각 회원국은 자신의 트래픽이 어디를 통해서 라우팅되고 있는지 알 권리가 있으며, 사기에 대응 및 보안의 목적으로, 이에 관한 라우팅 규제를 개선할 권리를 가지고 있다.

본 제안은 매우 형편없는 것 중 하나이며, 아마도 아랍 국가들이 이스라엘을 통한 라우팅에 대한 걱정이 반영된 것으로 보인다. (흥미롭게도 2012년 3월 미국의 로펌의 요약[200]에 따르면 미국은 이 제안에 대하여 최초에 반대하지 않았다고 한다. 그러나 향후에 미국은 영국과 스웨덴 그리고 CEPT의 반대에 동참하게 된다.) 본 제안의 의미는 어떠한 종류의 트래픽을 언급하고 있는지 여부에 달려있다. 만약 인터넷과 이를 이용한 정보 서비스가 국제 전기통신 서비스의 정의의 일부분에 포섭되지 않는다면, 라우팅에 대한 언급은 전기통신 회선에만 적용될 수 있을 것이다. 만약 인터넷 서비스가 포함된다면 이러한 규제는 BGP와 인터넷 라우팅에 대한 적법한 개입을 허용하는 것이 될 것이다. 그렇다고 하더라도 필자는 이미 인터넷 서비스 제공자와 통신회사에 대한 국내적 규제를 통해서도 이미 실현될 수 없는 것들이 이 중 어떠한 조항을 통하여 달성이 가능할 수 있는지 찾아낼 수 없다. '발신자 확인(Originating Identification)'에 대한 언급 역시 비슷한 분석이 가능한데, 만약 당신이 이러한 제안이 인터넷에 적용될 수 있다고 생각한다면 (사실상 그렇지 않고, 그럴 수도 없지만) 이는 매우 문제가 많은 것처럼 들릴 수 있다. 만약 SS7 전기통신 회선교환 환경에 의하여 가능케 된 발신번호 표시(calling line identification, CLI, 즉 caller ID)에 적용된다면 이는 일상적인 것들에 불과할 것이다.

합리적인 분석을 하던 마지막에 윈섹은 갑자기 우울한 심경을 표출한다. 그는 8A 섹션에 추가된 제안이 엄청난 위협을 포함하고 있다고 보았는데, 이는 통제되고 폐쇄적인 국내 인터넷 공간의 창설을 안내하고 있으며, 이러한 공간은 모든 면에서 국가의 제약 없는 힘에 종속되기 때문이다. 이러한 어두운 생각에 영감을 준 제안에는 아래와 같이 러시아의 기여가 컸다.

> 회원국들은 국제 전기통신 서비스에 대중이 제한 없이 접근하고 사용할 수 있도록 보장하여야 한다. 다만 국제 전기통신 서비스가 국내 정세(internal affairs)에 개입하거나 주권, 국가안보, 영토의 보전, 다른 국가의 공공 안전을 약화하거나 민감한 성격의 정보를 유출시키는데 사용되는 경우는 예외로 한다.

필자는 그 정도의 위협을 느끼지는 않는다. 우선 이는 다섯 개의 제안 중 하나에 불과하며 다른 제안에는 그러한 독소 조항이 포함되어 있지 않기 때문이다. 다른 제안들의 존재는 본 제안에 대한 합의가 이루어지지 않았다는 것을 의미한다. 또한 러시아의 2010년 전권회의에서 ITU의 역할을 확대하기 위한 제안이 모두 실패로 돌아갔다는 점도 지적할 수 있다.

---

200) http://files.wcitleaks.org/public/Sixth%20CWG%20-%20TD-43%20Summary.pdf

물론 많은 국가의 정부들은 국내의 인터넷 공간을 통제하고 제약하길 희망해왔던 것은 사실이다. 그러나 많은 국가의 정부들은 그렇게 하지 않았다는 점도 또한 사실이다. 대부분의 산업계, 엔지니어들 그리고 시민사회 활동가들은 그러한 제약에 강력하게 반대할 것이다. 그러나 이를 희망하는 정부가 목표를 달성하는 가장 쉬운 방법은 단독으로 이를 실행하는 방법이다. 그들 정부에게는 ITR이 필요 없는 것이다. 필자의 전제를 다시 한 번 상기하라. 인터넷 자유에 대한 가장 강력한 위협은 일국의 정부가 그들 영토 내에서 효과적인 통제를 하는 행위로부터 비롯된다는 점을.

만약 필자의 가정과는 반대로 ITR이 오히려 일국 차원에서 정부로 하여금 적법하게 억압적인 행동을 할 수 있는 기회를 제공한다면, 나는 이에 대하여 일부는 인정하지만, 일부는 인정할 수 없다. 시민사회가 지금과 같이 이 문제에 대하여 경계를 게을리 하지 않고 있다고 가정한다면 ITR 프로세스를 통하여 새로운 구속적인 규범을 확립하려는 시도는 공적인 논쟁으로 이어져서, 정보의 자유로운 흐름에 대한 공격에 대한 신빙성이 떨어질 것이고 이러한 시도가 정당화되지는 어려울 것이다. 더욱이 민감한 성격의 정보 유입을 차단하는 성격의 국제적 규제가 존재한다고 하더라도 이를 실행하는 수단이 자동으로 만들어질 것이라고 볼 수는 없다. 유비쿼터스(ubiquitous)한 성격의 태블릿과 모바일 디바이스를 사용하는 현재의 세계에서 이러한 기획은 쉽게 달성되기 어렵기 때문이다.

그렇다. 시민사회와 인터넷 자유 옹호세력들은 WCIT을 둘러싸고 세력화하여 인터넷 자유 규범을 증진시켜야 한다. 그러나 그들은 동시에 ITR에 대한 균형을 훼손해서는 안 된다. 사이버 보안, 프라이버시 그리고 표현의 자유를 둘러싼 유사한 정책 이슈들이 ICANN에서 그리고 무역 협정을 가장한 지적재산권 조약에서 그리고 유럽연합 집행위원회 지침에서 그리고 강력한 세력(super powers)에 의하여 국경을 초월하여 논의되고 있는 것이다. 필자의 생각에는 ITR 논의만이 그 중 특별히 중요한 의미를 가진 것은 아니다. 위협요소에 대한 평가는 정책 제안에 따르는 실행과정에서 요구되는 조건에 대한 이해와 더불어, 단순히 문서상의 내용에 쓰여 있는대로 190 여개의 국가로 번안되어 그대로 실행된다는 가정이 아니라 실제 집행과정에서 요구되는 정치적 지지획득 가능성에 대한 이해가 바탕이 되어야 한다.

모든 것이 동등하게 중요하다. 다만, 시민사회는 ITR이 인터넷에 적용가능하다는 점을 인정하면서 대응을 시작해서는 안 된다. ITR의 정의를 둘러싼 이슈는 여전히 매우 핵심적인 것이며, 여전히 그 가능성은 열려있기 때문이다.

THREAT ANALYSIS OF ITU' S WCIT

Milton Mueller[201)]

PART 1: HISTORICAL CONTEXT

The relevance of the International Telecommunication Union's World Conference of International Telecommunications (WCIT) to Internet governance is a hotly debated topic. There is an organized campaign to raise concern about it, with the latest entry being the scheduling of a hearing[202)] in the U.S. House of Representatives.

What this means is that 20 years after the opening of the Internet to the public, 13 years after the creation of ICANN, 7 years after the conclusion of WSIS, we are still having an intense debate about the relationship between nation-states and the governance of the Internet. This is precisely the topic I tried to treat comprehensively in my recent book, Networks and States.[203)] It might sound self-serving, but I think that a lot of participants in the current debate would benefit from the historical perspective and theoretically grounded analysis it provides.

There is no doubt that some governments, notably Russia, would like to see the ITU replace ICANN and other private sector-based Internet institutions. What most people don't realize, however, is that certain governments have advocated that position for more than a decade - and they have repeatedly failed to realize those goals.

The history is worth recounting. Start the story in 1996, when the ITU

---

201) Professor, Syracuse University School of Information Studies, Internet Governance Project http://www.internetgovernance.org/

202) http://thehill.com/blogs/hillicon-valley/technology/229231-house-to-hold-hearing-on-international-control-of-the-internet

203) http://www.amazon.com/Networks-States-Governance-Information-Revolution/dp/0262014599

attempted to take over the domain name system. At that time it was (extreme irony) allied with the Internet Society[204] in an attempt to privatize management of the DNS root and remove it from the hands of the US government. The U.S. squashed that effort like a bug, leading to the creation of ICANN.

The next episode, and the high water mark of the nation-state challenge to Internet governance, was the 2002 – 2005 World Summit on the Information Society.[205] At WSIS, governments started to grok ICANN and wake up to the lack of intergovernmental institutions with authority over the Internet. There was a huge expansion of the coalition in favor of a greater role for governments. The European Commission, led by the French, joined Brazil, Arab states, Iran, South Africa, numerous other African states, China and Russia in criticism of US control of the root and in favor of state-directed "globally applicable public policy principles." But they failed to alter ICANN's basic governance model, or the basic approach to Internet governance. WSIS did have an indirect effect of strengthening the role of governments inside ICANN, but that was mainly because the U.S., in its determination to stop the .xxx domain, aggressively used ICANN's Governmental Advisory Committee (GAC)[206] to intervene in policy making.

In 2009-2010, the ITU tried to gain a larger role for itself in the management of IP addresses.[207] Many of the same fears now expressed about the WCIT-12 were expressed about the ITU Plenipotentiary meeting in Guadalajara in 2010.[208] And yet, as our coverage[209] of the results of that meeting indicated, the resolutions emerging from the Plenipot not only did not "take over" anything, they made a concession, mentioning ICANN by name for the first time ever in an ITU resolution (albeit grudgingly, in a footnote). Proposals by countries such as Russia to transform ICANN's GAC into an intergovernmental organization with oversight powers, or to create a "progressive cooperation agreement between ITU and ICANN and define a mechanism to increase the participation of governments" were all struck from the text, another defeat for creeping intergovernmentalism.

Most recently, in 2011 there was a proposal by India, Brazil and South Africa to create a UN "Committee on Internet Related Policies" (CIRP).[210] Although this

---

204) http://www.isoc.org/
205) http://www.itu.int/wsis/index.html
206) https://gacweb.icann.org/download/attachments/1540116/GAC_25_Wellington_Communique.pdf?version=1&modificationDate=1312543504000
207) http://www.itu.int/dms_pub/itu-t/oth/06/2C/T062C0000010001PDFE.pdf
208) http://www2.afrinic.net/news/ITU_mexico.htm
209) http://www.internetgovernance.org/2010/10/28/free-online-access-to-itu-resolutions/
210) http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html

raised alarms about a "UN take over" the proposal actually involved the creation of a research and policy development committee that could make proposals to be considered by the UN General Assembly. CIRP had some weak non-governmental stakeholder representational structures, but no legislative or regulatory powers, only the ability to formulate proposals that governments would then have to negotiate and ratify as treaties. Not a good idea, in my opinion, but if major Internet-economy countries such as the US and in Europe refused to ratify those treaties, they could not have any effect. Yet even that proposal has been stoutly resisted. Brazil later disavowed the proposal. India is still backing it, contrary to some reports[211], but the Indian government's support for it has been openly criticized by legislators[212] and South-based civil society groups, who link it to India's domestic Internet censorship[213] efforts.

The CIRP proposal itself was a reflection of many governments' dissatisfaction with the Internet Governance Forum, especially emerging economies in what is called "the global South." IGF was the main outcome of the WSIS and was supposed to continue the unresolved debate over US control of critical Internet resources in an open, fully multistakeholder forum. But many of these critics of the Internet governance status quo became disenchanted with the IGF. Some governments wavered in their commitment to equal-status cooperation with other stakeholder groups. Some civil society critics claimed, not unreasonably, that players with a vested interest in the status quo were preventing the IGF from taking on controversial issues and from making recommendations. Business interests in the West contributed to this dissatisfaction by filling the IGF with meaningless happy talk about disaster relief and green IT, neither of which have anything to do with global Internet governance. This led to UN-based efforts to institute IGF "improvements." Of course, those "improvements," which tended to involve more bureaucratization of IGF, have been opposed and blocked by advocates of the weaker IGF.

So here's the bottom line:

1. There is no sudden UN or ITU effort to take over the Internet. There is, instead, a longstanding struggle between the Net and states at the national and international level. The WCIT is just the latest episode; and compared to WSIS, a minor one.

2. There is no evidence of any recent enlargement of the political support for

---

211) http://www2.afrinic.net/news/ITU_mexico.htm

212) http://indiatoday.intoday.in/story/mp-rajeev-chandrasekhar-global-internet-censorship-wsis/1/189131.html

213) http://www.timesofassam.com/headlines/censorship-on-internet-another-dictatorship-of-congress/

states and inter-governmental institutions such as ITU. The same players are taking the same positions. There may even be erosion of support for inter-governmentalism, e.g. Brazil's abandonment of CIRP.

3. The ITU is a paper tiger. Neither WSIS nor any other international development has strengthened or approved ITU efforts to gain control of pieces of the Internet since 1996.

4. Intergovernmentalism is a fading ideology. While developing countries and BRICs still resent US economic and political pre-eminance and tend to view intergovernmental institutions as a way to address those resentments, they have been persistently unsuccessful in re-asserting governmental control over the Internet in transnational institutions. Civil society and business within those countries are divided – they do not always support their governments' efforts. Most Internet-related activists are on the side of de-nationalized, multistakeholder governance.

5. The biggest threats are at the national level. States (including not just India, China and Russia but the US, Great Britain, and other Western democracies) have taken major steps to impose new regulations and controls on the Internet insofar as they can within their territorial jurisdiction. If the world's governments lock down the Internet nationally and then agree on how to control it globally, it would indeed be dangerous. But we are a long way away from such agreement.

So a more realistic assessment of the threats and their context is required before people run around sounding the alarms about the ITU, and its International Telecommunication Regulations (ITRs). In my next blog, I will look into more depth into the ITRs – and the real cause for concern about what they might do.

PART 2: TELECOMMUNICATIONS VS. INTERNET

To understand what is really happening at the International Telecommunication Union's WCIT, one must return to an old question: is the Internet "telecommunications" or is it something else? That seemingly obscure definitional question has been at the center of communication and information policy since the mid-1960s and it – not a "UN takeover of the Internet" – should be the point of departure for understanding WCIT.

More than 50 years ago, the U.S. Federal Communications Commission decided that basic telecommunications (which in the 1960s-70s was dominated by the AT&T monopoly) needed to be strictly regulated, while "enhanced" services (i.e., the emerging networked computer services industry that relied on the public

telephone network) needed to be opened up and deregulated. To facilitate this policy goal, the FCC created a regulatory distinction between "basic" and "enhanced" services. Telecommunication was straight transmission of signals while "enhanced service" added some "information processing" to telecommunications transmission.

At that time traditional telecommunication (layers 1 physical and 2 data link of the OSI model of data communications[214]), was provided by highly restrictive, protected and usually state-owned monopolies known as PTTs (postal, telephone and telegraph monopolies). By placing information services in a separate regulatory/legal category, information service providers could (when other countries agreed) ride unmolested on that telecommunications infrastructure, without being subject to all the entry restrictions and gatekeeping regulations of the telephone companies and/or their governments. During the 1980s and 1990s, many countries were more than happy to open up that tiny "information services" market a bit in exchange for continued protection of their gigantic voice telephony markets from foreign competition.

The separation of "telecommunications" and "information services" paved the way for an open, economically and politically free Internet. Internet protocol was basically software, and thus could be considered an "information processing" or "enhanced" service. And so when the Internet went viral in the early 1990s, it spread like rhizomes into the global path cleared for it by the international deregulation of information services.

From the 1980s on, layer 1-2 telecommunications services were liberalized as well. New competitors were allowed to enter the market worldwide. The public infrastructure became more diverse. State-owned PTTs were privatized. Many prices and features were deregulated. Mobile networks became substitutes for fixed networks. As the industry became more diverse and competitive, maintaining a clear, simple distinction between telecommunications and information services became complicated. The combination of Moore's law and expanding bandwidth allowed the application layer to provide services "over the top" that were substitutes for the offerings of traditional telecommunications and broadcasting networks, such as Internet telephony (VoIP), video streaming, or instant messaging. Instead of a single monopoly platform hosting thousands of services, we got multiple telecom platforms with multiple services. It was difficult if not impossible to keep the service providers out of telecom platforms – and vice-versa.

The ensuing debate between those favoring a free market, contractually-based, deregulated Internet model and those who wanted regulators to preserve the

214) http://support.microsoft.com/kb/103884

Internet of the 1990s by treating ISPs as regulated common carriers turned – once again – on the telecommunications-information distinction. The distinction was reaffirmed in 2005, when the U.S. Supreme Court upheld[215] the Powell FCC's classification of cable modem Internet as an "information service." Net neutrality advocates in the U.S. hated that decision, because classifying ISPs as "information services" instead of "telecommunications" released them from common carrier-style regulation. But it did keep network operators exempt from many potentially debilitating forms of political and regulatory intervention, especially around interconnection arrangements.

So what does all this have to do with the WCIT and the ITRs? It is this: the ITU's attempt to update the International Telecommunication Regulations (ITRs) is a new attempt to negotiate the boundaries between telecommunications and information services. Just as in the Brand X case, if certain things are defined as telecommunication they can be subject to certain (in this case, weak) forms of control under international regulations designed to support traditional telecommunications. The targets of most ITR amendments are the interconnection arrangements among ISPs. Because it comes from the ITU, this effort is driven in large part by the interests of foreign telecommunication incumbents and by developing country administrations who feel bypassed or marginalized by the burgeoning Internet economy at layer 4 and above. In that respect, it is somewhat reactionary and threatening.

But it would be wrong, and a bit silly, to talk about the ITU "taking over" the Internet. *It is, rather, the Internet that is taking over the world of telecommunications*, setting more and more of the terms and conditions under which the ITU and its operating entities function. The Internet-based services' growth in revenue has far outstripped that of the telecommunication operators. A fabulous new economy has emerged on top of the telecommunications platform.

The issue is primarily the economics of interconnection; i.e., the revenue sharing (or lack thereof) involved in taking and sending traffic. It is not in the slightest about taking over the IETF, ICANN or IP address registration. WCIT is also a clash between a transnational regime based largely on privately negotiated contracts and the permissionless service provision created by a globally interoperable, distance-insensitive Internet protocol, and the nation-state system of hierarchical regulation and bordered gatekeeping which was built up around telephone companies. The most important battleground in the WCIT is not censorship or security, but interconnection and the flows of funds among carriers attendant upon interconnection agreements. If you want national regulatory authorities to have more collective control over ISPs generally, and American ISPs

215) http://www.law.cornell.edu/supct/pdf/04-277P.ZO

and Internet services specifically, you should support the WCIT effort.

The ITU and its members are, as usual, in reaction mode, a step behind. The current ITRs were defined in 1988, before the public internet as we know it even existed. They have numerous archaic references. They still talk about telex, for example. If you think there should be ITRs at all, it is absurd not to update them. But that raises an interesting question that no one else seems to be asking: should there be ITRs at all? Why do we need them?

The existence of treaty-based telecommunication regulations administered by an intergovernmental organization made sense in a world where telecommunications were provided by state-owned monopolies. Negotiating telecommunication interconnection across national authorities was very much like negotiating a mutual passport/visa recognition agreement. Also, many governments had their own incompatible technical standards and a single, national telecommunication standards body as well, so having an intergovernmental organization around to negotiate international compatibility made sense.

The world of the Internet is very different. It is a world of liberalized trade in services, of transnational services and corporation, of dozens if not hundreds of private-sector voluntary technical standards forums, a world of multiple, competing private network operating entities, most of them no longer state-owned, and millions of Internet-based services riding on and crossing over those multiple platforms. So why are we treating governance of this sector as something that should be happening through treaty negotiations among governments?

Why do we need a special set of international telecom regulations at all? Every country has its own national regulations regarding interconnection, privacy, antitrust, consumer protection, and so on; compatibility across platforms and services is much easier technically than it was in 1930 and tends to get worked out in the market. International telecommunications is a form of trade in services, and the WTO agreements already provide a sufficient regulatory basis for foreign or multinational providers to enter national markets with different regulatory regimes, and to offer transnational services.

Another missing fact from the debate is exactly how weak the ITRs and the ITU are. If you don't follow a duly passed FCC regulation, you can get fined or you can get your license pulled and put out of business. The ITU doesn't have any police. The ITRs are just a bunch of verbal commitments from "member states" that they will agree to do something. If the member state doesn't agree, or chooses not to enforce what it agreed to, the words are meaningless.

I hope this re-framing of the WCIT helps observers to understand better what

the general context is. In the next post, we look at the specific language of proposed ITR revisions and explain the degree to which they do or do not create a threat to Internet freedom.

PART 3: CHARGING YOU, CHARGING ME

We have carefully reviewed the proposed modifications of the International Telecommunication Regulations (ITRs) contained in TD-64[216], as well as some other recent proposals and some ITU presentations made in the runup to WCIT.[217] This review confirms that the most important potential effects of the ITRs on the Internet would come from the ITRs' attempt to change international Internet connectivity arrangements in fixed networks. For a very useful summary of *ITU work on tariff and accounting matters, international mobile roaming, international Internet connectivity, and taxation issues*, see this presentation[218] from a February 2012 WCIT preparatory meeting in Bangkok. The motivations of these proposals are primarily economic; they have to do with the flow of funds and the role of national regulators in controlling operators and commercial negotiations, rather than censorship or "taking over" Internet resources.

We have gotten into some disputes with well-intentioned advocacy groups by insisting on the disconnect between censorship and the ITRs. (See the comments on this post[219]) While it might be politically convenient in the U.S. to paint the ITR modifications as a plot to control or limit the free flow of information, we academics have to insist on precision and on perspective and context. We understand that some kinds of threats "mobilize the base" better than others, but we don't think anyone benefits in the long run by misconstruing the nature of the problem. Indeed, such distortions might backfire. Changes in charging arrangements and economic regulation could have very important effects on the free flow of information. If we are to understand those threats and how to handle them we need to accurately identify what is being proposed, why it is being proposed and what its effects might be.

Summary of what's there

The word "Internet" appears in six proposed modifications of the ITRs in TD-64. There are a few other proposals that do not refer to the Internet directly

216) http://www.internetgovernance.org/2012/06/06/td-64-for-breakfast/
217) http://www.itu.int/en/wcit-12/Pages/default.aspx
218) http://www.itu.int/oth/T065B000010/en
219) http://www.internetgovernance.org/2012/06/07/threat-analysis-of-wcit-part-2-telecommunications-vs-internet/

but which could affect it. Certain definitions, such as those pertaining to spam or security, could also have an impact, but the direct references are the most important ones, and most of them concern the economics of international internet connectivity.

The first mention of the Internet comes in a proposed change to section 2.2, which defines international telecommunication service. It would extend the definition to include "Internet traffic termination." (There is a counter-proposal to simply delete section 2.2 entirely.) A similar proposal to modify section 4.2 would add "services for carrying Internet traffic and data transmission" to a laundry list of services that members states agree to cooperate to help provide.

A second direct reference to the Internet comes in a proposed new section 3.7. The ITRs would ask administrations to:

> take appropriate measures nationally to ensure that all parties (including operating agencies authorized by Member States) involved in the provision of international Internet connections negotiate and agree to bilateral commercial arrangements, or an alternative type of arrangement between administrations, enabling direct international Internet connections that take into account the possible need for compensation between them for the value of elements such as traffic flow, number of routes, geographical coverage and cost of international transmission, and the possible application of network externalities, amongst others.

This is similar in intent to the proposal by the European Telecommunication Network Operators Association (ETNO)[220], which was released publicly by the ITU at the request of ETNO. The ETNO proposal:

▪ Brings "IP interconnection" fully into the domain of the ITU by defining it in the ITRs

▪ Creates another two new definitions for "best effort" and "end to end quality" for the delivery of "packet data units" – in other words, packet switching becomes officially part of the ITRs.

Based on these definitions, the ETNO proposal then tries to do two things. First, it tries to ensure that member states allow interconnection arrangements designed to allow end to end quality of service as well as best-effort packet forwarding; second, it urges operating agencies involved in negotiations "to ensure an adequate return on investment in high bandwidth infrastructures," by making their commercial agreements "achieve a sustainable system of fair compensation for

220) http://files.wcitleaks.org/public/ETNO%20C109.pdf

telecommunications services and, where appropriate, respecting the principle of sending party network pays."

The next direct reference to the Internet comes in a proposed new section 6.7. One of the most interesting proposals, it says:

> 6.7 Member States shall ensure that each party in a negotiation or agreement related to or arising out of international connectivity matters including those for the Internet will have standing to have recourse to the competition authorities of the other party's country.

As far as we can tell, this means that international peering or interconnection negotiations would allow an unsatisfied party to drag the competition authorities of the other party's government into the negotiations. One can see why certain large U.S. companies might not like this, but one can also see how it might allow competing companies, from the U.S. or elsewhere, to challenge state-owned or private monopoly international gateways with appeals to local competition authorities. Another proposal modifies the above by adding "will have access to alternative dispute resolution mechanisms."

The last proposed ITR change that directly references the Internet is a proposed new section 8.A.4 which would say,

> 8A.4 Member States shall take measures to ensure Internet stability and security, to fight cybercrime and to counter spam, while protecting and respecting the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights.

Nice. The words here are unobjectionable in their literal meaning, but typical of the vague, impossible-to-operationalize language that often populates international agreements. We will have more to say about the intersection of cybersecurity issues and the ITRs in the next blog post in this series.

Another proposed revision that clearly targets the Internet, without mentioning it, would revise 3.1 of the ITRs to require operators to

> cooperate in the establishment, operation and maintenance of the international network to provide a satisfactory quality of service [and above a minimum level corresponding to the relevant ITU-T Recommendation].

The bracketed language (which indicates a lack of support) is a straight-up protectionist measure. A mandatory minimum quality of service would have the effect of banning many Internet-based services and applications, because so much of the Internet relies on best-effort packet forwarding. For example, a Voice over IP telephone service might often fall below regulatory minimums regarding quality

of service. Consumers often prefer low quality anyway, because they are willing to trade quality for lower cost (e.g., Skype).

Analysis

It is clear that several proposals revise definitions to make Internet, and especially "international Internet connectivity" a subject of the ITRs. Obviously, this continues the old debate about what is telecommunications and whether it includes Internet, as described in our last blog.[221] Defining Internet as a telecommunication service is not something we favor, because it would pave the way for regulating what are now privately negotiated, contract-based interconnection arrangements subject to market forces.

All the proposals discussed above show how many of the ITR modifications are not new attempts to "take over the Internet" but a continuation of long-running battles over the way the Internet has disrupted traditional telecom businesses and markets. The proposals reflect the desire of certain companies that operate layer 1 and 2 networks to be better compensated for carrying the burgeoning amount of data traffic at the application layer, or to be protected from it. For some administrations, mainly developing countries that might still have monopolies or state-owned champions running their networks, it reflects dissatisfaction with the Internet model of paying for your own connectivity to the Internet (sender pays), rather than the old shared-payment model, and some dissatisfaction with contractually negotiated as opposed to government-regulated interconnection.

The battle over international internet connectivity is not new; it goes all the way back to 1999, when various countries remote from the centers of Internet content, including for a while Australia, complained to the ITU about the new Internet model of paying for connectivity rather than sharing the cost of international bandwidth with your corresponding country operator. This resulted in ITU-T recommendation D.50[222], first passed in 2000 and since revised several times. D.50 is just a recommendation; some of the proposals try to make it more of a requirement by bringing it into the ITRs. This may be less of a threat than it seems, although it bears watching. The ITU has done endless studies and engaged in endless wrangling about how to measure and charge for Internet traffic. It has never come up with a solid, consensual proposal on how to do this. Just as AT&T's early effort to get YouTube and other application-layer players to pay more for the tubes never went anywhere[223], it is not entirely clear how ETNO's

---

221) http://www.internetgovernance.org/2012/06/07/threat-analysis-of-wcit-part-2-telecommunications-vs-internet/

222) http://www.itu.int/rec/T-REC-D.50/e

idea of "commercial agreements to achieve a sustainable system of fair compensation for telecommunications services" would be implemented. ETNO is also asking for a free pass to negotiate end to end quality of service interconnections; this should give net neutrality advocates pause, but national regulation could ensure that it is not used to discriminatory effect.

This entire effort, in our opinion, should be abandoned and not enshrined in the ITRs. ETNO's members already can negotiate any charging arrangements their partners will go along with. If they want regulators involved it must be because the market will not deliver what they want. The idea that connectivity charges should be rigidly governed by some regulatory-mandated metric like duration in minutes or traffic or number of packets or the direction of packet flows is simply an anachronism that does not reflect the heterogeneity of online services and the prevalence of multi-sided markets. Data is not voice, and telecommunication authorities pining for the good old days of predictable settlements simply need to wake up and face the facts about the way Internet applications work.

Mobile roaming

We have so far avoided the topic of international mobile roaming charges because it has traditionally been an area that could be unambiguously classified as telecommunications, at least when voice communications are involved. But we all know that data communications are taking over the mobile sphere just as they did in fixed telecommunications. And we also know that international data roaming charges are, if anything, even more outrageously overpriced than voice roaming charges.

As far as we can tell, the proposed ITR interventions focus on standard consumer protection matters such as transparency of prices, notification, and affording consumers an opportunity to decline additional paid roaming services. There does not seem to be any effort to regulate or control the charging system for mobile data interconnections specifically; indeed since most of the mobile data that crosses international boundaries probably does so through a fixed network, it is the fixed network charging arrangements that one has to watch. There is a new section 4.6 that tries to regulate the quality of service offered by mobile roaming agreements; this has little support however. The most salient section is this:

> 4.4 Member States shall ensure that operators providing international telecommunication services, in particular international roaming, provide transparent and up-to-date information on retail charges, including roaming charges. [In particular, each customer should also be able to easily have

223) http://arstechnica.com/uncategorized/2005/10/5498-2/

access to, and receive appropriate and timely pricing (including taxes) information free of charge when abroad on the relevant price plan, except when the customer has notified his home operator that he does not require this service].

Conclusion

There are several efforts in the ITRs to extend standard forms of telecommunications regulatory authority over international internet connectivity arrangements. These economic interventions could be damaging to the Internet's status as a relatively open platform for new services if passed, but it is unclear how much support they have. The most potentially disturbing proposal is that of ETNO, because it shows that major developed-world telecom companies want to incorporate international internet connectivity into the ITRs. But even their proposal would be limited in its impact because its proposed new charging arrangements, calling for "sustainable" and "fair" compensation, are so vague. It would, however, be a very bad long-term precedent to incorporate such things under the ITR if one believes in a market-driven, free and open Internet.

PART 4: THE ITU AND CYBERSECURITY

Previous blogs about the ITRs emphasized the importance of interconnection agreements and flows of funds in driving the WCIT agenda. These articles, while correct, may have underestimated the degree to which bringing cyber-security into the ITRs is also a central arena for conflict and negotiation.

I have argued that the securitization[224] of the Internet constitutes one of the main dangers to its freedom. Just as an appeal to patriotism was once described as the "last refuge of a scoundrel," all kinds of scoundrelly[225] proposals to stifle free expression, invade privacy, abolish anonymity, restrict new businesses and elevate state power invoke cyber security as the rationale. At the same time, who can oppose efforts to improve the security and privacy of digital services and the Internet infrastructure? The problems of cybercrime, botnets, DDoS attacks, rampant unauthorized surveillance, cyber-espionage and state-sponsored attacks are real. Thus, discussions of cyber-security must be careful and measured in their approach. They should be grounded in an awareness that there is a legitimate need for action, but mindful of the abuses and manipulations that can masquerade under the banner of security.

---

224) http://en.wikipedia.org/wiki/Securitization_%28international_relations%29
225) http://www.lexipedia.com/english/scoundrelly

It is clear that the ITU has seized on cyber-security as an arena in which it can assert its relevance.[226] But that is not surprising; such a strategy for gaining attention, participation and funding mirrors that of numerous Washington DC policy institutes[227] and various US government agencies.[228] Furthermore, most of what the ITU does around cybersecurity is basically education and capacity building.[229] ITU Plenipotentiary Resolutions 130 and 146[230] are typical of the kind of approach the ITU takes; if you can make your way through the bureaucratese, they involve providing assistance on request to developing countries.

Aside from its X.509 standards for public key infrastructure, which many applications have found extremely useful, the ITU-T has not won for itself a strong role in setting standards that are relevant to the full panoply of cyber-security issues. ITU has little regulatory capacity and relies almost entirely on member states for policing and enforcement of whatever rules it passes.

Thus it is hard to imagine the ITU as a powerful or uniquely threatening player in computer and Internet security. The U.S. government, which is powerful and (sort of) well-funded, has had enormous troubles[231] changing the network security practices of its own departments and agencies. The idea that the ITU can serve as the nexus for dictating and strongly shaping the security and identification practices of thousands of public operators, tens of thousands of private networks, and billions of devices worldwide lacks credibility.

In reality, the greatest cyber-security-related threats to Internet freedom come from national governments, not from the ITRs. National sovereignty and claims of national security already allow states to do all kinds of repressive, warlike things to all forms of international (and domestic) communications, such as block and filter content, ban or regulate devices, and restrict access. *Articles 34, 35 and 37 of the ITU constitution*[232] already recognize the right of sovereigns to promote their own national security and to cut off communications in various ways. Quite apart from those ancient rules, in a basically anarchic international system a sovereign state has a de facto right to do whatever it wants in matters of national security until and unless other states gang up on it. So it is difficult to see how modifications to the ITRs could dramatically increase the threat of kill switches and the like.

---

226) http://www.itu.int/cybersecurity/
227) http://csis.org/program/commission-cybersecurity-44th-presidency
228) http://www.hstoday.us/briefings/today-s-news-analysis/single-article/house-dhs-budget-boosts-border-security-cybersecurity-nixes-revamp-of-fema-grants/b14ad3c596ea16bc58a2b9b2cac1b57d.html
229) http://www.itu.int/ITU-D/cyb/
230) http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf
231) http://en.wikipedia.org/wiki/Einstein_%28US-CERT_program%29
232) http://www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx

Canadian scholar Dwayne Winseck emphasizes the degree to which current ITU treaties are based on the sovereigntist model. As he puts it, perhaps a bit excessively, the ITU treaties have been authorizing "Intercepting, Suspending and Blocking the Flow of Information since the 1850s." But even as it enables repressive action, sovereignty also serves as a check and balance. Each state has a high degree of autonomy, shielding them from regulations and practices adopted by other states. The national interests of different states can cancel each other out.

Thus, the most significant political drivers of law and public policy toward cyber-security are to be found at the national level. (In the private sector, in contrast, the perspective and scope of action tends to be transnational, contractual and operational.) Indeed, reading the relevant proposals in TD-62, one can only be impressed with how broad, unfocused, uninformed and sometimes naïve the cyber-security related proposals can be. Most of them ask member states to do generic things like "stop spam," "protect data and network integrity," or "supervise enterprises operating in their territory" to ensure that they "use ICTs in a rational way." Then there's my favorite: "ensure Internet security and stability." The African countries' proposal for a new Article on Security is almost lifted verbatim form a March 2010 US Presidential Declaration entitled "Cyberspace Policy Review."

At their worst, the ITR proposals try to prevent international communications that "interfere in their internal affairs," or undermine their "sovereignty, national security, or territorial integrity." Those proposals, which focus on "subversive content," sound quite reactionary in today's global public sphere, which was created by the borderless information flows of the Internet. But it is hard to see how they authorize anything that national governments cannot already do. We seem to forget that such proposals are not much of a departure from the legal and normative status quo. Current international communications, both legally and in operational reality, are already formed around the sovereigntist/national security model. That's why Bradley Manning is in jail and Wikileaks is persecuted; that's why China constructed the Great Firewall; that's why South Korea censors Internet access to North Korea and vice versa; that's why France prosecuted Yahoo for displaying Nazi memorabilia.

And that leads to our next point. The big push for cyber-security regulations in the ITRs is led by Russia. This may reflect Russia's inability to get the U.S. engaged in cyber-security treaty negotiations in other venues. Since 1998, Russia has supported – and the U.S. has opposed – the development of a treaty that would ban the use of cyberspace for military purposes. Although the U.S. position has changed under Obama and some new forms of cooperation are underway,[233] the

Russians still see themselves as the weaker party in the cyber-warfare game and would like a treaty similar to the chemical weapons agreements, which prohibit the use of certain technologies as weapons. The recent leaks about the US role in developing Flame and Stuxnet should make it clear why the US has been unwilling to bind itself to any such limitations. Coupled with its superior technical capabilities, its globally strong Internet industries and its control of the DNS root, the U.S. probably appears as a significant cyber-security threat to many other countries.

Similarly, the strong support of Arab states for some of the Russian cyber-security proposals stems not only from the fact that many of them are dictatorships uncomfortable with the free flow of information, but also from their concerns about Israel's technological superiority in network surveillance and monitoring technologies and its cooperation with the US in the joint development of cyber weapons.

So it is predictable that the Russians and other semi-hostile states would try to insert as many guarantees of cyber-security and cyber-sovereignty into the ITRs as possible. It is the vehicle most available to Russia and other countries who feel threatened by the cyber capabilities of other nations.

But this reliance on the ITRs is in many respects a sign of weakness. The ITRs are a fairly lame instrument with which to attempt shielding oneself from global information flows and cyber-attacks, much less for comprehensive regulation of computer and internet security. The ITRs are fundamentally about the relationships among public telecommunication network operators. While there are attempts to extend its definitions to include international Internet termination, as noted previously those definitional adjustments are contested by powerful states. Even if the definitions were broadened, it is unlikely that the ITRs can ever have a lot of teeth in the cyber-security arena. The Internet is a network not just of a few hundred public carriers but of tens of thousands of private networks, millions of applications and billions of heterogeneous devices. Technical standards are set by a diverse set of private, usually voluntary associations. Most of the relevant standards in the cyber domain are set by device, software and application providers over whom the ITU has little leverage. The ITU lacks a compulsory standard-setting capability even in its own realm, though there are proposals to make a few ITU-T recommendations "requirements."

The bottom line is that the biggest threats posed by the ITRs' proposed forays

233) A group of cybersecurity specialists and diplomats representing the United States, Belarus, Brazil, Britain, China, Estonia, France, Germany, India, Israel, Italy, Qatar, Russia, South Africa and South Korea agreed on a set of recommendations to the United Nations secretary general for negotiations on an international computer security treaty. See NYT: http://www.nytimes.com/2010/07/17/world/17cyber.html

into network security can be reduced to the definitional issue. If definitions are expanded to include Internet as an international telecommunication service and cyber-security as part of the ITRs' remit, we have a problem. The problem is not as epic as some make it out to be, and not as significant to end users as the threats posed by unilateral actions by their own national governments. But it would be troublesome indeed to mix telecom regulation with cybersecurity and Internet regulation, in an already complex ecosystem. And it would be a truly bad sign if a critical mass of governments wanted to regulate Internet security through the ITRs badly enough to alter the definitions over the objections of the U.S. and the Internet technical community.

On the other hand if the definitions are not expanded, there is little harm the ITRs can do to Internet security governance.Thus, civil society should insist that: a) ITU standards remain recommendations, not requirements; b) the ITRs and their definitions stick closely to their original mission regarding layers 1 and 2 of the infrastructure.

