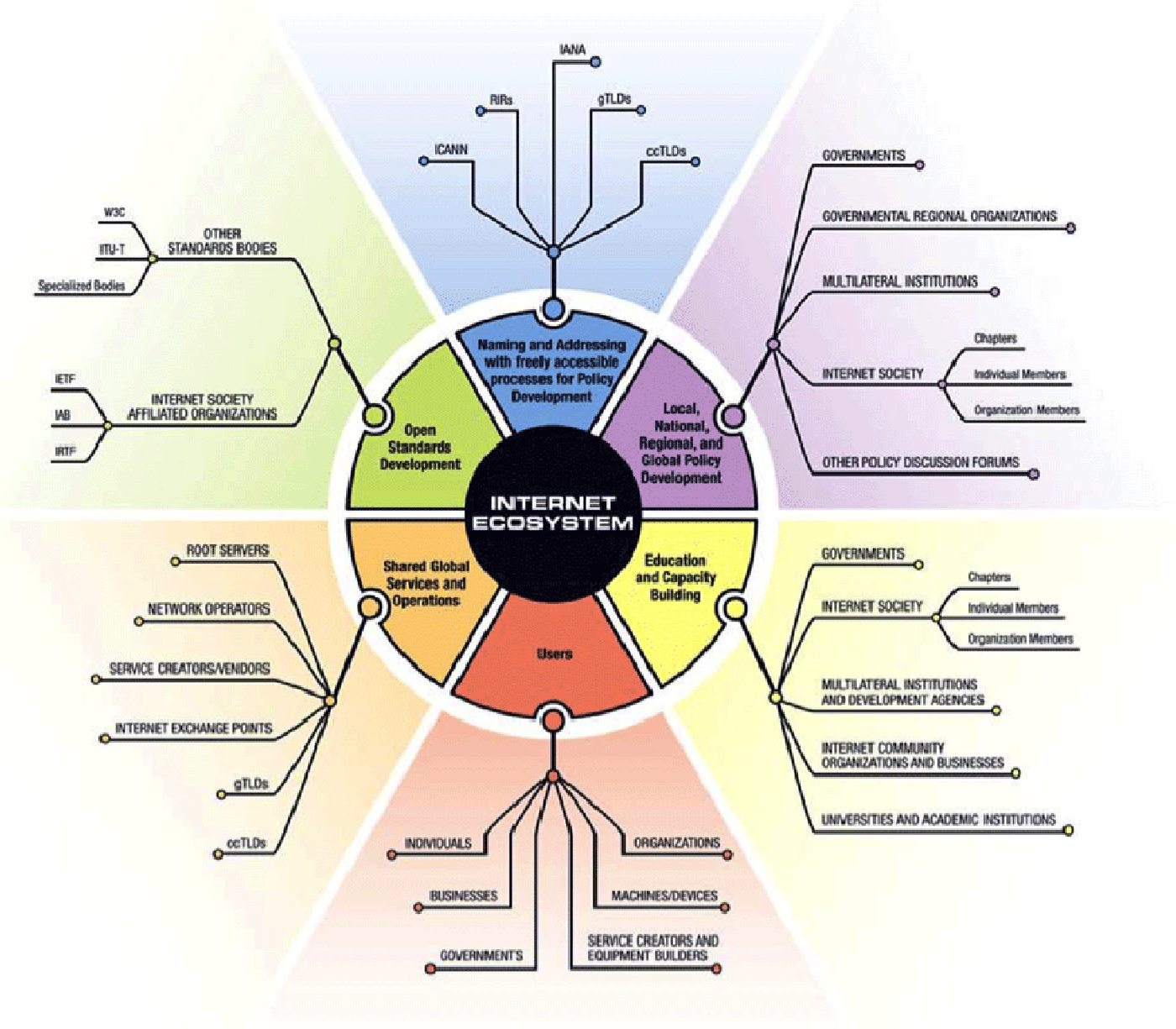


# International policy debates on Internet and broadband: A post WCIT view

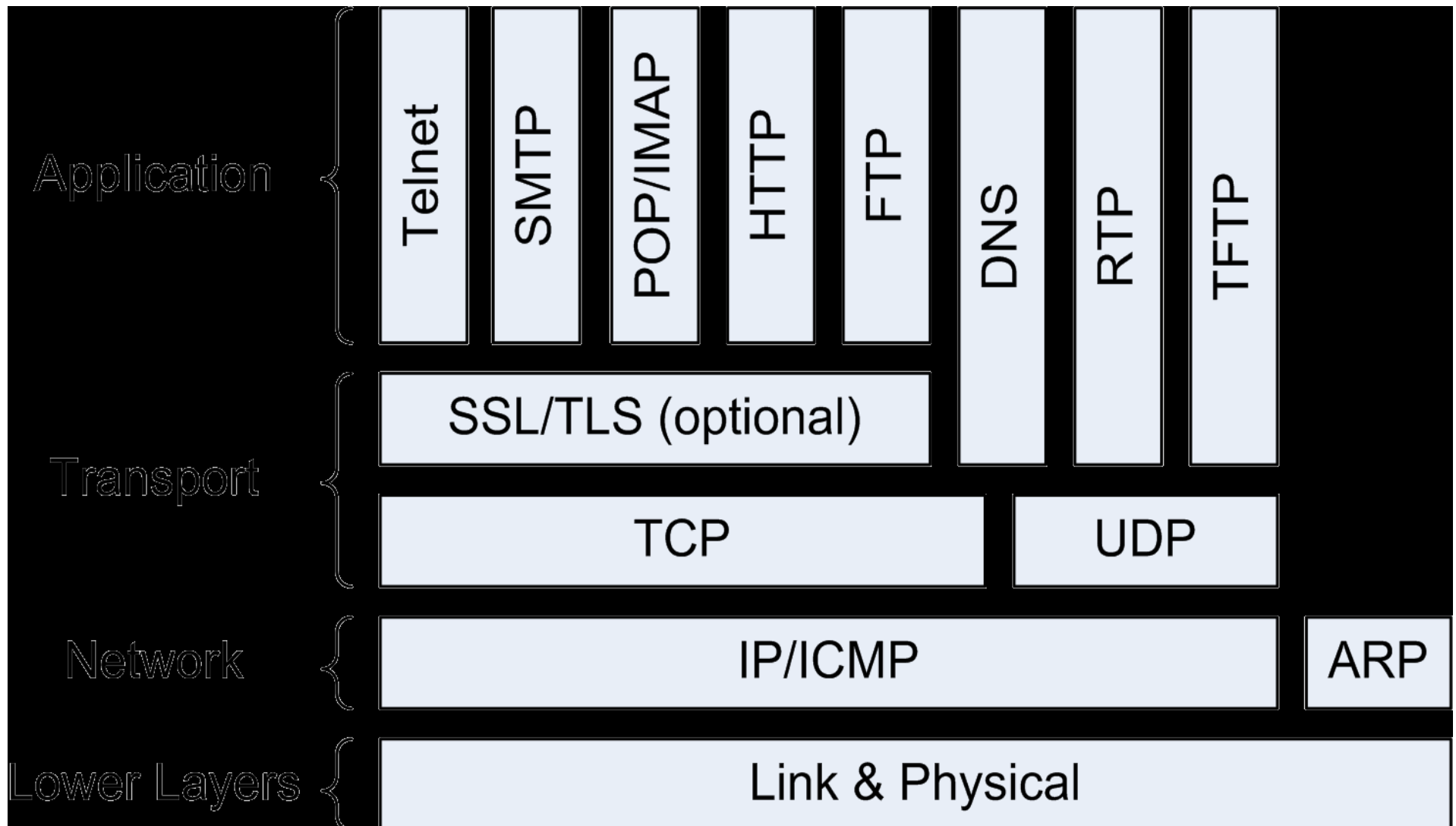
Rohan Samarajiva

