The "Dubai Clash" at WCIT-12: Freedom of Information, Access Rights, and Cyber Security

Deborah Housen-Couriel

> *It is clear that the world community is at a crossroads in its collective view of the internet and of the most optimal environment for the flourishing of the internet in this century.*
>
> US Ambassador Terry Kramer, speaking at a press conference at the conclusion of WCIT-12 in Dubai, December 2012

Critical decisions regarding the future of the internet, or internets, are upon us. In his seminal book published in 2008, entitled *The Future of the Internet: And How to Stop It*, Professor Jonathan Zittrain of Harvard Law School laid out the core dilemma behind these decisions.[1] On the one hand, the ubiquity of the world wide web, the richness of its resources, and the ease of access and transmission of information it provides for 2.7 billion people – which Zittrain calls the "generative internet" – have been determined by the web's original chaotic and largely unregulated design.[2] On the other hand, governments and inter-governmental organizations have become deeply challenged by the internet's freewheeling, "wild west" nature, and the facility with which it is leveraged for illicit activities, including costly cybercrime, due to the absence of multilateral, normative frameworks.[3] In the name of increasing cyber security concerns, and lacking effective global agreement on legal and policy parameters, governments have begun to regulate both content and access on their own. This pattern is at best counterproductive,

Adv. Deborah Housen-Couriel is a Research Fellow at Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security.

and at worst harmful and disruptive, given the global interoperability and interdependence of the internet.[4]

Zittrain opposed any overall tendency by regulators to stifle internet innovation and freedom of expression by its users, even in the name of cyber security. He called for a latter-day Manhattan Project to take on the challenge of moving the internet into its next global phase without a regulatory lockdown that would, in his view, sacrifice the innovative edge that characterized its genesis and early development.[5] Summarizing the importance of ensuring that state and non-state shareholders alike engage in this project, he wrote:

> Traditional cyberlaw frameworks tend to see the Net as an intriguing force for chaos…the name of the game is seen to be coming up with the right law or policy…to address the issues…. Stopping this future depends on some wisely developed and implemented locks, along with new technologies and a community ethos that secures the keys to those locks among *groups with shared norms and a sense of public purpose, rather than in the hands of a single gatekeeping entity,* whether public or private.[6] (emphasis added)

One of the catalysts for moving into this new stage of internet governance will be, he argues, "a collective watershed security moment," when governments and non-governmental actors will be forced to confront the vulnerability of the internet's infrastructure and operational flexibility.[7]

That critical moment in fact occurred in December 2012 in Dubai, at an inter-governmental conference held under the auspices of the UN's International Telecommunication Union (ITU). The conference, known as WCIT-12,[8] dealt with the ongoing revision of a relatively technical treaty establishing the principles for global telecommunication infrastructure, called International Telecommunication Regulations (ITRs).[9] Originally relating to telegraphy and telephony, the ITRs now also underpin the interconnection of systems utilizing telecommunication infrastructure for internet traffic. They address the development of new services, promotion of broad public access, system interoperability, mobile roaming, accounting rates, and priority for safety-of-life communications. The technical connectedness among global telecom systems that we experience as relatively seamless use of mobile phones and the web depends on ITR provisions.[10]

Despite its ostensibly technical nature, the WCIT-12 conference became a flashpoint of controversy around the future of internet governance months before it convened in Dubai. Underlying this controversy was the ongoing debate among states regarding the problematic relationship between internet governance and cyber security. Two recent reports of the US Council on Foreign Relations highlight this tension: [11]

> Cyberspace is now an arena for strategic competition among states, and a growing number of actors – state and nonstate –use the Internet for conflict, espionage, and crime. Societies are becoming more vulnerable to widespread disruption as energy, transportation, communication, and other critical infrastructure are connected through computer networks. At the same time, the open, global Internet is at risk. Nations are reasserting sovereignty and territorializing cyberspace. The justifications are many – national security, economic interest, cultural sensitivity – but the outcome of blocking, filtering, and regulating is the same: a fragmented Internet and a decline in global free expression.[12]

While there is currently no accepted definition of "cyber security" in international law, many states, including Israel, emphasize the elements included in the ITU approach, which encompasses the totality of state and organizational behaviors that are designed to protect cyberspace and its users from harm to computer systems, data, and personnel.[13] The differences center on domestic law and policy considerations of what constitutes "harm." Although most would agree that threats to cyber security include cyber crime, cyber espionage, and cyber attacks, in the absence of coordinated, mutually-agreed international legal norms, at present each state determines the legality of cyber activity independently, exclusively in accordance with its domestic law.[14]

The WCIT-12 galvanized and polarized these differences of approach: on the one hand, that of the Western democracies and their allies, led by the US and the EU and including Israel; and on the other, that of regimes more restrictive of the freedoms of expression and access, led by China, Russia, and some Arab states. The former held that the status quo of a light-handed and multi-stakeholder approach regarding internet governance should be maintained, including non-state actors that have so far played a key part in

internet evolution. The latter approach advocated heavier regulation, with a greater role for state intervention in both internet traffic and content.