I will review a few of the specific proposals in the known WCIT documents.[234] The proposed amendments include many references to spam, some of them poorly defined. Some have argued that these references open the door to internet content regulation. Here I agree with Winseck's analysis: the spam-related proposals seem anodyne in content, merely urging countries to adopt "national legislation" (many already have), "to cooperate to take actions to counter spam" (many already do), and "to exchange information on national findings/actions to counter spam" (what's wrong with that?). There is no evidence that spam references constitute the thin edge of a wedge that will lead to ITU jurisdiction over Internet content. Yet still, hewing to a hard line on the definitional issue, I would not want to see any mention of spam in the ITRs, because it is an information services issue rather than a telecommunications issue.

Another proposal says that

> A Member State shall have the right to know through where its traffic has been routed, and should have the right to impose any routing regulations in this regard, for purposes of security and countering fraud.

This proposal, a bad one, probably reflects the Arab states worrying about routing through Israel. (Interestingly, according to a March 2012 summary by a US law firm[235], the US did not initially object to this proposal, but later joined the Uk, Sweden and CEPT in opposition.) At any rate, the import of this proposal hinges on what kind of traffic we are talking about. If the Internet and its information services

234) http://www.wcitleaks.org/
235) http://files.wcitleaks.org/public/Sixth%20CWG%20-%20TD-43%20Summary.pdf

are not part of the definition of international telecommunication services, its references to routing apply only to telecommunication circuits. If Internet services are included, such a regulation might legitimate interference with BGP and Internet routing. Even so, I fail to see what such a provision accomplishes that could not already be accomplished by national regulation of their Internet service providers or telecom companies. The same is true of the references to "Originating Identification" in the proposed revisions. If you think this applies to the Internet (which it does not and cannot) it sounds troublesome. If it applies to calling line identification (CLI; i.e., caller ID) made possible by the SS7 telecommunications circuit-switched environment, it's routine stuff.

At the end of a reasonably sane overview, Winseck suddenly turns gloomy. He apparently feels that proposals to add a new section 8A contain "a raft of threats that, in their entirety, would usher in the foundation of controlled and closed national internet spaces that are subordinate to the unbound power of the state in every way." The proposal that seems to have inspired those dark musings was this Russian contribution:

> Member States shall ensure unrestricted public access to international telecommunication services and the unrestricted use of international telecommunications, except in cases where international telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other States, or to divulge information of a sensitive nature.

I just don't see that much of a threat. First, it should be pointed out that this is only one of about five different proposals for the same paragraph, and none of the others contain the bad language. The existence of other proposals indicates that there is no consensus on this one. One could also point out that all of the Russian proposals to enlarge the role of the ITU in Internet governance made at the 2010 Plenipot failed.

Of course it is true that many national governments would wish to have controlled and closed national Internet spaces, but it is also true that many national governments don't. Most businesses, engineers and civil society activists will strongly agitate against such closure. But governments that want to do this can accomplish the goal much easier by acting unilaterally; they don't need the ITRs. Remember my fundamental premise: the biggest threats to Internet freedom come from the actions of national governments with effective control over their territories.

If, contrary to my premise, someone asserts that the ITRs provide an opportunity to lend legitimacy to repressive actions at the national level, I would

partly agree, partly disagree. Assuming that civil society remains vigilant and observant, as it now is, any attempts to establish new, restrictive norms via the ITR process will lead to public debates that are more likely to discredit such assaults on the free flow of information than legitimize them. Furthermore, a mere assertion in an international regulation that one will block incoming information "of a sensitive nature" does not automatically create the means to do so. In a world of ubiquitous tablets and mobile devices, that's not easy to do.

So yes, civil society and internet freedom advocates should mobilize around the WCIT to promote Internet freedom norms. But they should not blow the ITRs out of proportion. Similar policy issues around cyber-security, privacy and freedom of expression arise in ICANN, in intellectual property treaties masquerading as trade agreements, in European Commission Directives and in the exercise of extraterritorial jurisdiction by superpowers. There is nothing especially momentous about the ITR negotiation, in my opinion. Threat assessment should be based on an understanding of the implementation requirements of the policy proposals and the likelihood that they will garner the needed political support, not just on reading words and assuming that such words can be instantly translated into operational practice across 190 nation-states.

Equally important, civil society should not begin by conceding that the ITRs are even applicable to the Internet. The definitional issue remains the crucial one. And it is still open.

국가 시대의 인터넷 자유

필자 제레미 말콤(Jeremy Malcolm)[236]
번역 오병일

개 요

지난 해 국제전기통신연합(ITU) 국제전기통신세계회의(WCIT)는 정부간 기구의 인터넷 통제 확대에 대한 인터넷 커뮤니티의 두려움을 불러 일으켰다. 이 두려움은 정당한 것이었지만, ITU에 대한 과도한 강조는 인터넷이 이미 비민주적인 방식으로 – 종종 정부에 의해서, 국내적/세계적 과정을 통해서 뿐만 아니라 기업의 이익에 의해서 – 통제되고 있다는 사실을 잊게 만든다. 이는 또한 때로는 정부가 가만히 있는 것이 이용자의 자유에 도움이 된다는 이유로, 인터넷 이용자의 권리를 지키기 위해 때로는 정부의 조치가 필요하다는 사실을 잊게 만든다.

각 수준에서의 적절한 거버넌스 메커니즘이 다르기는 하지만, 이는 국가적 수준에서와 마찬가지로 세계적 수준에서도 사실이다. 특히, 인터넷 거버넌스를 위한 세계적으로 적용 가능한 원칙의 개발이 소중하고 중요한 어떤 영역이 있다. 일반적인 믿음에도 불구하고, 그러한 세계적 원칙이 도움이 되는 중요한 공공정책 영역을 모두 포괄하는 세계적인 멀티스테이크홀더 절차나 기구의 네트워크는 존재하지 않는다. 그러나 '개발을 위한 과학기술 위원회'(CSTD) 산하에 '강화된 협력'에 대한 워킹그룹(Working Group on Enhanced Cooperation, WGEC)이 만들어지면서, 우리는 이제 이와 같은 공백을 메꿀 기회를 갖게 되었다.

지금까지 시민사회는 인터넷 거버넌스 체제의 진화를 위한 적극적인 의제의 개발에 참여하는데 매우 주저해왔다. 그러나 우리가 그렇게 하지 않는다면, 현상유지가 계속되거나 혹은 (ITU와 같이) 덜 민주주의적이고 멀티스테이크홀더에 기반하지 않은 대안들이 전면에 나설 것이다. 이 논문은 정보사회세계정상회의(WSIS)가 위임한 '강화된 협력'을 실현할 하나의 가능한 방식을 제안한다. 그러나 그 주된 요지는 여기서 제안한 방식과 무관하게, 지금이 인터넷 이용자의 권리와 자유의 보호를 위한 더 공식적인 제도적 플랫폼의 장점을 시민사회가 심각하게 고려해야 할 때라는 것이다.

236) 국제소비자연맹 수석정책관, jeremy@ciroap.org

도입

지난 해, 유럽에서 논란이 많았던 위조방지무역협정(ACTA)과 미국의 온라인해적행위방지법(SOPA) 및 지적재산권보호법안(PIPA)-양자 모두 중간서비스제공자로 하여금 소비자의 인터넷 이용을 추적하도록 요구하는 내용이었다.-의 패배에 뒤이어, 서구의 디지털 활동가들은 자연스럽게 인터넷 자유를 침해하는 정부들에 대한 민감성이 더 높아졌다.

지난 12월, 국제전기통신연합(ITU)의 전기통신세계회의(WCIT)에서의 모든 인터넷 관련 제안에 그들이 얼마나 격렬하게 반대했는지 보면 이를 알 수 있다. 이러한 두려움은, 비록 그 제안들이 별 것 아닌 것처럼 보여도, 기존의 더 개방적이고 포용적인, 멀티스테이크홀더 방식이 아니라, 순전히 정부간 절차를 통해서 정부가 인터넷 표현의 자유, 보안, 프라이버시와 같은 인터넷 거버넌스 이슈들을 더 폭넓게 다루려는 정부의 움직임을 보여주는 것이었다.

이러한 두려움의 기저에는 다음과 같은 세 가지의 가정이 있는 듯하다 :

1. 정부는 인터넷 거버넌스에 개입해서는 안 된다.

2. 정부가 인터넷 거버넌스에 개입한다면, 그것은 단지 국가적 수준에서 이며, 세계적 수준에서는 안 된다.

3. 정부가 세계적 수준의 인터넷 거버넌스에 개입한다면, ITU에 의지하기 보다는 그들의 관심사를 다룰 수 있는 기존의, 아래로부터의, 멀티스테이크홀더 체제가 존재한다.

그러나 세 가정 모두 틀렸다. 이것을 이해하지 못하는 것은 인터넷을 위한 정책을 수립하기 위해 많은 정부들이 정부간 메커니즘을 이용하도록 추동하는 힘을 잘못 이해하는 것이며, 우리가 바로 지금 이 힘을 일반적인 인터넷 이용자의 관심사에 더 잘 대응할 수 있는 방향으로 이끌 수 있는 기회를 간과하는 것이다. 사실, 세 가지 가정 모두 틀렸음이 입증된다면, 정부가 글로벌 인터넷 거버넌스에 참여할 수 있는 더 수용 가능한 방안을 찾는 것은 반드시 필요한 일이다. 그래서 이 가정들을 차례로 검토해보도록 하자.

국가적 수준에서 정부의 필요성

정부가 인터넷 거버넌스에서 정당한 역할을 가지고 있지 않다는 첫 번째 가정은 너무 터무니없어서 마치 내가 허수아비 주장을 내세운다고 비난받을지도 모르겠다. - 그러나 이는 사이버-자유주의라고 불리는 진지한 학파이며, “인터넷 자유" 운동으로서 (특히 미국의 활동가들에 의해) 온라인 권리와 자유를 옹호하는 관점으로부터 거의 공리처럼 유통된다. 더구나 이 사이버-자유주의 관점은 정치적 자유주의자들만 보유하고 있는 것이 아니다. 심지어 정치적으로 진보적인 활동가들도 오프라인보다는 온라인에서 정부의 개입을 더 불신하는 경향이 있다. 이는 인터넷 예외주의로 표현되는데, 인터넷은 다르고 더 규제 방임적 접근이 요구된다는 것이다.[237]

237) 사이버-자유주의자 및 인터넷 예외주의자들과 보수적인 “반예외주의” 사이의 고전적인 논쟁은 골드스미스(Jack L. Goldsmith)의 사이버 아나키에 대한 반대 L.65 U. Chi. L. Rev. 1199 (1998) 과 포스터(David Poster)의 답변 “'사이버 아니키에 대한 반대'에 대한 반대", 17 Berkely Tech.L.J.

사이버-자유주의적 명제를 수용하는 것은, 국가적 수준에서 다음과 같이 우리 중 많은 사람들이 적극적으로 지지하는 영역들에, 정부가 개입해야 할 역할을 부정하는 것이다.

- 네트워크 운영자가 특정한 형태의 인터넷 콘텐츠나 서비스를 차별하지 못하도록 망 중립성 규칙을 통과시키는 것
- 차세대 IP 버전인 IPv6로의 이행을 위한 인센티브를 제공하는 것 – 현재까지 시장이나 규범의 힘이 명백하게 실패해온 작업이다.[238]
- 일부 산업 분야에 의해 채택된 자발적인 미약한 실행규약에서 더 나아가 소비자의 개인 데이터 보호를 위한 강제력 있는 표준을 수립하는 것
- 지역의 소비자들이 도시 거주자와 동등하게 정보 사회에 참여할 수 있기 위해, 기본적인 수준의 인터넷 서비스를 보장받도록 보편적 서비스 정책을 확대하는 것

1993년에, 혹은 심지어 2003년에도 우리는 시장에 유리한 해석을 허용했고 이 영역에서 규제를 미루었다. 그러나 2013년, 자신의 프라이버시를 보호받으면서 오픈 인터넷에 저렴하게 접근할 수 있는 모든 소비자의 정당한 이익이 어떤 식으로든 정부의 개입 없이 보장될 수 있다는 것은 점차 믿기 어려워 보인다.

이것은 정부의 개입이 매우 자주 인터넷 이용자에게 해로운 영향을 준다는 것-예를 들어, 공정 이용과 혁신을 제한하는 지적재산권의 형사적 집행 조치를 통해, 우리의 온라인 커뮤니케이션에 대한 비밀스러운 감시를 통해, 사이버 전쟁에 사용할 목적의 악성 소프트웨어 생산을 통해, 혹은 인터넷 전화 (mVoIP)와 같은 특정한 인터넷 서비스의 이용을 금지함으로써-을 부정하는 것은 아니다.

그러나 정부가 인터넷을 규제하지 못하도록 하는 것은 올바른 답이 아니다. 최소한 산업 또한 종종 인터넷 이용자의 권리와 자유에 역행하는 행동을 하기 때문이다. 웹사이트는 우리도 모르게, 혹은 우리의 동의 없이 우리의 가장 사적인 정보를 수집하여 광고주에게 판매하고, 저작권자와 ISP들은 파일을 공유한 것으로 의심되는 이용자의 인터넷 접근을 옥죄는 비밀 협약을 맺고, 금융 중개자들은 위키릭스의 자금을 막기 위해 공모한다. 우리는 국내의 소비자 법률, 경쟁법, 혹은 프라이버시 및 데이터보호법, 혹은 세제 조치, 개발 보조금, 공동규제 규약 등 더 유연한 조치를 통해서 기업들의 나쁜 짓으로부터 우리를 보호해줄 것을 정부에 요구할 권리가 있다.

그러나 어떤 경우에는, (위키릭스의 사례와 같이) 정부와 기업이 우리의 권리와 자유를 침해하는데 공모하기도 한다. 그래서 우리 자신의 정부도, 시장도 온라인 권리 침해로부터 우리를 보호하지 못한다면, 우리는 무엇에 호소해야할까? 그러한 경우에 우리는 또 다른 거버넌스 메커니즘-예를 들어 규범, 혹은 기술 (잠시 후에 이와 같은 것을 더 얘기하겠다)-을 고려하거나, 혹은 세계적 수준을 고려할 수밖에 없다.

1365(2002)에서 찾아볼 수 있다. 팀 우(Tim Woo)는 골드스미스와 함께 <누가 인터넷을 통제하는가? 국경없는 세상에 대한 환상> (Oxford University Press, 1996)에서 그의 주장을 발전시켰다.

238) "인터넷의 아버지"인 빈트 서프(Vint Cerf)는 IPv6로의 이행을 촉진하기 위해 정부 인센티브의 필요성을 옹해했던 사람들 중 한명이다. : 제니퍼 스콧(Jennifer Scott), "스프가 IPv6로의 이행을 위해 정부 인센티브를 요구하다" 2010.11.11, http://www.itpro.co.uk/628531/cerf-calls-on-government-incentive-for-ipv6-migration

세계적 수준에서 정부의 필요성

이는 우리를 다음 가정으로 이끈다. 즉, 정부가 때로는 인터넷 거버넌스에 관여하는 것이 필요하지만, 그것은 단지 국가적 수준에 국한되어야 한다는 것이다. 이는 사실이 아니다. 왜냐하면, 정부가 국가적 수준에서 내린 (우리 중 다수가 어떤 경우에는 필요하다고 생각하는) 결정이 국경 밖으로 전파되는 일정한 경향을 갖고 있기 때문이다.

이는 인터넷 자체가 국경이 없고, 그래서 정부에 의한 것이든, 기업에 의한 것이든, 한 나라에서 만들어진 정책이 (그 정책 결정자들이 정당한 권한을 가지고 있지 않은) 전 세계 다른 곳의 이용자에게 영향을 미칠 수 있기 때문이다. 예를 들어, 2011년에 미국 정부기관은 미국 법에 따른 권한을 주장하며 rojedirecta.com 과 rojedirecta.org 도메인을 압류했는데, 그 도메인들은 스페인 회사의 소유였으며 스페인법에 따라 합법적인 것으로 결정되었었다. (그 도메인들은 이후에 반환되었다.)[239] 마찬가지로, 콘텐츠가 미국 디지털밀레니엄저작권법(DMCA)에 근거해서 삭제되었을 때, 이는 전 세계의 이용자에게 영향을 미친다. 왜 그 이용자들은 그것에 대해 참여할 권리가 없는가?

그들(이용자)이 그런 권리가 있다면, 우리는 '어떻게' 그들이 그러한 권리를 가질 수 있을지의 문제로 돌아온다. 위에서 언급한 바와 같이, 사이버-자유주의자들은 그것을 기술 혹은 규범의 이용에 한정하려는 경향이 있다. 전자의 사례로는, 전반적으로 규제되지 않는 온라인 공간과 커뮤니케이션 채널을 만들기 위해, 기술적인 지식이 있는 이용자들이 PGP나 Tor와 같은 강력한 암호 소프트웨어를 사용할 수 있다. 그러나 그러한 공간들을 개방적이고 자유롭게 만드는 인터넷 기술들의 특성들이 또한 정부나 기업의 남용에 반대하는 보호막으로서의 효과를 제한하기도 한다. 기술은 (온라인 사기에 대한 국경을 초월한 해결책을 제공하는 것과 같은) 적극적으로 권리를 주장하기에는 덜 효과적이기도 하다.

마찬가지로 규범은 유용할 수 있지만, 자기 강제력이 있는 것은 아니다. 우리는 어느 정도까지는 인터넷 규범을 강제하는 군중들의 힘에 의존할 수 있다. 이것이 지난 해 위조방지무역협정(ACTA), 온라인해적행위방지법(SOPA), 지적재산권보호법안(PIPA)를 물리치는데 매우 효과적이었다. 이것은 국내적 수준에서 민주적 과정이 취약하거나 부패한 곳에서 중요하지만, 정부가 국내적으로 인기가 없는 제안들의 "정책 세탁"을 위해서, (ITU와 같은) 전통적인 정부간 기구나 (ACTA와 환태평양동반자협정 TPP와 같은) 무역협상의 민주적 취약성에 의존하고 있는 세계적인 수준에서 훨씬 더 필수적이다.

그러나 정책 토론의 분위기가 사이버-자유주의의 현수막이 휘날리는 자극적인 열정에 휩쓸려 들어갈 때, 그 군중들은 또한 폭도가 될 수도 있다. 예를 들어, 핵티비스트(해커 활동가) 그룹인 어나니머스(Anonymous)는 정부, 광신도들, 기업들의 위협에 직면한 온라인 권리와 자유를 지키기 위해 많은 좋을 일들을 해왔다. 그러나 또한 WCIT 회의에서 ITU 웹사이트를 공격함으로써 그 회의에 원격으로 참여할 수 있는 유일한 공식 통로를 위태롭게 하여 시민사회 참여자들로부터 비판을 받은 바 있다. 따라서 어나니머스와 같은 풀뿌리 그룹을 통한 직접 행동은 최후의 수단으로서 소중하기는 하지만, 인터넷 정책을 형성하기 위한

239) 네이트 앤더슨(Nate Anderson), "정부가 패배를 인정하고 압류된 Rojadirecta 도메인을 되돌려주다", 2012.8.30.
http://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/

우리의 주요 수단이 될 수는 없다. 보안 전문가이자 저자인 브루스 쉬나이어(Bruce Schneier)는 최근 이렇게 썼다. :

> 대중들은 때로는 SOPA/PIPA, 아랍의 봄 등 특정한 이슈를 중심으로 조직화될 수 있고 권력자들의 어떤 행동을 막아낼 수 있다. 그러나 그것은 지속되지 않는다. 조직되지 않은 자들은 조직되지 않은 상태로 되돌아가고, 권력자의 이해관계는 주도권을 되찾는다.[240]

정부와 기업의 권리 남용을 막기 위한 효과적인 방안으로, 세계적 수준에서 조직화되는 것은 인터넷 관련 공공정책의 국경을 초월한 영향을 관리하기 위해 그들과 (협의)테이블에 앉는 것을 의미한다. 현재 이것은 TPP에서 비밀협상의 관객으로 참여하거나 세계지적재산권기구(WIPO) 청중석의 뒷줄에 앉는 것을 의미한다. 그것도 우리가 운이 좋을 경우이다. 다른 이슈들의 경우에는, 우리가 전혀 발언할 수 없다는 것을 의미한다. 왜냐하면 그러한 이슈들을 다룰 세계적인 논의공간이 없기 때문이다.

제도적인 진화의 필요성

그래서 우리는 세계적 수준에서 인터넷 정책 토론에 온라인 활동가들의 더 공식적으로 제도화된 참여 수단이, 자율규제, 기술기반 및 풀뿌리 기반의 시도들이 실패한 이후에 존재하는 공백을 메꿔줄 수 있는지 최소한 고려해 봐야 한다. 어떤 이슈 영역의 경우에는, 거의 그렇지 않을 것이다. 예를 들어, 우리는 인터넷 표준 개발과 IP 주소 및 도메인 이름의 할당에서는 IETF, W3C, ICANN과 같은 기관을 통해서 모든 이해당사자들이 참여할 수 있는 강력한 세계적 메커니즘을 이미 가지고 있다.

그러나 보안, 사이버범죄, 지적재산권 집행, 소비자 보호, 데이터 보호 및 프라이버시, 온라인 표현의 자유 등 다른 영역에서는, 우리는 현재의 제도적 방식의 진화를 고려할 필요가 있다. 이는 "현재의 조직, 시스템, 절차는 산업이 주도하는, 상향식의, 합의 기반의 절차를 통해 이해당사자의 요구를 성공적으로 충족하고 있기"[241]때문에 인터넷 거버넌스 체제의 어떠한 개혁도 필요 없다는 취지의, 위에서 강조한 세 번째 가정으로 우리를 이끈다. 그것이 사실이라면 말이다.

물론 이 이슈들과 관련된 세계적인 토론이 있다. 그러나 그들은 실제 정책 결과물에 실질적 영향을 미치기에는 너무 약하거나 (인터넷거버넌스포럼 IGF의 경우), 영향을 받는 모든 이해당사자의 의미있는 참여 기회를 제공하지 않는다. (OECD, APEC, WIPO, CSTD, TPP 뿐만 아니라 ITU 자체를 포함하여, 이러한 경우가 훨씬 많다.)

종종 이러한 기존의 체제에서 배제되는 것은 시민사회이다. ACTA에서 그랬고, 현재 TPP에서 그런 것처럼 말이다. 그러나 다른 경우에는 개발도상국 정부들이 배제되기도 하는데, 그들은 자신들의 이해관계는 바깥으로 밀려나고, G8이나 OECD와 같은 선진국 그룹이

240) 브루스 쉬나이어, "권력과 인터넷", 2013.1.31, http://www.schneier.com/blog/archives/2013/01/power_and_the_i.htmlnc=35.

241) 이러한 관점이 특정하게 공식화된 것은 ITU에 제출된 시스코의 의견서이다. 아래 사이트에서 볼 수 있다. http://www.itu.int/md/S12-WTPF13PREP-C-0014/en, 그러나 심지어 시민사회도 그와 같은 주장을 해왔다. 해럴드 펠드(Harold Feld)가 2012년 2월 5일, WCIT에 대한 미 하원에 제출한 의견서를 보라. http://www.publicknowledge.org/harold-felds-wcit-hearing-testimony-feb-5-2013.

이끄는 것을 보게 된다. 예를 들어, OECD는 이와 관련하여 자신의 의도를 상당히 분명하게 드러내 왔는데, 최근의 문서에서는 다음과 같이 말하고 있다.

> 인터넷의 세계적 속성과 인터넷 중개자들이 종종 제공하는 초국경적 서비스를 고려할 때, 비즈니스 영역에 효과적인 지침을 제공하기 위해서는, 인터넷 중개자에 대한 정책을 포함한 정책 개발을 위한 접근이 국제적으로 수렴하는 것은 필수적인 것으로 보여진다. OECD는 그러한 원칙의 도출을 돕고, 그 확산을 지원할 수 있을 것으로 인식되었다.[242]

마찬가지로, 미국 정부는 현재 OECD의 또 다른 인터넷 정책 문서인 '인터넷 정책결정에 대한 2011년 성명'에 대한 지지를 확대하려고 노력하고 있다. 지적재산권 집행에 있어서 중개자들의 역할을 지나치게 강조한 것이 부분적으로 이유가 되어, OECD의 '시민사회 정보사회 자문 위원회'는 그것을 지지하는 것을 거부했지만, 이 성명은 환영할만한 많은 내용을 담고 있다. 그러나, 이와는 별개로, 그것이 세계적인 논의공간에서 만들어지지 않으면, 그러한 문서가 세계적으로 정당한 것이 되기는 힘들다. 따라서, 미국의 정책결정자들이 이와 같은 미국 주도의 기획을 통해 개발도상국을 열외로 취급하면서, 더 폭넓은 (정부가 참여하고 있는) ITU를 "인터넷 자유의 적"[243]으로 돌리는 것은 위선적이다.

이와 같이 좁은 기술 영역 바깥에서 우리가 발견하는 것은 폭넓은 멀티스테이크홀더 체제가 아니라, 강력한 정부와 기업들이 인터넷을 위한 자신들의 규칙을 만들고 그것들을 나머지 전 세계에 부과하려는 노력이다. 우리는 그것을 ACTA, SOPA, PIPA에서 보았고, TPP에서 진행되고 있는 것을 보고 있으며, ITU와 심지어 OECD에서도 (좋은 의도에도 불구하고) 위와 유사한 배제적인 정책결정의 가능성을 보고 있다. 이것이 인터넷 거버넌스 현황(status quo)의 맨얼굴이며, 이는 지속가능하지 않다.

인터넷 원칙의 필요성

여기 일석이조로 기존 인터넷 거버넌스 방식의 진화에 영향을 미칠 수 있는 실제 기회가 있다.

1. OECD와 같은 더 협소한 기구에서 이미 개발된 것과 같은, 세계적 인터넷 거버넌스를 위한 공유된 원칙의 개발에 있어 개발도상국에 더 동등한 대표권을 부여하는 것, 그래서 이러한 이슈들을 ITU가 장악하게 하려는 현재진행중인 전투에 대한 대안을 제시하는 것.

2. 공공 인터넷 옹호자, 감시자, 그리고 규범, 표준, 규약의 풀뿌리 개발의 참여자로서의 그들의 기존 역할을 대체하는 것이 아니라 보완하면서, 시민사회의 인터넷 권리와 자유 활동가들이 세계적 인터넷 정책 개발 과정에 참여할 수 있는 견고한 제도적인 기반을 제공하는 것.

동시에 우리는 인터넷 이용자의 권리와 자유를 옹호하는 만큼 이에 대한 침해를 쉽게 허

242) OECD, 공공정책 목표 진전을 위한 인터넷 중개자의 역할, (OECD publishing, 2011), p.194. http://dx.doi.org/10.1787/9789264115644-en

243) 연방통신위원회(FCC), 맥도웰(Robert M McDowell) 위원의 성명, 2013.2.5, http://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-McDowellR-20130205.pdf.

가할 수 있는 정부간 기구가 무방비적으로 확장되지 않기를 원한다.

민주적인 책임성 메커니즘은 세계적 수준에서 더 취약하기 때문에, 우리는 세계적 수준에서 인터넷의 구속력 있는 규칙의 개발을 촉진하는 것에 대해 매우 신중해야 한다. 최소한 멀티스테이크홀더 감독 메커니즘이 매우 강고하게 자리 잡을 때까지는 말이다. 이는 그것이 결코 정당화될 수 없다는 것이 아니다. 실제로 자칭 인터넷 자유 활동가들은 WIPO에서 시각장애인 용도로 만들어진 저작물의 국경을 넘어선 교환을 허락하는 내용의 새로운 세계적 조약을 현재 지지하고 있는 사람들이다. 그러나 그것은 시민사회가 주도적으로 제기했던 조약이다.

훨씬 더 종종, 세계적 거버넌스를 연성법(soft law) 혹은 원칙으로 제한하는 것은 더 안전한 방법이다. 왜냐하면 그것이 그러한 원칙들을 국가적 수준에서 구현하는데 있어 더 유연함을 제공하고, 너무 종종 법적인 논쟁으로 빠져드는 조약 문구의 경우보다 더 강한 문구가 합의될 수 있기 때문이다. 또한 정책결정자들은 연성법 기구를 구성할 때에 공익 대표들의 참여에 훨씬 더 열려진 경향을 보인다.

그러한 연성화 된 세계적 원칙들의 개발은 국내적 법률가, 인터넷 엔지니어, 그리고 마찬가지로 사업가들이 (그러한 정책에 의해 영향을 받을 수 있는 국경 밖의 사람들의 이해관계를 고려하면서) 정책을 개발하는데 있어 지침을 제공할 수 있다. 그것은 또한 국가들이 세계인권선언과 같은 세계적인 규범의 침해에 책임을 지도록 보장할 수 있다. 실제로 세계인권선언 자체가 연성법 체제로 시작되었다. 단지 1948년에 그것이 통과된 지 30년이 지나서야 그 조항들이 국제 협약(그리고 그것의 영향을 받은 다른 경성법이나 조약들)의 형태로 강제력을 갖게 되었다.

그렇다면, 필요한 것은 정부, 기업영역, 시민사회를 포함한 모든 이해당사자들이 인터넷 거버넌스를 위한, 인터넷 이용자의 권리와 자유를 옹호하는 방식으로 각각의 공공정책 관심사를 다룰 수 있는, 구속력 없는 원칙의 개발을 위해 협력할 수 있는 메커니즘이다.

이것은 매우 무리한 요구인 것처럼 보인다. 그리고 물론, 많은 경우에 그러한 과정의 결과물은 조약이 아닐 것이다. 그러나 사실 그것이 오히려 더 낫다. 특정한 이슈에 대한 세계적 원칙의 개발 시도가 실패했다는 것은 그 이슈가 국내 의회에서, 혹은 자유 시장에서, 혹은 기술적인 방법과 같은 더 낮은 수준에서 결정되기 위해 실현되지 못한 것임을 의미하는 것이기 때문이다. 이것이 어쨌든 사이버-자유주의자의 구미에는 더 맞을 것이다.

실제적인 예를 든다면, 미국에 기반한 사업체가 세계적인 이용자를 대상으로 한 웹사이트를 개발할 경우, 그 사업체 및 미국의 규제자 모두에게 지침이 될 수 있는, 온라인 프라이버시를 위한 세계적 기준 원칙이 있어야 할 것이다. 그리고 그 원칙들은 영향을 받는 인터넷 이용자, 사업자, 그리고 전 세계 정부들의 충분한 참여 속에서 개발되어야 할 것이다. 결국 합의가 만들어지지 않는다면, 우리는 국내 법률, 기술적인 표준, 자율 규제 등의 이러 저러한 조합을 통해서 그 문제를 다루기 위해 노력을 계속해야 할 것이다. 그러나 이는 아마도 이전보다는 다른 이해당사자들의 관점을 조금 더 잘 이해한 상태에서 이루어질 것이다.

어쨌든 세계적 표준의 개발은, 우리가 그것에 관여하든 하지 않든, 이미 이루어지고 있다. APEC은 초국경적인 프라이버시 표준과 관련된 많은 작업을 (시민사회의 별다른 참여 없이) 해왔다. OECD의 작업은 이미 언급한 바 있고, ITU도 비슷한 야심을 가지고 있다. ITU는 2013년 5월에 있을 세계전기통신정책포럼(WTPF)이 “토론을 활성화하고, 현재진행형의

세계적 ICT 정책들, 세계적인 규제 및 표준화 노력들을 이끌기 위해 공유된 비전을 분명히 보여주는, '의견서(Opinions)' 형태로 표현된 멀티스테이크홀더 합의를 형성하기 위해 계획되었다"고 설명한다.[244]

바쿠(Baku)에서 열린 지난 IGF 회의에서, 멀티스테이크홀더 자문그룹(MAG)은 다른 곳에서 개발한, 인터넷 거버넌스 원칙에 대한 기존의 많은 성명문들의 개요를 종합할 것을 요구받았다. 그러나 이것이 중요한 첫 단계임에도 불구하고, IGF가 그러한 원칙들의 실제적인 개발을 위한 더 포괄적인 포럼으로 활용될 수 있기는 커녕, MAG이 IGF로 하여금 이러한 과제를 맡도록 할 것인지도 명확하지 않다.

IGF의 지난 7년간의 기록을 보면 그럴 것 같지 않다. 이를 보면, 지난해에 미국정부가 180도 방향을 전환하여 인터넷 공공정책 개발을 위한 별도의 체제나 기구를 설립하기 보다는, IGF가 정부의 협력을 강화하기 위해 활용될 수 있다고 제안했을 때, 왜 개발도상국 정부들이 미국에게 해볼 테면 하라고 했는지 알 수 있다.

강화된 협력의 필요성

개발도상국은 그것을 받아들이지 않을 것이다. 그래서 지난 12월 - 사실 두바이에서 열리고 있었던 WCIT 회의와 같은 시간에 - 뉴욕에서 열린 UN 총회는 인터넷 거버넌스의 미래에 사실상 훨씬 더 중요한 결의안을 통과시켰는데, 대부분은 그것을 간과했다. 그 결의안은

> 모든 회원국과 모든 다른 이해당사자로부터의 의견을 구하고, 집약하고, 검토함으로써, 튀니스 어젠다에 포함된 강화된 협력에 관한 정보사회세계정상회의의 위임사항(mandate)을 검토하기 위하여 개발을 위한 과학기술 위원회(CSTD) 의장에게 강화된 협력에 대한 워킹그룹을 설립할 것을 요청한다.
>
> 강화된 협력 워킹그룹은 위원회의 다섯개 지역 그룹에 속한 정부, 그리고 다른 모든 이해당사자, 즉 기업영역, 시민사회, 기술 및 학술 커뮤니티, 정부간 기구, 국제기구에 속한 초청자들이 (이들은 개발도상국과 선진국에서 동등하게 선출되어야 한다) 균형적으로 대표될 수 있도록 보장할 것을 개발을 위한 과학기술 위원회 의장에게 요청한다.[245]

이 결의안은 난데없이 나온 것이 아니다. 사실 이것은 2005년, 정보사회세계정상회의 튀니스 어젠다의 최종 결과문서로부터 시작된 것이다. "관심이 필요한, 영역을 가로지르는(cross-cutting) 많은 국제적 공공정책 이슈들, 그러나 현재의 체제에 의해 적절하게 다루어지지 않고 있는 이슈들이 있다"는 출발점으로부터, 튀니스 어젠다는 이러한 이슈들을 다루기 위한 멀티-스테이크홀더 논의 포럼으로서 IGF의 설립을 요청했고, 이와 함께

> 가능한 빨리 진행되고 혁신에 호응하는, 모든 이해당사자를 포함한 강화된 협력을 향한 광범위한 과정(broader process)을 요구했다. [이것은] 정부가 인터넷과 관련된 국제 공공정책 이슈에 동등하게 자신의 역할과 책임을 수행할 수 있도록 한다. 그러

244) http://www.itu.int/en/wtpf-13/Pages/overivew.aspx 를 보라.
245) 총회 결의안 A/RES/67/195, 개발을 위한 정보통신기술, http://unctad.org/meetings/en/SessionalDocuments/ares67d195_en.pdf.

나 국제 공공정책 이슈에 영향을 주지 않는, 일상적인 기술적, 관리적 문제는 제외한다.[246]

또한 튀니스 어젠다는 다음과 같이 명시하고 있다.

이것은 투명하고, 민주적이며, 다자간 과정이어야 하며, 정부, 기업영역, 시민사회, 그리고 국제 조직이 각자의 역할 속에 참여해야 한다. 이 과정은 필요한 경우, 그래서 이와 관련된 노력들의 협력효과를 높이기 위해 현재 방식의 계속되는 활발한 진화에 박차를 가할 수 있는, 적절한 체제 혹은 장치의 설립을 구상할 수 있다.

따라서 이 원칙은 이 점에서 명확하다. 즉, IGF는 인터넷 공공정책이 토론되는 멀티스테이크홀더 포럼이라는 것 (그리고, 이 점은 잊혀지고 있지만, 필요할 경우 그 이슈들을 해결할 권고들을 도출할 수 있다는 것), 또한 모든 정부들이 "국제 인터넷 관련 공공정책 이슈에 대한 권리와 책임"을 좀 더 참여적인 방식으로 수행할 수 있도록 하는 광범위한 과정의 일부라는 것. 이를 촉진하는, 아마도 새로운 체제나 장치를 통해서.

비어있는 부분은 이 광범위한 과정이 어떻게 구현되어야 하는가이다. 정상회의에 자문을 했던 멀티-스테이크홀더 그룹이었던 인터넷거버넌스 워킹그룹(WGIG)은 4가지 선택지를 제출했다. 그 중 3가지는 세계적 인터넷 위원회의 변종들인데, 국가 이익이 영향을 받을 수 있는 정책 영역, 그러나 기존의 정부간 체제의 영역 밖에 있는 정책 이슈들을 중재한다. (미국의 논평가는 "인터넷에 대한 UN의 장악"이라고 비판했다.[247]) 이 선택지들은 그러한 기구가 UN에 연결된 것인지 아닌지, 다른 비정부 이해당사자들의 참여는 어떻게 할 것인지에 따라 차이가 있다.

그 이후 몇 년 동안, 놀랍게도 강화된 협력 위임사항을 제도화하기 위한 어떠한 새로운 제안도 진지하게 제기되지 않았고, 2011년에야 인터넷 관련 정책 위원회(CIRP)라고 불리는 인도 정부의 제안이 있었는데, 이는 브라질, 인도, 남아프리카공화국 등 IBSA 3자 그룹에 의해 같은 해에 제안된 초기 모델에 기반한 것이었다.

CIRP는 50개 멤버로 구성되는 정부간 기구이고, IGF와 상호보완적이며, 시민사회, 기업영역, 정부간 기구, 국제기구, 기술 및 학술 커뮤니티를 위한 자문 기구를 두었다. OECD의 정보통신정책위원회(ICCP)가 이와 비슷한 방식의 구조인데, ICCP는 지역적으로 덜 포괄적이다.

CIRP 역시 "UN이 인터넷을 장악하다"라는 주장 속에 폐기되었다.[248] 정부에 편향적인 내재적 구조의 문제 이상으로, 그 제안에는 심각한 문제가 있었음은 분명한 사실이다. 가장 큰 문제는 그것이 "영역을 넘나드는 인터넷 관련 세계적 이슈의 조정과 일관성을 보장"(이것은 필요하다)하는 것을 넘어, "세계적 표준 수립을 포함하여, 인터넷의 기술적, 운영적 기능을 책임지는 기구에 대한 조정과 감독"(이것은 그렇지 않다)까지 제안하고 있다는 것이다.

어쨌든 UN의 새로운 위임을 통해 강화된 협력 과정을 새롭게 검토할 워킹그룹이 만들어짐으로써, 우리는 공공 및 민간 이해당사자의 이해관계 사이에서 (기존의 두 제안이나 현상

246) 정보사회를 위한 튀니스 어젠다(2005), http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.
247) 레스너(llessner)를 보라, "UN이 인터넷을 장악하려고 한다", 2005.8.17,http://www.humanevents.com/2005/08/17/unpoised-to-take-over-the-internet/.
248) 키렌 맥카시(Kieren McCarthy), "인도가 정부의 인터넷 장악을 공식적으로 제안하다", 2011.10.27, http://news.dotnxt.com/2011/10/27/india-proposes-government-control-internet.

