ITU WCIT의 위협 분석[1]

필자 밀튼 뮬러 (Milton Meuller)[2]
번역자 박지환

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[3]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)"[4]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)[5]와 함께 DNS 루트서버에 대한 관리를 민영화(privatize)하여 미국 정부의 손에서 DNS 관리권을 인수(take over)하려고 했다. 그러나 미국 정부는 이들의 이러한 노력을 철저하게 짓밟았고 ICANN의 출범을 주도하였다.

1) 이 번역문은 국가인권위원회의 2013년 인권단체협력사업의 지원을 받아 망중립성 이용자 포럼이 2014년 발간하는 『인터넷거버넌스를 말하다』라는 책에 실릴 예정입니다.
2) 시라큐스 대학 정보사회학 교수, mueller.syr.edu@gmail.com, 인터넷 거버넌스 프로젝트 운영. http://www.internetgovernance.org/
3) http://thehill.com/blogs/hillicon-valley/technology/229231-house-to-hold-hearing-on-international-control-of-the-internet
4) http://www.amazon.com/Networks-States-Governance-Information-Revolution/dp/0262014599
5) http://www.isoc.org/

국민국가의 인터넷 거버넌스에 대한 도전이 절정기에 이르는 다음 일화는 바로 2002년에서 2005년 사이에서 개최된 WSIS[6]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 적용가능한 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)[7]에서 정책 결정에 개입하려 했던 것이 더욱 결정적인 기여를 하였기 때문이다.

2009년과 2010년 사이 ITU는 IP 주소 관리[8]에 대한 스스로의 역할을 확대하기 위해 노력하였다. 최근 WCIT-12에서 표출되었던 많은 우려들은 2010년 과달라하라(Guadalajara)에서 개최된 ITU 전권회의[9]에서도 이미 표출된 바 있다. 2010년 전권회의의 결과에 대한 일련의 우리가 알고 있는 보고들[10]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.[11] 본 제안이 UN의 관리 권한 인수라는 측면에서 경종을

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

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 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[12] 인도 정부의 지지 의사가 인도 내 인터넷 검열[13]로 이어질 것을 우려하는 의회[14] 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 의미없는 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 정치

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

적 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 통제권을 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 정보정책의 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' 서비스

와 '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[15]의 layer 1 물리계층 및 Layer 2 데이터링크 계층)은 매우 엄격하고 경쟁 보호적이며, 대체로 정부 소유 방식에 의해 독점적으로 제공되었다. 정보 서비스(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 자

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

들 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[16]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 전기통신을 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 보안 문제가 아니다. 당신이 국가적 규제 당국이 ISP 일반에 대해 공동 규제(collective regutlation)

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

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 세계이다. 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 미치는

지, 혹은 그렇지 않은지에 대해 살펴볼 것이다.

3. 당신에게 과금(charging)하는, 나에게 과금하는

우리는 (TD-64[17]에 담겨 있는) ITR에 관해 제안된 수정 사항들은 물론, 최근 제안된 다른 사항들이나, WCIT[18] 준비 기간 동안의 ITU 발표 내용들을 면밀히 검토해보았다. 검토 결과, 인터넷에 대한 ITR의 잠재적인 영향력은 유선 네트워크로 된 국제 인터넷 연결 처리(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[19]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[20]을 보라.) ITR 수정 사항들이 자유로운 정보의 흐름을 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 관련되어있

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

다.

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[21]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.

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)이

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

나 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 이의제기를 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.

8A.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 서술[22]된 것처럼, 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 의

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

해 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 독점기업이 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[23]이 만들어졌고, 이는 2000년에 통과된 후 몇 번 수정되었다. D.50은 그저 권고(recommendation)에 불과하다. 그리고 몇 수정 제안은 그것을 ITR로 가져와서 이를 필요요건(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 만들어낼 수 없었다. 유튜브를 비롯한 다른 응용 프로그램 단의 업체들이 비용을 더 내도록 했던 AT&T의 초기 노력이 결코 사라지지 않은 것처럼[24] 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.

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

23) http://www.itu.int/rec/T-REC-D.50/e
24) http://arstechnica.com/uncategorized/2005/10/5498-2/

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 그들의 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)[25]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[26] 표현의 자유를 제약하고, 프라이버시를 침해하며, 익명성을 파괴하고, 새로운 사업 기회를 제약하며 사이버 보안을 언급하는 국가의 힘을 더해주는 행위와 다름 아니다. 누가 디지털 서비스와 인터넷 기반시설의 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[27]이라는 사실에 대하여 간파했다는 점은 이미 명백하다. 그러나 더 놀라운 것은 이 문제에 관심을 끌고, 참여하고, 펀딩을 받는 행위가 워싱턴 DC의 정책 연구기관[28]이나 다양한 미국 정부 기관들[29]이 하는 방식을 그대로 보여주고 있다는 점이다. 더욱이 ITU가 사이버 보안과 관련되어 하는 대부분의 것들은 기본적으로 교육과 역량강화[30]와 관련되어 있다. ITU 전권회의 결의안 130과 146[31]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 별개로 ITU-T는 그 자체로 사이버 보안 이슈와 관련된

25) http://en.wikipedia.org/wiki/Securitization_%28international_relations%29
26) http://www.lexipedia.com/english/scoundrelly
27) http://www.itu.int/cybersecurity/
28) http://csis.org/program/commission-cybersecurity-44th-presidency
29) 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
30) http://www.itu.int/ITU-D/cyb/
31) http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf

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.[32] 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*[33]*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 정세 하에서 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 얼

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

마나 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 관리 감독하라"면서 그 목표로 "ICT를 합리적인 방법으로 사용하도록 하기 위함"을 들고 있다. 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 구축하려하고, 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,[34] 러시아는 여전히 사이버 전쟁 게임에서 스스로를 매우 취약한 당사자로 판단하고 화학무기 관련 조약과 같은 성격의 조약을 희망

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

하고 있는 것이다. 플레임(Flame)과 스턱스넷(Stuxnet)[35]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 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

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

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[36] 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 각국에서 스팸에 대응하면서 얻게 된 정보와 조치 내용을 공유한다(무엇이 잘못되었는가?)는 내용에 불과하다. 따라서 스팸에 대한 언급이 ITU의 관할권을 인터넷 내용규제에까지 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[37]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 라우팅

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

에 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 공공안전을 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.

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 존

재한다고 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 무역협정을 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.