Figure 1 maps the voting patterns of ITU member states. The non-signatories, which amounted to 38 percent of conference participants, included the US, the EU, Canada, Japan, Australia, and Israel.[15]

■ – Signatories
■ – Non-signatories
■ – Countries not included in the ITU list

Figure 1. Voting Patterns among ITU Member States

Source: M. Masnick, *Who Signed the ITU WCIT Treaty…And Who Didn't*, TECHDIRT, December 14th, 2012

The end result was a sharp division between those countries that signed the ITR's 2012 revisions and those that refused to do so, remaining bound by the 1988 version of the ITRs. In rejecting the revisions, these countries dissented from what they perceived as a concerted project on the part of non-Western countries to inaugurate an interventionist and anti-democratic regulatory model of internet governance. The US State Department framed the clash in terms that echo Professor Zittrain's:

> We believe these provisions reflect an attempt by some governments to regulate the Internet and its content, potentially paving the way for abuse of power, censorship and repression…. We stand on one of our most cherished of principles, free

> expression, in not signing this treaty and seeking more positive outcomes in the future that support the open and innovative Internet. We believe an open Internet also is important for commercial growth in all parts of the world.[16]

The actual effect of the Dubai amendments to the ITRs on the future of internet operability and governance has yet to be seen.[17] Yet the perception by the US, Europe, and allied states that the China-Russia-India-Africa bloc was intent on preempting the future of the internet in ways hostile to democratic values polarized positions and led to the conference's conclusion in a legal and policy stalemate between countries supporting two different versions of the ITRs: the Melbourne 1988 version and the amended Dubai 2012 version. The clash at Dubai was Zittrain's "collective watershed security moment." It signaled to global decision-makers the high cost of what states believe to be at stake regarding the future of internet governance.

What follows is a review of the international legal and policy debate in the ITU that led up to WCIT-12, followed by an analysis of the legal issues of freedom of information on the internet and access to digitized information. The article then examines the Dubai Clash's ramifications for cyber security, and draws some conclusions regarding the steep normative, economic, and security costs of non-resolution of the present global debate around internet governance.

The International Debate around Internet Governance at the ITU

The revision of the ITRs prior to Dubai dates from 1988, when the internet had yet to become the economic, social, educational, political, and security phenomenon that it is today. The 1988 ITRs focused on then-relevant aspects of international telecommunications, such as interconnection routing and fees.[18] While the emergence of the web has changed international telecommunications in dramatic ways, these changes have taken place largely without intergovernmental regulation by bodies such as the ITU. On the contrary: development has moved ahead by involving a mix of non-governmental stakeholders focusing on the operational priorities through standards, communications protocols, and domain name management.[19] Organizations and extra-governmental groups such as ICANN,[20] the Internet Society,[21] and IETF[22] (MACHBA and the IIA in Israel)[23] have taken the lead

on rapid and overall effective resolution of these issues, technical in nature yet crucial to ensuring the open nature of web access. Perhaps predictably at the early stages, US-based bodies were dominant, largely supported by the EU[24] and other Western democracies, including Israel.

However, with the dramatic expansion of the internet over the two decades (*see* figure 2),[25] many states in the early twenty-first century began to express dissatisfaction with the multi-stakeholder governance model and the perception of US dominance. China and other developing countries first proposed an international treaty on internet governance in the months prior to the 2003 ITU World Summit on the Information Society (WSIS) held in Tunisia.[26] Disagreements among ITU member states advocating this new regime and those interested in maintaining the status quo (roughly the division later seen at WCIT-12) resulted in the matter being referred to the UN Secretary-General. He proceeded to establish a Working Group on Internet Governance (WGIG) in 2004, which in turn recommended the creation of an Internet Governance Forum as a non-binding intergovernmental forum for discussion on internet-related issues and internet governance.