유지보다) 좀 더 나은 균형을 찾기 위해, 특히 그 과정의 주요 목표로서 인터넷 이용자의 권리와 자유의 보장을 포함하기 위해, WGIG과 CIRP 제안을 개선할 기회를 갖게 되었다.

민주주의의 필요성

그러한 제안을 발전시키기 위한 우리의 출발점은 세계적인 인터넷 거버넌스 과정을 보다 민주적으로 만드는 것이다. 원칙적으로, 민주주의는 매우 간단하다. : 그것은 단지 책임성 있고 투명한 과정을 요구한다. 그래서 어떤 결정에 의해 영향을 받는 사람들이 그러한 결정이 어떻게 내려지는 지에 대한 동등한 권리를 갖는 것이다. 그러한 결정은 또한 모두의 기본적 인권을 존중해야 한다.

실제로는 좀 더 복잡하다. 특히 세계적 공공정책 결정에 의해 영향을 받는 사람들이 균형적으로 대표되는 것이 비현실적인 세계적 수준에서는 더욱 그러하다. 그렇지만, 인터넷 거버넌스의 맥락에서는 멀티-스테이크홀더 모델이 세계적 체제의 민주화를 위한 가장 나은 접근법이라는 합의가 형성되고 있다. 이 모델은 정책 개발 과정에서, 그들의 특정한 역할, 능력, 이해에 따라 대략 그룹화된, 영향을 받는 모든 사람의 견해를 포괄하도록 하기 때문이다.

민주적인 관행과 문화로부터 나타나며, 강화된 협력 체제나 장치를 위한 어떤 제안을 계발하는 데에서도 마찬가지로 중요하게 이해해야 할 점은 민주적인 과정이 숙고적(deliberative)일 때 더 나은 결정에 도달할 수 있다는 것이다. 이것이 의미하는 바는 우리가 단지 자신의 선호를 표현하는 것에 그치지 않고, 그것을 권력 불균형이 가능한 한 제거된, 포괄적인 포럼에서 토론해야 한다는 것이다.

IETF와 같이 기술표준을 책임지고 있는 기존의 풀뿌리 인터넷 거버넌스 기구는 본보기로 삼을만한 좋은 모델을 제공한다. 물론 그들도 완전하지는 않지만 말이다. 예를 들어, IETF는 포괄성(inclusivity)에 문제가 있으며, 자신 스스로 다음과 같은 우려를 표한 바 있다.

> IETF는 누가 이해당사자인지 확실하지 않다. 결과적으로, 특정한 이해당사자 그룹이 다소 배제되어 왔는데 (그렇지 않았으면 과정에서 중요한 의견을 제시했을 수도 있었지만), 이들에게는 IETF가 그들의 의견에 대해 적절한 중요성을 부여하지 않는 것으로 보였기 때문이다.[249]

그래서, IETF, W3C(공개표준 원칙)[250]을 포함한 인터넷 표준 기구들의 최근의 시도는 지나치게 시장 중심적이며, 포괄성과 같은 더 넓은 공익 목적에 충분한 관심을 기울이지 않는다고 시민사회 내에서 비판받아 왔다. 여기서 이것을 언급하는 것은 IETF를 비판하고자 하는 것이 아니다. 단지 멀티-스테이크홀더 거버넌스가, 심지어 매우 찬양을 받는 인터넷 기술 커뮤니티 조직조차 완전하게 구현하지 못한 것이라는 점을 지적하고자 하는 것이다.

그래서 우리는 또한 인터넷 기술 커뮤니티 외부로부터의 멀티-스테이크홀더 거버넌스의 혁신에도 열려있어야 한다, 심지어 UN 시스템 내부로부터의 혁신들에도 그래야 한다. WGIG가 그러한 혁신이었음을 고려해보자 - 그것은 진정으로 멀티-스테이크홀더 그룹이었으며, 숙고적인 민주적 과정을 통해 정책 권고안을 발전시켰다. 이는 전형적인 UN 외교 회

249) IETF, "IETF의 문제점 성명서", 2004년 5월, http://www.apps.ietf.org/rtf/rfc3774.html.
250) http://open-stand.org/ 참조.

의와는 사뭇 달랐다. WGIG는 직접 만나기도 했을 뿐만 아니라, 메일링리스트나 위키를 통해 온라인으로 작업을 수행했다. 그리고 문안에 대해 합의할 수 없었을 때에도 - 대표적으로 ICANN의 미래에 대해서 - 대화의 단절이나 교묘한 말로 이루어진 타협적 선언에 이르지 않고, 추가적인 논의를 위한 재료로서 4가지 대안을 제시했다.

강화된 협력을 위한 균형 잡힌 멀티-스테이크홀더 체제 혹은 장치를 개발하기 위한 창의성을 발휘하는데 있어서, 우리는 하나의 제한 하에서 작업해야 함을 인정해야 한다. - 그것은 튀니스 어젠다의 다음과 같은 선언이다. "인터넷 관련 공공정책 이슈에 대한 정책 권한은 국가의 주권이다. 그들은 국제적인 인터넷 관련 공공정책 이슈에 대한 권리와 책임이 있다." 이것은 많은 인터넷 자유 활동가들이 수용하기 힘든 명제이다. 그러나 WSIS에 참여한 모든 정부 참여자들이 (그렇다, 심지어 미국조차도) 이에 동의했다. 심지어 그 이전에도, 사실 2000년 즈음에도 국가 도메인에 대한 효과적인 주권 선언을 통해 정부는 이러한 주장을 한 바 있다.[251]

궁극적으로 우리 중 많은 사람들은 세계적 거버넌스에서 국가가 지배적인 역할을 행사하는 것이 아니라, 개인들의 초국경적 네트워크가 자발적으로, 중복될 가능성이 있지만, 우리의 삶을 관장할 규칙과 원칙들에 대한 협상을 하는 그러한 세계를 보고 싶어 한다. 그러나 그러한 세계는 아직 실현될 것 같지 않다. 그리고 그동안 인터넷 거버넌스의 미래는 균형에 달려있다. 특히 우리가 시장, 기술, 규범과 같은 비국가적 거버넌스 체제(이는 위에서 설명한 것처럼 지지하기 힘들다)에 제한받고 싶지 않다면, 우리는 당분간 우리가 원하는 것보다는 (최소한 공식적으로는) 좀 더 폭넓은 정부의 역할을 수용할 수밖에 없다.

그러나 실제로 이러한 역할이 엄격하게 제한되고, 실질적인 측면에서 다른 이해당사자와 가능한 동등한 역할이 되도록 하는 것은 우리에게 달려있다. WGIG는 이러한 사례를 제공하고 있지만, 우리는 그것보다 훨씬 이전의 선례를 가지고 있다. - 예를 들어, 국제노동기구(ILO)는 1919년 설립 이후부터 시민사회와 산업계 대표들을 완전한 투표권을 가진 회원으로 포함하고 있다. 오르후스 협약(Aarhus Convention)은 정책 수립 과정에 일반 국민을 완전하고 동등한 이해당사자로 대우하는 정부간 기구의 또 다른 사례이다.[252]

구체적인 제안의 필요성

그래서 시민사회가 당면한 과제는 창조적으로 되는 것이다. 결국 튀니스 어젠다는 정부 사이의 합의였다. (시민사회는 WSIS 최종 문서를 반대하는 독자적인 성명을 발표했다.)[253] 그런 만큼 적어도 다른 이해당사자들은 문구의 유연한 해석을 주장할 수 있다. 세계적 인터넷 정책 개발을 위한 균형 잡힌 체제를 위해 제안될 수 있었고, 제안되어야만 하는 많은 선택지들이 있다. - 몇 가지만 언급한다면, 위키피디어 방식의 협력 프로젝트, 해적당 방식의 유연한 민주주의(liquid democracy), 혹은 기트허브(Github : 오픈소스 프로젝트 개발을 위한 협력 플랫폼)에 영감을 받은, 우수 사례(best practice) 문서의 응용 등. 최근에 시민사회가 제안한 강화된 협력 작업반(ECTF)은 IETF의 절차모델을 상당히 빌려온 것이다. - 그

251) ICANN 정부자문위원회(GAC), 국가도메인의 위임과 관리 원칙, 2000.2.23, http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm.

252) 공식적으로 정보접근에 대한 UNECE 협약, 정책 결정 과정에의 공공의 참여 및 환경 문제 정의(justice)에 대한 접근 (1998), http://www.unece.org/env/pp/treatytext.html.

253) "더 많은 것들이 달성될 수 있었다", 정보사회세계정상회의에 대한 시민사회 성명, 2005.12.18, http://www.itu.int/wsis/docs2/tunis/contributions/co13.pdf.

러면 왜 안되는가?[254]

내 견해를 말하자면, 내 연구(및 정부가 무엇을 수용할 것이고, 무엇을 수용하지 않을 것인지에 대한 경험)에 따라, 연합 혹은 합의 민주주의라고 불리는 조직 형식을 선호한다. 이것은 모든 이해당사자들이 숙고의 과정을 통해서 함께 정책 입장을 개발하는 구조이면서, 각 그룹에 서로 관심이 있는 제안에 대한 거부권을 효과적으로 부여함으로써, 궁극적으로 개별 이해당사자 그룹이 합의에 이를 것을 요구하는 구조이다. 내 생각에는 이것이 정부로 하여금 강화된 협력 과정에 참여할 수 있도록 요구하는 유일한 방법인데, 이렇게 하지 않으면 그들에게 다른 이해당사자 그룹보다 우월한 지위를 부여하게 되기 때문이다. 이 아이디어를 처음 발전시킨 문서 320쪽에서, 나는 다음과 같이 썼다.

> 인터넷 거버넌스를 위한 초국경적 네트워크의 적절한 구조는, 모든 이해당사자 그룹의 멤버들이 합의를 목적으로 심도있는 토론을 할 수 있는, 개방적이고 투명한 포럼으로 구성될 수 있다. 이는 각 그룹이 합의에 의해 혹은 민주적 수단으로 지명한 대표로 이루어진 능력있는 집행 위원회가 주도하며, 포럼의 모든 결정은 합의에 의해 승인될 필요가 있다.[255]

이와 같은 그룹은 기존 인터넷 거버넌스 기구들을 (대체하는 것이 아니라) 보완하는 역할을 하며, 편의상 IGF에 부속될 수 있다. 이것은 세계적 수준에서 공공정책 원칙의 개발을 위한 민주적이고, 멀티-스테이크홀더 과정이 없는 영역만을 담당한다. 이것은 규제자, 온라인 사업자, 그리고 정책을 일관성 있고 조정되는 방식으로 구현할 필요가 있는 다른 이해당사자들에게 지침을 제공하기 위하여, 그 정책의 영향을 받는 모든 사람들의 관점과 인권을 고려하는 원칙들에 대해 가능한 한 합의를 찾으려 노력한다. 그 권고의 실제 이행은 현재와 마찬가지로 전반적으로 분산화 된 방식으로 이루어질 것이며, 또한 각 개별 이해당사자 그룹에 의한, 그 그룹 자체가 동의한 어떠한 절차에 따른, 해당 권고안의 승인 여부에 의존할 것이다.

물론 이는 하나의 선택지일 뿐이다. 이건 그 나름의 단점이 있다. 요점은 이 특정한 제안을 다른 것들을 배제하면서 밀고자 하는 것이 아니라, 강화된 협력 위임사항을 진전시킬 수 있는 이와 같은 구체적인 제안에 대한 대화를 시작하는 것의 중요성을 강조하고자 하는 것이다. 우리의 머리를 모래 속에 박고, 그 위임사항이 없어지기를 바라는 것이 아니라.

올해 1월에 CSTD 의장은 강화된 협력 워킹그룹을 개시하기 위한 이미 수립된 절차의 개요를 서술했는데, 이는 어떤 식으로든 강화된 협력 위임사항이 인터넷 거버넌스 체제의 진화를 통해 어떻게 구체화될 것인지 결정하는데 도움이 될 것이다.[256] 다음 단계는 우리에게 달려있다. 우리는 세계적 인터넷 거버넌스 체제에서 공공 이익을 대표하기 위한 견고한 제도적 기반을 제공하기 위해 생산적으로 참여할 것인가, 혹은 자신의 입장을 고집하면서 그러한 체제가 1998년과 같은 형태로 영원히 고정될 것을 고집할 것인가?

우리의 결정이 무엇이든, 그것은 인터넷의 미래를 결정할 것이다. 우리는 시민사회가 세계적 거버넌스 체제와 장치의 중대한 변화를 옹호할 수 있는 힘을 과소평가해서는 안된다.

---

254) http://enhanced-cooperation.org/RFA/1.html 참조. 나는 이 제안서의 감사인사 부분에서 언급되었다.
255) 제레미 말콤, 멀티-스테이크홀더 거버넌스와 인터넷 거버넌스 포럼 (Terminus Press, 2008), p.320.
256) http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=391&Sitemap_x0020_Taxonomy=Commission%20on%20Science%20and%20Technology%20for%20Development 참조.

예를 들어, 지뢰 금지 조약은 시민사회의 노력이 없었다면 존재하지 않았을 것이며[257], 장애인 협약[258] 역시 마찬가지다. 인터넷 거버넌스의 좀 더 특수한 맥락에서, 우리는 브라질의 국가 수준에서 마르코 시빌(인터넷에서의 시민권리 옹호를 위해 국회에 제안된 법안)의 통과를 위해 싸웠던 이들의 노력을 본받아야 한다. 그들이 궁극적으로 성공하지 못했지만 말이다.[259]

우리가 SOPA, PIPA, ACTA에 반대하는 투쟁을 확대한 것과 같이, 네트워킹, 로비, 홍보, 연구, 역량 강화를 통해서 이 제안들을 촉진하기 위해 많은 노력과 비용이 필요할 것이다. 이러한 옹호 활동의 대상은, 인터넷 거버넌스 체제의 진화를 자연스럽게 의심하고 “인터넷을 장악"하려 한다는 소문을 무비판적으로 수용하려 하는 광범한 인터넷 이용자 커뮤니티뿐만 아니라, CSTD 워킹그룹, IGF MAG, 국내 정부, 산업계 그룹, 인터넷 기술 커뮤니티를 포함할 것이다.

결론

국가 시대에 인터넷 권리와 자유를 보장하기 위한 전투는 쉬운 일은 아니다. 그러나 우리는 모든 방면에서 반드시 이를 수행해야 한다. 우리 자신을 부정적이고, 대응적인 접근으로 제한하는 것은 지속가능하지 않다. 그렇지 않으면 우리는 증가하는 위협의 공세를 영원히 방어하는데 우리의 제한된 시간과 자원을 소진하고 말 것이며, 그러한 위협을 야기하는, 기저에 있는 이해관계에 대해서는 정면으로 다룰 수 없게 될 것이다. 그것보다는 우리는 이와 같은 이해관계를 장기적으로 진전시킬 수 있는 적극적인 제안의 필요성을 인식할 필요가 있다. 그리고 이러한 제안은 국가적 수준에서만큼, 세계적 수준에서도 발전되어야 한다.

국가들이 ITU에 눈을 돌리기보다는 이해당사자들이 참여할 수 있는 멀티-스테이크홀더 인터넷 거버넌스 기구의 포괄적인 네트워크가 이미 존재한다는 주장은 거짓이다. 그리고 인터넷 거버넌스 체제의 자연스러운 진화를 더 이상 억제하지 않도록 그것이 폭로될 필요가 있다. 기술 영역 밖에서는 아직 멀티-스테이크홀더 과정이 없는데, 이해당사자들에게 멀티-스테이크홀더 과정을 통해서 관심 있는 정책 이슈들을 다루라고 요구하는 것은 정말 터무니없는 일이다. 특히 개발도상국은 이에 속아 넘어가지 않을 것이며, 인터넷 거버넌스 과정에서 자신들의 이해가 반영되어야 한다는 요구가 충족되지 않는다고 이러한 요구가 그냥 없어지지는 않을 것이다.

기술표준과 인터넷 자원의 할당 영역의 기존의 멀티-스테이크홀더 기구의 업무에 영향을 주지 않으면서도, 그 영역 밖에서 모든 정부들과 다른 이해당사자들의 이해가 균형을 이룰 수 있는 더 세계적으로 포괄적이고 민주적인 체제 혹은 장치를 발전시키기 위한 충분한 여지가 있고, 매우 긴급한 필요가 있다.

기존의 인터넷 거버넌스 체제의 진화적인 확장은, 그것이 충분히 숙고적이고 투명하다면, 억압과 통제에 기반한 정부의 제안들을 드러내고 제거할 것이다. 왜냐하면 이것들은 멀티-

257) 공식적으로, 인명살상용 지뢰의 이용, 비축, 생산, 이전의 금지 및 파괴에 대한 협약(1997). 1992년에 6개 NGO에 의해 시작된 세계적 네트워크인 지뢰 금지 국제 캠페인은 이 조약을 이끈 노력을 인정받아 노벨평화상을 수상하였다. http://www.icbl.org/ 참조.

258) 유사하게도, 장애인 권리 협약(2006)은 전 해의 5개 국제 장애인 NGO의 요청에 따라 2001년 총회에서 시작되었다.

259) http://culturadigital.br/marcocivil/ 참조.

스테이크홀더의 관문을 결코 통과하지 못할 것이기 때문이다. 비록 동시에, 그 권한이 그것들의 구현이나 집행이 아니라 원칙의 개발에 제한될지라도 말이다. 이것은 또한 미래에 ACTA나 TPP와 같은 새로운 배제적인 과정의 출현을 사전에 예방하는데 도움이 될 것이다. 그렇지 못하더라도, 이것은 최소한 (배제적인 과정들의) 권위를 약화시키고, 보다 쉽게 그것들을 물리칠 수 있는 무기가 될 것이다.

"인터넷 자유" 문화적 전통이 이런 필수 업무를 담보하기에는 적절하지 않다. 규제가 없는 상황에서 상향식의 규범 정립은 인터넷 커뮤니티의 중요하고 계속되는 전통이지만, 그러한 규범이 국가의 법이나 산업 관행에 적절하게 반영되기 위해서는, 이러한 규범 정립에 공식적으로 정당성을 부여할 수 있는 정치적인 과정의 일정한 형식이 때때로 요구된다. 어쨌든 자유뿐만 아니라 권리는 인터넷 이용자에게 중요하고, 어떤 지점에서는 이러한 권리들을 법률입안자, 산업 및 기술 커뮤니티에 지침이 될 수 있는 공공 정책 원칙들로 발전시킬 수 있는 민주적인 과정이 필요하다.

현상유지가 지속가능하다는 잘못된 가정 하에 인터넷 거버넌스 체제의 진화를 위한 제안을 거부하거나 무시하면서 우리가 이것에 눈감고 있는 한, 우리는 ITU가 세계적으로 적용 가능 한 인터넷 공공정책 원칙들을 권위를 가지고 개발할 수 있는 유일한 세계적 기구가 될 수 있는 위험에 놓일 수 있다.

그 대신에, 우리는 ITU보다 더 나은, 진정으로 멀티-스테이크홀더 대안을 설계하는데 협력할 수 있다. 이는 권력을 가진 사람들과 그렇지 못한 사람들의 이해관계가 균형을 이룰 수 있는 숙고적이고 민주적인 포럼에서, 모든 이해당사자들이 중요한 공공정책 이슈들에 자신의 관점을 제시하고, 인터넷 이용자의 권리와 자유를 옹호할 수 있는, 더 사려깊고, 정당하며, 포괄적인 권고들을 생산할 수 있도록 할 것이다.

이를 위한 견본은 없다. 그것은 IGF의 기존 MAG을 강화하는 것, 이전 섹션에서 대략 그려본 바와 같이 합의 민주주의에 기반한 새로운 부속 기구의 개발, 혹은 누구나 아직 생각하지 못했던 또 다른 새로운 체제나 장치를 포함할 수 있다. 나는 우리가 무엇을 내놓을 수 있을지 기대하고 있다. 당신도 참여하겠는가?

Internet freedom in a world of states

Jeremy Malcolm[260)]

Abstract

Last year's ITU WCIT conference inflamed the community's fears of the extension of intergovernmental control over the Internet. Whilst this fear was legitimate, an overemphasis on the ITU can obscure the fact that the Internet is already controlled in undemocratic ways – often by governments, through both national and global processes, but also by corporate interests. It also obscures the fact that government action is sometimes necessary to uphold the rights of Internet users, just as government inaction can sometimes support their freedoms.

This is no less true at the global level than at the national level, although the appropriate mechanisms of governance at each level differ. Specifically, there are some areas in which developing globally-applicable principles for the governance of the Internet could be valuable and important. Despite popular belief, there is no network of global multi-stakeholder processes or institutions that covers all of the important public policy areas in which such global principles could be useful. However, with the convening of a new CSTD Working Group on Enhanced Cooperation, we now have the opportunity to fill that gap.

To date, civil society has been very reluctant to participate in the development of such a positive agenda for the evolution of Internet governance arrangements. But if we do not, either the status quo will prevail or less democratic and multi-stakeholder alternatives (such as the ITU) will come to the fore. This paper suggests one possible format for operationalising the enhanced cooperation mandate from WSIS, but its principal message is that regardless of the format adopted, now is the time for civil society to seriously consider the merits of a more formal institutional platform for the protection of the rights and freedoms of Internet users.

260) Senior Policy Officer, Consumers International

Introduction

In the wake of last year's defeat of the controversial ACTA treaty in Europe and of the SOPA and PIPA bills in the United States, both of which called on intermediaries to police consumers' use of the Internet, digital rights activists in the West have naturally gained a heightened sensitivity to their governments intruding on Internet freedoms.

One indication of this was how aggressively they opposed all Internet-related proposals at the World Conference on International Telecommunications (WCIT) of the International Telecommunications Union (ITU) last December. The fear was that although many of those proposals seemed modest, they were the vanguard of a movement from governments to more broadly address Internet governance issues such as online freedom of expression, security and privacy through purely intergovernmental processes, rather than through existing, more open and inclusive, multi-stakeholder mechanisms.

There are three assumptions that seem to underlie this fear:

1. Governments should not be involved in Internet governance.
2. If governments are involved in Internet governance, it should only be at the national level, not at the global level.
3. If governments are involved in Internet governance at the global level, there are existing, bottom-up multi-stakeholder mechanisms through which they can address all their concerns, instead of resorting to the ITU.

However, all three assumptions are wrong. To fail to comprehend this is to misunderstand the forces that drive many governments towards the use of intergovernmental mechanisms to set policies for the Internet, and to overlook the opportunity that we have right now to channel these forces in a way that is more responsive to the concerns of ordinary Internet users. In fact, if all three assumptions are disproved, it follows that finding a more acceptable way for governments to participate in global Internet governance is imperative. So let's examine those assumptions in turn.

The need for governments at the national level

The first assumption, that governments don't have a legitimate role in governance of the Internet, seems so far-fetched that I might be accused of raising a straw-man argument – yet it is a serious school of thought called cyber-libertarianism, and flows almost as an axiom from the framing of advocacy for online rights and freedoms (particularly by activists from the United States) as

the “Internet freedom” movement. Moreover this cyber-libertarian framing is not reserved to those who are otherwise politically libertarian. Even politically progressive activists are inclined to be more distrustful of governmental intervention online than offline, in an expression of Internet exceptionalism, which holds that the Internet is different, and deserving of a more hands-off regulatory approach.[261)]

To accept the cyber-libertarian proposition is to deny any role for government intervention at the national level, in areas that many of us actively support, such as:

- Passing network neutrality rules that would prevent network operators from discriminating against particular types of Internet content or services.
- Providing incentives for the migration to the next generation version of the Internet protocol, IPv6 – a task at which the forces of markets and norms have so far manifestly failed.[262)]
- Setting enforceable standards for the protection of consumers' personal data, that go further than the weak voluntary codes of practice adopted by segments of industry.
- Extending universal service policies so that consumers in rural areas are guaranteed a basic level of Internet service, enabling them to participate in the information society on an equal footing with their city-dwelling peers.

In 1993 or even 2003 we might have given the market the benefit of the doubt and held off from regulating in these areas. But in 2013, it seems increasingly implausible that the legitimate interests of all consumers in having affordable access to the open Internet, whilst maintaining their own privacy, can be secured without targetted government intervention of some sort or other.

This is not to deny that government intervention also very often has deleterious effects on Internet users; for example through punitive intellectual property enforcement measures that limit fair use and innovation, through secretive surveillance of our online communications, through the production of malware for use in cyber-war, or through banning the use of particular Internet services such as Internet telephony or VoIP.

---

261) A classic debate between the cyber-libertarian and Internet exceptionalist viewpoint on the one hand, and a conservative “unexceptionalism” is found in Jack L. Goldsmith, Against Cyberanarchy L. 65 U. Chi. L. Rev. 1199 (1998) and David Post's response “Against 'Against Cyberanarchy',” 17 Berkeley Tech. L.J. 1365 (2002). Tim Wu joined Goldstein in updating his argument in Who Controls the Internet? Illusions of a Borderless World (Oxford University Press, 1996).

262) The “Father of the Internet”, Vint Cerf, is one of those who has supported the use of government incentives to promote IPv6 migration: Jennifer Scott, “Cerf calls on Government incentive for IPv6 migration” 11 November 2010, http://www.itpro.co.uk/628531/cerf-calls-on-government-incentive-for-ipv6-migration.

But excluding governments from regulating the Internet is the wrong answer, not least because industry also often acts against the rights and freedoms of Internet users. Websites collect and sell our most private details to advertisers without our knowledge or consent, copyright owners and ISPs enter into closed-door pacts to throttle the Internet access of users suspected of sharing files, and financial intermediaries collude to choke off funds from Wikileaks. We are entitled to look to

our governments to protect us against misbehaving corporations through domestic consumer law, competition law or privacy and data protection law, or through less intrusive measures such as tax incentives, development grants or co-regulatory codes.

In some of these cases though (such as the Wikileaks example), governments and corporations are complicit in the infringement of our rights and freedoms. So what recourse do we have if neither our own governments nor the market can protect us against infringements of our rights online? In such cases we either have to look to another mechanism of governance – such as norms, or technology (more on these shortly) – or we have to look to the global level.

The need for governments at the global level

This brings us to the next assumption, which is that if governments do sometimes need to involve themselves in Internet governance, it should only ever be at the national level. That can't be true, because the decisions that governments make at the national level (for which most of us would accept the need in certain cases) have an invariable tendency to spill outside the country's borders.

This occurs because the Internet itself is borderless, and so policies made in one country, whether by governments or by private actors, can affect users anywhere in the world, over whom the policymaker has no legitimate claim of authority. For example, in 2011 United States authorities seized the domain names rojedirecta.com and rojedirecta.org claiming authority to do so under US law, although the domains were owned by a Spanish company and had been ruled legal under Spanish law (the domains were later returned).[263] Similarly, when content is taken down under authority of the US Digital Millennium Copyright Act (DMCA), it affects users throughout the world. Why shouldn't those users have any say in

263) Nate Anderson, "Government admits defeat, gives back seized Rojadirecta domains", 30 August 2012, http://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/.

that?

If they should, then we turn to the question of how they should have this say. As alluded to above, the cyber-libertarian is inclined to limit it to the use of technology or norms. As an example of the former, technologically knowledgeable users can use strong encryption software, such as PGP and Tor, to craft online spaces and communications channels that are largely unregulatable. But many of the same features of Internet technologies that make them open and free, also limit their effectiveness as shields against government or corporate abuses. Technology is even less effective in promoting positive rights, such as providing cross-border remedies for online fraud.

Similarly norms can be useful, but they are not self-enforcing. We can to some extent rely on the power of the crowd to enforce Internet norms; this is what was so effective in defeating ACTA, SOPA and PIPA last year. This is important where democratic processes at the national level are weak or corrupt, but is even more vital at the global level, where the democratic deficits of traditional intergovernmental institutions (such as the ITU) and trade negotiations (such as ACTA and the Trans-Pacific Partnership or TPP) are relied upon by governments to facilitate the "policy laundering" of domestically unpopular proposals.

But that crowd can also become a mob, in which the nuances of policy debates are swept away in a heady fervour of cyber-libertarian banner waving. For example the hacktivist group Anonymous has done much good work in upholding online rights and freedoms in the face of threats from governments, cults and corporations alike. But it was also criticised by civil society participants at WCIT for attacking the ITU's website and thereby jeopardising the only official channel for remote users to participate in that meeting. Therefore, whilst direct action through grassroots groups such as Anonymous is valuable as a last resort, it should never become our primary means to shape Internet policy. As security specialist and author Bruce Schneier recently wrote:

> The masses can occasionally organize around a specific issue – SOPA/PIPA, the Arab Spring, and so on – and can block some actions by the powerful. But it doesn't last. The unorganized go back to being unorganized, and powerful interests take back the reins.[264)]

To be organised at the global level, in a way that is effective to curb the rights abuses of governments and corporations, implies sitting at the table with them to manage the cross-border implications of Internet-related public policies.

---

264) Bruce Schneier, "Power and the Internet", 31 January 2013,

http://www.schneier.com/blog/archives/2013/01/power_and_the_i.html?nc=35.

Currently, this means sitting on the sidelines of the secret negotiations at the TPP, or in the back row of the auditorium at WIPO (the World Intellectual Property Organisation). And that's if we're lucky. On other issues, it means we have no say at all because there is no global forum dealing with these issues.

The need for institutional evolution

So we should at least consider whether a more formally institutionalised means of engagement of online activists in Internet policy discussions at the global might bridge the gap that exists after selfregulatory, technology-based and grassroots-led initiatives have failed. For some issue areas, this may be seldom; for example, we already have strong global mechanisms for the participation of all stakeholders in Internet standards development, and in the allocation of IP addresses and domain names, through institutions such as the IETF, the W3C and ICANN.

But in other areas, such as security and cybercrime, intellectual property enforcement, consumer protection, data protection and privacy, and online freedom of expression, we do need to look at the evolution of current institutional arrangements. This moves us to the third assumption highlighted above, to the effect that there is no need for any reform to Internet governance arrangements, since “the current organizations, systems and processes successfully meeting the needs of its stakeholders via its industry-led, bottom-up, consensus-based processes.”[265] If only that were true.

There are global discussions of these issues, of course – but they are either too weak to have a tangible impact on actual policy outcomes (this is the case of the Internet Governance Forum or IGF), or they do not offer the opportunity for meaningful participation from all affected stakeholders (a much longer list, including the ITU itself, as well as the OECD, APEC, WIPO, the CSTD and the TPP).

Often it is civil society that is excluded from these existing arrangements – as was the case with ACTA, and now the TPP – but in other cases it is the governments from developing countries, who see developed-country groupings such as the G8 and OECD taking the lead, whilst their own interests are sidelined. The OECD, for example, has been quite explicit about its intentions in this regard, stating in a recent paper:

Given the global nature of the Internet and the cross-border services that

265) That particular formulation of this view comes from a Cisco submission to the ITU available at http://www.itu.int/md/S12-WTPF13PREP-C-0014/en, but even civil society has made much the same claim, see eg. Harold Feld's submission to the US House of Representatives hearing on WCIT of 5 February 2012, available at http://www.publicknowledge.org/harold-felds-wcit-hearing-testimony-feb-5-2013.

Internet intermediaries often provide, an international convergence of approaches for the development of policies involving Internet intermediaries was viewed as essential, to provide effective guidance to the business sector. The OECD was identified as being able to help the emergence of such principles and to support their diffusion.[266]

Similarly, the United States government is currently seeking to broaden support for another Internet principles document of the OECD, the 2011 Communiqué on Internet Policy-making. There is much to welcome in this Communiqué, though in the end the OECD's Civil Society Information Society Advisory Committee declined to support it partly due to a perceived over-emphasis on the role of intermediaries in intellectual property enforcement. But even aside from this, such an instrument cannot be globally legitimate unless it is developed in a global forum. Therefore it is hypocritical for US policy-makers to label developing countries sidelined by US-driven initiatives such as these, and turning to the more inclusive (of governments) ITU, as "Internet freedom's foes".[267]

Thus outside of narrow technical areas, what we find is that far from being an inclusive multistakeholder regime, powerful governments and companies are making their own rules for the Internet and then seeking to impose them on the rest of the world. We saw it with ACTA, SOPA and PIPA, we see it in progress at the TPP, and we see the potential for similar exclusionary rulemaking at the ITU and even, despite all good intentions, at the OECD. This is the true face of the status quo of Internet governance, and it is unsustainable.

The need for Internet principles

There is a real opportunity here to influence the evolution of existing Internet governance arrangements in a way that would kill two birds with one stone:

1. To provide developing countries with more equitable representation in the development of shared principles for global Internet governance, such as those already being developed by narrower bodies such as the OECD, and thereby to provide an alternative in what will otherwise be an ongoing battle to have these issues taken up at the ITU.

2. To provide a firm institutional foundation for the participation of Internet rights and freedom activists from civil society in global Internet policy development

266) OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, (OECD Publishing, 2011), p.194. http://dx.doi.org/10.1787/9789264115644-en

267) Statement of Commissioner Robert M McDowell, Federal Communications Commissioner, 5 February 2013, http://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-McDowellR-20130205.pdf.

processes, supplementing rather than supplanting their existing roles as public interest advocates, watchdogs, and participants in the grassroots development of norms, standards and code.

At the same time we want to guard against the unguarded expansion of intergovernmental authority that could as easily sanction the violation of Internet users' rights and freedoms, as uphold them.

Because the mechanisms of democratic accountability are much weaker at the global level, we must be very cautious about encouraging the development of binding rules for the Internet at the global level, at least until very robust mechanisms of multi-stakeholder oversight are in place. This is not to say that it will never be justified – indeed, self-professed Internet freedom activists are amongst those now supporting a new global treaty at WIPO, that would allow copyright works that have been adapted for the use of the blind to be exchanged across borders. But that is a treaty that civil society was instrumental in initiating.

Much more often, limiting global governance to soft law, or principles, is the safer bet, as it provides more flexibility in the implementation of such principles at the national level, and much stronger text can be agreed than in the case of treaty text, which too often descends into legalistic wrangling. Policy-makers also tend to be far more open to the participation of public interest representatives in the development of soft law instruments.

The development of such soft global principles can provide guidance for national lawmakers, Internet engineers and businesses alike in developing policies that take into account the interests of those outside their borders who are likely to be affected by those policies. It can also ensure that countries are held to account for infringements of global norms, such the Universal Declaration of Human Rights. Indeed, the Universal Declaration itself began as a soft law instrument; only 30 years after its passage in 1948 did its provisions become binding in the form of the International Covenants (and other hard laws and treaties that it influenced).

What is needed, then, is a mechanism by which all stakeholders, including governments, the private sector and civil society, can collaborate on the development of non-binding principles for Internet governance that address their respective public policy concerns in a way that also upholds the rights and freedoms of Internet users.

It sounds like a pretty tall order – and of course, in many cases, the outcome of such a process will not be agreement. But, in fact, that is all the better – a failed attempt at developing global principles on a particular issue means that the issue will fall through for determination at a lower level, such as in national

parliaments, or by the free market, or through technological means – which are more palatable to the cyber-libertarian anyway.

To give a practical example, if United States-based businesses are developing websites targetted to a global audience, it makes sense that there should be global baseline principles for online privacy that both those companies, and US regulators, can be guided by, and that those principles should be developed with the full participation of affected Internet users and businesses and their governments from around the world. If, in the end, a consensus cannot be reached, then we will continue to muddle through by handling the issue through a patchwork of national laws, technical standards and self-regulation – but perhaps with a little more insight into the perspectives of the other stakeholders than we had before.

In any case, the development of global standards it is already happening, with or without us. APEC has done a lot of work on cross-border privacy standards (without much civil society involvement), the OECD's work has already been noted, and the ITU has similar ambitions; it describes its upcoming May 2013 World Telecommunication Policy Forum (WTPF) as being "designed to foster debate, [and] build multi-stakeholder consensus expressed in the form of 'Opinions' illustrating a shared vision to guide ongoing global ICT policies, regulatory and standardization efforts worldwide."[268]

At the last meeting of the IGF in Baku, the Forum's Multistakeholder Advisory Group (MAG) was urged to put together a compendium of the many existing statements of Internet governance principles that others had developed. But although this is an important first step, it is unclear whether its MAG will allow the IGF to take this mandate up, let alone to allow the IGF to be used as a more inclusive forum for the actual development of such principles.

The record of the IGF's last seven years suggests not – which is why developing countries called the United States government's bluff when it finally about-faced last year and suggested that the IGF could be used to strengthen government collaboration in Internet public policy development, rather than establishing a separate framework or mechanism for this process.

The need for enhanced cooperation

Developing countries would have none of it, and so last December – in fact at the same time as the WCIT meeting was taking place in Dubai – the UN General Assembly in New York passed a resolution that was actually much more significant for the future of Internet governance, although it was overlooked by most. The

268) See http://www.itu.int/en/wtpf-13/Pages/overview.aspx.

resolution

> *Invites* the Chair of the Commission on Science and Technology for Development to establish a working group on enhanced cooperation to examine the mandate of the World Summit on the Information Society regarding enhanced cooperation as contained in the Tunis Agenda, through seeking, compiling and reviewing inputs from all Member States and all other stakeholders... [and]
>
> *Requests* the Chair of the Commission on Science and Technology for Development to ensure that the working group on enhanced cooperation has balanced representation between Governments from the five regional groups of the Commission, and invitees from all other stakeholders, namely, the private sector, civil society, technical and academic communities, and intergovernmental and international organizations, drawn equally from developing and developed countries;[269]

This resolution didn't come out of the blue; in fact, it has been in train since 2005, in the final output document of the World Summit on the Information Society (WSIS), the Tunis Agenda. From the starting point "that there are many cross-cutting international public policy issues that require attention and are not adequately addressed by the current mechanisms", the Tunis Agenda called for creation of the IGF as a multi-stakeholder discussion forum to address these issues, together with a broader

> process towards enhanced cooperation involving all stakeholders, proceeding as quickly as possible and responsive to innovation … [which would] enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.[270]

The Tunis Agenda also specifies that this is to be a

> transparent, democratic, and multilateral process, with the participation of governments, private sector, civil society and international organizations, in their respective roles. This process could envisage creation of a suitable framework or mechanisms, where justified, thus spurring the ongoing and active evolution of the current arrangements in order to synergize the efforts in this regard.

The principle, then, is clear enough - that the IGF should be a

---

269) General Assembly Resolution A/RES/67/195 , Information and communications technologies for development , http://unctad.org/meetings/en/SessionalDocuments/ares67d195_en.pdf.

270) Tunis Agenda for the Information Society (2005), http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

multi-stakeholder forum where Internet public policy issues can be discussed (and – though this part of its mandate has been forgotten – where recommendations to address those issues can be developed where appropriate), as part of a broader process that will also allow governments to carry out their "rights and responsibilities for international Internet-related public policy issues" in a more participatory way, perhaps through a new framework or mechanism that would facilitate this.