Bangalore, April 5-8, 2013

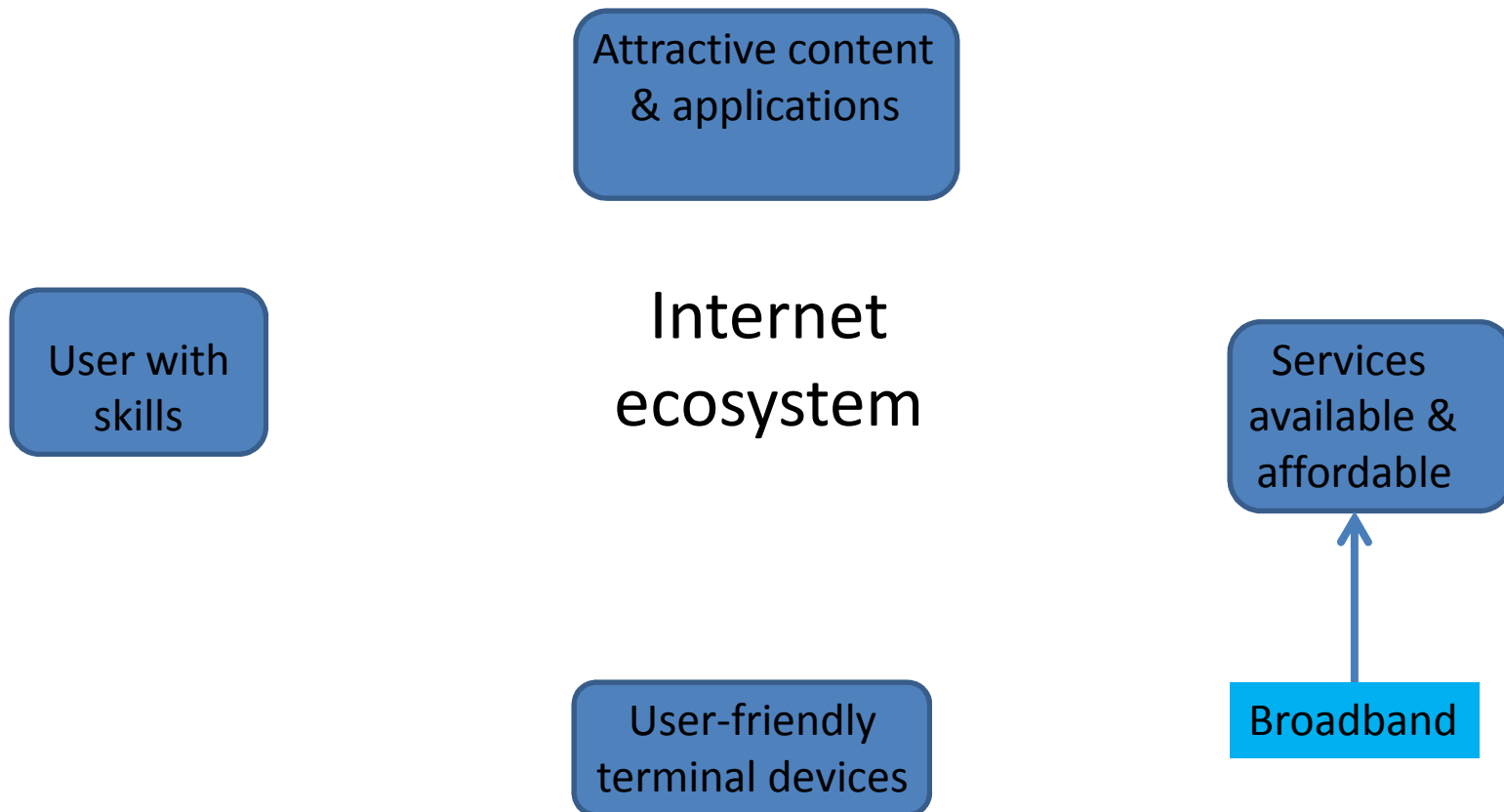




# Our focus: Lowest layer: physical layer below IP/ICMP and ARP



# Another conceptualization



# Users

- Within national territory
- Education is the principal input
- Within the control of national/local governments; no significant international influence?