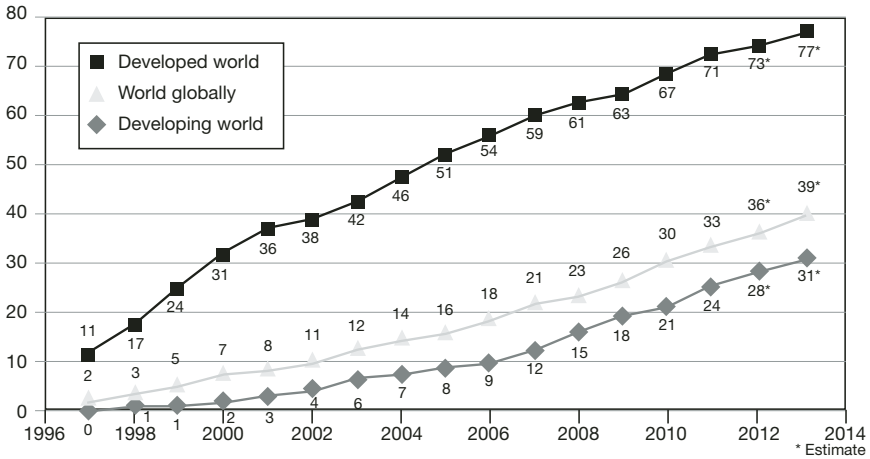

Figure 2. Internet Use

Source: ITU, *Internet Users per 100 Inhabitants 2006-2014* (May 2013)

Article 4 of the Tunis Declaration reached at the conclusion of the 2003 WSIS conference reflected a consensus regarding freedom of expression over the internet.[27] The article promotes freedom of trans-border expression and access to data embodied in Articles 19 and 20 of the Universal Declaration on Human Rights (reviewed in Section III below), and is important as a

substantive basis for internet governance discussions within the UN system. Indeed, it had ramifications at WCIT-12 as well, having been incorporated into the binding legal norms of the ITU.[28]

In light of the UN organizational initiatives and the dramatically-altered international telecommunication environment, the ITU decided in 2006 to convene WCIT-12. The stated goal was to adapt the ITRs to contemporary telecommunication realities, including vastly expanded global internet traffic. The road from the 2003 WSIS to the WCIT-12 is charted in figure 3.

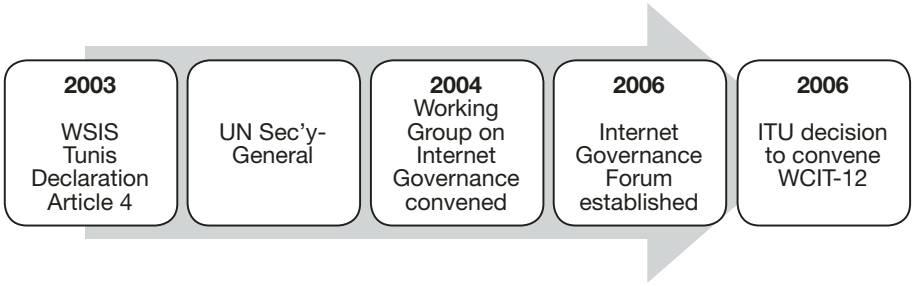

Figure 3. Selected Points of Engagement of the ITU and UN on Internet Governance

Prior to the conference, ITU Secretary-General Hamadoun Touré stated publicly that WCIT-12 would seek consensus around the technical issues with which the ITRs have traditionally dealt. Touré wanted to avoid earlier controversies at the WSIS and the WGIG around the governance conundrum, and to keep off the table the issues of freedom of speech on the internet and electronic access that had become so much more politically divisive since the 2003 Tunis Declaration. In particular, tensions were running high around the role played by the internet in the Arab Spring uprisings and other social unrest around the globe.[29] Yet delegates had already understood the inevitability of a clash at WCIT-12 between the opposing approaches that had come to the fore since Tunis, as controversial proposals were submitted in the months leading up to the conference.[30]

Freedom of Information on the Internet and Access to Digitized Information

Substantive Norms under General International Law

Domestic law reflects the internal balance that governments strike between the issues of freedom of information and access to data and other constraints

such as national security, privacy, and intellectual property rights. When communications cross state borders, international law considerations also become relevant, in particular, the right to receive and transmit information across national borders. This freedom is recognized in Article 19 of the Universal Declaration of Human Rights:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers.*[31] (emphasis added)