What remains lacking is the detail of how this broader process should be implemented. The Working Group on Internet Governance (WGIG), which was a multi-stakeholder group that advised the World Summit, produced a set of four options; three of which had some variant of a global Internet council, which would intercede in policy areas where national interests were impacted, but which fell outside the scope of existing intergovernmental arrangements (and were railed as a "UN takeover of the Internet" by US commentators[271]). There was variation between these options on whether such a body would be UN-linked or not, and how other non-governmental stakeholders would participate in it.

In the years since then, surprisingly no new options to institutionalise the enhanced cooperation mandate have been seriously put forward, other than a 2011 proposal by the Indian government called the Committee on Internet Related Policies (CIRP), which built upon an earlier model put forward that same year by the IBSA trilateral grouping of Brazil, India and South Africa.

The CIRP would have been a 50-member governmental body, complementary to the IGF, with advisory bodies for civil society, the private sector, inter-governmental and international organisations, and the technical and academic community. The OECD's Information & Communications Policy Committee (ICCP) is structured along very similar lines, but is less geographically inclusive.

The CIRP too was shot down amidst claims of a "UN takeover of the Internet".[272] There were, true enough, significant problems with it, beyond its inherent structural bias towards governments. The biggest of these was that it proposed to go further than "ensuring coordination and coherence in cross-cutting Internet-related global issues" (which is needed), to also "coordinate and oversee the bodies responsible for technical and operational functioning of the Internet, including global standards setting" (which is not).

In any case, with the new UN mandate for a working group to consider the

271) See Ilessner, "UN poised to take over the Internet", 17 August 2005, http://www.humanevents.com/2005/08/17/unpoised-to-take-over-the-internet/.

272) Kieren McCarthy, "India formally proposes government takeover of Internet", 27 October 2011, http://news.dotnxt.com/2011/10/27/india-proposes-government-control-internet.

enhanced cooperation process afresh, we have the opportunity to improve upon the WGIG and CIRP proposals in order to strike a better balance between the interests of public and private stakeholders than either those proposals or the status quo, and in particular to enshrine the protection of Internet users' rights and freedoms as the primary objective of the process.

The need for democracy

Our starting point in developing such a proposal should be to make global Internet governance processes more democratic. In principle, democracy is very straight-forward: it simply requires an accountable and transparent process by which those who will be affected by a decision have an equal say in how that decision is made, provided that the decision also respects the fundamental human rights of all.

In practice, it becomes more complex, particularly at the global level where the proportional representation of those impacted by global public policy decisions is impractical. Even so, a consensus has emerged that in the context of Internet governance, the multi-stakeholder model is the best approach to the democratisation of global institutions, in that it promotes the inclusion of all affected viewpoints in the policy development process, roughly grouped according to their typical roles, competencies and interests in that process.

Another insight that has emerged from democratic practice and literature, and of equal importance in the development of any proposal for an enhanced cooperation framework or mechanism, is that better decisions are reached when democratic processes are deliberative. What this means is that we should not merely express preferences, but debate them, in an inclusive forum where power imbalances are, as far as possible, taken out of the equation.

The existing grassroots Internet governance institutions responsible for technical standards, such as the IETF, offer a good model to emulate – though they are certainly not perfect. The IETF, for example, has problems with inclusivity, and has expressed its own concerns that

> The IETF is unsure who its stakeholders are. Consequently, certain groups of stakeholder, who could otherwise provide important input to the process, have been more or less sidelined because it has seemed to these stakeholders that the organization does not give due weight to their input.[273]

Thus, a recent initiative of Internet standards bodies including the IETF and

273) IETF, "IETF Problem Statement", May 2004, http://www.apps.ietf.org/rfc/rfc3774.html.

W3C (the OpenStand Principles)[274] has been criticised within civil society as being too market-focused, and paying insufficient attention to broader public interest objectives such as inclusion. To mention this here is not to criticise the IETF, but simply to point out that multi-stakeholder governance is not something that even the much-lauded Internet technical community organisations have yet perfected.

We should therefore also be open to innovations in multi-stakeholder governance from outside the Internet technical community, and – yes – even those from within the UN system. Consider that WGIG was such an innovation – it was a truly multi-stakeholder group, that developed a set of policy recommendations through a deliberative democratic process, quite unlike the stereotypical United Nations diplomatic conference. WGIG not only met in person, but also conducted its work online through mailing lists and a wiki, and when text could not be agreed – notably on the future of ICANN – this did not result in the collapse of the discussions, or in a compromise declaration full of weasel words; rather, four alternatives were given as food for further consideration.

Admittedly, in our creativity to develop a balanced multi-stakeholder framework or mechanism for enhanced cooperation we are working under one limitation – the Tunis Agenda's pronouncement that "[p]olicy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues." This is a proposition that it will be difficult for many Internet freedom activists to accept. Yet all governments participating at WSIS (yes, even the United States) agreed to this. Even before that, in fact as early as 2000 with their effective declaration of sovereignty over country-code domain names, governments had thrown down the gauntlet in this regard.[275]

Ultimately, many of us would all like to see a world in which the nation state does not exercise a dominant role in global governance, but in which transnational networks of individuals, voluntarily entered into and potentially overlapping, negotiate the rules and principles under which we live. But that world has not yet come to pass, and in the meantime the future of Internet goverance hangs in the balance. Essentially, unless we are happy to be confined to the use of non-state mechanisms of governance such as markets, technology and norms – which as explained above is untenable – then we have no choice for the time being but to accept a role for states that is (at least in formal terms) broader than we might wish.

It is incumbent upon us however to ensure that in practice, this role is strictly

274) See http://open-stand.org/.

275) Governmental Advisory Committee, ICANN, Principles for Delegation and Administration of ccTLDs, 23 February 2000, http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm.

circumscribed, and in practical terms is as near as possible to an equal role with that of the other stakeholders. WGIG provides an example of this, but we have precedent much further back than that – the International Labour Organisation (ILO), for instance, which incorporated civil society and industry representatives as full voting members since its inception in 1919. The Aarhus Convention is another example of an intergovernmental instrument that treats the public as a full and equal stakeholder in policy development processes.[276]

The need for a concrete proposal

So the challenge for civil society is to be creative. The Tunis Agenda, after all, was an agreement between governments only (civil society wrote its own, dissenting WSIS outcome document),[277] and as such the other stakeholders can, at the very least, advocate for a flexible interpretation of its language. There are many options that we could, and should, be putting forward for a balanced framework for global Internet policy development – a Wikipedia-style collaborative project, a Pirate Party style liquid democracy, or Github-inspired set of "forks" of best practice documents, just to name a few. A recent civil society proposal, the Enhanced Cooperation Task Force or ECTF, borrows heavily from the processes of the IETF – and why not?[278]

For my part, my research (and my experience of what governments will and won't accept) leads me towards an organisation style called the consociation, or consensus democracy. This is a structure in which all stakeholders develop policy positions together in a deliberative process, yet ultimately are also required to come to a consensus as individual stakeholder groups, effectively giving each group

a right of veto over proposals of mutual concern. This, as I perceive it, is the only way in which governments might be induced to participate in an enhanced cooperation process that did not otherwise accord them a dominant position over the other stakeholder groups. 320 pages into my original development on this idea, I wrote that:

> an appropriate structure for a transnational network for Internet governance could consist of an open and transparent forum within which members of all stakeholder groups deliberate with the aim of reaching consensus, led by a meritocratic executive council to which each group appoints its representatives

276) Formally, the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (1998), http://www.unece.org/env/pp/treatytext.html.
277) "Much more could have been achieved" Civil Society Statement on the World Summit on the Information Society, 18 December 2005, http://www.itu.int/wsis/docs2/tunis/contributions/co13.pdf.
278) See http://enhanced-cooperation.org/RFA/1.html. Disclosure: I am credited in the acknowledgments section of this proposal.

using consensual or democratic means, and which would be required to ratify all decisions of the forum by consensus.[279]

Such a group could act as a complement to (not as a replacement for) the existing Internet governance institutions, and might conveniently be attached to the IGF. It would address only those areas that in which there is not already a democratic, multi-stakeholder process for developing public policy principles at the global level. It would seek to reach a consensus on such principles where possible, to provide guidance to regulators, online businesses and other stakeholders who have a need to implement policies in a coherent and coordinated way, that takes account of the

perspectives and human rights of all those who will be affected by those policies. The actual implementation of its recommendations would largely continue to be decentralised as it is at present, and would also depend on upon the ratification of those recommendations by each individual stakeholder group according to whatever procedures that group itself had agreed.

This is just one option, of course, and it may have its faults. The point is not to push this particular proposal to the exclusion of others, but rather to underline the critical importance of beginning a conversation on such concrete proposals that could take the enhanced cooperation mandate forward, rather than digging our heads into the sand and wishing that mandate away.

In January this year the Chair of the CSTD outlined the process that is already in train to convene a Working Group on Enhanced Cooperation, that will help to determine, one way or another, how the enhanced cooperation mandate will be expressed through the evolution of Internet governance arrangements.[280] The next steps are up to us. Will we participate productively to provide a firmer institutional foundation for the representation of the public interest in global Internet governance

arrangements, or will we dig in our heels and insist that those arrangements remain forever stuck in the same mould as in 1998?

Whatever our decision is, it may determine the future of the Internet. We should not underestimate the power that civil society can have to advocate for significant changes to global governance frameworks and mechanisms. The Mine Ban Treaty, for example, would not exist but for the efforts of civil society,[281] and

---

279) Jeremy Malcolm, Multi-stakeholder Governance and the Internet Governance Forum (Terminus Press, 2008), p.320.

280) See http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=391&Sitemap_x0020_Taxonomy=Commission%20on%20Science%20and%20Technology%20for%20Development.

281) Formally, the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of

neither would the Disability Convention.[282] In the more specific context of Internet governance, we should emulate the efforts of those who fought for the passage of the Marco Civil at the national level in Brazil, even though they ultimately did not succeed.[283]

Just as much effort and expenditure may be needed to promote these proposals through networking, lobbying, outreach, research and capacity building as we expended fighting against SOPA, PIPA and ACTA. Targets for this advocacy work will include the CSTD Working Group, the IGF MAG, national governments, industry groups and the Internet technical community, as well as the broad community of Internet users who will be naturally suspicious about the evolution of Internet governance arrangements, and may be inclined to uncritically accept rumours of a "takeover of the Internet".

Conclusion

The battle to secure Internet rights and freedoms in a world of states is a hard one, but it is imperative that we undertake it on all fronts. Limiting ourselves to a negative, reactive approach is not sustainable – otherwise we will be forever fending off an increasing volley of threats, exhausting our limited time and resources, while the underlying interests that produce these threats are not being squarely addressed. Rather, we need to recognise the need for positive proposals that can advance these interests for the long term, and these proposals should be advanced at the global level just as much as at the national level.

Claims that there already is a comprehensive network of multi-stakeholder Internet governance institutions that stakeholders can join, rather than – for states – having recourse to the ITU, is a lie, and one that must be exposed as such so that it can no longer constrain the natural evolution of Internet goverance arrangements. It is indeed absurd to ask stakeholders to address policy issues of concern through multi-stakeholder processes, when those processes – outside of the technical – do not yet exist. Developing countries, in particular, will not fall for this, and the unmet need for the representation of their interests in Internet governance processes will not simply go away.

There is not only enough room, but indeed an urgent need, for the development

---

Anti-Personnel Mines and on their Destruction (1997). The International Campaign to Ban Landmines (ICBL), a global network initiated by six NGOs in 1992, was awarded the Nobel Peace Prize in recognition of its efforts to bring about the treaty: see http://www.icbl.org/.

282) Similarly, development of the Convention on the Rights of Persons with Disabilities (2006) was initiated by the General Assembly in 2001 following a call the previous year from the five international disability NGOs.

283) See http://culturadigital.br/marcocivil/.

of a more globally inclusive and democratic framework or mechanism to balance the interests of all governments and other stakeholders, outside of the realm of technical standards and Internet resource allocation and without impinging upon the work of existing multi-stakeholder bodies in those areas.

This evolutionary extension to existing Internet governance arrangements will, if it is sufficiently deliberative and transparent, expose and eliminate proposals from states that are based upon repression and control, since these would never pass muster in a multi-stakeholder environment – though at the same time, its authority should be limited to the development of principles, rather than their implementation or enforcement. It may also help preclude the emergence of new exclusionary processes such as ACTA and the TPP in the future, and even if it doesn't, it will at least drain them of their claimed legitimacy and arm us to defeat them more easily.

The “Internet freedom” meme is not adequate to encapsulate this imperative, and whilst bottom-up norm-setting in the absence of regulation is an important and continuing tradition of the Internet community, some form of political process to render this norm-setting formally legitimate is sometimes required in order to make sure that those norms are reflected as appropriate in national laws and industry practices. After all, rights as well as freedoms are important to Internet users, and at some point, democratic processes have to be allowed to develop these rights into public policy principles for the guidance of lawmakers, industry and technical community alike.

For as long as we remain blind to this, rejecting or ignoring proposals for the evolution of Internet governance arrangements on the false assumption that the status quo is sustainable, we risk assuring the ITU's future as the only global body capable of authoritatively developing globally-applicable public policy principles for the Internet.

Alternatively, we can collaborate on the design of a better, truly multi-stakeholder alternative to the ITU, that would allow all stakeholders to contribute their perspectives on important public policy issues in a deliberatively democratic forum that would balance the interests of the powerful with those of the powerless, and produce more thoughtful, just and inclusive recommendations that uphold the rights and freedoms of Internet users.

There is no template for this; it might involve the enhancement of the IGF's existing MAG, the development of a new adjunct body based on consensus democracy as I briefly sketched in the last section, or perhaps some other framework or mechanism that nobody has even thought of yet. I'm looking forwared to seeing what we can come up with. Are you in?

인터넷 거버넌스 :
멀티스테이크홀더 과정에서 시민사회와의 협력 강화

"인터넷은 그 누구의 소유물이 아니며 모든 사람들이 이용할 수 있고 모든 사람들이 발전시킬 수 있다. 그것은 인터넷 거버넌스에 있어서도 마찬가지이다."[284]

필자 조이 리디코트 (Joy Liddicoat)[285]
번역 신훈민[286]

도입

2013년이 끝나가는 시점에서, 2012년에 있었던 WCIT의 강도 높은 논쟁은 오랜 전 일처럼 느껴진다. 그러나 ITU에 인터넷 관련 콘텐츠 규제 권한이 주어질 수 있다는 우려 때문에 시민사회가 국제통신규칙(ITR)에 대한 정확하고 엄격한 범위를 포함하는 세계적 인터넷 공공 정책의 조정을 강력히 요구한지 1년도 채 되지 않았다.[287] 2013년에 많은 이슈가 대두되었는데, 이중 일부는 새롭고(예를 들어, 개인의 인터넷 사용과 통신 기술에 대한 대규모의 감시) 일부는 오래된(예를 들어, 튀니지 어젠다에 나온 강화된 협력의 의미) 것이다. 그 결과 정부와 다른 이해당사자들을 압박하여 인터넷 거버넌스에 대한 새로운 대화의 장으로 이끌었다. 이 글은 2005년 튀니스 어젠다 이후의 발전에 대해 간략하게 서술하고, 현재의 맥락을 조명해보며, 시민사회가 다양한 이해당사자 프로세스에서 동등하게 참여할 수 있는 방안을 검토하고자 한다. 이 글은 인터넷 거버넌스에 대한 APC의 경험을 크게 다루었고, UN '강화된 협력 워킹그룹'에 제출한 APC의 2013년 의견서를 광범하게 인용하였다.[288]

---

284) 안리에트 에스터휴센(Anriette Esterhuysen), 진보통신연합 APC 사무총장, "CSTD 강화된 협력 워킹그룹의 설문에 대한 APC의 답변"에서, 2013.9.10, p 11.
285) 진보통신연합 APC의 인터넷권리와 인권 프로젝트 코디네이터, http://rights.apc.org , joy@apc.org
286) 변호사, 진보네트워크센터 상근활동가, snunecro@gmail.com
287) 발레리아 베타코트(Valeria Betancourt), 국제전기통신 개정에 대한 APC의 견해 (2012.11.3): https://www.apc.org/en/news/apc-perspectives-revision-international-telecommun
288) 필자는 워킹그룹 멤버로 지명된 5명의 시민사회 참여자 중 한명이다.

배경

2005년에는 세계적, 지역적, 국가적 차원에서 인터넷 관리에 관여하는 정부가 거의 없었다. 인터넷이 중요하고 정부가 역할을 해야 한다는데는 대부분 동의하였으나, 많은 사람들이 기존의 '인터넷 거버넌스 체제'에 불만족스러워 했다. 그러나 어떻게 문제를 해결할 것인가에 대해 그들은 합의를 이룰 수 없었다. 불만의 핵심은 ICANN과 IANA와 같은 몇몇 인터넷 거버넌스 기구가 충분히 국제화되어 있지 않다는 것인데, 그 기구들이 미국 내에 위치해있었고, 어떤 측면에서는 미국 정부의 책임 하에 있었기 때문이다. 한편으로는 인터넷 관리가 널리 분산되고 분권화되어 있음에도 불구하고, 인터넷 관리 내부의 권력과 이에 대한 영향력은 선진국(global north)에 집중되어 있었다. 또한 어떤 정부는 기존 국제 정부간 시스템에는 공공 정책 이슈를 논의하거나 해결하기 위한 명확한 공간이 없다고 생각했다.

인터넷은 2005년 이래로 많은 발전을 했음에도 불구하고, 이런 긴장과 우려가 여전히 남아 있는 것이 현실이다. 인터넷거버넌스포럼(IGF)은 인터넷 정책 토론을 위한 과정으로서 설립되었고, 더 '성과지향적'이어야 할 임무가 있다.[289] 오늘날 점차 더 많은 수의 국가들이 자체적인 국가 IGF나 IGF와 유사한 프로세스를 거쳐 국가적 수준에서 인터넷 정책 이슈를 다루고 있다. 이러한 것들 중 일부는 아시아 태평양 지역의 IGF와 같은 지역 IGF 프로세스와 연결되어 있다. 국제 IGF에 대응하여 발전한 이러한 국가적, 지역적인 IGF 프로세스는 인터넷 정책 형성-토론 과정에서의 '강화된 협력'의 명확한 사례이다. 또한 ITU, 유네스코, UNCTAD와 기타 여러 유엔 기구들도 인터넷 관련 정책 과제를 다루고 있다. 이에는 자신의 권한 내에서 인터넷 관련 인권 과제를 가장 다룰 것 같지 않은 기구 중 하나인 인권이사회가 놀랍게도 포함되어 있다. 유럽연합 집행위원회와 아프리카 연합 위원회 등과 같은 지역 정부간 기구 또한 그들의 권한 내에서 광범한 인터넷 정책 과제를 다루고 있다.

이와 같이 분산되고, 아직은 국제적으로 연결되지 않은 프로세스와 기구들에, 시민사회 역시 참여하고 있다. 시민사회의 개인이나 단체 그리고 네트워크들은 자신들의 역할을 수행하고 인권을 준수하는 인터넷 관련 공공 정책을 위한 건설적인 의제를 제시하기 위해 이러한 다양한 공간에 걸친 복잡한 네트워크 전략에 관여하고 있다. 2013년이 끝나가는 만큼, 어떻게 시민사회가 계속해서 이 긴장된 상황을 헤쳐 나갈 수 있는지와 어떻게 현재 WGEC에서 논의되고 있는 '강화된 협력'에 대한 새로운 논의에 적극적인 의제를 진전시킬 수 있을지에 대해 돌이켜 보는 것이 중요하다.

'강화된 협력'이란 무엇인가?

강화된 협력(EC)이 무엇을 의미하는지에 대해서는 인터넷거버넌스에 참여하는 다양한 이해당사자들만큼이나 다양한 관점이 존재한다. 어떤 이들은 '강화된 협력'을 오직 정부와 관련된 것으로 보는 반면, 다른 이들은 시민사회, 기술 커뮤니티, 민간부문, 학계를 포함한 모든 이해당사자들의 협력과 관련된 것으로 주장한다. APC는 긍정적인 의미의 '협력'이 중요한 초점이며, "협력을 강화하거나 향상시키는 것에 대한 논의를 정부의 역할에 한정하는 것

289) Arising from ECOSOC via the United Nations Commission on Science and Technology for Development's Working Group on IGF improvements (2012).

은 (더 발전된 논의를 할 수 있는) 기회를 잃어버리는 것"[290]이라고 생각한다. 또한 베스트 비트 연합[291]도 튀니스 어젠다와 관련하여 '강화된 협력'의 범위는 "공공정책 과제에 대해 전 세계적으로 적용되는 원칙의 개발을 포함하여야" 하고, "필요하다면, 적절한 체제나 메커니즘의 형성을 그려볼 수 있"지만, "국제 공공정책 과제에 영향을 주지 않는, 일상적인 기술 및 운영 문제에" 정부의 개입을 예정해서는 안 된다고 주장하였다.[292] 핵심적인 과제는 강화된 협력과 그 안에서 시민사회의 역할에 대한 이해와 합의를 확대하는 것이다.

시민사회 - 우리의 역할은 무엇인가?

시민사회에 기업 및 정부와 동등한 권력 및 영향력을 부여하고, 소수가 아니라 모든 이해당사자들 사이의 평등과 형평성을 보장하기 위해 시민사회의 참여에 각별한 관심이 필요하다. 튀니스 어젠다 제35 (c)항은 시민사회는 "특히 커뮤니티 수준에서, 인터넷 문제에 대해 중요한 역할을 수행한다"고 규정하고 있다. 하지만 이러한 정의는 명백하게 적절하지 않으며 UN의 다른 맥락에서 이용되는 정의와도 일관되지 않는다. 시민사회의 다양성을 온전히 아우르는 합의된 정의를 발전시키기 위해 더 많은 노력이 필요하다.[293]

2003년 12월 제네바에서 열렸던 제1차 WSIS의 마무리에서 나온 시민사회 선언문은 다음과 같이 명시하고 있다. : "공정한 정보사회의 완전한 실현을 위해서는 개념, 구현, 운영 측면에서 시민사회의 완전한 참여가 필요하다."[294]

APC는 시민 사회가 아래와 같은 역할을 담당한다고 본다.[295]

> 소외되고 불리한 조건에 처해있는 그룹의 이익을 보호하고 인터넷 정책 문제에 권리와 개발의 관점을 포함하도록 하는데 있어서 핵심적 역할을 수행한다. 이러한 역할은 특히 정부와 비지니스 권력에 대한 균형추의 하나로서 특히 중요하다. 즉, 시민사회는 정부와 기업의 활동이 책임성과 투명성을 갖도록 지원하고 비판적으로 분석하며 적극적으로 문제제기할 수 있다.

일반적으로 우리는 인터넷 거버넌스에서 이해당사자들의 책임과 역할은 고정된 것이 아니라는 것을 워킹그룹이 인식해야 한다고 주장한다. 그것들은 문제가 되는 이슈, 과정, 혹은 업무에 따라 달라질 것이다.

IGF 2013

이해당사자들 사이의 힘의 불균형으로 인한 긴장을 감안할 때, 2013년 IGF에서 시민사회

290) Above n 1, p 1.
291) 베스트 비트는 시민사회 단체의 연합체이며, CSTD WG 설문에 답변을 제출했다. APC는 이 답변에 연명하였으며, 이 답변은 http://bestbits.net/ec/ 를 참조하라.
292) 69-71절 참조. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html
293) 예를 들어, 반기문 UN 사무총장의 다보스 세계경제포럼에서의 2009년 성명을 보라. "우리 시대는 리더십에 대한 새로운 정의, 즉 세계적 리더십을 요구하고 있습니다. 우리 시대는 국제협력의 새로운 형태를 요구합니다. 그것은 집합적인 세계적 선을 위해 정부, 시민사회, 기업 영역이 함께 일하는 것입니다."
294) http://www.itu.int/wsis/docs/geneva/civil-society-declaration.pdf
295) Above n 1, p 3.

가 거의 2:1의 비율로 이해당사자 참가자들의 최대 그룹이었던 점은 우연이 아니다.[296] 8차 정기 IGF가 인도네시아 발리에서 “브리지 구축 - 성장과 지속가능한 개발을 위한 멀티-스테이크홀더 협력 증진”이라는 주제로 열렸다. 협력과 개발에 대한 강조는, 인터넷에서의 신뢰 회복과 그것을 어떻게 통치할 것인지가 중요해진 시점에, 공개적이고 비판적인 토론의 기회를 촉진하고 형성하기 위한 것이었다.

인권, 인터넷 거버넌스 원칙, 멀티-스테이크홀더 협력을 위한 원칙에 대한 집중 세션이 포함된 것 또한 고무적이었다. 많은 참가자들이 비공식적인 자리에서, 2005년 이후 IGF 논의가 상당히 성숙해졌다는 의견을 표했다. 2005년 당시에는, 예를 들어, 인권은 어려운 주제였고, 많은 이해관계자들, 특히 정부와 기업 부문은 그것을 공개적으로 토론하고 싶어하지 않았다. 이와 같은 대화의 성숙은 인터넷에서의 인권의 중요성을 확인하는 것이고, 세계적, 지역적, 국가적 인터넷 공공 정책 수립 과정에서 책임성과 투명성 강화에 대한 실질적인 토론을 위한 기회이기도 하다. 또한 IGF와 같은 정책 형성 공간에 인권 문제를 제기해야 할 시민사회의 역할을 확인하는 것이다.

매우 중요한 현재의 인권 문제는 다음과 같은 것을 포함한다. :

- 여성의 권리와 인터넷 거버넌스
- 인터넷 거버넌스 원칙
- 멀티-스테이크홀더 협력의 원칙
- 접근성 및 다양성
- 프라이버시, 보안, 표현과 결사의 자유

게다가 미국 NSA가 자행한 광범한 대량감시와 데이터 수집에 대한 폭로는 인터넷 커뮤니티를 흔들어 놓았고, 스스로를 “인터넷 자유” 운동의 리더라고 칭했던 정부와 기업 행위자의 정당성을 손상시켰다. 이에 대응하면서 어떤 국가들은, 어떻게 보면 기회주의적으로, ICT 정책 과정에 대한 더 많은 정부간 (기구에 의한) 감독 및 통제를 다시 촉구했다.

의사 표현의 자유 유엔 특별 보고관인 프랭크 라 뤼를 포함한 인권 전문가들은 기존의 인권과 법적 체제가 인터넷에서의 프라이버시권을 보호한다는 것을 강조함으로써 대응하였다. 인권, 통신감시 법률, 정책과 기술 분야의 국제 전문가들에 의해 발전되고, 200여개가 넘는 시민사회 그룹의 지지를 받았으며, 유엔 특별보고관 프랭크 라 뤼의 문서와 완전히 일치하는, ‘통신 감시에서 인권 적용에 대한 국제원칙’[297]은 국제인권의무의 맥락에서, 통신감시 기술 및 기법을 고려하여, 온라인 환경에서 국제인권법이 어떻게 적용될 수 있는지 설명하고 있다.

이런 충격적인 폭로에 대한 가장 긍정적이고 도전적인 결과물은 시민사회가 포함된 IGF에서 구축될 수 있고 구축되어야만 한다. APC는 “IGF는 인터넷 모임들이 울분을 토하고, 서로를 마주할 수 있는 공간(물론 이것이 우리가 멀티-스테이크홀더 공간에서 함께 온 이유

296) 돈 홀랜더가 2013.10.15일 필자에게 보낸 이메일에 따르면, “(중복을 포함하여) 카테고리별 추정치 : 시민사회 - 629, 정부 - 319, 국제기구 - 111, 미디어 - 43, 기업 부문 -260, 기술 - 196”

297) www.necessaryandproportionate.org 참조

이지 않겠는가?)이며, 과정으로서의 인터넷 거버넌스의 신뢰를 회복하기 위해 앞으로 나아갈 방향을 확인하는 공간이며 기관, 행위자, 분석가, 활동가들로 구성된 생태계이다. 현 상태에 안주할 선택권은 없다." 라고 지적했다.[298]

또한, 시민사회가 사회의 가장 취약한 계층을 포함하여 가장 다양한 범위의 그룹을 대표한다는 것을 인식하는 참여 방식을 보장하기 위한 시민사회의 역할을 중요하게 바라볼 필요가 있다. 따라서 시민사회, 특히 개발도상국(global south)의 시민사회에 국제적, 지역적, 국가적 수준에서 더 많은 발언권과 영향력이 주어질 필요가 있다. 정부는 세계적 인터넷 관련 회의에 시민사회의 대표를 공식 대표단에 지속적으로 초대하고, 그들이 이러한 행사의 의제에 따라 정책적 입장의 개발에 참여할 수 있도록 함으로써, 시민사회와의 협력 강화를 위한 실질적인 대책을 강구해야 한다.

결론

시민사회는 인터넷 거버넌스 과정에서 다른 이해당사자들과 동등한 지위와 참여를 보장받기 위한 복잡한 도전에 직면하고 있다. 만약 시민사회와 다른 이해당사자들 사이에서의 힘의 불균형이 해결되고, 인터넷 거버넌스 회의의 문이 모두에게 열린다면, 이런 환경에서 협력적 전략이 발전되어지고 필요해질 것이다. 다양한 시민사회 그룹으로부터, 특히 자신만의 공유한 경제, 문화, 사회적 맥락을 지난 아시아 지역의 시민사회 그룹의 강력한 리더십이 필요하다.

298) "8차 IGF에서의 APC의 우선순위"
https://www.apc.org/en/pubs/priorities-eighth-internet-governance-forum-igf-ba

Internet Governance: Enhancing cooperation with civil society in multi-stakeholder processes

"The internet belongs to no one, everyone can use it, and everyone can improve it. That also applies to its governance."[299]

Joy Liddicoat[300]

Introduction

As 2013 draws to an end, the intensity and debate of the WCIT in 2012 seems long ago. Yet it has been less than a year since concerns that the ITU might be given responsibility for internet related content regulation resulted in strong civil society calls for coordination of global internet public policy including precise and tight scoping of the International Telecommunications Regulations.[301] In 2013, many issues have emerged, some new (such as mass surveillance of individuals' internet and other communications technologies), some old (such as the meaning of enhanced cooperation in the Tunis Agenda). The result is a convergence of compelling forces pushing governments and other stakeholders into new conversations about Internet governance. This article briefly outlines developments since the Tunis Agenda in 2005, focuses on current context and considers opportunities for civil society to be an equal participant in multi-stakeholder processes. This article draws heavily on APC's experience in internet governance, and cites extensively from APC's 2013 submission to the United Nations' Working Group on Enhanced Cooperation.[302]

---

299) Anriette Esterhuysen, Executive Director, Association for Progressive Communications in "Response from the Association for Progressive Communications to the CSTD Working Group on Enhanced Cooperation Questionnaire", 10 September 2013, at p 11.

300) Association for Progressive Communications, http://rights.apc.org

301) Valeria Betancourt, APC Perspectives on the Revision of the International Telecommunications Regulations (3 Nov 2012): https://www.apc.org/en/news/apc-perspectives-revision-international-telecommun

302) The author is a member of the Working Group, appointed as one of five civil society participants.

Background

In 2005 few governments had any involvement in the management of the internet at global, regional or national level. While most agreed that the internet was important, and that governments should have a role, many were not satisfied with existing 'internet governance arrangements.' However, they could not reach consensus on how to proceed. Dissatisfaction centred on the fact that some internet governance bodies like ICANN and IANA were not fully internationalised, being located in the United States and, in some respects, accountable to the US government. While on the one hand internet management was widely distributed and decentralised, power within and influence over this management was concentrated in the 'global north'. Some governments also felt there were public policy issues without a clear place for discussion or resolution within the existing international inter-governmental system.

While the internet has evolved a lot since 2005, the reality is that these tensions and concerns remain. The Internet Governance Forum (IGF) was established as a process for internet policy dialogue and has a mandate to be more outcome-oriented.[303] Today an increasing number of countries address internet policy issues at national level including through their own national IGF or IGF-like processes. Some of these are linked to regional IGF processes, including the Asia Pacific Regional IGF. These national and regional IGF processes developed in response to the global IGF and are a clear example of increased cooperation in internet policy shaping and dialogue. The ITU, UNESCO, UNCTAD and many other United Nations bodies also now address internet-related policy issues. This includes the Human Rights Council which has been, perhaps surprisingly, one of the last UN bodies to consider internet related human rights issues within its mandate. Regional inter-governmental bodies such as the European Commission and the African Union Commission also now address a wide range of internet policy issues within their mandates.

It is amongst this distributed yet interconnected set of processes and bodies that civil society also participates. Civil society individuals, organisations and networks are engaging in complex networking strategies across these multiple spaces in order to fulfil their roles and take forward constructive agendas for human rights compliant internet related public policy. As 2013 draws to a close it is important to reflect on how civil society can continue to navigate these tensions and take forward a positive agenda into the new discussions on enhanced

303) Arising from ECOSOC via the United Nations Commission on Science and Technology for Development's Working Group on IGF improvements (2012).

cooperation which is currently under discussion with the WGEC.

What is “enhanced cooperation”?

There are almost as many views about what “Enhanced cooperation”(EC) implies as there are stakeholders involved in internet governance. Some consider EC relates only to governments, others that it relates to cooperation among all stakeholders, including civil society, the technical community, the private sector, and academia. APC considers one key focus must be on “cooperation” as a positive term and that “limiting the discussion of enhancing, or improving cooperation, to the role of governments would be a lost opportunity.”[304] The Best Bits coalition has also noted,[305] in relation to the Tunis Agenda, that the scope of EC “should include the development of globally-applicable principles on public policy issues” and “also could envisage creation of a suitable framework or mechanisms, where justified”, but does not envision the involvement of governments “in the day-to-day technical and operational matters, that do not impact on international public policy issues.”[306] A key challenge is to increase the shared understandings and agreement about enhanced cooperation and the role of civil society within it.

Civil Society - what is our role?

A particular concern is for CS participation to be strengthened in order to bring its power and influence in line with that of business and government and ensure equality and equity among all stakeholders, rather than a few. The Tunis Agenda para 35 (c) describes CS has having “...played an important role on internet matters, especially at the community level”. This definition is plainly inadequate and is not consistent with definitions used in other UN contexts. More work is needed to developed shared definitions that encompass the full diversity of CS.[307]

As stated in the CS Declaration at the conclusion of the first phase of the WSIS in Geneva in December 2003: “The full realisation of a just information society requires the full participation of CS in its conception, implementation, and operation”.[308]

---

304) Above n 1, p 1.

305) Best Bits is a coalition of CS organisations that submitted a response to the CSTD WG questionnaire. APC has endorsed this response which is available at http://bestbits.net/ec/

306) See paras 69-71 http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

307) See for example, Secretary General Ban Ki-moon's 2009 statement at the World Economic Forum in Davos: "Our times demand a new definition of leadership - global leadership. They demand a new constellation of international cooperation - governments, CS and the private sector, working together for a collective global good."

308) http://www.itu.int/wsis/docs/geneva/civil-society-declaration.pdf

APC considers that civil society has:[309)]

> … a key role to protect the interests of marginalised and disadvantaged groups, and to incorporate rights and development approaches into internet policy matters. This role is especially important as one of the counterweights to the power of government and business; CS can support, critically analyse, and positively challenge the accountability and transparency of government and business actions.

In general we urge the WG to recognise that the roles and responsibilities of stakeholders in internet governance cannot be fixed. They will vary depending on the issue, process or task at hand.

IGF 2013

Given the tensions over power imbalances between stakeholders perhaps it is no coincidence that civil society was the largest group of stakeholder participants represented at the IGF in 2013 by almost 2:1.[310)] The eighth annual IGF took place Bali, Indonesia, with the theme was "Building Bridges - Enhancing Multi-stakeholder Cooperation for Growth and Sustainable Development." The emphasis on cooperation and development was encouraging, creating the opportunity for open and critical debate at a time when restoring trust in the internet, and how it is governed, is crucial.

The inclusion of focus sessions on human rights, internet governance principles, and principles for multi-stakeholder cooperation was also encouraging. Many participants reflected informally that the IGF dialogue has matured considerably since 2005, when human rights, for example, was a difficult topic and many stakeholders, especially government and the private sector, did not wish to discuss it openly. This maturing of dialogue affirms the importance of human rights on the internet and is an opportunity for substantive discussion about strengthening accountability and transparency in global, regional and national internet public policy making. It also affirms the role of civil society in bringing forward human rights into policy shaping spaces such as the IGF.

Some of the current human rights issues of critical importance include:

- Women's rights and internet governance

309) Above n 1, p 3.

310) Don Hollander "estimated count (including duplicates) by category: Civil Society – 629; Government – 319; IGO – 111; Media – 43; Private Sector – 260; Technical – 196" by email 15 October 2013 to author)

- Internet governance principles
- Principles of multi-stakeholder cooperation
- Access and diversity
- Privacy, security and freedom of expression and association.

In addition, revelations about mass surveillance and data collection by the US National Security Agency (NSA) have shaken the internet community and undermined the legitimacy of actors from government and business who had positioned themselves as leaders of the "internet freedom" movement. In response, some states have, opportunistically to some degree, renewed calls for more intergovernmental oversight and control of ICT policies processes.

Experts in human rights, including UN Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue, have responded by emphasising that existing human rights and legal frameworks protect the right to privacy on the internet. Developed by international experts in human rights, communications surveillance law, policy and technology, endorsed by over 200 civil society groups and fully consistent with work of UN Special Rapporteur Frank La Rue, the 'International principles on the application of human rights to communications surveillance'[311] explain how international human rights law applies in the online environment, in light of communications surveillance technologies and techniques in the context of international human rights obligations.

The most positive – and challenging – outcomes of these disturbing revelations can and must be built on by civil society including at the IGF. As APC has noted "The IGF is a space where the internet community can let off steam, confront one another (surely that is why we come together in multi-stakeholder spaces?), and identify how to move forward to restore trust in internet governance as a process, and an ecosystem made up of institutions, actors, analysts and activists. Complacency is not an option."[312]

There is also a need to look critically at the role of CS society ensure that modalities of participation also recognise that CS represents the most diverse range of groups, including the least powerful sectors of society. CS, particularly from the global South, therefore needs to be given greater voice and influence at global, regional and national level. Governments should take practical steps towards enhanced cooperation with CS by consistently inviting CS representatives onto official delegations at global internet related conferences, and involving them in

311) See more at www.necessaryandproportionate.org
312) "APC Priorities at the 8th Internet Governance Forum"
https://www.apc.org/en/pubs/priorities-eighth-internet-governance-forum-igf-ba

developing policy positions in response to the agendas of these events.

Conclusion

Civil society faces complex challenges in its quest to ensure equal participation and footing with other stakeholders in internet governance processes. Collaborative strategies are being developed, and are needed, in this environment if the power imbalances between civil society and other stakeholders are to be equalised and the doors of internet governance meetings are to remain open to all. Strong leadership is needed from diverse civil society groups, particularly from the Asia region, which has its own unique economic, cultural and social contexts.