The evolution of the legal norm embodied in Article 19, the article of the same number in the 1966 International Covenant on Civil and Political Rights, along with similar provisions in several regional human rights treaties,[32] has an interesting history rooted in the nineteenth century concepts of democracy and freedom of expression in domestic legal systems.[33] While acknowledging that freedom of information emerged as a legal concept on the international level only in the second half of the twentieth century, Malancuk has noted that:

> From the very beginning, individual liberal constitutions have attached particular importance to freedom of opinion and expression, freedom of the press, and freedom of information of the individual in the sense of the right to receive, impart and seek information and ideas regardless of frontiers.[34]

The scope of freedom of information across national borders – and the enforcement of this provision – has waxed and waned in accordance with both technological developments and the state practice that reflects them. Debate remains among scholars regarding whether Article 19 embodies a customary norm of international law,[35] although the question of derivation of this right from international treaty law or customary law may, in the event, be largely moot, given the widespread accession of states to treaties containing an "Article 19" provision and the body of domestic and international jurisprudence surrounding it.[36] According to Mayer-Schonberger and Foster, "While speech has never enjoyed – and never will enjoy – absolute protection, the principle of freedom of speech has become part of a minimum standard of freedoms for the great majority of nations.[37]

Metzl has also argued convincingly that there is a "strong presumption" in international law supporting the international right to communicate, although it may have limitations in extreme circumstances such as the Rwanda radio broadcasts inciting to engage in genocide of the Tutsis in the early 1990s. He argues that these broadcast may have legitimately been jammed by other states, and that there may even be a duty to jam broadcasts that violate *jus cogens*, or in circumstances where the jamming can mitigate a humanitarian crisis.[38] This conclusion is supported by UN Charter Article 41, which permits the Security Council to call upon members to interrupt "postal, telegraphic, radio and other means of communication" as a response to a threat to peace, danger to peace or aggression.[39]

Extending the analysis above into the context of internet communication, freedom of information is codified at the international level as a technology-neutral right, although there are specific limitations on its scope due to illegal content, such as incitement of racism, child pornography, and the like.[40] In particular, freedom of information in cyberspace, as with other types of trans-border communication, may be limited by the international community for *jus cogens* considerations, such as the prevention of incitement to genocide.[41]

ITU Treaty Law

The ITU regime also provides a strong normative backbone for ensuring open and uninterrupted international communications. Trans-border freedom of information and access are supported by several principles of the ITU constitution that govern the global use of telecommunication infrastructures and resources.[42] The first is embodied in Article 33, prescribing the non-discriminatory use of communications infrastructure:

> Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference.[43]

This "public right" may be limited by the authority of states under Articles 34 and 35, which permit states to suspend ingoing and outgoing communications with respect to their own national territory, conditional upon public notification of stoppage or suspension.[44] This authority, stemming from a state's capacity

as a sovereign to control the flow of information domestically, does not extend beyond its borders.

Under Article 38, states are required to ensure optimal technical conditions for uninterrupted international telecommunications, and to refrain in particular from disrupting operations in other states. These constitutional principles are incorporated into Article 1 of the ITRs as follows:

> These Regulations establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services.[45]

Article 3 states that any user "has the right to send traffic," subject to domestic law. And under Article 4, "International telecommunication services," member States "shall promote the development of international telecommunication services and shall foster their availability to the public."[46]

In summary, trans-border freedom of expression, information, and access to data, as codified in Article 19 of the Universal Declaration of Human Rights and the ITU constitution, are broadly recognized principles of international law. In addition, ITU treaty law prescribes a free flow of information across borders at both the technical and substantive levels. Differences in interpretation and enforcement of these principles by countries relate to the types of content that are covered by them. They leave open the controversial issue of content regulation in trans-border communication, which was the basis for the clash of approaches at WCIT-12.