‘강화된 협력’ 과 국제 인터넷 거버넌스의 미래

오병일[313]

1. ‘강화된 협력' 논의의 배경

2005년 튀지니 튀니스(Tunis)에서 개최된 제2차 정보사회세계정상회의(WSIS)의 결과로 만들어진 ‘튀니스 어젠다’[314]는 ‘인터넷 거버넌스'를 ‘정부, 민간부문, 시민사회가 각자의 역할을 통해, 인터넷의 발전 및 이용에 영향을 미치는, 공유된 원칙, 규범, 규칙, 의사결정 절차 및 프로그램의 개발 및 적용'이라고 규정하고 있다.[315] 그러나 지난 2012년 12월, UAE 두바이에서 개최된 국제전기통신세계회의(WCIT-12)를 통해 나타난 갈등은 인터넷 관련 공공정책 형성을 위한 원칙 및 체제와 관련하여, 국가간 그리고 다양한 이해당사자 사이의 입장 차이가 작지 않음을 보여주었다. 미래 인터넷 거버넌스가 어떠한 원칙하에, 어떠한 방식으로 이루어져야 하는 지에 대한 긴장은 계속 되고 있다. ‘강화된 협력(enhanced cooperation)’을 둘러싼 국제적인 논쟁은 이러한 긴장을 보여주는 동시에, 향후 인터넷 거버넌스 지형을 변화 시킬 계기가 될 수 있다는 점에서 주목되고 있다.

‘강화된 협력'의 역사적 맥락

‘강화된 협력'을 둘러싼 논의를 이해하기 위해서는 우선 역사적인 맥락을 이해할 필요가 있다.[316] 인터넷 거버넌스는 2003년 WSIS 제네바 회의부터 논쟁적인 이슈가 되었다. 당시에 도메인 네임, IP 주소 등 인터넷 주소자원에 대한 국제적 관리는 비영리 기구인 인터넷 주소관리기구(ICANN)가 맡고 있었는데, ICANN은 양해각서(Memorandum of Understaning)를 통해 미국 정부의 감독 하에 있었다.[317] 비록 인터넷이 미국의 군사, 학술

---

313) 진보네트워크센터 상근 활동가로 망중립성이용자포럼 및 인터넷거버넌스 관련 활동에 참여, 한국인터넷거버넌스협의회(KIGA) 주소인프라분과 위원, 정보공유연대 IPLeft 대표, antiropy@gmail.com

314) TUNIS AGENDA FOR THE INFORMATION SOCIETY, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

315) 34. A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

316) 역사적인 맥락에 대한 설명은 아래 글 참조. Wolfgang Kleinwächter, Enhanced Cooperation in Internet Governance: From Mystery to Clarity?, CircleID, 2013.11.12, http://www.circleid.com/posts/20131112_enhanced_cooperation_in_internet_governance_mystery_to_clarity/

317) 2005년 이후 현재까지 ICANN은 상당히 변화를 겪어왔다. ICANN이 2009년 미국 정부와 ‘Affirmation of

네트워크로부터 출발했다고 하더라도, 이미 전 세계적인 네트워크로 성장한 상황에서 인터넷이 작동하기 위한 핵심 기반인 주소자원에 대한 감독권한이 단지 한 국가(미국)에 주어져 있는 것에 대해 다른 국가들이 불만을 갖는 것은 당연한 일이다. 이에 일부 정부들은 WSIS에서의 논의를 통해 인터넷 주소자원에 대한 감독을 국제전기통신연합(ITU)과 같은 정부간 기구로 이관하고자 하였다. 그러나 당시에는 '인터넷 거버넌스'를 어떻게 규정할 것인지, 그리고 인터넷 관련 공공정책 이슈를 국제적으로 어떻게 다루어야 할지 아무런 합의가 없었다. 이에 WSIS 제네바 회의에서는 합의를 할 수 없었고, 코피아난 UN 사무총장에게 '인터넷 거버넌스 워킹그룹(WGIG)'을 구성하여, 1) 인터넷 거버넌스를 어떻게 정의할 것인지, 2) 인터넷 거버넌스와 관련된 공공정책 이슈는 무엇인지, 3) 정부, 기업, 시민사회 등 각 이해당사자의 역할과 책임은 무엇인지 등을 검토할 것을 요청했다.

WGIG는 정부, 기업, 시민사회 등 다양한 이해당사자 그룹을 대표하는 40명으로 구성되었다. WGIG는 당시의 인터넷 거버넌스 체제를 검토하면서 이를 개선하기 위한 몇 가지 제안을 내놓았다.[318] 첫째, 모든 이해당사자들이 동등하게 대화할 수 있는 포럼의 형성, 둘째, 전 세계적인 공공정책과 감독 체제, 셋째, 제도적인조정(institutional coordination)과 지역 및 국가 단위에서 이해당사자의 조정 등이다. 전 세계적인 공공정책과 감독 체제와 관련해서는 4가지 모델을 제시하였다. 1) 모델 1은 미국 상무성이 맡고 있는 감독기능과 ICANN 정부자문위원회(GAC)를 대체하는 UN 산하의 글로벌인터넷위원회(GIC) 설립안. 이는 스팸, 보안과 같은 인터넷 관련 공공정책도 담당한다. 2) 모델 2는 특별한 감독기구 없이, ICANN GAC의 역할 강화. 3) 모델 3은 ICANN/IANA 기능과 관련하여 미국의 감독 역할을 국제인터넷위원회(IIC)로 대체, 4) 모델 4는 정부가 중심이 된 (그리고 기업 및 시민사회는 참관으로 참여하는) 글로벌 인터넷정책위원회(GIPC) 설립을 통한 공공정책 수립 및 민간이 중심이 된 WICANN(World ICANN) 설립. WICANN은 GIPC의 감독을 받는다.[319]

WGIG의 보고서는 2005년 WSIS 튀니스 회의에 제출되었다. 그러나 튀니스 협상에서 정부들은 인터넷 거버넌스의 정의와 '인터넷 거버넌스 포럼'(IGF) 설립에는 합의하였으나, 공공정책 및 감독과 관련된 새로운 인터넷 거버넌스 체체 수립의 합의에는 실패하였다. 일부 참여자는 정부간 인터넷 위원회에서 원칙 수준의 정책 결정을 하는 새로운 모델을 수립할 것을 주장했지만, 미국 등 또다른 참여자 그룹은 기존의 시스템은 잘 작동되어 왔으며, 정부간 기구는 인터넷 자유에 위협이 될 수 있다고 우려하였다. 결국 정상회의의 실패를 막기 위해 모호한 용어로 합의를 할 수밖에 없었는데, 이것이 '튀니스 어젠다' 69-71항에 규정되어 있는 '강화된 협력'이다.

> 69. 인터넷과 관련된 국제 공공정책 문제에 모든 정부가 대등하게 맡은 역할과 책임을 수행할 수 있도록 추후에 '강화된 협력'의 필요성을 인식한다. 다만, 국제 공공정책 문제에 영향을 미치지 않는 일상적인 기술 및 운영 측면의 문제는 예외로 한

Commitments'(AoC) 계약을 체결하면서, 더 이상 미국 정부에의 보고 의무를 지지 않게 되었으며, 현재 ICANN의 국제화(globalization)를 계속 추진 중이다. ICANN 내의 정부자문위원회(GAC)의 위상도 강화되었다. 그러나 최상위 도메인네임 목록을 관리하는 루트서버(Root Server)에 대한 감독 권한은 여전히 미국 정부에 주어져 있다.

318) Report of the Working Group on Internet Governance, 2005.6, http://www.wgig.org/docs/WGIGREPORT.pdf

319) WGIG에도 참여했던 Wolfgang Kleinwächter는 이를 각각 Status Quo plus plus, Status Quo, Status Quo minus, Status Quo plus 로 칭했다.

다.[320]

70. 그와 같은 협력에는 관련 국제단체를 통해 중요 인터넷 자원 배정 및 관리와 관련된 공공정책 문제에 대한, 세계적으로 적용가능한 원칙을 수립하는 일도 포함돼야 한다. 이런 취지에서 우리는 인터넷과 관련된 핵심 작업을 책임지는 조직이 공공정책 원칙을 효과적으로 수립할 수 있는 환경을 조성하는 데 일조할 것을 촉구한다.[321]

71. 2006년 1사분기 후반부에 UN 사무총장의 지휘 하에 모든 관련 조직의 참여로 시작될 '강화된 협력' 과정에는 모든 이해당사자가 각자의 역할에 충실하고 법적 절차에 따라 가급적 신속하게 진행되면서도 혁신에 발 빠르게 대응할 수 있어야 한다. 그리고 관련 조직은 모든 이해당사자를 포함한 '강화된 협력' 과정을 시작해야 하며, 가능한 빠르게, 그리고 혁신에 대응하면서 진척시켜야 한다. 관련 조직은 연간 성과 보고서를 제출해야 한다.[322]

'강화된 협력'이라는 용어는 서로 대립하는 그룹들이 각자 자신의 성과라고 해석할 수 있는 절충이었다. 그러나 이와 같은 모호한 합의는 추후 지속된 논란을 야기할 수밖에 없었다. 일부는 '강화된 협력'이 말 그대로 현재의 인터넷 거버넌스 체제에서 협력을 강화하는 과정이라고 주장하였으며, 다른 측은 이것이 UN 산하의 새로운 국제 거버넌스 체제에 대한 논의를 시작해야 함을 의미하는 것이라고 주장하였다.

'강화된 협력' 워킹그룹 활동

7년 간의 논의 끝에, 2012년 12월에 개최된 67차 UN 총회에서 '강화된 협력' 논의를 위한 워킹그룹을 설립하기로 결정하였다.[323] '강화된 협력 워킹그룹(Working Group on Enhanced Cooperation, WGEC)은 UN '개발을 위한 과학기술 위원회'(CSTD) 산하에 만들어졌으며, 2013년 초에 22개 정부 대표 및 기업, 기술 커뮤니티, 시민사회 영역에서 각 5명 씩을 포함하여, 총 42명으로 구성되었다.

2013년 5월 30-31일, 첫 회의를 한 WGEC는 '강화된 협력'에 대한 당사자의 의견을 수렴하기 위한 설문조사를 하기로 하였다. 18개의 질문으로 구성된 설문 문항에 대해 총 69

320) 69. We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.

321) 70. Using relevant international organizations, such cooperation should include the development of globally-applicable principles on public policy issues associated with the coordination and management of critical Internet resources. In this regard, we call upon the organizations responsible for essential tasks associated with the Internet to contribute to creating an environment that facilitates this development of public policy principles.

322) 71. The process towards enhanced cooperation, to be started by the UN Secretary-General, involving all relevant organizations by the end of the first quarter of 2006, will involve all stakeholders in their respective roles, will proceed as quickly as possible consistent with legal process, and will be responsive to innovation. Relevant organizations should commence a process towards enhanced cooperation involving all stakeholders, proceeding as quickly as possible and responsive to innovation. The same relevant organizations shall be requested to provide annual performance reports.

323) UN GENERAL ASSEMBLY RESOLUTION A/RES/67/195, http://unctad.org/en/PublicationsLibrary/ares67d195_en.pdf

개의 답변이 들어왔다.[324] 2013년 11월 6-8일 개최된, WGEC 2차 회의에서 의장은 설문 답변을 다음과 같은 총 5개 그룹으로 구분하였다. 1) '튀니스 어젠다'의 이행 관련, 2) 공공정책 이슈 및 실현 가능한 체제, 3) 각 이해당사자의 역할, 4) 개발도상국의 역할, 5) '강화된 협력'에 대한 참여 장벽.

이 중 가장 논란이 많았던 부분은 2번, 즉 향후 인터넷 거버넌스 체제를 어떻게 발전시킬 것인 지에 대한 것이었다. 2005년 이후, 인터넷은 전 세계로 더욱 확장되었고, 모바일, 소셜 네트워크, 크라우드 서비스 등 인터넷 환경도 변화되었지만, 튀니스 회의 이전 WGIG에서 나타났던 긴장과 갈등은 지금까지 계속되고 있다. WGIG에 제출된 설문 답변을 분석해보면, 다양한 이해당사자들이 각자 현재의 거버넌스 체제의 문제점은 무엇인지, 미래 인터넷 거버넌스 체제가 어떻게 변화되어야 한다고 생각하는지 드러난다. 이 글에서는 설문 답변을 근거로 주된 쟁점에 대해서 분석해보기로 한다.

2. '강화된 협력'의 주요 쟁점

1) '강화된 협력'은 무엇을 의미하는가?

WGEC 설문의 질문 2, 4는 튀니스 어젠다에서 규정하고 있는 '강화된 협력'의 중요성, 목적과 범위, 그리고 지난 8년 동안 '강화된 협력'이 구현되었는지 여부를 묻는 것이었다. '강화된 협력'의 목적과 범위를 알기 위해서는 우선 튀니스 어젠다를 참고하지 않을 수 없다.

튀니스 어젠다 69항은 '강화된 협력'이 필요하다고 하면서, "모든 정부가 '대등하게' 맡은 역할과 책임을 수행할 수 있도록"이라고 '정부'의 역할을 특별히 언급하고 있다. 또한, 70항은 그러한 협력이 '중요 인터넷 자원 배정 및 관리와 관련된 공공정책 문제'를 포함한다고 명시하고 있다. IP주소 및 도메인 이름 등 인터넷 자원의 배정 및 관리는 당시, 그리고 역사적으로 ICANN, 지역인터넷등록소(RIR), IETF 등 민간 기관들이 담당해왔던 문제들이다. 이들 민간 기관들은 누구나 참여할 수 있도록 열려 있었지만, 인터넷에 대한 기술과 경험이 풍부하고, 자금력이 있었던 서구의 기업이나 엔지니어가 중심이 될 수밖에 없었다. 정부는 '중요 인터넷 자원'과 관련한 정책의 주요 참여자가 아니었고, ICANN에서도 '자문위원회'에 머물러 있었다. 민간 영역에서 활발히 참여하고 있는 선진국 정부와 달리 개발도상국의 정부들은 이러한 상황에 불만을 가질 수밖에 없었다. 튀니스 어젠다의 69, 70항은 이와 같은 개발도상국의 불만이 일정하게 반영된 것으로 볼 수 있다.

'인터넷 거버넌스 프로젝트'를 이끌고 있는 밀튼 뮬러 교수도 '강화된 협력' 개념이 '인터넷 거버넌스에서 정부의 역할을 강화하는 것'이라는 것을 인정하는데, 바로 그러한 이유로 튀니스 어젠다 자체가 잘못되었다고 비판한다.[325] 즉, 미국이라는 한 국가만이 ICANN에 특정한 역할을 갖고 있다는 것 자체는 문제가 있지만, 그 해결책이 국가 전반의 통제를 강

---

324) 정부 29개, 시민사회 23개, 학계/기술 커뮤니티 11개, 기업 8개 등이다. 답변자별 및 질문별로 정리된 설문에 대한 답변 및 이를 정리한 보고서는 모두 인터넷에 올라와있다.
http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=396

325) WGEC 설문에 대한 IGP의 답변 참조.

화하는 것으로 귀결되어서는 안된다는 것이다. '강화된 협력'을 이해당사자 사이의 소통과 상호작용의 발전된 어떤 형태로 해석하는 입장에 대해서도 비판한다. 튀니스 어젠다 35항은 정부, 기업부문, 시민사회, 정부간 조직, 국제기구 등의 역할에 대해서 규정하고 있는데, '인터넷 관련 공공정책 이슈에 대한 정책 권한은 국가의 주권'[326]임을 명확하게 규정하고 있다는 것이다. 물론 밀튼 뮬러 교수는 이러한 규정에 반대하며, 따라서 '정부의 역할 강화'를 전제로 한 '강화된 협력'의 구현 방안을 논의하는 것은 잘못된 방향 설정이라는 것이다.

그러나 그 외의 다른 그룹들은 '강화된 협력'을 다른 방식으로 해석하고자 한다. 즉, 현재의 거버넌스 체제 유지의 입장에 있는 그룹은 '강화된 협력'을 인터넷 거버넌스의 다양한 수준에서 각 이해당사자 간 소통과 협력을 강화하는 것으로 이해한다. 인터넷 관련 공공정책에 관심이 있는 시민사회 단체들은 '강화된 협력'을 '정부의 역할 강화' 이상을 의미하는 것으로 해석한다. 예를 들어, 국제 시민사회 네트워크인 '베스트 비트(Best Bits)'는 '강화된 협력'을 현재 거버넌스 체제의 결점을 해결하는 것으로 본다.[327] 그 '결점'에는 앞서 언급했던 ICANN에 대한 미국 정부만의 감독 권한 문제도 있지만, 다른 공공정책 이슈에 대한 거버넌스 체제 역시 문제가 있다고 본다. 예를 들어, 주소자원과 관련한 정책 외의 인터넷 관련 공공정책 - 예를 들어, 보안, 프라이버시, 지적재산권 등 -은 UN이나 FTA와 같은 국가간 기구를 통해 정부 주도로 만들어지고 있으며, 시민사회의 참여는 매우 제한적이다. 그래서 WGEC의 구성과 '강화된 협력' 논의를 오히려 인터넷 관련 공공정책 결정 과정의 민주화를 위한 계기로 활용하고자 한다. ICT 영역의 전 세계적 시민사회단체 네트워크인 진보통신연합(APC) 역시 '강화된 협력'을 '모든 수준에서 인터넷 거버넌스를 증진시키고 민주화하는 것'이라고 본다.[328] 이들은 정부의 역할과 관련해서도 69항이 정부의 역할을 특별히 강조하고 있다고 해서 '강화된 협력'이 정부'만'을 위한 것으로 해석되지 않으며, 튀니스 어젠다 전체적으로 다양한 이해당사자의 역할과 협력을 전제하고 있는 것으로 본다.

'강화된 협력'에 대한 이해의 차이는 그것이 지금까지 얼마나 구현되었는가 하는 질문과 연결된다. '강화된 협력'의 구현 여부와 관련하여, WGIG는 설문에 대한 답변을 1) 구현되지 않았다, 2) 상당한 진전이 있었다, 3) 일정한 진전이 있었지만 개선되어야 할 지점이 있다 등 3개 그룹으로 구분했다. '강화된 협력'이 인터넷 관련 공공정책을 논의할 새로운 체제의 형성 및 인터넷 주소자원 감독 권한의 국제화를 의미하는 것으로 이해하는 측(러시아 정부, 사우디아라비아, CITC, 인도 시민단체인 IT for Change 등)은 '전혀 강화된 협력이 구현되지 않았다'고 판단한다. 사우디아라비아는 인터넷 관련 공공정책은 국가의 주권임을 강조하고 있다. 그나마 현재까지 '강화된 협력'을 가장 근접하게 구현한 사례로 ITU의 '국제 인터넷 관련 공공정책에 대한 위원회 워킹그룹'(ITU Council Working Group on International Internet-related Public Policy)을 제시한다.[329] 반면, 상당한 진전이 있었다고 평가하는 측은 '강화된 협력'을 계속되는 과정(ongoing process)으로 이해한다. 스위스, 미국, 핀란드, 스웨덴, 영국, 일본 등 주로 선진국 정부와 JNIC, ARIN, RIPE NCC, LACNIC 등 주소관리기관들, CDT 등 시민사회, ICC 등 기업 등이 이러한 입장을 가지고 있다. 후자의 관점에서

326) Policy authority for Internet-related public policy issues is the sovereign right of States.
327) 베스트비트의 설문 답변은 http://bestbits.net/ec/ 참조.
328) APC의 설문 답변은 http://www.apc.org/en/node/18526/ 참조.
329) 그러나 국제 시민사회는 이 워킹그룹이 정부 중심으로 폐쇄적으로 운영될 것을 우려하고 있는데, 이에 베스트비트는 이 워킹그룹이 다양한 이해당사자의 참여를 폭넓게 허용할 것을 요구하는 성명을 발표한 바 있다. http://bestbits.net/ko/cwg-internet/

보자면, 지난 8년 동안 일정한 진전이 있었던 것도 사실이다. 예를 들어, ICANN에서 정부자문위원회(GAC)의 위상이 강화되었고, 8회에 걸친 IGF 회의가 개최되었으며, 개도국의 역량을 강화하기 위한 많은 프로그램이 있었다. '일정한 진전이 있었지만 개선되어야 할 지점이 있다'고 본 그룹(브라질 등 정부나 APC와 같은 시민사회단체)은 일정한 진전이 있었던 것에는 동의하지만, 현재의 거버넌스 체제에 대해 비판적인 문제의식을 가지고 있는 경우다. 물론 이 그룹 역시 현재의 거버넌스 체제를 어떻게 개선할 것인가에 대해서는 다양한 스펙트럼의 입장을 가지고 있다.

지난 8년 동안 얼마나 협력이 증진되었는지 논쟁을 할 필요는 없다. WGEC 2차 회의에서 의장이 한 얘기처럼, 물이 반 정도 차 있는 컵을 보고, 물이 반이나 차 있다고 볼 수도 있고, 물이 반 밖에 없다고 볼 수도 있는 것이다. 또한 새로운 거버넌스 체제의 형성을 지지하는 입장에서도 국내, 지역, 국제적으로 이루어지는 이해당사자간 협력의 노력이나 개발도상국에 대한 역량 강화를 부정할 이유는 없을 것이기 때문이다. 중요한 것은 여러 이해당사자들이 현재 거버넌스 체제에 대해 느끼는 문제점이 무엇인지, 실제로 합의할 수 있는 문제점이 무엇인지를 규정하는 것일 것이다. WGEC의 설문 답변에 대한 정리 보고서에서는 이에 대한 분석이 제대로 이루어지지 않았으며, 이를 제대로 분석하고 합의를 이끌어내는 것이 향후 어떠한 권고를 도출하기 위한 WGEC의 중요 과제가 될 것으로 보인다.

현재 거버넌스 체제의 문제점으로 제기되고 있는 것들은 다음과 같다. 첫째, ICANN에 대한 감독 권한 문제다. 이에 대한 문제 제기는 오래된 것이다. 2005년 WGIG 보고서에서도 '하나의 정부가 국제 인터넷 거버넌스와 관련하여 지배적인 역할을 해서는 안된다'고 규정하고 있다. 둘째, 개발도상국이 인터넷 거버넌스 논의에 동등하게 참여할 수 있도록 하는 문제 역시 오래된 과제이며, 대다수가 공감하는 문제이다. 이번 WGEC의 설문도 상당한 문항을 개발도상국 이해당사자들의 역할과 참여를 어떻게 촉진할 것인지에 할애하였다. 셋째, 인터넷 관련 공공정책을 논의할 국제적인 메커니즘이 없다는 것이다.[330] 물론 IGF를 통해서 여러 가지 공공정책 문제들이 제기될 수는 있지만, IGF는 논의하는 것 이상으로 권고와 같은 어떤 구체적인 정책 결과물을 내놓지 못하고 있다. 이는 정부, 시민사회 모두가 갖고 있는 문제의식이지만, 인터넷 관련 공공정책을 다룰 단일한 기구의 필요성에 대해서는 여러 이해당사자간 이견이 존재한다. 넷째는 현재의 정책결정 메커니즘이 충분히 민주적인가 하는 점이다. APC는 인터넷 거버넌스의 모든 수준에서 "이해당사자의 참여를 충분히 보장하고 있는지, 투명하고 책임성이 있는지" 문제제기하고 있다. 그러나 이 문제는 인터넷 거버넌스에 있어서, 혹은 인터넷 관련 공공정책의 결정에 있어서 각 이해당사자의 역할을 어떻게 볼 것인지의 문제와 연결된다. 튀니스 어젠다에서도 규정하고 있듯이, 정부만이 정책결정 '권한'을 가지고 있다는 것이 상당히 많은 정부들이 공유하고 있는 시각이기 때문이다. 물론 튀니스 어젠다에서도 인터넷 거버넌스에서 기업, 시민사회 등 다양한 이해당사자의 충분한 참여의 필요성에 대해서 언급하고 있지만, 소위 '멀티스테이크홀더리즘'

330) 예를 들어, 브라질 정부는 현재 거버넌스 체제의 문제를 다음 세 가지로 지적한다. 첫째는 보안과 프라이버시와 같은 새롭게 부상하는 중요한 이슈에 대해 정책결정(최소한 합의의 형성)할 수 있는 공간의 부재, 둘째, 정부가 인터넷 관련 공공정책을 전체적으로, 서로 다른 영역을 아울러서(in an holistic and cross-cutting manner) 다룰 수 있는 세계적인 플랫폼의 부재, 셋째, 인터넷 주소자원 기구에 대한 감독을 담당할 국제적 수준의 메커니즘 부재 등이다. 인도의 시민사회단체인 IT for Change 역시 인터넷 관련 공공정책을 전반적으로 다룰 민주적 공간의 부재 및 인터넷 주소자원기구에 대한 감독의 국제화 결여를 핵심 문제로 지적하고 있다.

(Multi-stakeholderism)의 해석에 대한 정부와 시민사회의 간극은 여전히 큰 것이 사실이다.

2) '강화된 협력'을 구현하기 위한 '새로운' 거버넌스 체제

흥미롭게도 이번 WGEC의 설문 답변자들 다수는 현재의 분산된 인터넷 거버넌스 체제가 다양한 이해당사자의 관심을 보다 유연하게 반영하는데 보다 효과적인 것으로 보고 있다.[331] 다만, 상당한 수의 응답자들이 새로운 이슈들을 논의할만한 적절한 공간이 기존의 거버넌스 체제에 없을 경우, 새로운 체제의 설립을 고려하는 것에 열려있었다. 그러나 그 새로운 체제는 멀티스테이크홀더 모델에 따라, 개방적이고 투명하며, 모든 이해당사자를 포괄해야 하고, 아래로부터의 정책 결정 과정에 기반해야 한다는 의견이 주류를 이루었다.

새로운 거버넌스 체제에 대한 제안들

그러나 '강화된 협력'이 충분히 구현되지 않았다고 보는 답변자들은 새로운 거버넌스 체제의 필요성을 제기하고 있다. 러시아 정보통신부는 '강화된 협력'을 구현하기 위해서 모든 정부가 동등하게 참여해야 하며, '필요할 경우' 다른 이해당사자와 협의할 수 있다고 주장한다. 그러한 체제로 ITU와 같은 정부간 조직 내의 플랫폼을 제안한다. 사우디아라비아는 최종적인 정책 결정은 회원국에 의해 만들어져야 하며, 사무국에 의해 뒷받침되는 기구의 설립을 제안하고 있다. 이 기구는 사무국과 위원회를 두며, 1년에 2회 만나서 의제 설정, 토론, 정책 결정을 한다.

브라질은 새로운 거버넌스 체제의 필요성을 인정하면서도 좀 더 조심스럽게 접근한다. 브라질은 지금까지 '강화된 협력'이 일정하게 진전되어 왔음을 인정함과 동시에, 현 체제의 문제점도 지적하고 있는데, 특히 보안 및 프라이버시 등 인터넷 관련 공공정책의 논의 공간 부재, 그리고 세계적인 플랫폼의 부재를 지적하고 있다. 그러나 당장 어떤 단일화된 기구의 설립을 주장하는 것은 아니다. 브라질은 새로운 체제에 대한 논의 이전에, 현재 거버넌스를 담당하고 있는 기구, 포럼, 절차 등에 의해 수행되고 있는 활동들을 파악하고(mapping), 이에 대한 평가를 통해 어떠한 개선이 필요한지 규정하는 것이 우선 되어야 한다고 주장한다. 어떻게 할 것인지 이전에, 우리가 '무엇을 원하는지' 먼저 토론해야 한다는 것이다.

새로운 거버넌스 체제와 관련하여, 가장 원대하고 구체적인 제안을 한 곳은 인도의 사회단체인 IT for Change이다.[332] IT for Change는 두 개의 새로운 인터넷 거버넌스 체제를 제안한다. 그 하나는 '인터넷 관련 공공정책을 위한 UN 기구의 설립'이고, 다른 하나는 '인터넷 기술 감독 및 자문 위원회'이다. UN 기구는 UN의 특별 기관 혹은 UN 총회 산하의

331) 물론 이는 설문 답변자만을 대상으로 한 것이고, 설문 답변자가 인터넷 커뮤니티 전체를 대표하는 것이 아니기 때문에, 다양한 입장들에 대한 검토로는 의미가 있어도, 특정한 입장을 지지하는 비율을 의미한다고 보기는 힘들 듯하다.

332) IT for Change의 설문 답변은 http://www.itforchange.net/civil_society_input_to_the_UN_Working_Group_for_global_governance_of_the_Internet 참조.

위원회가 된다. 이 기구는 다양한 이해당사자로 구성되는 '이해당사자 자문그룹' 형태로 공개적인 자문 기능을 둔다. 이 기구의 기능은 국제적인 인터넷 공공정책을 개발하고, 각 국의 법을 조화시키며, 국제적인 협약이나 협정을 촉진하고, 다른 국제기구와 인터넷 관련 이슈에 대한 조정을 담당한다. '인터넷 기술 감독 및 자문 위원회'는 현재 미국 정부가 하고 있는 역할을 대신하여, ICANN을 감독한다. 루트 서버의 감독도 이 위원회가 맡는다. 위원회는 전문성, 지역 등을 고려하여 10-15명 정도의 위원을 민주적인 절차를 거쳐 선출한다. IETF와 같은 독립적인 기술 조직들은 현재와 마찬가지로 운영된다. 이와 같은 두 개의 기구와 함께, '인터넷에 대한 기본 협약(Framework Convention on the Internet)'을 제안하고 있다. 계속적으로 새로운 이슈가 부상하는 인터넷의 특성 상, 특정한 이슈에 대한 협약 이전에 인터넷과 관련된 기본적인 법적 구조를 만들 필요가 있다는 것이다. 이 협약은 기후변화에 대한 기본 협약과 비슷한 역할을 할 것이다.

중앙화된 거버넌스 체제에 대한 반대 입장들

그러나 대체적으로 시민사회의 입장은 인터넷 공공정책에 대한 단일화된 중앙의 기구, 특히 정부간 기구를 설립하는 것에 대해 부정적이다. APC는 인터넷 생태계의 조정과 감독을 위한 중앙화된 기구의 설립에 반대한다. 현재 인터넷 생태계는 '인터넷에 특화된' 기구들뿐만 아니라, 일반 공공정책과 인터넷 거버넌스가 혼재된 기구들도 많다. 이러한 생태계는 한편으로는 복잡하고 불투명하지만, 깊이와 다양성과 참여의 기회를 증가시킨다. APC는 정책 수립이나 감독을 위한 새로운 기구를 만드는 것보다, 개발도상국이나 시민사회의 실질적인 참여를 보장하는 방식으로 기존의 체제를 변화시키는 것이 필요하다고 주장한다. 다만, 어떤 경우(예를 들어, 정부의 대량 감시로 인한 인권 침해 문제 해결 등을 위해)에는 새로운 체제가 필요할 수도 있지만, 우선 기존의 체제를 통해 해결될 수 있는지 먼저 검토해볼 필요가 있다고 본다. 인도의 '인터넷 민주주의 프로젝트'를 이끌고 있는 안야 코박스(Anja Kovacs) 역시 '강화된 협력'은 분산된 인터넷 거버넌스 시스템에 기반한다고 주장한다. 소수가 모든 인터넷 공공정책을 주도하는 중앙집중적 체제보다는 다양한 참여자가 자신의 전문성과 관심에 따라 특정 영역의 정책에 참여할 수 있는 구조가 바람직하다는 것이다.

베스트 비트는 새로운 거버넌스 체제를 주장하는 IT for Change 에서부터, 이에 반대하는 APC나 '인터넷 민주주의 프로젝트'까지 다양한 입장의 시민사회단체가 참여하고 있기 때문에, 베스트 비트의 입장은 어느 정도 절충적이면서도 '최소한 반대하지는 않는' 입장이라고 볼 수 있다. 베스트 비트의 입장은 1) 거버넌스 체제의 변화가 단계적으로 진행될 것이라는 것, 2) 해결해야 할 중요한 인터넷 공공정책 이슈들이 있고, 특히 아직 지구적으로 적절한 논의 공간이 없는 이슈(orphan issue)의 경우 새로운 체제가 필요할 수 있지만, 이는 다양한 이해당사자의 충분한 참여가 보장되어야 한다는 것, 3) 정부간 시스템을 통해 정부가 주도하고 있는 일반 공공정책 이슈 영역과 ICANN이 주도하는 주소자원 이슈 영역 모두 개혁이 필요하다는 것 등이다. 물론 베스트 비트가 언급하고 있는 새로운 체제는 공공정책 전체를 포괄하는 하나의 기구이거나 UN 산하에 만들어져야 한다는 것은 아니다. 관련하여 새로운 글로벌 체제가 만들어진다면 논리적으로는 UN이 기반이 됨을 인정하고 있지만, 지금까지의 UN 체제가 투명성이나 시민사회의 참여 측면에서 매우 취약하다는 점을 지

적한다. 이와 같이 시민사회가 UN 중심의 중앙집중화된 거버넌스 체제에 반대하는 이면에는 UN 체제에 대한 불신과 정부 중심의 정책 결정 과정이 될 것에 대한 우려가 존재한다.

ICANN 이슈와 다른 공공정책 이슈의 분리 접근

새로운 거버넌스 체제에 대한 논의에서 ICANN이 이미 담당하고 있는 주소자원 이슈와 다른 공공정책 이슈를 분리할 필요가 있다는 제안은 타당해 보인다. 앞서 얘기했듯이, 베스트 비트는 '정부간 시스템을 통해 정부가 주도하고 있는 일반 공공정책 이슈 영역과 ICANN이 주도하는 주소자원 이슈 영역 모두 개혁이 필요하다'는 것을 인정한다. 그리고 ICANN 관련 이슈의 경우, 새로운 국제 감독 위원회(international oversight board)라는 형태를 통해 미국 정부'만'이 감독 권한을 갖는 현 체제를 개혁할 필요가 있지만, 이를 UN 내에 두는 것은 반대한다. 이 새로운 감독 위원회는 지리적 다양성을 고려해야 하고, ICANN은 국제기구로서 미국(혹은 기구가 위치할 다른 국가)과 주관국 계약(host country agreement)을 체결하여, 미국법이나 다른 형태의 통제로부터 면책된다. 이 위원회는 현재 미국 정부가 행사하는 것과 같은 '좁은' 범위의 감독 권한만을 갖는다. 그러나 이 위원회가 다른 공공정책까지 관여할 필요는 없으며, 오히려 분리하는 것이 낫다. 왜냐하면, 인터넷 주소자원의 관리와 관련된 멀티스테이크홀더 모델은 이미 성숙된 상태이기 때문이다. ICANN에 대해 미국 정부'만'이 감독권한을 갖는 것에 대한 문제제기가 타당함에도 불구하고, '현상유지'를 주장하는 입장의 배경에 기존의 민주적 과정 및 다양한 이해당사자 참여가 위축되고 정부의 통제가 강화되는 것에 대한 우려가 있음을 고려하면, ICANN을 비롯한 다양한 기술 커뮤니티들이 지금까지 해 왔던 역할을 그대로 유지하면서 감독 권한의 문제만 국제화하는 방식으로 해결하는 것이 바람직해 보인다. 또한, 이렇게 할 경우, 다른 인터넷 관련 공공정책을 위한 거버넌스 체제에 대한 논의도 ICANN을 둘러싼 긴장에 영향을 받지 않고 이루어질 수 있을 것이다. 그러나 베스트 비트는 다른 인터넷 공공정책을 위한 새로운 거버넌스 체제의 구체적인 상에 대해서는 제시하지 않았다. 이는 베스트 비트 내에서 구체적인 상에 대한 합의가 이루어지지 않았기 때문이다.

브라질 정부 역시 주소자원 관리 이슈와 인터넷 관련 공공정책 이슈를 분리해서 접근할 것을 제안하고 있다. 그리고 인터넷 관련 공공정책 이슈의 경우, 단일한 공간/플랫폼이 필요하다고 주장한다. 이러한 공공정책 이슈의 많은 부분이 이미 기존의 국제 조직에서 이루어지고 있지만, 인터넷 관련 문제들이 전체적으로, 영역을 아울러서 조정될 필요가 있기 때문이다. 다른 기구에서 이미 다루고 있는 이슈의 경우에는, 이 단일화된 기구에서 '인터넷 관련 정책'이라는 관점에서 조정 역할을 할 수 있을 것이다. 예를 들어, 저작권 이슈의 경우 세계지적재산권기구(WIPO)에서 다루고 있지만, 저작권 정책이 인터넷과 연관될 경우, 새로운 기구는 저작권 정책이 인터넷에 미치는 영향을 검토하고 WIPO에 의견을 제시하는 등 조정과 협력을 할 수 있을 것이다.

강화된 협력과 IGF

많은 설문 답변자들이 IGF를 '강화된 협력'의 주된 근거로 보거나 최소한 '강화된 협력'을

위한 주요한 논의 공간으로, 혹은 '강화된 협력'을 위한 단계로서 IGF의 개혁 및 활용을 주장하고 있음도 주목할 만하다. 물론 IGF를 '강화된 협력'을 보여주는 주된 근거로 보는 입장은 '현상유지(Status Quo)'를 바라는 세력의 립서비스로 볼 수도 있다. 한편, 시민사회는 IGF가 UN에 기반하고 있으면서도 다양한 이해당사자의 참여가 그나마 가장 잘 이루어지는 공간이라는 점에서 긍정적인 시각을 가지고 있으면서도, IGF가 단지 '풍성한 말잔치'로 끝나는 것이 아니라, 좀 더 유의미한 역할을 할 수 있기를 바라고 있다. IGF를 '강화된 협력'의 구현으로 동일시하지는 않더라도, '새로운 거버넌스 체제'를 위한 징검다리 역할로서 인터넷 관련 공공정책에 대한 토론이나 가이드라인, 혹은 권고안 제시 정도의 기능을 기대하는 것이다. 이는 '새로운 거버넌스 체제'가 단기간 내에 만들어질 경우 정부 중심의 기구가 될 가능성이 높은 반면, IGF는 일정하게 다양한 이해당사자가 참여하는 메커니즘이 구축되었기 때문이다.

APC는 IGF와 협력하는 것을 전제로 한 '정보 교환 및 정책 조사 기구(information clearing houses and policy observatories)'를 제안하고 있다. 베스트 비트의 코디네이터인 제레미 말콤(Jeremy Malcolm)이 일하고 있는 국제소비자연맹(Consumer International)은 IGF 에 '멀티스테이크홀더 인터넷 정책 위원회'(Multistakeholder Internet Policy Council, MIPC)를 둘 것을 제안하고 있다. MIPC는 정부, 시민사회, 기업, 기술 및 학계 등의 대표로 이루어지며, 각 이해당사자 그룹의 소위원회가 만들어질 수 있다. 이를 위해서는 IGF 전체 회의(plenary session)가 각 이해당사자 그룹이 제대로 대표되고 실질적 토론이 가능하도록 잘 조직화되어야 한다. 각 이해당사자 그룹의 소위원회별 토론 및 전체 토론이 서로 피드백을 주고받으며 일정 기간의 토론을 거쳐서 합의가 형성되면 IGF의 권고로 발표가 된다. 국제소비자연맹 외에도, 구체적인 형태는 조금씩 다르지만 이와 유사한 제안들이 나오고 있다. 그러나 어떤 형태로든 이러한 제안이 실현되기 위해서는 IGF가 현재와 같이 '다수의 워크샵'이 아니라, 실질적인 토론과 권고가 이루어질 수 있도록 IGF의 구조와 역할이 개혁될 필요가 있다.