The Dubai Clash and Cyber Security

Internet Governance and Cyber Security

The breadth and depth of public interest in the Dubai conference marked a significant departure from ITR conferences of the past.[47] In the months leading up to WCIT-12 the unprecedented media attention included high profile op-eds in the *New York Times* and the *International Herald Tribune*,[48] a public protest by Google on its "Take Action" website,[49] a global petition to "Protect Global Internet Freedom,"[50] and a Wikileaks-style website publishing conference documents.[51] This activity was prompted by several conference proposals submitted by member states, perceived by the US, Europe, and their allies as threats to cyber security by their calling into

question the multi-stakeholder status quo and enhancing state sovereignty and discretion over internet infrastructure.[52] For instance, Russia proposed the addition of an ITR article providing an alternative to the current ICANN domain name scheme:

> Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of the basic Internet infrastructure.[53]

Other controversial proposals by China and the Arab bloc dealt with altering the financing model for internet communications (to a "sending party pays" model), adjusting network security, broadening the jurisdictional scope of the ITRs to include private operating agencies such as internet service providers, and blocking spam.[54]

The controversy around spam provides an example that is especially relevant to the freedom of speech and access issues around which much of the WCIT-12 debate pivoted. The new ITR Article 5B prohibiting spam states:

> Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.[55]

Inclusion of the new article raises two questions: the first regarding the potentially *ultra vires* expansion of the scope of the ITRs to an issue that arises exclusively in the context of internet communications, rather than telecommunications as a whole. The second relates to the US-Europe perception that the blocking of spam by governments (and the decision of what constitutes spam) marks a slippery slope to internet content regulation.[56] While the domestic law of member states defines illicit content in accordance with each country's legal system irrespective of the ITRs, Article 5B is perceived by Western countries as providing superfluous and detrimental international legal cover for unwarranted content regulation.[57] The potential for abuse of power by states claiming to implement cyber security measures vis-à-vis spammers but in fact wanting to crack down on dissidents was understood by the US and its allies as a threat to freedom of communication

and digital access. A recent report by the Council on Foreign Relations summarized this normative tension at WCIT-12:

> Confronted with this challenge, the global community faces a dilemma. The neutrality of the Internet has proven to be a formidable ally of democracy, but the cost of protecting users' freedom is skyrocketing. Critical services, such as e-commerce or e-health, might never develop if users are not able to operate in a more secure environment. Moreover, some governments simply do not like ideas to circulate freely.[58]

Thus, while the Dubai ICT revisions may not constitute radical de facto changes in the present model of internet governance, the perception of Western democracies that basic values were undermined by their inclusion in international treaty law brought about the current stalemate.

Israel's Position at WCIT-12

The Israeli position at WCIT-12 regarding internet governance and cyber security remained squarely in the camp of the Western democracies. Its "Proposals for the Work of the Conference" took a position against any reform of the ITRs affecting the internet: [59]

> It is our strong belief that the existing global, transparent, multistakeholder, bottom-up model of Internet governance is effective and inclusive, and must remain in effect.
> Recognizing the immense contribution of the Internet to economic growth and to human welfare, as well as to the promotion of free speech and human rights, Israel shares the concern of many, that the development of this invaluable asset may only be hindered if it is brought under governmental or intergovernmental regulation.[60]

In addition to opposing future ITR provisions furthering global internet governance in any form, the Israeli proposal opposed the conference's adoption of any specific business or commercial model, mandatory telecom standards, any departure from technological neutrality, jurisdiction over spam, and the determination of any architectural preference pertaining to the internet.[61] The position regarding cyber security encompasses an especially

clear expression of Israeli governmental policy regarding its minimalist view of the scope of the ITRs, and refers to the Article 19 rights reviewed above:

> Cybersecurity is outside the purview of the ITU […]. We believe that any text in the ITRs related to security should be narrowly focused on international telecommunication networks, should not involve content or information security, should avoid topics related to law enforcement or national security, and should be fully consistent with Member State commitments under the UN Declaration on Human Rights.

Israel voted with the US-EU bloc at the conclusion of WCIT-12.[62]

Trends and Conclusions

In purely legal terms, the result of the Dubai Clash at WCIT-12 presents the anomaly of an international treaty that as of January 1, 2015 will be in force in two different versions for two groups of ITU member states. It is an open question whether this anomaly will prove to have significant impact on the ongoing functioning of the internet and the future of internet governance.

In any event, this situation constitutes serious evidence of the "Zittrain moment" that will determine the future structure of cyberspace. Will blocs of countries decide to cede from the open, unrestricted access of the present world wide web into their own virtual private networks (VPNs) with restricted content? Will a "grey internet" develop, providing access from these VPNs to illicit content for a price? Are we on the way to content tiering, with information of a higher quality available at steeper rates for those who can pay, or only data paid for by the wealthy being widely accessible, as hinted at in the current hearings on net neutrality in the US Court of Appeals for the District of Columbia?[63] As one observer wrote at the end of WCIT-12:

> The real story here is a world in which there are two competing visions for the future of the internet—one driven by countries who believe the internet should be more open and free—and one driven by the opposite. Whether or not the [ITRs are] ever meaningful or effective, these two visions of the internet are unlikely to go away any time soon.[64]

The global dilemma regarding the internet's future may not in fact have a successful resolution. At its heart are issues of state sovereignty over the

types of information that governments believe their citizens should by right be able to transmit and receive, in a global context of ever-increasing cyber security concerns. The requisite balance of information and access rights with security and law enforcement concerns has yet to be achieved within many countries, much less globally.[65] Perhaps the legal and policy vacuum exposed by the Dubai conference might only be effectively addressed, and potential damage mitigated, by a highly pragmatic and forward-looking initiative of major internet stakeholders, anchored in the steep normative, economic, and security costs of ongoing non-resolution. Specifically, in the absence of clarification of the normative parameters of internet governance for freedom of information and access, global cyber security will continue to be characterized by normative uncertainty and the absence of state and organizational responsibility for illicit behavior on the internet. The upcoming ITU Plenipotentiary Conference of all member states in 2014 in Busan, Korea will provide an important opportunity to make progress beyond the Dubai clash.

Notes

1 J. Zittrain, The Future of the Internet and How to Stop It (2008).

2 In Q2 2012, the site *Internet World Stats* showed 2,405,518,376 users (www.internetworldstats.com/stats).

3 See, for instance, Center for Strategic and International Studies, The Economic Impact of Cybercrime and Cyber Espionage (July 2013); observations on the US-China consultations on illegal uses of the internet (*Admit Nothing and Deny Everything*, The Economist, June 8th, 2013); and "Digital Wildfires" in World Economic Forum, Annual Report (2013).

4 *See* European Union, European Internet Security Strategy (April 2013): "Even if sovereignty considerations have become increasingly important, there is evidence that the participation to international cooperation or policy frameworks is positively related to the cyber security performance of a country; additionally, cyber-threats are not confined by administrative borders as network and information systems are globally interconnected." Lest we think that only non-Western, non-democratic governments engage in the regulation of internet access, it is worth noting the recent FCC hearings in Washington D.C. on access regulation. *See* E. Wyatt, *Verizon-F.C.C. Court Fight Takes On Regulating Net*, The New York Times, September 8th, 2013.

5 Zittrain and others have since focused on particular examples of this tension. In his 2011 book, Access Contested (J. Zittrain, R. Deibert, J. Palfrey and R. Rohozinsky, eds., 2011), he examines "the interplay of national security, social and ethnic identity, and resistance" in the context of internet regulation by Asian governments.

6 Zittrain, *supra* note 1, 5.
7 *Ibid*., 51.
8 Formally, the conference is named the *World Conference on International Telecommunications*.
9 WCIT convenes periodically as an intergovernmental conference under the auspices of the International Telecommunication Union (ITU), the UN specialized agency responsible for international communications infrastructures and development. *See generally,* A. Noll, *The ITU in the 21st Century*, 5 Singapore Journal of International and Comparative Law 63 (2001). See also the ITU website for the Final Acts of WCIT-12, December 14th, 2012, http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.
10 WCIT-12 Final Acts *, ibid*., at Article 1.3, "Purpose and Scope of the Regulations." A comprehensive explanation of the challenges of interoperability can be found in OECD, Communications Outlook 137-176 (2013), http://dx.doi.org/10.1787/comms_outlook-2013-en.
11 "The question becomes more urgent every day: Should the Internet remain an end-to-end, neutral environment, or should we sacrifice Internet freedom on the altar of enhanced security?" A. Renda, *Cybersecurity and Internet Governance*, Council on Foreign Relations, May 13th, 2013, http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621.
12 Defending an Open, Global, Secure, and Resilient Internet 67 (J. Negroponte and S. Palmisano, eds., 2013).
13 The operative definition was drafted by Study Group 17 of the ITU Telecommunication Sector: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, Confidentiality." (ITU-T X.1205, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx). For Israel's definition, see *Government Decision No. 3611* of August 7, 2011. http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.
14 The Council of Europe's Convention on Cybercrime is the one exception. Israel is presently in the process of accession (Convention on Cybercrime, 23 November, 2001, 185 CETS).
15 190 ITU Member States were party to the 1988 ITRs. For various procedural reasons, only 144 delegations had voting rights at WCIT-12. 89 states signed the revised ITRs (in black) and 55 did not (in red). In terms of population, the signatories represent 3.8 billion people, and the non-signatories 2.6 billion; *see* M. Masnick, *Who Signed the ITU WCIT Treaty…And Who Didn't*, Techdirt, December 14th, 2012.