3) 국가를 포함한 이해당사자(stakeholder)의 역할

인터넷 거버넌스를 둘러싼 갈등의 이면에는 크게 두 가지 축의 역학관계가 존재하는 것으로 보인다. 첫째는 ICANN에 대한 미국 정부만의 감독 권한으로 대표되는, 좀 더 폭을 넓히면 인터넷 거버넌스를 주도하고 있는 선진국과 개발도상국의 역학 관계, 둘째는 인터넷에 대한 국가의 주권과 권한을 주장하는 정부와 다양한 이해당사자의 참여를 보장할 것을 요구하는 정부 외 이해당사자, 특히 시민사회의 역학 관계이다. 물론 이 두개의 축은 별개로 존재하지 않고 복잡하게 얽혀있다. 즉, 미국이나 유럽 등 선진국이 시민사회 등 다양한 이해당사자의 참여를 보장하는 '멀티스테이크홀더리즘'을 주장하는 것은 이것이 그들의 국가적 이해관계와 일치하기 때문인 것으로 이해된다. 누구나 참여할 수 있는 오픈된 논의 플랫폼은 결국 정부뿐만 아니라, 기업이나 시민사회 역시 인터넷 거버넌스에 대한 전문성, 경험, 자원을 모두 가지고 있는 선진국에게 유리할 수밖에 없기 때문이다. 반면, 각 국가가 동등하게 1표를 행사할 수 있는 UN 시스템이 개발도상국 정부들이 목소리를 내기에 유리할 수 있다. 반면, 시민사회 입장에서는 지금까지의 인터넷 관련 공공정책(주소자원 이슈이든, 다른 인터넷 정책 이슈이든)은 정부와 기업에 의해 주도되어 왔으며, 따라서 모든 수준에서

시민사회의 참여 폭을 확대하고 논의 과정 자체를 투명하게 공개하는 등 민주화할 것으로 요구하고 있다. 또한, 스노든에 의해 미국 NSA의 대량 감시가 폭로 되었듯이 선진국의 정부 역시 예외는 아니지만, 중국이나 아랍 국가 등 정부들(이들은 주로 인터넷에서의 국가 주권을 주장하는 정부들이다)이 노골적으로 인터넷에 대한 감시와 통제를 강화하고 있음을 고려할 때, 인터넷 거버넌스를 정부간 기구에서 주도하는 것을 우려하지 않을 수 없다.

'강화된 협력' 논의의 기반이 되는 튀니스 어젠다는 제35항에서 정부, 기업, 시민사회, 정부간기구, 국제기구 등의 역할을 규정하고 있으며, 특히 "인터넷 관련 공공정책에 대한 정책 권한은 각 국가의 주권"임을 선언하고 있다.[333] 반면, 시민사회의 역할은 '특히, 커뮤니티 수준에서 인터넷 문제에 중요한 역할을 하고 있다'고 제한하고 있다. 물론 29항[334]에서 "인터넷에 대한 국제적인 관리는 다자간의, 투명하고 민주적인, 그리고 정부, 기업, 시민사회, 국제 조직의 충분한 참여 속에서 이루어져야 한다"고 언급하는 등 곳곳에서 다양한 이해당사자의 참여와 협력을 강조하고 있지만 말이다.

이와 같은 튀니스 어젠다에 기반하여, 주로 새로운 거버넌스 체제를 주장하는 측은 국가의 주권과 정책 권한을 강조한다. 예를 들어, 러시아는 "국제적인 수준에서, 국가간 대화의 주 참여자는 국가의 공공 기관의 인가받은 대표자들이다"라고 주장한다.

인터넷 거버넌스 프로젝트를 이끌고 있는 밀턴 뮬러 교수는 반대편 극단에 있다. 그는 인터넷 공간은 서로 국경으로 분리되어 있는 공간의 집합이 아니라, 수천 개의 독립적으로 운영되는 자율적인 시스템으로 구성된 글로벌 공간이며, 따라서 인터넷 공공정책은 '국제적(international)'이 아니라, '초국적(transnational)'이라고 주장한다. 대부분의 인터넷 정책 이슈는 국경으로부터 독립적이며, 정부 역시 이해당사자의 하나일 뿐이다.

정부가 인터넷 업체 등에 대한 규제를 통해 일정하게 국내적 정책을 인터넷에 (최소한 부분적으로는) 관철시키고 있는 현실, 즉 현실적으로 가장 강력한 이해당사자임을 논외로 하더라도, 인터넷 관련 공공정책의 상당 부분이 인터넷 외의 다른 정책영역과 연결되어 있고,

---

333) 35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:
a. **Policy authority for Internet-related public policy issues is the sovereign right of States.** They have rights and responsibilities for international Internet-related public policy issues.
b. The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.
c. **Civil society has also played an important role on Internet matters, especially at community level,** and should continue to play such a role.
d. Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.
e. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

334) 29. We reaffirm the principles enunciated in the Geneva phase of the WSIS, in December 2003, that the Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. **The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations.** It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.

각 국에서 공공정책을 이행할 권리와 의무가 정부에 있음을 고려할 때, 인터넷 거버넌스와 각 국가의 정책결정 시스템(정부, 국회 등)이 어떻게 연결될 수 있을지는 좀 더 많은 논의가 필요할 것으로 보인다.

그럼에도 불구하고, 최소한 튀니스 어젠다의 규정은 여러 가지 문제점을 가지고 있으며, 대다수의 시민사회 답변자들이 이를 비판하고 있다. 정부의 정책 결정권은 논외로 하더라도, 시민사회의 역할을 '특히, 커뮤니티 수준에서' 중요한 역할을 수행하고 있다고 본 것은 현실과도 맞지 않는다. 시민사회 참여자들은 커뮤니티 수준에서 뿐만 아니라, 기술적, 이론적, 정책적 측면 등 다양한 수준에서 역할을 하고 있기 때문이다.

나아가 '이해당사자를 정부, 시민사회, 기업 등으로 구분하여 규정하는 것이 타당한가' 라는 문제제기도 있다. 이와 같은 구분은 지나치게 인위적이라는 것이다. 시민사회를 어떻게 규정할 것인지, 기술 커뮤니티나 학계도 포함하는 것인지 등도 모호할 뿐더러, 여러 이해당사자 그룹의 역할을 동시에 수행하고 있는 (예를 들어, 기업의 입장을 대변하는 민간단체, 기업에 소속해 있지만 개별적으로 인권단체 활동을 하는 사람, 전직 정부 관료이면서 기업에서 일하는 사람 등) 경우도 많다. 같은 이해당사자 그룹 내에서도 다양한 입장이 있을 수 있음은 물론이다.

궁극적으로 '모든 개인 이용자'가 자신만의 의견을 갖고 있는 하나의 이해당사자라고 할 수도 있다. 물론 현실적으로는 그룹별로 집합적인 목소리를 내거나 이해당사자 그룹의 대표들로 위원회를 구성해야 하는 경우가 많다. 이 경우 이해당사자 그룹을 어떻게 규정할 것인가의 문제가 발생한다. 그러나 최소한 튀니스 어젠다와 같이 모든 경우에 통일적인 이해당사자 그룹과 역할을 규정하는 것은 지나치게 경직된 것이라는 비판을 피할 수 없을 듯 하다.

튀니스 어젠다에 기반하여 활동하고 있는 WGEC이 최종결과물에 이 문제를 포함할지는 알 수 없으나, 이해당사자의 규정문제를 해결하지 않는다면, 즉, 튀니스 어젠다의 관련 규정이 어떤 식으로든 수정되지 않는다면, 향후의 인터넷 거버넌스 관련 논의에서 반복적으로 제기될 수밖에 없을 것이다.

3. '강화된 협력' 논의의 향후 전망과 평가

지금까지의 논의를 바탕으로 필자의 생각을 정리해보면 다음과 같다.

지난 2005년 튀니스 어젠다 이후, 인터넷 환경도 상당하게 변화하였고, 또 인터넷 거버넌스도 많은 진전을 이루어온 것이 사실이다. 그러나 여전히 현실 인터넷 거버넌스 체제는 많은 한계 역시 가지고 있다. 그러나 새로운 거버넌스 체제를 '어떻게' 구현할 것인가를 논의하기 이전에, 그 한계와 문제점이 무엇인지, 그래서 우리가 원하는 거버넌스 체제는 무엇인지에 대한 공감대가 우선 형성될 필요가 있다.

관련하여, 인터넷 거버넌스에서 다루고자 하는 공공정책을 구분해서 접근할 필요가 있다. 앞서 얘기했듯이, 주소자원의 관리 이슈와 다른 인터넷 관련 공공정책 이슈는 별개로 접근하는 것이 타당하다고 생각한다. 인터넷 관련 공공정책 이슈도 좀 더 구분할 필요가 있다.

새로운 인터넷 이슈들은 앞으로 계속 나타날 것이기 때문에, 이슈의 목록을 제한할 필요는 없다고 하더라도 이슈의 성격에 따라 몇 가지 그룹으로 나눌 수는 있을 것이다. 이미 튀니지 어젠다 이전 WGIG의 보고서는 이를 4가지로 구분하고 있다. 첫째는 인터넷 주소자원과 관련한 이슈들. 이 이슈들은 인터넷 거버넌스와 직접 관련되며, ICANN 등 기존의 기구에서 다루고 있는 이슈들이다. 둘째 스팸, 보안, 사이버 범죄 등 인터넷의 이용과 관련된 이슈들. 이 이슈들 역시 인터넷 거버넌스와 직접 관련되지만, 글로벌 협력 체제가 잘 갖춰지지 않은 것들이다. 셋째, 인터넷과 관련되지만, 인터넷 이상의 공공정책과 관련된 이슈들이다. 이들 중 일부는 지적재산권 이슈와 같이 기존 기구에서 다루고 있는 것도 있다. 넷째는 인터넷 거버넌스의 개발 측면의 이슈들, 특히 개발도상국의 역량 강화 이슈 등이다. 이러한 이슈 영역 각각에 대해 현황, 성과, 문제점 등이 정리될 필요가 있다.

ICANN 등 주소자원 관리 체제의 국제화, 혹은 미국 정부 일방의 감독 체제를 탈피하는 문제는 공감대가 형성되어 있는 듯 하다. 다만, 이를 UN 체제로 가져갈 것인지에 대한 이견이 존재한다. ICANN 및 주소자원 관련 기구들이 지금까지 개방적이고 민주적인 거버넌스 모델을 형성해온 것을 고려했을 때, 미국 정부 일방의 감독 체제를 극복하되 이를 정부간 기구로 대체하는 것이 아니라, 다양한 이해당사자들이 동등하게 참여할 수 있는 모델로 개편할 필요가 있다. WGEC에서의 논의와 별개로 이미 이 문제에 대한 논의가 진행되고 있다. 미국 NSA의 대량감시가 폭로된 이후, 지난 10월 7일 인터넷소사이어티(ISOC), IETF, W3C 및 각 지역의 주소자원을 관할하는 NIC 등 인터넷 기술 커뮤니티 대표들이 모여 몬테비데오 선언을 발표했다.[335] 이 선언에서 이들은 미국의 감시행위를 비판하는 한편, 다양한 이해당사자가 동등하게 참여하는 방향으로 '인터넷주소관리기구(ICANN) 및 IANA 기능을 국제화(globalization)'할 것을 요구한 것이다. 이어 10월 9일에는 CANN CEO 파디 세하디가 브라질 대통령을 만나 2014년에 인터넷 거버넌스를 논의하는 국제회의를 제안하였고, 브라질 대통령이 이를 수용하였다. '인터넷 거버넌스의 미래에 대한 글로벌 멀티스테이크홀더 회의'(Global Multistakeholder Meeting on the Future of Internet Governance)라고 이름 붙여진 이 회의는 2014년 4월 23-24일, 브라질 상파울로에서 개최될 예정이다. 구체적인 의제는 아직 정해지지 않았지만, ICANN의 국제화는 하나의 의제가 될 것으로 보인다.

다른 공공정책 이슈의 경우는 기존 국제기구에서 다루고 있는 이슈와 적절한 글로벌 논의 플랫폼이 존재하지 않는 이슈로 나눌 수 있다. 새로운 기구가 만들어지더라도 기존 기구의 역할을 대체하지는 않을 것이다. 그렇기에 기존의 국제기구에서의 논의가 좀 더 투명하고 민주적으로 이루어질 수 있도록, 그리고 인터넷의 특성을 잘 고려할 수 있도록 개선될 필요가 있다. 예를 들어, ITU, WIPO, UN 인권이사회 등이 그러하며, 정부 간에 폐쇄적으로 이루어지는 자유무역협정(FTA) 논의가 공공정책을 훼손하지 않도록 통제될 필요가 있다.

보안 문제 등 인터넷에 특화된 공공정책 논의를 위한 글로벌 공간이 필요한 것은 사실이다. 그러나 현재와 같이 UN이 무능력하고 비민주적으로 운영되는 상황에서 UN 산하의 기구를 만드는 것에 대한 우려가 제기될 수 밖에 없다. 우선 UN 산하든, ICANN과 같이 독자적인 기구가 되든, 인터넷 관련 공공정책을 논의할 글로벌 기구가 어떤 원칙에 의해 운영되

335) Montevideo Statement on the Future of Internet Cooperation,
http://www.internetsociety.org/news/montevideo-statement-future-internet-cooperation

어야 하는지 합의될 필요가 있다. 예를 들어, 논의 과정이 투명하게 공개가 되어야 하고, 다양한 이해당사자가 동등하게 참여할 수 있어야 한다는 등의 원칙이 제안될 수 있을 것이다. 그러나 현실적으로 일부 정부들이 이러한 제안을 수용할 수 있을지는 회의적이다. 거꾸로 정부 중심의 기구 설립에 대한 반대도 크기 때문에, 이에 대한 입장 차이가 해소되지 않는다면 인터넷 관련 공공정책을 담당할 새로운 거버넌스 체제 논의는 당분간 표류할 수밖에 없다.

인터넷 관련 공공정책이 제안되고, 논의되고, 일정한 권고나 가이드라인을 제시할 수 있도록 IGF를 개혁하는 것이 하나의 타협 가능한 방안이 될 수 있다. 물론 현재까지의 IGF 역시 많은 한계를 가지고 있다. 예를 들어, IGF의 프로그램을 담당하는 '멀티스테이크홀더 자문 그룹'(Multi-Stakeholder Advisory Group, MAG)[336]의 경우 멤버들이 어떻게 임명되는지조차 불투명하다. IGF의 업무를 뒷받침할 사무국의 역량도 미약하고 재정 역시 취약하다. IGF가 좀 더 적극적인 역할을 할 수 있기 위해서는 사무국의 역량도 강화되어야 하고 MAG 운영도 민주화될 필요가 있다.

인터넷 거버넌스에 개발도상국이 동등하게 참여할 수 있도록 해야한다는 방향에 대해서는 큰 이견이 없지만, 문제는 실질적인 방안이다. ICANN과 같이 형식적으로는 모두의 참여를 개방한다고 해도, 개발도상국의 참여를 촉진할 실질적인 조치가 뒷받침되지 않는다면, 선진국 및 기업의 참여자에 의해 여전히 주도될 것이기 때문이다. 이러한 불균형은 개발도상국 정부가 ITU 등 UN 시스템에 호소하게 만드는 힘으로 작용할 것이다.

'강화된 협력'의 국내적인 의미

이번 WGEC의 설문에 대해 한국에서는 정부, 기업, 시민사회 아무도 답변을 제출하지 못했다. 글로벌 인터넷 거버넌스에의 참여 부족과 입장의 부재라는 서로 연결된 두 가지 문제가 있을 듯하다.

한국 정부는 인터넷 거버넌스에 대해 나름의 어떤 가치에 기반한 입장을 갖고 대응하기보다는, 미국, 중국 등과의 정치적 관계의 고려에 치중하는 모습을 보여 왔다. 물론 정부 입장에서 외교적 관계를 무시할 수 있는 것은 아니나, 그러한 정치적 판단의 근거가 될 수 있는 내부적인 기준이 없다면 장기적인 전략을 가질 수 없다. 통상 '국익'을 고려한다고 하지만, '국익' 역시 추상적이기는 마찬가지다. 한국 기업의 이익이 국익일까? 그렇다면, 한국 기업이 해외 이용자의 권리를 침해하더라도 기업의 수익이 도움이 된다면 지원을 해야 하는 것일까?

정부를 포함한 한국의 참여자들도 이제 우리가 생각하는 바람직한 거버넌스 방향이 무엇인지 고민을 해야 한다. 그리고 함께 논의를 해야 한다. 물론 '한국의 참여자'라고 해서 '국가'를 기반으로 인터넷 거버넌스를 바라봐야 한다는 것은 아니다. 정부, 기업, 시민사회 등 이해당사자에 따라 관점의 차이가 존재하기 때문이다. 다만, 이러한 대화는 글로벌 거버넌스와 연결되거나 중첩되는 국내적인 거버넌스의 발전을 위해서 중요할 것이다.

---

336) IGF MAG 홈페이지 참조. http://www.intgovforum.org/cms/magabout

한국의 이해당사자들은 정부의 역할과 다른 이해당사자의 역할에 대해 어떠한 입장인가. 글로벌 인터넷 거버넌스는 정부간 기구에서 주도해야 한다고 생각하는가, 아니면 다양한 이해당사자가 동등하게 참여해야 한다고 생각하는가. 한국에서의 인터넷 거버넌스는 충분히 개방적이고 민주적인가. 현재 한국의 상황을 보면, 글로벌 거버넌스 논의에서 투명성과 민주성을 주장하고, 다양한 이해당사자의 참여를 주장하기는 힘들 것 같다. 만일 우리가 이러한 원칙에 동의한다면, 국내에서부터 그러한 원칙을 어떻게 구현할 것인지 함께 고민할 필요가 있다. IGF가 전 세계적, 지역적 수준에서 이와 관련된 논의 공간으로 자리 잡고 있는 것처럼, 한국 IGF를 통해 이러한 논의를 진행하는 것도 좋을 것이다.

WGEC 2차 회의의 논의 결과

지난 2013년 11월 6일-8일 개최된 WGEC 2차 회의는 설문 답변에 대한 의장의 사전 분석을 반영하여 답변을 5개의 그룹으로 나누어 진행하였다.[337] 회의는 5개 그룹 각각의 답변에 대해 토론하는 방식으로 진행되었다. 앞서 설문 답변을 토대로 분석한 바와 같이, 2차 회의에서도 인도, 이란, 사우디아라비아 정부 및 인도 시민사회(IT for Change)는 '강화된 협력'의 완전한 이행을 위해 인터넷 거버넌스에 대한 포괄적 접근을 요구했으며, 새로운 중앙집중식의 글로벌 정부간 체제을 주장했고, 시민사회를 포함한 다른 당사자들은 이에 반대하며 현재의 시스템의 문제가 무엇인지 보다 잘 이해하는 것이 우선되어야 한다고 주장했다. 또한, 많은 참가자들이 IGF의 강화 필요성을 강조했다.

WGEC 2차 회의 후, 권고안을 만들기 전에 답변에 대한 추가적인 분석이 필요하다고 결정되었고, 'WGEC의 의견교환그룹'(Correspondence group of the WGEC)을 통해 2014년 1월 말까지 '지도그리기(mapping)' 작업을 하기로 했다. 이 그룹은 모두에게 공개적으로 진행된다. 한편, 인도 정부가 제안한 '권고 프레임워크 초안'에 대한 검토도 이루어졌는데, 이는 WGEC 3차 회의에서 마무리될 예정이다. 3차 회의는 2014년 2월 24일-28일, 제네바에서 개최된다.

WGEC 멤버인 볼프강은 다음과 같은 사항들에 대해 대강의 합의가 이루어질 수 있다고 보았다.[338]

- 개발도상국의 동등한 참여를 위한 인터넷 인프라 개발 및 역량 강화
- 개발도상국의 동등한 참여를 제한하는 공식적, 비공식적인 장벽의 제거
- 새로운 인터넷 거버넌스 이슈를 다룰, 멀티스테이크홀더 방식에 따른, 혁신적인 절차 및 메커니즘의 개발
- 멀티스테이크홀더 메커니즘에서 개별 이해당사자, 특히 정부의 역할 명확화 및 인터넷 정책 결정 과정에서 이해당사자의 실질적인 상호작용 방식
- 모든 이해당사자들이 동등하게 참여하는 방향으로의 ICANN 및 IANA 기능 등 인터

337) 2차 회의 결과에 대한 APC 정책 코디네이터인 Joy의 보고 참고. http://www.apc.org/en/node/18717/

338) Wolfgang Kleinwächter, Enhanced Cooperation in Internet Governance: From Mystery to Clarity?, CircleID, 2013.11.12, http://www.circleid.com/posts/20131112_enhanced_cooperation_in_internet_governance_mystery_to_clarity/

만일 이와 같은 합의가 만들어질 수 있다면, 현재 단계에서 가능한, 글로벌 거버넌스 체제의 진전으로 보인다.

2014년에는 미래 인터넷 거버넌스의 향방에 영향을 미칠 국제회의가 연이어 개최될 예정이다. WGEC는 3차 회의 후 권고안을 CSTD에 보고를 해야하며(2014년 5월), 이는 경제사회이사회(ECOSOC)를 거쳐 2014년 9월 69차 UN 총회에 제출되게 된다. 이에 앞서 2014년 4월에는 WSIS 10년을 평가하고 향후 방향을 논의하기 위한 고위급 회의(WSIS+10 High Level meeting)가 개최되고, 브라질 상파울로에서는 '인터넷 거버넌스의 미래에 대한 글로벌 멀티스테이크홀더 회의'가 개최된다. 2014년 9월 터키 이스탄불에서 개최될 예정인 9차 IGF 회의에서는 2014년 상반기에 진행될 거버넌스 논의의 후속 논의가 이루어질 것이다. 2014년 11월에는 부산에서 ITU 전권회의가 개최될 예정이다. ITU는 국가 중심의 인터넷 거버넌스를 추진하는 주된 공간인만큼, 그 이전 논의의 결과에 따라 ITU 전권회의도 영향을 받을 것으로 보인다. 한국의 참여자들도 국제적인 인터넷 거버넌스 논의에 뒤쳐지지 않고, 나름의 입장을 갖고 참여할 수 있기를 기대해본다.

ABSTRACT

Enhanced Cooperation and the future of global internet governance

Oh, Byoungil[339)]

'Enhanced Cooperation', which was the mandate of Tunis Agenda in 2005, was the product of political compromise after failing to reach a consensus on global internet governance mechanism. In 2012, UN General Assembly decided to establish CSTD 'Working Group on Enhanced Cooperation (WGEC)' to find out what could and should be done to implement the Tunis Agenda. After a first meeting, WGEC sent out a questionnaire to collect extensive opinions from internet communities. Replies to the questionnaire showed a broad spectrum of perspectives on the problem of existing internet governance arrangement and how to improve it. This article analysed different perspectives, based on replies, especially regarding the concept and implementation of the Tunis Agenda, public policy issue and possible mechanisms, and the role of stakeholders including government. The recommendation of WGEC will be submitted to UN GA passing through CSTD and ECOSOC, in 2014, which is expected to have great impact on the future of internet governance.

339) Activist of Korean Progressive Network 'Jinbonet', Network Neutrality User Foru, representative of IPLeft, Member of Advisory Group of ccTLD in KISA

2014 브라질 회의로 가는 길

전응휘[340]

1. 통신의 국제협력/조정과 인터넷 거버넌스

세계적으로 연결되어 있는 통신네트워크가 정상적으로 작동하기 위해서는 통신 상대자 간에 세계적인 협력과 조정의 방식과 틀이 필요하다. 그런 이유에서 전통적인 통신서비스는 유선이든 무선이든 범세계적인 협력과 조정의 형식을 구축하여 유지해 왔다. 유선망의 경우에는 네트워크 간에 필수적으로 요청되는 상호접속이, 무선망의 경우에는 통일적인 주파수의 배정이, 그리고 유선망이든 무선망이든 기술적인 호환성을 위한 표준 수립이 필요했고, 이를 기존의 통신관련 국제적인 기구(ITU나 CCITT 등)들이 이러한 조정과 협력의 역할을 수행하여 왔다. 무선전신이나 전화를 기반으로 한 이러한 세계적인 조정과 협력의 역할은 개별 국가가 전기통신서비스를 국가의 공공적인 독점서비스로 제공하고 있었기 때문에 자연스럽게 국가간의 협력과 조정의 틀을 통해서 이루어질 수 있었다.

그러나 인터넷은 이러한 전통적인 전기통신서비스의 세계적인 협력과 조정의 틀과는 전혀 다른 방식으로 작동해 왔다. 인터넷은 출발부터 공공적인 프로젝트로 시작하는 경우에도 네트워크 간의 연결과 확장은 네트워크들 간의 자발적인 네트워킹을 통해서 이루어졌다. 인터넷의 기술표준은 IETF(Internet Engineering Task Force)/IAB(Internet Architecture Board)와 같은 그룹 안에서 엔지니어, 학자들의 자발적인 토론과 합의를 통해, 그리고 관련 기술에 대한 자발적인 선택과 수용을 통해 채택되어 왔고, 통신을 위해 필수적인 IP주소블록의 할당은 IANA(Internet Assigned Numbers Authority)/RIRs(Regional IP Registries, 대륙별로 ARIN, RIPENCC, APNIC, LACNIC, AFRINIC)와 같은 기구를 통해 해당 주소를 이용하고자 하는 사업자들의 협의를 통해서 이루어져왔다. 오늘 인터넷을 가장 보편적으로 확산하는데 크게 기여한 웹서비스가 사용하는 공통적인 표현형식인 표준적인 HTML(HyperText Markup Language)은 W3C(World Wide Web Consortium)에서 자발적인 모인 엔지니어들과 서비스사업자들, 학자들에 의해서 합의된 것이 세계적으로 사용되고 있다. 인터넷 교신을 위해서 일반 이용자들이 사용하는 가장 기본적인 주소체계인 도메인이름체계는 2000년 이전까지는 초창기 이를 관리했던 존 포스텔(Jon Postel)에 의해 유지되고 있었으나 인터넷주소관리기구(Internet Corporation for Assigned Names & Numbers,

340) 사단법인 오픈넷 이사장, 녹색소비자연대 이사, 한국인터넷거버넌스협의회 주소인프라분과위원, ehchun@gmail.com

ICANN) 설립 이후에는 여러 이해당사자들의 협의를 통해 최상위도메인의 생성, 유지, 관리, 분쟁조정 등의 작업이 이루어지고 있다. 우리 사회의 경우에는 조금 다른 길을 걸었지만, 대부분의 사회에서 인터넷은 그 나라에서 인터넷관련 기술에 일찍 접근했던 연구자들과 기술자들을 중심으로 한 인터넷협회(ISOC, Internet Society)를 통해 주로 보급되었다.

인터넷의 작동에 필요한 세계적인 협력과 조정이 실제로 이와 같은 분산적이며(decentralization), 상향식(bottom-up)으로 이해당사자들 간의 합의를 거쳐(multistakeholder consensus) 이루어져 왔다는 사실 외에도 인터넷이 웹서비스를 통해 본격적으로 대중화하는 90년대 중반 무렵에는 이미 대부분의 사회가 전기통신사업을 전통적인 국가의 공공부문 독점사업으로 추진하던 것에서 민간의 자본유입과 경쟁을 통해 보다 인프라를 강화하려는 민영화(privatization)로 전환하고 있었다는 점이 중요하다. 바로 그 이유 때문에 인터넷의 상호접속은 국가간 개별 국가망의 접속을 위한 협상을 통해서가 아니라 민간사업자들 간에 다양한 사업파트너와의 협약형태로 이루어졌던 것이다.

전통적인 전기통신서비스가 과거에 전국적으로 설치된 전기통신망에 대한 독점 위에서 제공되었기 때문에 민영화 이후 거의 모든 국가들은, 전기통신시장에 뛰어드는 신규사업자가 경쟁할 수 있도록 하기 위하여, 민영화된 종전 국가독점사업자가 신규 경쟁사업자에 대하여 상호접속의무를 가지도록 기간통신사업자(common carrier) 규제를 도입한다. 그런데 인터넷의 경우에는 특정 물리망에 종속되지 않는다는 특성이 있어 처음부터 기존통신망을 보유하지 못한 사업자의 경우에도 케이블망(catv)과 같은 여타 통신망을 임차할 수 있다면 이 시장에 별다른 어려움 없이 진출할 수 있었다. 이처럼 인터넷접속서비스가 특정 물리망에 종속되지 않는다는 점(인터넷프로토콜[Internet Protocol]은 어떠한 물리망[유무선망, 전화회선, 전용회선, 광케이블, 케이블회선, 심지어 전력선까지]이라도 그 위에서 구현되는 특성을 갖는다), 또한 인터넷의 특성의 하나인 패킷전송은 특정 데이터 전송경로에 국한되지 않을 뿐만 아니라 접속서비스 제공자는 전체 네트워크의 극히 일부만을 보유하고서도 충분히 다른 네트워크와의 연결망을 제공할 수 있다는 특징을 갖는다. 이런 이유에서 인터넷 접속서비스는 누구나 시장에 경쟁적으로 진입할 수 있고, 필수설비가 아니라는 이유에서 대부분의 국가에서는 비규제 서비스(혹은 부가서비스)로 분류되었다.[341]

인터넷서비스가 민간 사업자에 의해 제공되며, 사업자들 간의 경쟁이 가능해 국가의 규제를 받을 필요가 없는 비규제 서비스라는 점 때문에 인터넷망 간의 상호접속 문제는 사업자들 간의 상호협약의 문제로 간주되었고, 따라서 이 문제는 해당 사업자가 속해 있는 국가들 간의 협상의 문제로 다뤄지지 않았다. 2012년 말 WCIT를 둘러싼 논란에서 전통적인 통신(telecommunication) 개념에 인터넷(internet)을 포함시킬 수 있느냐 여부가 민감한 쟁점이 되었던 이유는 근본적으로 국가규제를 받지 않는 민간사업자의 서비스협정을 전통적인 전기통신서비스에 관한 국가간 협상의 대상과 동일하게 다루려고 한 데에 있었다.[342] 따라서 이

341) 2005년 미국 연방대법원의 Brand X 판결은 인터넷접속서비스를 telecommunication service (common carrier로서 국가규제의 대상)가 아니라 information service(국가가 규제하지 아니하는 영역의 서비스)라고 결론지었다. NATIONAL CABLE & TELECOMMUNICATIONS ASSN. V.BRAND X INTERNET SERVICES

342) "ETNO paper on Contribution to WCIT-ITRs Proposal to Address New Internet Ecosystem" http://www.etno.eu/datas/itu-matters/etno-ip-interconnection.pdf WCIT에 제출한 프랑스의 ETNO의 문서는 바로 이 문제를 가장 잘 보여주는 예이다. 이 문제에 대한 프랑스의 시민단체 la quadrature du net의 의견도 참조. http://www.laquadrature.net/wiki/ETNO_contribution_to_WCIT

미 인터넷접속서비스를 민영화하고 비규제로 하고 있는 나라들에게는 국가간 협상을 통해 인터넷을 포함하여 상호접속의 조약[343]을 맺자는 제안 자체는 근본적으로 수용하기 어려운 것이었다. 결국 WCIT 협상의 최종문서는 telecommunication에서 internet을 거의 완전히 제외하였다.

인터넷 거버넌스란 이처럼 실제 오늘날 세계 인터넷이 정상적으로 작동하기 위해서 기본적으로 필요한 기술, 표준, 주소체계, 상호접속 등과 같은 요소들에 대하여 누가 어떠한 원칙위에서 어떤 방식으로 어디에서 어떤 절차를 걸쳐 어떠한 형식으로 의사결정을 이끌어 내느냐 하는 것에 관련된 문제이다.[344]

2. 인터넷주소체계 거버넌스와 ICANN

인터넷 거버넌스와 관련된 논의에서 인터넷 도메인주소 문제가 가장 먼저 논의된 이유는 인터넷이용자들이 범용으로 사용해 오던 .COM, .NET, .ORG와 같은 인터넷 도메인주소를 특정 사업자(Network Solutions)가 독점적으로 운영하면서 상표(trademark)와 충돌하는 문제를 일관성 없이 대처하고 있다는 데에서 시작된 불만 때문이었다.[345] 주소 문제는 여기에서 그치지 않았다. 특정 주권범위 안에서 사용할 수 있도록 할당된 국가코드도메인(ccTLD)의 경우에는 존 포스텔에 의해서 개개인 운영자들에게 배분되었으나 시간이 경과하면서 운영자가 해당 주권영토 밖에 거주하거나 상업 서비스사업자에게 이전되는 경우 등이 생겨나면서 주권 및 사업권의 충돌과 같은 문제들을 낳았다.[346]

인터넷 도메인주소 문제는 특정 사업자의 주소독점 문제와 함께 지적재산권과의 충돌 문제를 포함하고 있었기 때문에 기본적으로는 도메인 분쟁해결정책과 신규 최상위도메인을 얼마나 어떻게 생성하느냐 하는 문제가 가장 중심적인 정책적 문제였다. 이 문제를 해결하기 위하여 초기에는 인터넷협회(ISOC)과 존 포스텔(IANA), IETF/IAB 등이 ITU나 세계지적재산권협회(World Intellectual Property Association, WIPA), 국제상표협회(International Trademark Association, ITA) 등과 함께 IAHC(Internet Ad-Hoc Committee)를 구성하여

---

343) 근본적으로 WCIT은 “International Telecommunication Regulations”로서 전통적인 telecommunication망의 국제적인 접속환경을 규율하기 위해, 인터넷이 대중적으로 보급되지 않았던 1988년에 만든 조약을 개정하기 위한 것이었다. 아래 참조. 이 문서 뒤에 첨부되어 있는 Resolution 3과 5는 인터넷과 관련된 내용을 포함하고 있으나 이들 문서는 본회의의 결의문으로서 구속력을 갖는 ITR 본문과는 별개의 문서이다. http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

344) 제1차 정보사회세계정상회의(WSIS) 이후 유엔 사무총장에 의해 인터넷 거버넌스 문제 논의를 위해 작업을 맡겼던 인터넷 거버넌스 워킹그룹(WGIG, Working Group for Internet Governance) 보고서는 인터넷 거버넌스를 다음과 같이 규정한 바 있다. “Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.” http://www.wgig.org/docs/WGIGREPORT.pdf

345) 1995년에 당시 일반최상위도메인(gTLD)을 운영하던 Network Solutions 사는 독자적인 도메인 분쟁해결정책을 마련하여 도메인 등록 시 이를 준수하도록 하여 법원의 명령이나 중재자의 도메인 이전요청에 대하여 대응하였으나 그렇다고 계속 이어지는 소송을 피할 수는 없었다. p.120 “ruling the root”, Milton Mueller, 2002 The MIT Press

346) 존 포스텔은 일반최상위도메인(gTLD)과 국가코드도메인(ccTLD)의 생성을 RFC1591 (http://www.ietf.org/rfc/rfc1591.txt)에서 밝힌 원칙에 따라 시행하였으나 많은 제한이 있었다. 이에 대해서도 Milton Muller의 윗책 pp.125-127 참조

7개의 새로운 최상위도메인을 제안[347]하면서 여러 이해당사자들을 모아서 gTLD-MoU[348]를 토대로 이에 서명하는 운동을 전개하기도 했다.

그러나 이러한 움직임은 미국연방정부가 존 포스텔이 해오던 IANA의 운영에 대한 근본적인 문제를 제기함에 따라 실패로 돌아갔고[349], 미연방정부 주도로 ICANN을 구성하는 것으로 바뀌었다.

결국 ICANN은 인터넷이 대중적으로 보급되기 시작하는 1995년 이래 꾸준히 문제로 제기되어온 신규 최상위도메인의 생성문제, 도메인 분쟁문제, 기존 gTLD/ccTLD의 법적 지위의 문제와 같은 문제들을 숙제로 안게 되었고, gTLD의 독점 문제는 등록기관(Registry)과 등록대행기관(Registrar)의 분리운영과 신규 최상위도메인의 생성[350]으로 해결해왔고, 도메인 분쟁문제는 UDRP(Uniform Dispute Resolution Policy)[351]로 해결하였다. 그리고 도메인의 운영주체와의 법적 지위문제는 gTLD의 경우에는 ICANN/IANA와 Registry/Registrar 간의 계약으로, ccTLD와의 관계에서는 별도의 협약이나 서신교환방식으로 정비하였다.[352] ICANN은 아직도 신규 최상위도메인의 생성에 따라 빚어질 상표와의 충돌문제 때문에 상표권을 좀 더 보호하기 위한 지적재산권 보호방안(현재 제시되고 있는 지적재산권 clearing house안[353])과 도메인 분쟁해결을 위한 등록자에 대한 정보공개문제[354](whois policy)를 중요한 정책과제로 논의하고 있으나 기본적으로 위와 같은 규칙들을 모든 이해당사자들의 개방적인 참여와 논의를 통해 정비함으로써 인터넷 도메인주소에 대한 실효성있는 거버넌스의 틀로서의 역할을 해온 것이다.

3. 인터넷 거버넌스 논의의 확장과 IGF

그러나 그럼에도 불구하고 ICANN이 인터넷 주소체계에 대한 거버넌스 역할을 수행하는 것에 대해서는 여전히 유보적인 태도가 지속되고 있었는데[355] 바로 이 때문에 2005년 제2차 정보사회세계정상회의(World Summit on the Informaiton Society, WSIS)의 최종합의

---

347) http://en.wikipedia.org/wiki/IAHC 참조
348) http://www.itu.int/net-itu/gtld-mou/gTLD-MoU.htm 참조
349) gTLD-MoU를 주도하던 존 포스텔의 루트서버 이동시도와 이에 제동을 건 백악관의 Ira Magaziner의 에피소드는 pp.80-86, "사이버세계를 조종하는 인터넷권력전쟁", 잭골드스미스, 팀우 지음, 송연석옮김, NEWRUN, 2006년 11월 3일 참조.
350) 다국어도메인 생성 문제는 원래 문화적 다양성 혹은 다양한 언어공동체의 최상위도메인 생성에 대한 동등한 참여라는 차원에서 제기되었으나 IETF의 기술표준 논의과정에서 기존 DNS와의 7bit 호환성에 대한 고려로 인해 8bit 표준을 채택하지 못했으며, 다국어 최상위도메인 생성 문제도 신규 최상위도메인생성 일반정책의 한 부분으로 다루어짐으로써 별도의 정책틀을 구성하지는 못하였다. 다국어도메인에 대한 기술관련 논의에 대해서는 Geoff Huston의 "Internationalizing the Internet", December 2006. http://www.potaroo.net/ispcol/2006-12/idn.html 참조
351) http://www.icann.org/en/help/dndr/udrp/policy 참조
352) 이러한 정비가 이루어지기 전까지는 IANA-gTLD, IANA-ccTLD간의 관계를 규율하는 원칙은 RFC1591이 유일한 것이었다. 이들 계약이나 협약들은 다음 링크 참조
http://www.icann.org/en/about/agreements
353) http://blog.icann.org/2012/11/trademark-clearinghouse-update/ 참조
354) 아래 링크 참조
http://www.icann.org/en/about/learning/webinars/whois-recommendations-implementation-24apr13-en
355) 당시 이에 대한 미국연방정부의 입장은 Condoleezza Rice 국무장관이 EU에 보낸 서한에 구체적으로 나타나 있다. http://www.theregister.co.uk/2005/12/02/rice_eu_letter/ 참조

문서인 튀니스 어젠다(Tunis Agenda)에서는 “인터넷 네이밍과 주소”(58. “internet naming and addressing”)를 향후 논의할 인터넷 거버넌스의 주제에 포함시키게 된다.

실질적으로 ICANN이 인터넷 주소체계에 대한 체계적이고 일관성 있는 정책을 이해당사자들의 합의를 통해 개발하고, 이를 구현하고 있음에도 불구하고 여전히 ICANN의 정당성에 대한 유보가 존재하는 이유는 주소체계에 있어서 가장 핵심적인 역할을 하는 최종 루트 서버에 대한 운영권한이 여전히 미연방정부에 있으며[356], 인터넷주소체계에 대한 ICANN의 자율적인 조정역할도 여전히 미상무부의 감독을 받는 구조[357]를 갖고 있기 때문이다.

이러한 이유에서 제2차 WSIS 이후에도 유엔은 인터넷 주소체계의 문제를 비롯하여 여타 인터넷에 관련된 공공정책문제를 논의하기 위한 터전으로 인터넷거버넌스포럼(Internet Governance Forum, IGF)을 개최하기 시작하였다. IGF의 출발은 인터넷 주소체계와 관련된 문제 논의에서 시작하였으나, WSIS의 합의에 따르면 인터넷 주소체계 문제 외에도 다양한 인터넷 관련 공공정책 문제들을 관련 이해당사자 및 유관 국제기구, 개발도상국 등의 적극적인 참여를 통해서 논의하도록 하고 있었다.[358]

실제로 IGF에서 논의된 주제들은 ICANN이 다루고 있는 과제인 신규 최상위도메인 생성 문제, IANA function과 미연방정부와의 계약문제와 같은 인터넷 주소체계에 관한 문제 뿐 아니라 인터넷 안전(Safety)문제, 보안(Security)문제, 네트워크/사이트 차단 및 프라이버시 문제, 표현의 자유문제, 인터넷 접속권(Internet Access Rights)문제, 지적재산권 문제, 개발(Internet Governance for Development) 문제, 이동통신 단말기와 플랫폼문제 등 다양한 주제들을 광범하게 다루어왔다.[359]

---

356) IANA function이란 유일한 궁극의 루트 서버를 운영하면서 그 서버 안에서 최상위 도메인들의 ip주소를 기록하고 있는 root zone file을 업데이트하는 권한을 말하는 것인데 이것은 인터넷 초기부터 존 포스텔에 의해서 유지되어 오다가 ICANN이 설립된 이후 2000년 2월 9일부터는 ICANN과 미연방정부 NTIA와 계약으로 지속되어 오고 있다. 가장 최근에는 2012년 11월 10일 NTIA가 IANA의 공개입찰 RFP를 공표한 바 있는데, 그에 따르면 IANA 계약당사자는 미국이 소유하고 운영하는 업체나 미국이 승인한 대학이나 미국 내에 상장된 법인으로서 주법에 따라 설립된 업체로 자격을 제한하고 있다.
http://www.ntia.doc.gov/files/ntia/publications/sa1301-12-rp-0043-_final_04.16.2012.pdf Section C.2.1 참조

357) ICANN 설립초기부터 미상무부는 Memorandum of Understanding(1998-2006/9/30), Joint Project Agreement(2006-2009/9/30), Affirmation of Commitments (2009- no expiration date)로 일정 시기마다 형식을 바꾸면서 ICANN과 상무부와의 관계를 규정해왔는데 이들 협약문에서는 항상 DNS의 기술적인 조정권한을 언젠가는 민간부문으로 이전하는 것이 미상무부의 정책목표라고 기술하고 있다. 현재의 AoC에서는 “in recognition of the conclusion of the Joint Project Agreement and *to institutionalize and memorialize the technical coordination of the internet’s domain name and address system(DNS), globally by a private sector led organization*”라고 기술되어 있다.
http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm

358) WSIS의 최종합의문인 Tunis Agenda의 72.번 참조, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html 특히 아래 다섯 항목은 IGF의 임무가 주소체계 외에도 다양한 인터넷관련 공공정책 영역들을 망라하도록 범위를 설정하고 있다.
a. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
b. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
g. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
j. Discuss, inter alia, issues relating to critical Internet resources.
k. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.

다른 한편, IGF가 인터넷과 관련된 다양한 공공정책 문제에 대해 논의를 하기는 하지만, 실효성 있는 어떠한 결정도 할 수 없는 담론의 장이라는 점에서 본질적인 한계를 안고 있다.[360] 이러한 한계를 극복하기 위하여 유엔 경제사회이사회(ECOSOC)는 IGF의 개선을 위한 작업반을 구성하여 개선방안을 제안하도록 하였는바, IGF를 실질적으로 준비하는 현행 멀티스테이크홀더 자문그룹(Multistakeholder Advisory Group, MAG)의 선출과정을 좀 더 체계화하고, IGF 회의의 준비과정이나 실제 회의진행의 기록, 보고서의 작성 등을 정비하도록 했으며, 사무국을 강화하고 재원조달을 강화하도록 건의한 바 있다.[361] 다른 한편 ECOSOC은 이와 함께 원래 IGF의 과제였던 '강화된 협력'(enhanced cooperation)에 대한 보다 포괄적인 의견수렴을 위해 이를 위한 작업반을 구성하여 설문조사를 실시하고 이에 대한 보고서를 준비 중이다.[362]

이러한 개선노력과 함께 2013년 10월 발리 IGF에서는 MAG이 사전에 제출된 여러 워크샵 주제들을 주요 주제들을 중심으로 통합하는 방식을 취하여 좀 더 집중적인 논의를 하도록 하였고, 추후 해당 정책과제에 대한 논의를 Dynamic Coalition[363]으로 계속 이어가고 있다.

이처럼 인터넷 거버넌스 관련 정책 과제들에 대하여 실질적인 논의의 진전을 이루고 있지 못하다는 부담을 안고는 있으나, 다른 한편 IGF는 인터넷 관련 공공정책에 대하여 이해당사자들이 개방적으로 참여하여 논의를 진행시키고 있는 유일한 플랫폼으로 정착되어 가고 있다.[364]

4. 인터넷 주소체계 외의 인터넷 거버넌스 정책과제들

ICANN과 IGF에서의 인터넷관련 정책과제들이 논의되고 있는 것과는 별개로, OECD는

---

359) 2012년 IGF 회의 보고내용 참조 http://www.intgovforum.org/cms/2012-igfbaku

360) 이러한 이유에서 2011년 인도, 브라질, 남아프리카공화국은 공동으로 인터넷공공정책을 다루는 기구를 유엔안에 두자는 제안을 하기도 했고, 인도는 이러한 논의의 연장선 상에서 유엔인터넷정책위원회(UN Committee for Internet-Related Policies - CIRP)를 제안하기도 했다. (http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf 과 http://igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp 참조)

361) Report of the Working Group on Improvements to the Internet Governance Forum, UN ECOSOC 16 March 2012, http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf IGF가 인터넷 거버넌스에 대한 실질적 논의를 진전시키지 못하고 현상유지에 머무르고 있다는 비판과 이 작업반의 보고서에 대한 평가는 Milton Mueller, "IS THERE ANY HOPE FOR THE INTERNET GOVERNANCE FORUM?", July 30, 2012 참조 http://www.internetgovernance.org/2012/07/30/is-there-any-hope-for-the-internet-governance-forum/

362) UNCSTD의 WGEC(working group for enhanced cooperation)의 구성 및 배경에 대해서는 https://www.apc.org/en/blog/un-working-group-enhanced-cooperation-report-secon 참조. WGEC의 설문조사결과에 대한 최근의 분석자료는 다음 링크 참조 http://unctad.org/meetings/en/SessionalDocuments/WGEC_Summary_of_Responses.pdf

363) Dynamic Coalition은 2006년 첫 IGF 회의 때부터 구성해 왔는데 현재까지 주제별로 총 11개의 dynamic coalition이 구성되어 있다. http://www.intgovforum.org/cms/dynamiccoalitions 참조

364) 현재 2014년에는 터키의 이스탄불, 2015년에는 브라질, 2016년에는 멕시코로 회의 개최국이 정해졌다. 이것은 간접적으로 IGF가 실질적으로 인터넷관련 공공정책에 대한 개방적인 논의의 장으로서 안정적으로 작동하고 있음을 의미한다.

꾸준히 인터넷 관련 공공정책에 대한 입장들을 천명해왔고[365] 특별히 인터넷 보안(security)[366]과 관련된 문제에 대해서는 영국이 시작한 사이버스페이스 총회(Cyberspace Conference)가 별도로 이에 관한 논의를 전개해 왔다.[367]

다른 한편 2013년 5월에 열린 ITU의 세계전기통신정책포럼(World Telecommunication/ICT Policy Forum, WTPF) 회의[368]는 다시 인터넷 관련 공공정책을 어떻게 논의할 것인가 하는 문제를 주제로 다루었는데, 실제로는 의사결정에 있어 다자간 논의방식(multi-lateral 혹은 inter-governmental 방식)과 이해당사자들의 개방적인 참여방식(multi-stakeholder participation)에 대한 논의가 주축을 이루었다.

그런데 WTPF 회의에서 좀 더 명확해진 것은 기존의 이해당사자의 개방적 참여모델에 따른 인터넷 거버넌스 구조가 협력과 조정의 대상[369]이라는 점과 다자간 논의방식을 통해 논

---

365) OECD가 2012년 초 채택한 "인터넷 정책결정에 관한 원칙"(OECD Council Recommendation on Principles for Internet Policy Making, 13 December 2011) 문서는 이해당사자의 참여원칙을 비롯하여 인터넷중개사업자(ISP)의 책임제한 등 가장 기본적인 정책원칙들을 규정하고 있다. 이 문서에서 합의된 내용은 향후 인터넷 거버넌스 원칙수립에 있어서도 기본적인 논의의 기반이 될 것이다. http://www.oecd.org/sti/ieconomy/49258588.pdf 참조

366) 인터넷 보안(security)문제에 대해서는 이미 1988년부터 유엔에서 논의가 시작되어 2010년에 17개 국가 전문가들이 기초적인 원칙에 대하여 합의한 문서("Developments in the Field of Information and Telecommunications in the Context of Internet Security"-약칭 GGE[Group of Government Experts] Report라고 칭함)가 있다. http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf 참조. 그러나 이 문서에서 합의된 내용은 신뢰구축, 정보교환, 역량구축 등 가장 기본적인 수준의 합의에 지나지 않는다.
"(i) Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;
(ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
(iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
(iv) Identification of measures to support capacity-building in less developed countries;
(v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25." 위 문서의 recommendation 부분

367) 2013년 서울 사이버스페이스 총회가 채택한 "Seoul Framework for and Commitment to Open and Secure Cyberspace" 문서 내용 http://www.seoulcyber2013.kr/en/media/View.do?media_id=2242 참조. 이 문서는 본질적으로 앞의 GGE 보고서 및 OECD, G8 회의 등에서 확인한 내용들을 재확인한 것에 지나지 않는다. 다만 영국에서 시작된 사이버스페이스 총회는 미흡하나마 이해당사자들의 개방적 참여라는 원칙을 유지해 왔다는 점에서 여타 국제적인 논의와 차이가 있다.

368) WTPF 회의는 ITU의 전권회의(Potentiary Conference)의 위임에 따라 특정 정책사안에 대하여 논의하는 구속력 없는 협의의 장이다. 2013년 5월의 WTPF 회의가 특히 주목을 받은 것은 2012년 말 WCIT 회의에서 다시 추후 인터넷관련 논의를 할 것을 결의안으로 채택한 데 이어 이 문제를 본격적으로 다루는 회의로 부각되었기 때문이다.

369) "•*On the basis of reciprocity, to explore ways and means for greater collaboration and coordination between ITU and relevant organizations* – including, but not limited to, the Internet Corporation for Assigned Names and Numbers (ICANN), the Regional Internet Registries (RIRs), the Internet Engineering Task Force (IETF), the Internet Society (ISOC) and the World Wide Web Consortium (W3C) – involved in the development of IP-based networks and the future internet, through cooperation agreements, as appropriate, in order to increase the role of ITU in Internet governance so as to ensure maximum benefits to the global community." THE ITU SECRETARY-GENERAL'S REPORT for the Fifth World Telecommunication/Information and Communication Technology Policy Forum 2013, http://www.itu.int/md/S13-WTPF13-C-0003/en 참조

의해야 할 인터넷 관련 정책과제들[370]이 좀 더 구체적으로 제시되었다는 점이었다.

현재 ECOSOC은 2014년 4월 이집트에서 열릴 예정인 WSIS+10 고위급회의(WSIS+10 High Level Event)를 전후로 WSIS의 후속작업에 대한 평가와 함께 '강화된 협력 워킹그룹'(WGEC)의 결과물을 취합하여 총회에 보고할 예정[371]이며, ITU는 WTPF 회의의 결과를 포함하여 2014년 10월 부산에서 열릴 예정인 ITU 전권회의에서 이에 대한 후속논의를 이어가게 된다.[372]

IGF는 이미 인터넷 주소체계 이외의 인터넷 관련 공공정책 과제들을 다양하게 논의해 왔고, IGF에서도 반복해서 중요한 과제로 제시되었던 인터넷 보안문제는 또 다른 이해당사자들의 논의의 장인 사이버스페이스 총회에서 논의를 이어가고 있다. 또한 이미 2012년 WCIT에서의 논의과정에서 인터넷 상호접속 문제를 중심으로 한 정책과제들이 의제로 제시된 바 있었으며, 2013년 WTPF 회의 역시 인터넷의 기술표준이나 주소체계에 관련된 정책과제와는 별도로 인터넷 관련 공공정책 과제들을 제시한 바 있다. 이러한 흐름 속에서 인터넷 기술표준이나 주소체계와 같은 정책과제가 아닌 여타 인터넷 공공정책 문제를 논의해서 어떤 결정으로까지 나아갈 수 있는 논의의 장이 필요하다는 인식[373]은 공감대가 형성되었으나 현재까지는 그러한 논의의 장이 이해당사자들 간의 개방적 참여방식(multistakeholderism)으로 구성되어야 하는 것인지, 다자간 협의의 틀(multilateral 혹은 intergovernmental decision making)로 구성되어야 하는 것인지 국제사회의 합의를 이루지 못하고 있다.

5. 인터넷 거버넌스의 세계화와 브라질 회의

앞에서 이미 설명한 바 있지만 ICANN을 통해 이루어지고 있는 인터넷 주소체계에 대한 정책수립 및 집행과 관련하여 IANA function 및 ICANN에 대한 감독권한이 미연방정부에 종속되어 있다는 점은 여전히 국제사회의 이에 대한 유보적 태도를 유지시켰고, 2013년 미국 국가안보국(NSA)의 대량감청에 대한 스노든의 폭로는 인터넷 거버넌스에 대한 미연방정부의 신뢰를 근본적으로 훼손하는 중요한 계기가 되었다.

브라질 대통령 지우마 루세프(Dilma Rousseff)의 유엔총회 연설[374]은 이 문제에 대한 가

370) 이러한 정책들로서는 인터넷 상호접속문제인 IXP(Internet Exchange Point) 문제, 인터넷 인프라 투자 및 관련정책 강화문제, IPv6의 전환정책 및 역량강화문제, 이해당사자 참여(multistakeholderism)문제 및 협력강화(Enhanced Cooperation) 문제 등이 정책과제로 제시되었다. 위 WTPF 사무총장 보고서 Annex B:Draft Opinions 부분 참조

371) UNCSTD WGEC의 결과물은 그 상위기구인 ECOSOC에 보고되며 ECOSOC은 이를 토대로 2014년 9월에 열리는 제69차 UN총회의 제2위원회(Second Committee)에 최종 보고서를 제출하게 된다.

372) 이러한 인터넷가버넌스 일정 전반에 대해서는 http://bestbits.net/wp-uploads/diagram.html 참조

373) 이처럼 인터넷의 정상적인 운용과 진화발전을 위해서 세계적인 조정이나 협력이 필요한 정책 사안이지만 적합한 논의의 장이 마련되고 있지 못한 정책 사안들을 일컬어 orphan issues라고 지칭한다. orphan issue의 범위에 대해서는 다양한 의견들이 존재하지만 Chris Marsden 같은 학자는 IPv6나 상호접속 문제 외에도 사물인터넷("the internet of Things")이나 망중립성/Over the Top 서비스와 같은 주제들을 포함할 수 있다고 본다. Chris Marsden, "Internet Governance Series: The Road from Bali to Rio… to Dystopia?" http://blogs.lse.ac.uk/mediapolicyproject/2013/10/31/internet-governance-series-the-road-from-bali-to-rio-to-dystopia/ 참조

374) 지우마 루세프(Dilma Rousseff)의 2013년 10월 유엔총회 연설문 참조.

장 대표적인 비판으로서 여러 나라들의 반향을 받았다. 지우마 대통령은 이 연설에서 NSA의 대량감청이 인권에 대한 침해이자 주권국가에 대한 무례라고 비난하면서, 그러나 정보통신기술이 국가들의 또 다른 전장이 되어서는 안 되며, 이를 위해 사이버공간을 전쟁무기로 사용하지 못하도록 해야 한다고 주장했다. 지우마 대통령은 그러한 구체적인 방안의 하나로 "인터넷 가버넌스와 인터넷 이용을 위한 민간차원의 다자간 협력틀"("civilian multilateral framework for the governance and use of the internet")을 창설할 것을 제안했다.[375]

다른 한편, 이제까지 인터넷의 기술표준 및 인터넷 주소체계에 대한 정책수립과 운영을 담당해온 기구들[376]은 2013년 10월 우루과이에서 모여 스노든의 NSA 대량감청에 대한 폭로를 계기로 훼손된 신뢰를 회복하기 위하여, 미연방정부 중심의 인터넷 주소체계 거버넌스의 틀을 세계화해야 한다는 내용을 핵심으로 하는 몬테비데오 선언[377]을 공표하였다.

ICANN의 CEO 파디(Fadi)는 몬테비데오 선언 직후 브라질을 방문하여 대통령과 면담하면서 브라질의 지우마 대통령이 유엔총회 연설에서 제안한 "민간차원의 다자간 협력틀"에 대한 구상을 구체화할 것을 요청하는 한편, 그 논의에서 몬테비데오 선언에서 천명된 입장을 포함[378]하고, 그간 세계 인터넷 거버넌스 논의를 통해서 다양하게 제시되어온 인터넷 주소체계 이외의 인터넷 거버넌스 정책 사안들(혹은 앞에서 말한 orphan issues)에 대한 논의의 틀을 구성하는 문제를 함께 논의할 수 있는 회의를 개최해 줄 것을 요청하였고 브라질 대통령은 이를 수락했다.

지난 달 말 브라질 정부는 두 차례에 걸쳐서 "브라질 회의"(Global Multistakeholder Meeting on Internet Governance, GMMIG) 준비 일정과 내용에 대하여 세부적인 내용을 밝혔다.[379][380]

---

http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

375) 지우마 대통령은 이 연설에서 아주 구체적으로 이러한 민간 다자간 협력틀이 다음과 같은 원칙위에서 수립되어야 한다고 제시했다.
"1 - Freedom of expression, privacy of the individual and respect for human rights.
2 - Open, multilateral and democratic governance, carried out with transparency by stimulating collective creativity and the participation of society, Governments and the private sector.
3 - Universality that ensures the social and human development and the construction of inclusive and non-discriminatory societies.
4 - Cultural diversity, without the imposition of beliefs, customs and values.
5 - Neutrality of the network, guided only by technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes."

376) 몬테비데오 선언에는 RIRs, IETF, IAB, W3C, ISOC, ICANN이 참여하였다. 이러한 기구들은 포괄적으로 I*(star) organizations 혹은 technical community라고 지칭된다.
http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm 참조

377) 이 선언에서는 인터넷 주소체계 거버넌스에서 핵심적인 IANA/ICANN에 대한 감독권한을 세계화하는 문제에 대하여 "이해당사자 참여방식에 의한 세계화"("the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing.")를 주장하였다.

378) 현재 IANA contract와 ICANN의 AoC를 어떻게 개정할 것인지에 대해서는 구체안이 제시된 적은 없지만, ICANN CEO 파디는 여러 곳에서 이러한 계약의 당사자가 미연방정부가 아니라 "세계 이해당사자 집단"(Global Multistakeholder)이어야 한다고 주장하고 있다. 파디가 ICANN Webinar에서 자신의 견해를 설명한 http://audio.icann.org/ig-1900-08nov13-en.mp3 참조. 이 문제를 ICANN의 membership의 문제로 분석한 Milton Mueller의 "A CONTRACT WITH YOU" November 5, 2013
http://www.internetgovernance.org/2013/11/05/a-contract-with-you/ 도 참조.

379) 공식 기자회견문은 http://www.nic.br/imprensa/releases/2013/rl-2013-62.htm 참조, 보다 구체적인

- 회의의 명칭은 세계인터넷거버넌스회의(“Global Multistakeholder Meeting on Internet Governance”)로 한다.

- 회의 일정은 2014년 4월 23일과 24일 양일간 상파울로에서 개최한다.

- 회의의 목적은 1) 인터넷 거버넌스에 대한 보편적 원칙과, 2)인터넷 거버넌스의 제도적 틀을 개선하기 위한 방안, 3) 그러한 제도적 틀로 나아가기 위한 로드맵에 대한 합의를 도출하는 것이다.

- 인터넷 거버넌스 원칙과 이해당사자 참여방식에 따르는 제도적 틀 두 가지에 대한 최종 공동선언문을 발표한다.

- 내부검토와 제안문을 다듬는데 걸리는 시간 최소 60일을 고려하여, 제안서는 2014년 3월 1일을 제출 마감시한으로 한다. 누구나 어떤 집단이나, 이때까지 위 회의목적에 관련된 제안을 할 수 있다.

- 여러 제안들 중의 하나로 ICANN의 “인터넷의 미래에 관한 전략패널”은 서던캘리포니아대학(The University of Southern California)/아넨버그재단(Anenberg Foundation)과 세계경제포럼(the World Economic Forum)과 함께 협력하여 “인터넷 거버넌스 원칙과 제도적 틀에 대한 제안문”을 제출하며, 그 최종제안서 제출시한은 2월말까지로 한다.

- 회의에는 정부, 시민사회, 학술분야, 국제기구, 기술자 집단 및 사업자 집단이 모두 참여한다.

- 회의 전체는 브라질 인터넷 운영위원회(Brazilian Internet Steering Committe, CGI.br)가 담당하며, 정보정책을 담당하는 Virgílio Fernandes Almeida 교수가 관장한다. 전체 운영위원회(global multistakeholder steering committee)는 브라질 CGI와 브라질정부, 1net의 대표자(기술자집단, 학술집단, 시민사회, 사업자집단 포함)가 함께 참여한다.

- 회의 운영을 위하여 집행운영위원회(Logistics and Organizational Committee)를 비롯하여 4개의 위원회를 둔다. 집행운영위원회는 전적으로 브라질 CGI가 운영한다. 정부자문위원회(Government Advisory Committee)는 정부 참가자들의 의견을 수렴한다. 정부자문위원회는 브라질 외무부의 베네딕토 대사(Ambassador Benedicto)가 관장한다. 고위이해당사자위원회(High Level Multistakeholder Committee)는 모든 이해당사자들의 관련 정책 사안에 대한 의견을 수렴한다. 이 위원회는 8명의 정부 고위급인사와 8명의 중견급 인터넷 관련 인사들로 구성한다. 실무적인 운영을 위해 이해당사자 실무위원회(Executive Multistakeholder Committee)를 둔다. 실무위원회는 회의 의제 설정, 초청자 관리 및 전체회의 기록을 담당하며, 2014년 3월 1일까지 제

세부내용은 지난달 18일 브라질정부와 1net.org의 Adiel Akplogan가 협의한 내용을 참조. https://nro.net/pipermail/i-coordination/2013-November/000077.html

380) 브라질 회의는 브라질 쪽(CGI.br과 브라질정부)과 인터넷 이해당사자 집단 두 축에 의해 준비되고 있는데 이 이해당사자 집단은 몬테비데오선언을 주도한 I* 그룹들(혹은 기술자집단, 혹은 이들 집단의 coalition이라고 부름)을 주축으로 하여 시민사회단체들과 사업자집단 등을 포함하여 구성된다. 이 후자의 이해당사자 집단은 브라질회의를 위한 정보 및 의견교환을 위해 1net.org라는 사이트에 메일링리스트를 구축했으며 이 메일링리스트는 AFRINIC에 의해 운영되고 있다. http://1net.org/ 참조

출된 여러 제안서들을 하나의 제안서로 통합하는 작업을 담당한다. 실무위원회는 6명의 정부대표자와 6명의 인터넷관련 이해당사자 집단 대표로 구성한다. 인터넷관련 이해당사자 대표는 사업자집단, 시민사회, 기술자집단 각 2명씩 할당하여 구성한다.

- 회의진행에 소요되는 전체비용은 브라질정부가 담당한다.

결국 브라질 회의에서는 현재 인터넷 주소체계에 대한 거버넌스를 담당하는 ICANN의 IANA function 및 ICANN 감독과 관련된 현행 계약구조의 세계화 방안과 함께, 이제까지 산발적으로 논의되어 왔던 인터넷 기술표준 및 주소체계 문제와는 별개의 인터넷관련 정책사안들을 이해당사자 참여원칙에 따라 논의할 수 있는 제도적 틀을 구성하는 방안을 집중적으로 논의하게 될 것이다. 그리고 그 가장 토대가 되는 제안은 아마도 ICANN의 "인터넷 협력의 미래를 위한 전략패널"(Strategic Panel on the Future of Global Internet Cooperation)이 2월말까지 제출할 문서에서 제시될 것으로 보인다. 이 패널은 2013년 12월 12일과 13일에 영국 런던에서 첫 회의를 가지며 2014년 초까지 제안서 초안을 작성, 공표하고 이에 대한 의견을 수렴할 것이라고 밝혔다.[381]

6. 맺음말

인터넷의 운용에 관한 공공정책을 누가 어디에서 어떤 방식으로 어떤 원칙에 따라 조정하고 의사결정을 하느냐 하는 인터넷 거버넌스의 문제는 단지 이해당사자 집단의 개방적 참여를 통해서 하느냐 혹은 정부간 다자간 협력구도에서 결정하느냐 하는 선호에 따르는 단순한 선택의 문제는 아니다. 이미 인터넷의 기술표준이나 주소체계에 대해서는 이해당사자 집단의 개방적 참여를 통해 정책결정이 이루어지고 있고, 그러한 결정에 대한 인터넷 이용당사자들에 의한 선택과 수용이 이루어지고 있기 때문이다. 현재 인터넷 주소체계를 다루는 거버넌스 구조가 미연방정부의 독점적 감독권한에 의존하고 있어서 그 정당성에 대한 문제는 꾸준히 제기되어 왔고 개선방안이 논의되어 왔고 또 새롭게 개선방안이 모색되고 있으나, 그렇다고 해서 현재와 같은 인터넷 주소체계의 거버넌스 구조가 근본적으로 뒤바뀔 수 있을 것으로 보이지 않는다.

그러나 지금까지 인터넷의 안정적인 운용을 위해 국제사회가 협력하고 조정해야 할 정책사안은 계속 새롭게 제기되고 있다. 이러한 사안에는 표현의 자유/프라이버시, 인터넷 보안(security), 인터넷상 호접속, IPv6, 인터넷 인프라 투자 및 개발, 사물 인터넷(Internet of Things), 망중립성과 응용서비스(Over the Top application services) 등이 제시되고 있다. 이러한 인터넷 관련 정책사안들은 사안에 따라 유엔인권위원회나 OECD, ITU/WTPF, IGF, 사이버스페이스 총회 등에서 다양하게 논의되고 있으나, 현재는 모두 공통적으로 어떤 합의를 통해 실질적인 정책결정에 이르지 못하고 있다는 문제를 안고 있다. 브라질 회의는 이처럼 새롭게 대두하는 다양한 인터넷 관련 정책 사안들을 어떠한 원칙과 어떠한 제도적 틀 안에서 다룰 수 있을지에 대하여 이해당사자간 합의를 이루어 보고자 하는 회의이다. 이 회의는 또한 인터넷 거버넌스 논의에서 처음으로 이해당사자들과 정부대표자들이 공동으로 동등하게 참여하여 그러한 합의를 도출하고자 하는 회의이기도 하다.[382]

---

381) "인터넷협력의미래를 위한 전략패널"의 구성과 향후 계획에 대해서는 해당 링크 참조.
http://www.icann.org/en/news/announcements/announcement-2-17nov13-en.htm

정부는 정부대로 이해당사자들은 이해당사자들대로 이러한 다양한 인터넷관련 정책과제들에 대한 세계적 합의를 유도해 낼 수 있는 거버넌스 원칙과 제도적 틀에 대한 유효하고도 실질적인 의견을 정리해야 할 때이다.

382) 2003년과 2005년의 WSIS 회의 역시 유엔 총회가 이해당사자들의 참여원칙을 요구하였으나 실질적으로는 정부대표자들이 여타 이해당사자들의 의견을 참조만 하고 배타적으로 정부대표자들만이 의사결정을 하는 전통적인 유엔의 의사결정방식을 그대로 따르는 데에 머물렀다.

ABSTRACT

A Glimpse into Brazil Conference

Chun Eung Hwi[383)]

This short report introduces the general background why Brazil conference is being prepared and what topics would be undertaken and what goals are being taken into account.

It overviews what differences from traditional telecommunication governance, internet governance has had in its historical development and how such differences had been formed from its technological differences and the regulatory policy shift from common carrier regulation to privatization. Moreover, the fact that open, voluntary, bottom-up, diverse stakeholder's participation had evolved throughout the historical development of the internet, had established the present multistakeholder governance model from technological standardization to addressing scheme policies. ICANN, which has governed internet addressing schemes since the earlier 2000s, had developed address policies including IANA function from Jon Postel and technical community's legacy management system into contract based formation between ICANN and gTLD, ccTLD registries. And it made dispute resolution policies responding to trademark disputes and resolved gTLD monopoly issue by introducing new TLD generation and the separation of registry and registar. However, there had been challenges on the legitimacy of ICANN due to its dependency on the Federal Government of the U.S. particularly in its oversight role over ICANN and IANA contract.

WSIS raised up internet governance issues including addressing governance, and set up IGF as a discussion platform for multistakeholders to discuss and share all views on other internet related public policies. IGF's loose and non-binding discussion once frustrated governments and other stakeholders, but more focused discussion and visible outcomes have consolidated its unique role for internet governance discourses. Particularly, IGF addressed many emerging internet related issues like cybersecurity, privacy, net neuratlity, development related issues. WTPF of 2013, after WCIT debate on whether traditional telecommunication regulation could be applied to internet infrastructure, suggested other governance issues such as the transition to ipv6, IXP coordination etc.

---

383) Chairperson of OpenNet Korea

How to make sure the legitimacy of internet addressing governance and how and where other internet related public policies could be undertaken are fundamental tasks for internet governance. Brazil conference, which has been motivated by the breakdown of trust in internet governance from NSA mass surveillance revealed by Snowden, faces these questions and try to make consensus on principles, institutions and roadmap for internet governance in multistakeholder participation way.

사이버스페이스란 무엇인가?

필자 전길남[384]
번역 전응휘

1. 들어가는 말

사이버스페이스는 2010년대 초부터 주목을 받기 시작했다. 이 무렵에 컨퍼런스도 많이 열렸고 관련 기구들도 많이 생겼다. 이 글은 그때 열렸던 컨퍼런스나 단체에서 논의했던 사이버스페이스 거버넌스 문제를 포함해서 사이버스페이스 문제를 좀 더 규명해 보려는 목적에서 쓰여졌다.

사이버스페이스는 1980년대부터 언급되었는데 윌리엄 깁슨(William Gibson)의 "뉴로맨서"도 그 한 예이다. 여러 곳에서 사이버스페이스는 인터넷이라는 말과 유사하게 사용되었고 인터넷 문화나 인터넷 응용프로그램 등을 지칭하기도 했다.

2010년에는 미국백악관이 사이버스페이스 국제 전략이라는 제목의 보고서를 발표했다. 미연방정부는 육상, 해양, 공중, 외계에 이어 다섯 번째 영역으로 사이버사령부를 창설했다. 유럽연합과 영국정부도 유사한 기구를 잇달아 만들었다. 이런 움직임 때문에 사이버스페이스나 사이버전쟁이란 말이 세계적으로 주목을 받게 되었다.

2010년대 초에는 사이버스페이스를 가장 중요한 주제로 삼는 컨퍼런스나 기구들이 여럿 생겨났다. 이 중에서 몇 가지만 들어본다면, 다음과 같은 것들이 있다.

- 하버드-MIT가 공동으로 만든 사이버국제관계연구회(Explorations in Cyber International Relations, ECIR)는 여러 차례 워크샵을 가졌는데 그 중의 하나는 "누가 사이버스페이스를 통제하는가?"를 주제로 했다.
- 토론토대학 캐나다세계안보연구센터가 주최하는 사이버 다이얼로그 컨퍼런스(Cyberspace Dialogue Conference)
- 2011년 런던에서 시작한 연례 국제 사이버스페이스 총회(International Cyberspace Conference)

사이버스페이스를 주제로 하는 이러한 여러 행사들은 사이버스페이스가 갖고 있는 여러

384) 한국과학기술원 교수, 일본 게이오대학교 교수, chonkn@gmail.com

측면 중에서도 특히 사이버안보(cyber security)에 초점을 맞추고 있다.

2. 사이버스페이스

2.1 사이버스페이스, 리얼스페이스(real), 혼합스페이스(mixed)

리얼스페이스는 우리가 사는 물리세계인데 반하여 사이버스페이스는 전형적으로 인터넷에 기반한 가상공간이다. 그런가 하면 사이버스페이스와 리얼스페이스 두 가지가 중첩되는 혼합스페이스도 있다.

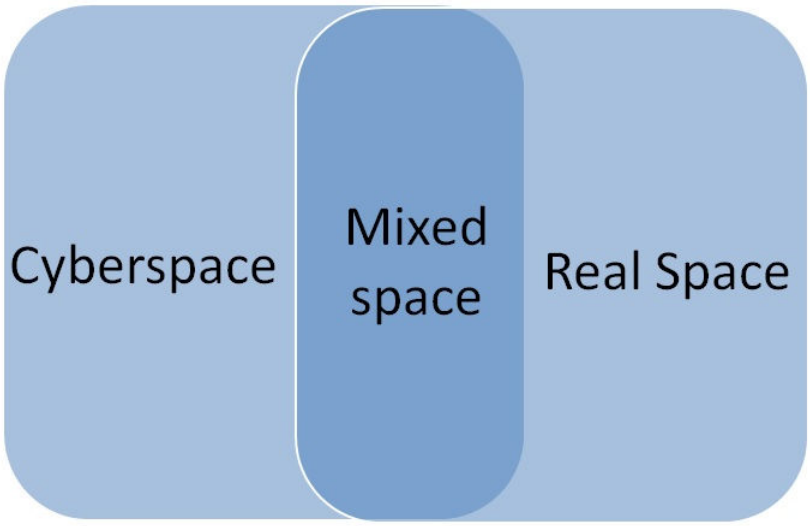

그림 11 사이버스페이스/혼합스페이스/리얼스페이스

이 혼합스페이스 중에 어떤 것은 센서기반 네트워크 시스템과 같은 사이버물리시스템도 있는데 이 경우에는 인터넷을 쓰는 경우도 있지만 쓰지 않는 경우도 있다. 인터넷에 기반하는 공간들은 대부분 리얼스페이스를 배제하는 순수한 사이버스페이스이기 보다는 이러한 혼합스페이스인 경우가 많다.

2.2 사이버스페이스와 인터넷

사이버 사회나 사이버 보안과 같은 사이버스페이스는 대부분 인터넷을 하부구조로 하고 있다. 그러나 어떤 사이버스페이스는 인터넷과는 분리되어 있는 일반전화시스템이나 센서기반의 네트워크 시스템이나 인터넷과는 분리되어 있는 텔레비전과 같은 것들도 있다. 어느 경우이든 사이버스페이스에는 사이버 사회나 사이버 보안, 사이버 경제, 사이버 환경과 같은 여러 측면들이 있다.

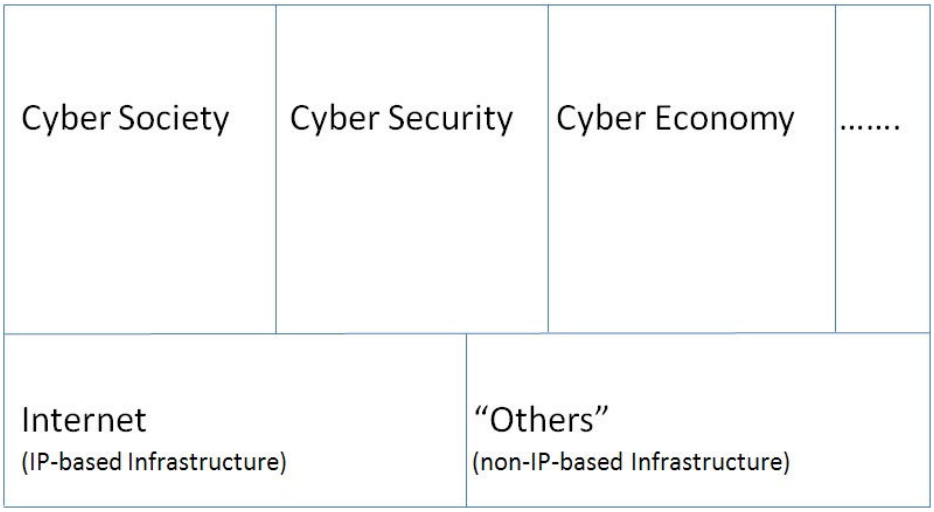

그림 12 사이버스페이스의 여러 측면들과 그 하부구조

3. 사이버스페이스의 여러 측면들

사이버스페이스는 관점에 따라 다양한 측면들을 보여준다. 데이빗 클라크(David Clark)는 사이버스페이스를 보는 세 가지 관점"("Three Views of Cyberspace")이라는 자신의 논문에서 다음 세 가지 관점을 제안했다. [Clark 2011]

- 사이버 안보
- 사이버 경제
- 사이버 사회

앤서니 기든스(Anthony Giddens)는 "세계화의 네 가지 차원"("Four Dimensions of Globalization")이라는 자신의 논문에서 세계화가 가지는 네 가지 측면을 제시했는데 가브리엘라 테자다(Gabriela Tejada)는 여기에 다섯 번째 차원을 추가했다. [Tejada 2007, Giddens 1991]

- 세계자본주의경제(World Capitalist Economy)
- 국민국가체제(Nation-State System)
- 세계군사질서(World Military Order)
- (국제)노동의 분화([International] Division of Labor)
- 문화(Culture)

이를 토대로 나는 다음과 같은 측면들을 제안하고자 한다.[Chon 2012]

- 사이버 사회
- 사이버 안보

- 사이버 경제
- 사이버 국민국가들
- 사이버 환경

물론 사이버 교육이나 사이버 미디어 혹은 사이버 노동과 같은 여러 측면들도 생각해 볼 수 있다.