16 Cited in W. Rash, *WCIT Treaty Talks End in Dubai With Walkout of U.S., Allies*, EWeek, December 15th, 2012, http://www.eweek.com/cloud/wcit-treaty-talks-end-iin-dubai-with-walkout-of-us-allies-2#sthash.mRAJCe98.dpuf.

17 Although the jury is still out on the final result of ITU member state ratification processes, which need to conclude by January 1, 2015 when the revised ITRs enter into force, some observers are skeptical that the amended ITRrs will have significant impact on internet operation. See M. Mueller, *ITU Phobia: Why WCIT was derailed*, Internet Governance Project, December 18th, 2012.

18 *See* International Telecommunication Regulations, Melbourne (1988), http://www.itu.int/pub/T-REG-ACT-1988.

19 D. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, 17 ASIL Insights, February 7th, 2013.

20 ICANN is the Internet Corporation for Assigned Names and Numbers, famously incorporated in California as a non-profit public benefit corporation. For an example of challenge to ICANN's accountability, see D. Lindsay, *ICM Registry v. ICANN: Introductory Note*, 49 International Legal Materials 956, 956-1002 (2010).

21 The Internet Society is a Geneva-based non-profit (www.internetsociety.org). *See generally* the Internet Society 2012 Annual Report.

22 The Internet Engineering Task Force, *see* www.ietf.org.

23 MACHBA, or the Inter-University Computation Center (IUCC), is a non-profit organization established in 1984 by eight Israeli universities and is supported by the Council for Higher Education; the Israel Internet Association was established in 1994.

24 *See* European Parliament Resolution on the forthcoming World Conference on International Telecommunications (WCIT-2012) of the International Telecommunications Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP), 20/11/2012); and C. Franzen, *European Parliament Adopts Resolution Vowing to Fight ITU Internet Regulation*, TPM IdeaLab, November 23rd, 2012.

25 In addition, according to Cisco's VNI Forecast, global IP traffic volume has grown eightfold over the period 2006-11.

26 *See, The Future of Internet Governance*, 101 Proceedings of the Annual Meeting of the American Society of International Law 201, 201-213 (March 28th-31st, 2007).

27 "We recognize that freedom of expression and the free flow of information, ideas, and knowledge, are essential for the Information Society and beneficial to development." (WSIS-05/TUNIS/DOC/7-E, 18, Article 4, November 2005).

28 The ITU Constitution and Convention set out substantive norms such as the public's right to trans-border communication (Constitution, Article 33) and states' responsibility for the maintenance of international infrastructures (Constitution, Article 38), www.itu.int/aboutitu/Basic_Text_ITU-e.pdf.

29 For a review of some of the tensions between Arab governments and their citizens regarding the use of the internet in mid-2012, see T. Pavel, *Continuing as Usual*, Makor Rishon 8, April 27th, 2012.

30 In an attempt to perhaps soften the divide, the head of the United States' delegation welcomed the increasingly non-Western character of the World Wide Web in a

December 13 interview, at the conclusion of the conference. *See* J. Crook, *United States Rejects International Telecommunications Union Conference Outcome, Fearing Interference with Internet Freedom,* in J. Crook, *Contemporary Practice of the United States Relating to International Law*, 107(2) American Journal of International Law 431 (2013).

31 UNGA 217 A (III) 1949. Article 29 potentially tempers the scope of Article 19 and other rights set forth in the Declaration by prescribing "respect for the rights and freedoms of others" and the requirement of "meeting the just requirements of morality, public order and the general welfare."

32 *See* Article 10 of the European Convention on Human Rights, 4 November 1950, E.T.S. No. 5; Article 9 of the African Charter on Human and Peoples' Rights, 26 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982); and Article 13 of the American Convention on Human Rights, 22 November 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123.

33 See P. Malancuk, *Information and Communication, Freedom of*, in 9 Encyclopedia of International Law 148, (R. Bernhardt et al. eds., 1986).

34 *Ibid.*

35 Malancuk does not agree that an international custom has been established (*ibid*., 168).

36 *See, e.g.*, Autronic AG v. Switzerland, 22 May 1990, ECHR, Application No. 12726/87; Khursid et al v. Sweden, 16 December 2008, ECHR, Application no. 23883/06; and *Satellite jamming and freedom of expression*, statement of Article 19 organization regarding the jamming of LuaLua TV in Bahrain, 21 November 2011, http://www.bahrainrights.org/en/node/4855.