3.1 사이버 사회

사이버 사회는 사이버 문화를 포함하는데 유사한 문제들을 안고 있다는 점에서 인터넷에 가장 가깝다고 할 수 있다. 사이버 사회의 거버넌스는 당연히 인터넷 거버넌스에 가장 가깝다. 이 둘은 프라이버시나 개인차원의 보안, 오남용, 몰입이나 폭력과 같은 여러 사회문제들을 안고 있다. 사이버사회와 사이버문화는 콘텐츠의 여러 측면들을 모두 그대로 직면한다. 반면 인터넷은 부분적으로 이러한 문제들을 마주하게 되는 것 같다.

여러 다른 지표들은 단지 경제적인 측면만을 다루고 있는데 반해서, 웹파운데이션(Web Foundation)이 공표하는 웹인덱스(Web Index)는 사이버사회의 여러 가지 측면들을 다루는 유일한 지표이다.

3.2 사이버 안보

사이버 안보는 최근 10년간 가장 두드러지게 부각되고 있는 사이버스페이스의 한 측면이다. 아마도 부분적으로는 2011년에 육상, 해양, 영공과 외계와 같은 기존의 네 가지 영역에 더하여 미국과 유럽연합과 영국이 군사력에 사이버영역을 추가한 것이 영향을 미쳤을 것이다.

- 미국 : 사이버사령부(Cyber Command [USCYBERCOM])
- 유럽연합 : 유럽네트워크/정보보안청(European Network and Information Security Agency [ENISA])
- 영국 : 정부통신본부(Government Communications Headquarters)

2010년대 초에 사이버스페이스 문제를 다루는 여러 컨퍼런스가 열리기 시작했으며 이런 모임들은 주로 사이버안보 문제에 초점을 맞추었다. 다음은 그 예이다.

- 사이버 보안에 관한 국제컨퍼런스 (International Conference on Cyber Security)
- 사이버 다이얼로그 (Cyber Dialogue)
- 사이버국제관계연구회(ECIR)가 주최하는 워크샵 (ECIR Workshops)
- AFCEA 사이버스페이스 심포지엄 (AFCEA Cyberspace Symposium)

이코노미스트지는 다음과 같은 사이버전쟁에 관한 기사를 실었다.

- 사이버 전쟁 : 제5의 영역에서의 전쟁, 이코노미스트지 2010. 7/1

- 사이버 전쟁 : 인터넷에서의 위협, 이코노미스트지 2010 7/1

2011년의 스턱스넷(Stuxnet) 사건이나 에스토니아에 가해진 사이버공격은 사이버안보의 지형을 바꾸어 놓았으며 사이버전쟁이나 사이버무기와 같은 개념들을 쓰기 시작하는 계기가 되었다. [Sanger 2012]

3.3 사이버 경제

사이버 경제는 금세기에 가장 많이 이야기 되는 사이버스페이스의 또 다른 측면인 바, 전체 경제에서 사이버경제가 차지하는 부분은 G20 국가들의 GDP 기준으로 약 4%에 달한다. [Boston 2011] 한국이나 영국과 같은 나라들은 이 지표가 현재 7%를 넘는다. [Boston 2011]

사이버 경제를 이야기 할 때 이용할 수 있는 지표가 여러 가지 있는데 보스턴컨설팅그룹이 제시하는 e-Intensity나 맥킨지사가 제시하는 Internet Matters, 세계경제포럼(World Economic Forum)이 발표하는 Network Readiness Index와 같은 것들이 있다. [Boston 2011, McKinsey 2012, World 2012]

3.4 사이버 국민국가

사이버 국민국가는 사이버스페이스의 법체계나 사이버스페이스의 국제관계를 포함하는데 이러한 것들은 리얼스페이스와는 실질적으로 다를 수 있다.

사이버국제관계연구회(ECIR)가 사이버 국민국가 문제를 다루는데 특히 국제관계 문제를 광범하게 다룬다. 사이버스페이스 국제 컨퍼런스(International Conference on Cyberspace)도 사이버 국민국가의 국제관계 측면을 다루고 있다.

3.5 사이버 환경

사이버 환경은 앞으로 연구되어야 할 사이버스페이스의 새로운 단면이다. 사이버 환경은 사이버환경 자체가 지속가능해야 한다는 점과 함께 사이버 환경이 지속가능한 물리환경을 지탱한다는 두 가지 점에서 대단히 중요하다.

사이버 환경이 지속가능해야 한다고 할 때 우리는 또한 사이버 환경과 리얼 환경으로 이루어지는 혼합 환경 -여기에는 사이버물리 체계(cyber physical systems)도 포함된다-도 지속가능할 수 있도록 고려해야 한다.

3.6 여타 측면들

다음과 같이 몇 가지 추가적으로 중요한 여러 측면들을 생각해 볼 수 있다.

- 사이버 교육

- 사이버 미디어
- 사이버 노동
- 사이버 보건

4. 사이버 영토 (Cyber Territories)

사이버 영토는 다음과 같은 것들로 이루어진다. : IP주소, 이름, 루트서버와 주파수대역

- IP주소

IPv4와 IPv6와 같은 IP주소와 AS번호(Autonomous System Number)와 같은 번호들은 현재 번호자원기구(Number Resource Organization, NRO)가 인터넷주소자원관리기구(Internet Corporation on Assigned Names and Numbers, ICANN)/인터넷할당번호관리기관(Internet Assigned Numbers Authority, IANA)과 긴밀한 협력 속에서 관리한다.

-루트서버(Root Server)

루트서버라고 불리우는 최상위도메인(Top Level Domain Names)을 할당하고 있는 도메인네임서버들은 ICANN의 조정을 통해 관리되고 있다.

- 무선주파수(Radio Spectrum)

국제무선주파수대역은 국제전기통신연합(International Telecommunication Union, ITU)이 관리하고 있다.

5. 세계 표준

사이버스페이스의 세계 표준은 국가표준화기구, 대륙별표준화기구나 세계표준기구들과 긴밀한 협력 하에 여러 기구들이 관여한다. 그 중에는 다음 기구들이 포함된다.

- Internet Engineering Task Force(IETF)

IETF는 인터넷프로토콜들의 표준을 다루는 기구이다. 60년대 말에 시작된 미국방성 ARPANET 프로젝트 당시 네트워크워킹그룹을 이어 받아 1986년 설립되었다.

- World Wide Web Consortium (W3C)

W3C는 웹문서 표준언어인 HTML과 웹프로토콜인 HTTP와 같은 월드와이드웹 관련 기술 표준을 다루는 기구이다.

- The 3rd Generation Partnership Project (3GPP)

3GPP는 미국, 유럽, 중국, 일본, 한국의 통신협회들간의 협력기구로 3세대 이동통신전화 시스템 표준을 개발하고 있다.

6. 제기되는 문제들

1) 사이버스페이스의 여러 측면들

데이빗 클라크(David Clark)는 사이버스페이스의 안보, 경제, 사회 세 가지 관점을 제시했으며 앤서니 기든스(Anthony Giddens)는 세계자본주의경제, 노동의 국제 분화, 세계군사질서, 국민국가 체제로 세계화의 네 가지 차원을 제시했고, 가브리엘라 테자다는 여기에 제5의 차원으로 문화를 추가적으로 제시한다. 필자는 이러한 제안들을 토대로 하여 사이버사회, 사이버안보, 사이버경제, 사이버국민국가, 사이버환경 등과 그밖에 몇 가지 추가적으로 가능한 측면들을 포함하여 다섯 가지 이상의 사이버스페이스의 여러 측면들을 생각해 볼 수 있다고 본다.

사이버스페이스의 이러한 여러 측면들을 각각 보다 정교하게 분석할 수 있도록 몇 가지 측면들을 정식화할 필요가 있다.

2) 혼합 스페이스

사이버스페이스와 리얼스페이스가 중첩되는 영역이 있는데 이것을 혼합스페이스라고 할 수 있다. 혼합스페이스는 별개의 특징을 갖는 별개의 측면으로 규정할 필요가 있다.

3) 인터넷 거버넌스에 대한 세계포럼

정보사회세계정상회의(World Summit on Information Society, WSIS)는 유엔이 2003년과 2005년 두 차례 개최하였다. WSIS는 인터넷 거버넌스의 출발점이었으며 인터넷거버넌스포럼(Internet Governance Forum, IGF)을 출범시켰고, IGF는 2006년부터 매년 열리고 있다. 2005년 튀니스 WSIS 이후 10년이 지난 2015년에는 WSIS+10 회의가 열릴 예정이다.

4) 사이버스페이스에 대한 세계포럼

아래와 같은 몇 가지 사이버스페이스에 대한 세계포럼들이 있다.

- 사이버 다이얼로그 컨퍼런드(Cyber Dialogue Conference)
- 국제 사이버스페이스 컨퍼런스(International Cyberspace Conference)
- 사이버국제관계연구회 (Explorations in Cyber International Relations, ECIR)

사이버스페이스 문제를 다루는 세계포럼은 이제 시작되었으며, 그 대부분은 2010년대 초에 시작했다. 이제는 개별 국가단위에서, 대륙단위에서 그리고 세계적인 차원에서 사이버스페이스문제를 고려해야 할 때가 되었다.

7. 결론적 제언

사이버스페이스와 사이버스페이스의 여러 측면들, 그리고 사이버 거버넌스는 아직 초기단계에 있고, 이 글에서는 이 문제를 실험적으로 다루었다. 특히 리얼스페이스나 인터넷과의 관계에서 사이버스페이스를 어떻게 정의할 것인가 하는 문제를 생각해 보고자 했다. 그리고 사이버스페이스의 여러 측면들, 사이버스페이스 거버넌스, 사이버스페이스의 통제문제도 생각해 보았다. 또한 사이버스페이스가 제기하는 몇 가지 문제들도 생각해 보았다. 사이버스페이스, 사이버스페이스에 대한 통제, 사이버스페이스 거버넌스 문제에 대하여 향후 연구가 필요하다.

참고 문헌

[Black 2010] Black Hat Computer Security Conference, July 2010.

[Boston 2012] Boston Consulting Group, e-Intensity Index, 2012.

[Chon 2012] Kilnam Chon, Ecological Internet, NORDUNET, 2012.

[Clark 2011] David Clark, Three Views of Cyberspace, ECIR, Harvard-MIT, 2011.

[Clarke 2010] Richard Clarke, Cyber War, 2010.

[CyberCommons 2012] CyberCommons.net

[CyberDialogue 2013] Cyber Dialogue, CyberDialogue.ca

[Cyberspace 2013] Cyberspace 2013, Brno, Czech, Cyberspace.muni.cz

[Economist 2010] Cyberwar, Economist, 2010.7.1.

[ECIR 2012] ECIR Workshop: Who Controls Cyberspace?, 2012.

[ECIR 2013] Explorations in Cyber International Relations, ECIR.MIT.edu

[IGF 2013] Internet Governance Forum, www.IntGovForum.org

[McKinsey 2012] McKinsey, Internet matters, 2011.

[Munich 2011] Munich Cyber Security Conference, 2011.

[Nye 2011] Nuclear lessons for cyber security, 2011.

[Sanger 2012] David Sanger, Confront and Conceal, 2012.

[Seoul 2013] International Conference on Cyberspace, Seoul, 2013.

[Tejada 2077] Gabriela Tejada, The four dimensions of globalization according to Anthony Giddens, GLOPP, 2007.

[Whitehouse 2011] Whitehouse, International Strategy for Cyberspace, 2011.

[Web 2012] Web Foundation, Web Index.

[World 2012] World Economic Forum, Network Readiness Index, 2012.

보론 : 사이버스페이스 거버넌스

유엔 인터넷거버넌스 워킹그룹(WGIG)은 인터넷 거버넌스를 다음과 같이 정의하였다.

“인터넷 거버넌스란 각국 정부, 민간부문과 시민사회가 인터넷의 진화를 형성하고 인터넷을 이용하는 데 있어서 함께 공유하는 원칙과 규범, 규칙, 의사결정 절차 및 프로그램들을 각자의 역할 안에서 개발하여 적용하는 것을 말한다.”

"Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.”

http://www.wgig.org/docs/WGIGREPORT.pdf

사이버스페이스에 대해서는 아직 사이버스페이스의 여러 측면들이 초기단계에 있으므로 통제와 거버넌스 두 가지를 모두 보아야 한다.

그런 점에서 ECIR이 워크샵에서 “누가 사이버스페이스를 통제하는가?” 하는 주제를 택한 것은 중요한 의미가 있다. 우리는 아직 사이버스페이스의 통제문제를 잘 모르기 때문이다. 다음과 같은 사이버스페이스의 여러 측면들을 볼 필요가 있다.

ECIR이 분석대상으로 제시하는 여러 층위들(Layers)

여러 측면들(Aspects)

국가와 지역(Nations and regions)

사이버스페이스 거버넌스에 대해서 말하는 것은 지금도 사이버 사회와 같은 측면에서는 적절할 수 있는데 사이버 사회는 인터넷과 상당히 중첩되기 때문이다. 반대로 사이버 안보 거버넌스는 1950년의 핵기술처럼 아직 논의하기에 이른 점이 있다. [Nye 2011] 사이버 안보는 궁극적으로는 핵기술처럼 사이버 안보 거버넌스 문제로 다루어야 하지만 현재로서는 사이버 안보통제가 더 적절할 것으로 생각된다.

Cyberspace: What Is It?

Kilnam Chon[385]

1. Introduction

Cyberspace has drawn much attention since early 2010s with various conferences and organizations founded in early 2010s. This paper tries to clarify on the cyberspace including cyberspace governance discussed in these conferences and organizations.

Cyberspace was mentioned since 1980s including William Gibson's book, Neuromancer. In many cases, cyberspace is used similarly to the Internet including its culture and applications.

In 2010, Whitehouse in USA issued a report, International Strategy for Cyberspace. US Government created Cyber Command as the fifth domain after land, sea, air and space. European Union as well as UK Government followed with similar organizations. These moves made cyberspace and cyber war attract attention globally.

In early 2010s, several conferences and organizations were created with cyberspace as a core issue including;

- Explorations in Cyber International Relations (ECIR) at Harvard-MIT with various ECIR Workshops including ECIR Workshop: "Who Controls Cyberspace?"
- Cyber Dialogue Conference by Canadian Centre for Global Security Studies at University of Toronto
- Annual International Cyberspace Conference started in London in 2011

Many of these and other activities on the cyberspace focuses more on cyber security than other aspects of cyberspace.

---

385) Professor, Korea Advanced Institute of Science and Technology, Keio University (Japan)

2. Cyberspace

2.1 Cyberspace, Real space and mixed space

Cyberspace is virtual space which is typically based on the Internet whereas real space is physical world we live. Then, we have mixed space consists of cyberspace and real space. See Figure 13 on these three spaces.

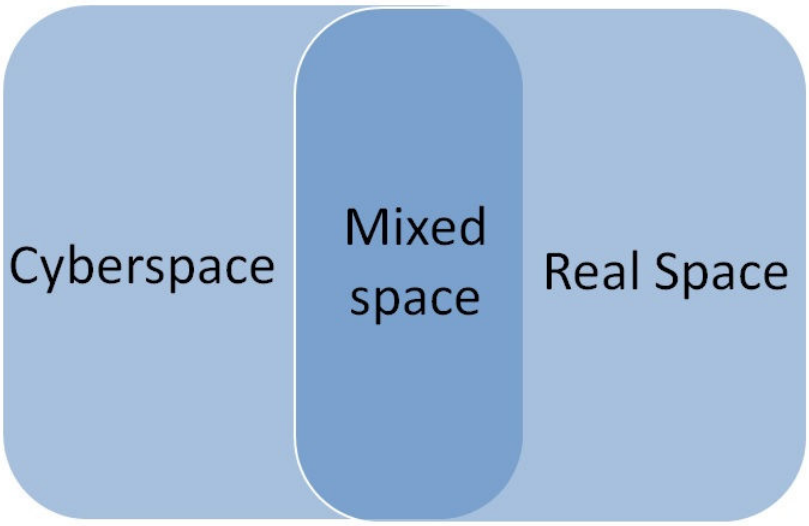

Figure 13 Cyberspace, Mixed Space and Real Space

Some of mixed spaces are called a cyber physical system such as a sensor-based network system where the Internet may or may not be used. Many of the Internet-based space tend to be mixed space rather than pure cyberspace without any real space.

2.2 Cyberspace and the Internet

Cyberspace such as cyber society and cyber security has the Internet as its infrastructure in many cases. But some of cyberspace have other infrastructure such as a telephone system without the Internet, a sensor-based network system and/or a television system without the Internet. Cyberspace has various aspects including cyber society, cyber security, cyber economy and cyber environment. See Figure 14 on cyberspace's infrastructure including the Internet as well as cyberspace's aspects.

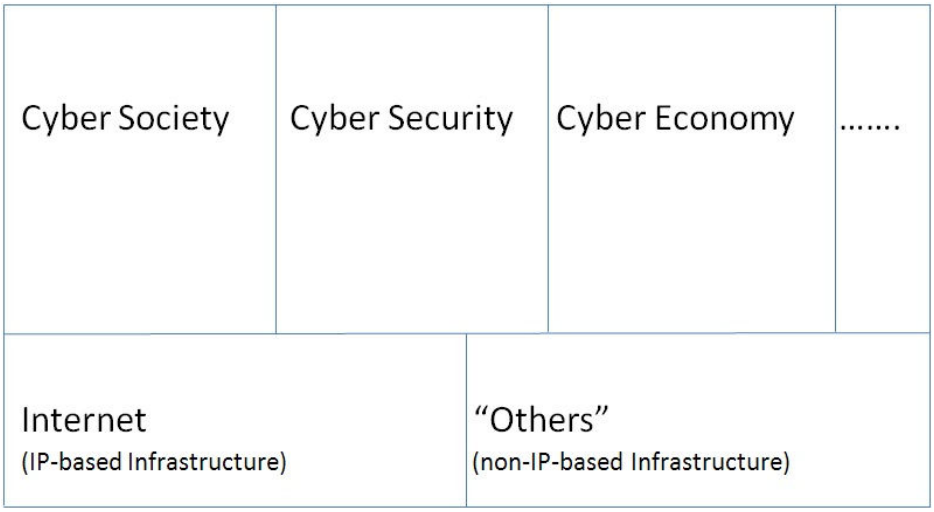

Figure 14 Cyberspace aspects and its infrastructure

3. Aspects of Cyberspace

Cyberspace has various aspects reflecting its viewpoints. David Clark in his paper, Three Views of Cyberspace, proposed three views [Clark 2011];

- Cyber Security
- Cyber Economics
- Cyber Society

Anthony Giddens in his paper, Four Dimensions of Globalization, proposed four dimensions of globalization in addition to fifth dimension proposed by Gabriela Tejada [Tejada 2007, Giddens 1991];

- World Capitalist Economy
- Nation-State System
- World Military Order
- (International) Division of Labor
- Culture

We proposed the following major aspects [Chon 2012];

- Cyber Society
- Cyber Security
- Cyber Economy
- Cyber Nation States

- Cyber Environment

More aspects such as Cyber Education, Cyber Media and Cyber Labor may be considered.

3.1 Cyber Society

Cyber society including cyber culture is closest to the Internet as they cover similar topics. Cyber society governance would be closest to the Internet governance, naturally. Both cover many social issues such as privacy, personal security, abuse, addiction and violence. Cyber society and culture covers various aspects of contents, but the Internet tends to cover partially.

Web Index by Web Foundation may be the only index to cover various aspects of cyber society as many indexes tend to cover only economical aspect.

3.2 Cyber Security

Cyber security is the most visible aspect of cyberspace in this decade, partly due to addition of cyber domains to military forces of USA, EU, and UK among others in 2011 to the existing four domains; land, sea, air and space;

- USA: Cyber Command (USCYBERCOM)
- EU: European Network and Information Security Agency (ENISA)
- UK: Government Communications Headquarters

Many conferences on cyberspace were founded in early 2010s, and they tend to focus on cyber security including the following;

- International Conference on Cyber Security
- Cyber Dialogue
- ECIR Workshops
- AFCEA Cyberspace Symposium

Economist among others published articles on cyberwar such as

- Cyber war: War in the fifth domain, Economist, 2010.7.1.
- Cyber war: The threat from the Internet, Economist, 2010.7.1.

Stuxnet incident in 2011 as well as cyber attacks on Estonia changed cyber security landscape bringing concepts of cyber war and cyber weapon [Sanger 2012].

3.3 Cyber Economy

Cyber economy is another aspect of cyberspace which is covered very well in this century with the current share of the cyber economy in the total economy in term of GDP among G20 countries is around 4%.[Boston 2011] Some countries such as South Korea and UK, the figures exceed 7% now [Boston 2011].

There are several indexes on cyber economy are available including e-Intensity Index of Boston Consulting Group, Internet Matters by McKinsey, and Network Readiness Index by World Economic Forum [Boston 2011, McKinsey 2012, World 2012].

3.4 Cyber Nation State

Cyber Nation State aspect may cover legal systems for cyberspace as well as international relations for cyberspace which may be substantially different from real space.

Explorations on Cyber International Relations (ECIR) covers on cyber nation state, in particular on international relations extensively. International Conference on Cyberspace also covers on international relations aspect of cyber nation state.

3.5 Cyber Environment

Cyber environment is a new aspect which should be studied well. Cyber environment on its own is very important including both (sustainable) cyber environment itself, and cyber environment to support sustainable physical environment.

While we work on sustainable cyber environment, we also need to works on mixed environment which consists of cyber and real environments including cyber physical systems.

3.6 Other Aspects

We may consider some of the following aspects as additional important aspects;

- Cyber Education
- Cyber Media
- Cyber Labor

- Cyber Health

4. Cyber Territories

Cyber territories may consist of the following and others; IP addresses, names, the root server and spectrum.

- IP Addresses

IP addresses including IPv4 and IPv6 as well as other numbers including Autonomous System Number are managed by Number Resource Organization (NRO) with close cooperation of Internet Assigned Numbers Authority (IANA) of Internet Cooperation on Assigned Names and Numbers (ICANN) now.

- Name

Domain names are managed by ICANN including Top Level Domain Names (TLDs) in English and other languages. Other names are managed by other organizations including World Wide Web Consortium (W3C) and private companies such as Facebook and Google.

- Root Server

Domain name servers for Top Level Domain Names, called the Root Server are coordinated by ICANN.

- Radio Spectrum

International radio spectrum is being coordinated by International Telecommunications Union (ITU).

5. Global Standards

Global standards for cyberspace are handled by various organizations with close collaborations of national and regional standard bodies as well as among global standard bodies, which include the following;

- Internet Engineering Task Force (IETF)

IETF is the standard body on the Internet protocols, and it was founded in 1986, taking over Network Working Group of ARPANET Project which stated in late 1960s.

- World Wide Web Consortium (W3C)

W3C is the standard body on WWW-related technology such as HTML and HTTP.

- The 3rd Generation Partnership Project (3GPP)

3GPP is a collaboration among telecommunications associations of USA, Europe, China, Japan and Korea to develop the third-generation mobile phone system standards.

6. Issues

(1) Aspects of Cyberspace

David Clark proposed three views of cyberspace; security, economy and society. Anthony Giddens proposed four dimensions of globalization; world capitalist economy, international division of labor, world military order, and nation state system, and Gebriela Tejada added culture as the fifth dimension. Kilnam Chon proposed five or more aspects of cyberspace including cyber society, cyber security, cyber economy, cyber nation state, and cyber environment with possible addition of more aspects.

We need to come up with an appropriate set of aspects with elaborate analysis of each aspect soon.

(2) Mixed Space

There is an overlapping area between cyberspace and real space which may be called mixed space. The mixed space needs to be defined in each aspect including its characteristics.

(3) Global forum on Internet governance

World Summit on Information Society (WSIS) was organized twice by United Nations in 2003 and 2005. WSIS may be the beginning of the Internet governance, and this community founded the Internet Governance Forum (IGF) which has been held annually since 2006. This community will have WSIS+10 in 2015 after the ten years of the second WSIS in Tunis in 2005.

We need to look into what we need to govern the Internet in the coming decades.

(4) Global forum on cyberspace

We have a few global forums on cyberspace including

- Cyber Dialogue Conference
- International Cyberspace Conference
- Explorations in Cyber International Relations (ECIR)

The global forums on cyberspace are only beginning now as all of them were founded in early 2010s. We need to look into what we need in this area globally, regionally and nationally.

7. Concluding Remark

Cyberspace including its various aspects and cyber governance is still in its early stage, and it is explored in this paper. We specifically explored definitions of cyberspace with respect to real space and the Internet. Then, we explored various aspects of cyberspace, and on cyberspace governance as well as cyberspace control. We also raised several issues on cyberspace. We would like to see further studies on cyberspace as well as cyberspace control and governance.

References

[Black 2010] Black Hat Computer Security Conference, July 2010.

[Boston 2012] Boston Consulting Group, e-Intensity Index, 2012.

[Chon 2012] Kilnam Chon, Ecological Internet, NORDUNET, 2012.

[Clark 2011] David Clark, Three Views of Cyberspace, ECIR, Harvard-MIT, 2011.

[Clarke 2010] Richard Clarke, Cyber War, 2010.

[CyberCommons 2012] CyberCommons.net

[CyberDialogue 2013] Cyber Dialogue, CyberDialogue.ca

[Cyberspace 2013] Cyberspace 2013, Brno, Czech, Cyberspace.muni.cz

[Economist 2010] Cyberwar, Economist, 2010.7.1.

[ECIR 2012] ECIR Workshop: Who Controls Cyberspace?, 2012.

[ECIR 2013] Explorations in Cyber International Relations, ECIR.MIT.edu

[IGF 2013] Internet Governance Forum, www.IntGovForum.org

[McKinsey 2012] McKinsey, Internet matters, 2011.

[Munich 2011] Munich Cyber Security Conference, 2011.

[Nye 2011] Nuclear lessons for cyber security, 2011.

[Sanger 2012] David Sanger, Confront and Conceal, 2012.

[Seoul 2013] International Conference on Cyberspace, Seoul, 2013.

[Tejada 2007] Gabriela Tejada, The four dimensions of globalization according to Anthony Giddens, GLOPP, 2007.

[Whitehouse 2011] Whitehouse, International Strategy for Cyberspace, 2011.

[Web 2012] Web Foundation, Web Index.

[World 2012] World Economic Forum, Network Readiness Index, 2012.

Appendix: Cyberspace Governance

The Working Group on Internet Governance (WGIG) of the United Nations defined the Internet governance as follows;

"Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

http://www.wgig.org/docs/WGIGREPORT.pdf

For cyberspace, we may look into both control and governance since many aspects of cyberspace are in its early stages.

ECIR workshop on "Who controls cyberspace?" is of great interest since we don't know on the control of cyberspace yet. We may need to look into multiple dimensions including

- Layers as being analyzed by ECIR
- Aspects
- Nations and regions

Cyberspace governance may be appropriate now in some aspects such as cyber society which has significant overlap with the Internet. On the other hand, cyber security governance may be premature like nuclear technology in 1950s[Nye 2011].

cyber security control may be more appropriate for time being even though we need cyber security governacne eventually like nuclear technology.

부 록

용어 설명

‘강화된 협력’ 워킹그룹 : Working Group on Enhanced Cooperation : WGEC

정보사회세계정상회의(WSIS) 2차 회의의 결과물인 튀니스 어젠다에서 규정하고 있는 ‘강화된 협력(Enhanced Cooperation)’의 의미와 구현방안을 논의하기 위해, 2012년 UN 결의에 따라 ‘개발을 위한 과학기술 위원회’(CSTD) 산하에 만들어진 워킹그룹. (강화된 협력과 국제 인터넷거버넌스의 미래, 오병일 참고) http://unctad.org/en/Pages/CSTD/WGEC.aspx

국제인터넷표준화기구 : Internet Engineering Task Force : IETF

인터넷의 운영, 관리, 개발에 대해 협의하고 프로토콜과 구조적인 사안들을 분석하는 인터넷 표준화 작업기구이다. 인터넷 아키텍처 위원회(IAB)의 산하기구로 인터넷의 운영, 관리 및 기술적인 쟁점 등을 해결하는 것을 목적으로 망 설계자, 관리자, 연구자, 망 사업자 등으로 구성된 개방된 공동체이다. 주로 자발적인 참여와 논의 과정을 통하여 인터넷 관련 기술표준을 마련하고 있다. (위키백과) http://www.ietf.org/

국제전기통신세계회의 : World Conference on International Telecommunications : WCIT

전기통신과 관련한 세계적인 규칙인 국제전기통신규칙(International Telecommunications Regulations, ITRs) 논의를 위해 국제전기통신연합(ITU)이 주관하는 국제회의다. 지난 2012년 12월, 두바이에서 WCIT-12 회의가 개최되었는데, 인터넷 관련 내용을 ITRs에 포함시킬 것인지를 두고 큰 논란이 있었다. (인터넷 거버넌스 모델로서의 멀티스테이크홀더, 이영음, ITU WCIT의 위협 분석, 밀튼 뮬러 참고) http://www.itu.int/en/wcit-12/Pages/default.aspx

국제전기통신연합 : International Telecommunication Union : ITU

세계적인 주파수의 분배, 전기통신 관련 기술 표준의 개발 등을 담당하는 국제연합(UN) 산하의 정부간 국제기구. http://www.itu.int

멀티스테이크홀더리즘 : Multi-stakeholderism

어떤 사안을 관리하는데 있어서 그 사안에 이해관계가 있는 다양한 집단들이 참여하여 서로 간의 어느 정도의 협의를 통해 관리의 원칙, 규범, 및 의사결정 절차 등을 정하는 것을

의미한다. (인터넷 거버넌스 모델로서의 멀티스테이크홀더, 이영음 참고)

멀티스테이크홀더 자문그룹 : Multistakeholder Advisory Group, MAG

인터넷거버넌스포럼(IGF)의 프로그램 및 일정 등에 대해 자문하기 위해, 정부, 기업, 시민사회, 학계 및 기술 커뮤니티 등 56명의 멤버로 구성된 자문그룹.

http://www.intgovforum.org/cms/magabout

베스트 비트 : Best Bits

인터넷 거버넌스에 참여하고 있는 세계 시민사회 네트워크로서, 2012년 WCIT-12에 대한 시민사회의 공동 대응을 계기로 만들어졌다. 전체 시민사회 그룹의 단일한 입장을 목표로 하기 보다는 특정한 이슈를 중심으로 시민사회 사이의 논의와 협력을 모색하는 플랫폼으로서의 역할을 하고 있다. http://bestbits.net

세계전기통신정책회의 : World Telecommunication/ICT Policy Forum : WTPF

국제전기통신연합(ITU)가 정보통신관련 정책 이슈에 대한 의견을 교환하기 위한 고위급 회의. 2013년 5월 14-16일, 5차 WTPF 회의가 제네바에서 개최되었다.

http://www.itu.int/en/wtpf-13/Pages/default.aspx

시민사회 인터넷거버넌스 코커스 : Civil Society Internet Governance Caucus : IGC

인터넷거버넌스 관련 시민사회 단체 및 개인들의 네트워크. 정보사회세계정상회의(WSIS)에 참여한, 개인 및 단체를 포함한 시민사회 참여자의 네트워크로 출발하였다. IGC는 시민사회의 토론 및 활동을 위한 포럼을 제공하고 인터넷거버넌스 과정에 시민사회를 대표하고자 한다. http://igcaucus.org

인터넷거버넌스 워킹그룹 : Working Group on Internet Governance : WGIG

2003년 제1차 정보사회세계정상회의(WSIS)는 원칙선언 및 행동계획의 '인터넷 거버넌스'와 관련된 대화를 계속해 나갈 것에 동의했다. 2005년 튀니스에서 열린 제2차 WSIS에서 결정할 수 있는 근거를 마련하기 위하여, UN 사무총장에게 이를 논의할 워킹그룹 구성을 제안했다. WGIG는 멀티스테이크홀더 방식으로 구성되었으며, 그 목표는 인터넷 거버넌스에

대한 적절한 제안을 2005년 WSIS 회의에 제출하는 것이었다.

http://www.wgig.org/index.html

인터넷거버넌스포럼 : Internet Governance Forum : IGF

2005년 튀니스 어젠다에 따라 열리게 된, 인터넷 거버넌스 이슈에 대한 멀티스테이크홀더 사이의 대화를 위한 포럼이다. 2006년 그리스 아테네에서 처음 개최되었으며, 이후 매해 개최되고 있다. IGF는 UN이 주관하는 회의이지만, 여타 UN 회의와는 다르게 정부, 기업, 시민사회, 학계 및 기술 커뮤니티 등 다양한 이해당사자들이 동등하게 참여할 수 있는 포럼이다. 포럼의 기획은 멀티스테이크홀더로 구성된 '멀티스테이크홀더 자문그룹'(Multi-stakeholder Advisory Group, MAG)의 자문을 받는다. (글로벌 거버넌스 공론장으로서 IGF의 의미, 박지환 참고) http://www.intgovforum.org/

인터넷주소관리기구 : Internet Corporation for Assigned Names and Numbers : ICANN

1998년에 설립된 인터넷의 비즈니스, 기술계, 학계 및 사용자 단체 등으로 구성된 기관으로 인터넷 DNS의 기술적 관리, IP 주소공간 할당, 프로토콜 파라미터 지정, 루트 서버 시스템 관리 등의 업무를 조정하는 역할을 한다. (위키백과) http://www.icann.org/

인터넷할당번호관리기관 : Internet Assigned Numbers Authority : IANA

세계적인 IP 주소의 할당, AS 번호 할당, 도메인네임시스템(DNS)의 루트 존 관리 등을 감독하는 미국의 비영리 단체. 1998년 ICANN 설립 이전에는 주로 서던캘리포니아대학의 정보과학협회(Information Sciences Institute, ISI)의 존 포스텔이 IANA를 운영하였다. 현재는 ICANN이 미국 상무성과의 계약 하에 이에 대한 책임을 맡고 있다.

정보사회를 위한 튀니스 어젠다 : Tunis Agenda for the Information Society

2005년 11월 16-18일 튀니스에서 개최된 제2차 정보사회세계정상회의(WSIS)의 합의문서이다. 튀니스 어젠다에 따라 2006년부터 인터넷거버넌스포럼(IGF)이 개최되었다. 또한 '강화된 협력'(Enhanced Cooperation)에 대한 논란이 계속된 끝에, 2012년 UN은 '강화된 협력 워킹그룹'(WGEC)을 구성하여, 강화된 협력의 의미와 구현방안을 논의하도록 하였다. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

정보사회세계정상회의 : World Summit on Information Society : WSIS

2002년 1월 31일 UN이 채택한 결의안에 근거하여, 국제전기통신연합(ITU) 주관 하에 개최되었다. 이 회의의 목적은 정보사회와 관련된 광범한 질문을 제기하고, 공통의 비젼과 사회변화에 대한 이해를 마련하기 위한 것이다. 1차 회의는 2003년 12월 10-12일 제네바에서 열렸으며, 그 결과 제네바 원칙선언(Geneva Declaration of Principles)과 제네바 실천계획(Geneva Plan of Action)이 채택되었다. 2차 회의는 2005년 11월 16-18일 튀니스에서 열렸고 정보사회를 위한 튀니스 약속과 튀니스 어젠다가 채택되었다. http://www.itu.int/wsis

정부자문위원회 : Governmental Advisory Committee : GAC

ICANN 내에서 정부들의 입장을 대변하는 그룹. ICANN 이사회에 GAC 대표를 보내기는 하지만 투표권은 없다. ((인터넷 거버넌스 모델로서의 멀티스테이크홀더, 이영음 참고)

지역인터넷등록소 : Regional Internet Registry : RIR

특정 지역 내에서 IP 주소, AS 번호 등 인터넷 번호자원의 할당 및 등록을 관리하는 단체. 현재 5개의 RIRs이 각 지역을 나누어 관리하고 있다.

- 아프리카 : African Network Information Centre (AfriNIC)

- 북미 및 캐리비안 일부 : American Registry for Internet Numbers (ARIN)

- 아시아-태평양 : Asia-Pacific Network Information Centre (APNIC)

- 남미 및 캐리비안 일부 : Latin America and Caribbean Network Information Centre (LACNIC)

- 유럽, 러시아, 중동, 중앙아시아 : Réseaux IP Européens Network Coordination Centre (RIPE NCC)

진보통신연합 : Association for Progressive Communications : APC

사회정의를 위한 인터넷 활용과 자유롭고 개방적인 인터넷을 위한 공공정책 수립을 옹호하는 전 세계 시민사회단체의 네트워크이다. 2010년 12월 기준으로, 35개국, 50여개 단체가 회원으로 가입되어 있다. 1990년 5월 설립되었으며, 1995년 6월 유엔 협의적 지위를 획득하였다. http://www.apc.org

필자 소개

▮김지연 spring900@gmail.com
고려대학교 과학기술학 박사
고려대학교 과학기술학연구소 선임연구원
서울과학기술대학교 강사

▮이영음 yesunny@knou.ac.kr
방송통신대학교 미디어영상학과 교수
ICANN ccNSO 위원회 위원
한국인터넷진흥원 이사
인터넷주소정책심의위원회 위원
한국인터넷거버넌스협의회 주소인프라분과 위원장
2013 한국방송학회 부회장

▮김재연 jaeykim2@gmail.com
전 세계 풀뿌리 언론가 네트워크인 Global Voices Online 활동가
국제 인터넷 검열 감시 조직인 Global Voices Advocacy 회원
Creative Commons Korea 활동가

▮박성훈 cyber152@humanrights.go.kr
고려대학교 정부학연구소 연구원
국가인권위원회 인권정책과 정보인권 담당

▮박지환 bobpark925@gmail.com
법률사무소 혜윰
사단법인 오픈넷 자문 변호사
망중립성 이용자포럼 활동

▮윤복남 bnyun@hklaw.co.kr
법무법인(유) 한결 변호사
한국인터넷거버넌스협의회 주소인프라분과위원

▮김기창 keechang.kim@gmail.com
변호사, 법학박사, 고려대학교 법학전문대학원 교수
사단법인 오픈넷 비상임 이사

▌매티스 반 베르겐 (Matthijs van Bergen) m.vanbergen@ictrecht.nl
ICTRecht 법률자문
네덜란드 NGO인 Bits of Freedom 자원활동가
유럽평의회(Council of Europe)의 망중립성 전문가로 활동

▌김보라미 squ24n@gmail.com
변호사, 망중립성 이용자포럼 코디네이터

▌밀튼 뮬러 (Milton Meuller) mueller.syr.edu@gmail.com
시라큐스 대학 정보사회학 교수
인터넷 거버넌스 프로젝트 운영. http://www.internetgovernance.org/

▌제레미 말콤 (Jeremy Malcolm) jeremy@ciroap.org
국제소비자연맹(Consumer International) 수석정책관

▌조이 리디코트 (Joy Liddicoat) joy@apc.org
진보통신연합(APC)의 인터넷권리와 인권 프로젝트 코디네이터, http://rights.apc.org

▌오병일 antiropy@gmail.com
진보네트워크센터 활동가
정보공유연대 IPLeft 대표
한국인터넷거버넌스협의회 주소인프라분과 위원

▌전응휘 ehchun@gmail.com
사단법인 오픈넷 이사장
녹색소비자연대 이사
한국인터넷거버넌스협의회 주소인프라분과 위원

▌전길남 chonkn@gmail.com
한국과학기술원 교수
일본 게이오대학교 교수

본 보고서는 국가인권위원회 2013년 인권단체협력사업의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다.