37 *See* V. Mayer-Schonberger and T. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, in Borders in Cyberspace 243 (B. Kahin and C. Nesson eds., 1999).

38 Mayer-Schonberger and Foster also advocate a *jus cogens* approach *(ibid.). See also* Prosecutor v. Ferdinand Nahimana et al*,* Case No. ICTR -99-52-T (3 December 2003).

39 The article states: 'The Security Council may ... call upon the Members of the United Nations to apply such measures [as] complete or partial interruption of ...postal, telegraphic, radio, and other means of communication....' , Article 41, Charter of the United Nations, 26 June, 1945, 1 UNTS 14.

40 See the Additional Protocol to the Convention on Cybercrime (28 January 2003, CETS 189) concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems: Council of Europe, 2003. Some jurists have proposed that a *jus cogens* approach to prohibited content on the internet may lead the way to resolution of the current impasse.

41 Prosecutor v. Ferdinand Nahimana et al, *supra* note 39.

42 For discussion of the customary elements of the ITU regime, see P. Malancuk, *Telecommunications*, *International Regulation*, in 9 Encyclopedia of Public International Law 367 (R. Bernhardt et al., eds., 1986).

43 ITU Constitution, *supra* note 29, at Article 33.

44 They are respectively entitled 'Stoppage of Telecommunications' and 'Suspension of Services', ITU Constitution, *ibid.,* note 29.

45 Article 1, Purpose and scope of the Regulations, *supra* note 9.
46 *Ibid.*
47 WCIT convenes periodically as an intergovernmental conference under the auspices of the International Telecommunication Union (ITU), the UN specialized agency responsible for international communications infrastructures and development. On the ITU in general, see A. Noll, *The ITU in the 21st Century*, 5 Singapore Journal of International and Comparative Law 63 (2001).
48 V. Cerf, *Keep the Internet Open*, The New York Times, May 24th, 2012; and *Global Internet Diplomacy*, The International Herald Tribune, December 12th, 2012.
49 *Google attacks UN's internet treaty conference*, BBC News, November 21st, 2012.
50 The petition stated: "Internet governance decisions should be made in a transparent manner with genuine stakeholder participation from civil society, governments and the private sector. We call on the ITU and its member states to embrace transparency and reject any proposals that might expand ITU authority to areas of internet governance that threaten the exercise of human rights online."
51 The site is WCITleaks.org. Although the conference materials were not confidential, access was limited by the need for registration and a password.
52 *Supra* note 12.
53 Russian Federation, *Proposals for the Work of the Conference*, Document 27, WCIT-12, 17 November 2012, Article 31B.
54 For a full review of the relevant provisions, see Fidler, *supra* note 19. He focuses on the revised Preamble, the addition to Article 1, the revision of Article 1.1, new Articles 5A and 5B, and Resolution 3.
55 WCIT Final Acts, *supra* note 9.
56 Fidler, *supra* note 19.
57 *Ibid.*
58 A. Renda, *supra* note 11.
59 Israel (State of), *Proposals for the Work of the Conference*, Document 28, World Conference on International Telecommunications, 19 November 2012.
60 *Ibid.* Despite the final paragraph quoted here, Israel does in fact regulate the internet, as do the US, the EU and other countries that opposed the adoption of the WCIT-12 Final Acts. The divisive issue is international, not domestic, regulation of the web.
61 *Ibid.*, at I and II.
62 See also the Ministry of Communication's recent notice regarding the Telecom Network Neutrality Bill, which passed its first Knesset reading on October 28, 2013, http://www.moc.gov.il/sip_storage/FILES/5/3355.pdf.
63 See the current US hearings around internet tiering, E. Wyatt, *Judges Hear Arguments on Rules for Internet*, The New York Times, September 10th, 2013, at B1.
64 *Supra* note 15.
65 Melissa Hathaway has recently lamented the plethora of international bodies now engaged with these issues, in her words an "operational collision" of competing interests that are stifling any progress that might be made. (M. Hathaway, *Change the Conversation, Change the Venue and Change Our Future*, Harvard Kennedy School Belfer Center, May 13th, 2013, http://www.technologyandpolicy.org/2013/05/14/change-the-conversation-change-the-venue-and-change-our-future/#.UnuDkXC9klk).