# Terminal devices

- Globalized design and manufacture
- Lots of R&D required to make terminal devices more usable for people
- Not much intervention from government other than extracting taxes
  - In a few countries, industrial policy actions to increase manufacturing within the country

# Content & apps

- Can be from within country or outside
- Primary interest of government is in controlling content, and possibly some apps
- Telcos care most about video that imposes demand on their networks
- Also care about apps such as Skype that may eat into their revenues

# Services (this is where broadband fits)

- Provided by regulated entities, who are subject to national law, regulations, license conditions, international treaties that have the effect of national law
- Historically, “administrations” have been bound to act according to International Telecom Regulations (ITRs) and International Radio Regulations (IRRs), both within the jurisdiction of the ITU
  - This was in a different context, when “administrations” for the most part were government-owned monopolies and the ITRs governed bilateral monopolies where both sides agreed to exploit each other’s customers
  - 1988 Melbourne WCTTI marked the beginning of the transition to a competitive environment
    - Article 6 still talked about Sending Party Network Pays, but Article 9 allowed for commercial agreements that were bilaterally agreed upon



# In sum

- In theory, ITU had
  - A significant role to play with regard to telecom services, including infrastructure
  - An important role in spectrum regulation, especially for aeronautical, marine, satellite communication
    - But most importantly in terms of spectrum and standards
  - A role in equipment standards
  - But not content and not apps

# Gradual displacement of ITU

- IETF, IEEE etc. had assumed a much larger role in equipment standards over time
  - What are WiFi standards called?
  - What are WiMAX standards called?
- Even where ITU decisions had formal importance (as in Spectrum), industry consensus was reached outside and brought to ITU for formalization
- Until 2000, ITU Telecom World was the major meeting place for industry, govt, etc. where ideas were explored and consensus achieved
  - Now, almost eclipsed by GSM Mobile World (73,000 attendance in 2013) and other conferences
- ITU-D continues to supply “expertise” to development countries in competition with World Bank and regional banks

# World Summit on Information Society and Internet Governance Forum

- 2002-2005 WSIS 1 & 2
  - ITU organized
  - But under UN Secretary General, who
    - Kept UNESCO, UNCTAD etc. involved
    - Created a multi-stakeholder platform known as Internet Governance Forum that has been meeting yearly since 2006
- IGF does not have any formal powers
  - “Just a talk shop”

# Who wants authority over the Internet?

- ITU, which sees its domain shrinking
- Russia and China
  - Who want control over all aspects of the Internet
- Other countries that chafe at the control exerted by the US
  - Those who want some checks and balances against unilateral moves such as SOPA & PIPA

# WCIT & Internet governance

- Dubai was a debacle for ITU
  - Unprecedented failure of consensus building that is likely to damage the viability and credibility of the ITU
    - Possible that ITU will have to retrench and become a smaller organization with a smaller remit
- Is IGF and multi-stakeholderism the solution?
- Is there a problem that requires a solution?

# Ron Diebert on post-WCIT intellectual agenda

- At the core of the **distributed security model** are several key principles, which in turn can form the basis for the pillars of global cyber security policy: mixture, division, and restraint.
  - Mixture = intentional combination of multiple actors with governance roles and responsibilities in a shared space
  - Division = a design principle that no one of these actors is able to control the space in question without the cooperation and consent of others
  - Restraint
- “As an approach to global cyberspace security and governance, these can provide a more robust foundation for the empty euphemism of ‘multi-stakeholderism,’ and a principle upon which to counter growing calls for a single global governing body for cyberspace.”
- Citizens, the private sector, and governments all have an important role to play in securing and governing cyberspace—but none to the exclusion or preeminence of the others

Ronald Deibert, *The Growing Dark Side of Cyberspace ( . . . and What To Do About It)*, 1 Penn. St. J.L. & Int'l Aff. 260 (2012).

Available at: <http://elibrary.law.psu.edu/jlia/vol1/iss2/3>

# Follow the money

- ETNO proposals (appearing in modified form in Africa and Arab States proposals) focused on Article 6 & sought to
  - Reaffirm international settlements regime for voice (not reversing the Melbourne compromise embodied in Article 9)
  - Extend the Melbourne compromise to the Internet through imposition of sending party network pays principle
- Voice provisions more liberal than Melbourne; data language failed to make the final text

# Final text from WCIT Chairman

- **42A International telecommunication arrangements**

**42B 6.1**

*Subject to applicable national law, the terms and conditions for international telecommunication service arrangements may be established through commercial agreements or through accounting---rate principles established pursuant to national regulation.*

**42C 6.1.1**

*Member States shall endeavour to encourage investments in international telecommunication networks and promote competitive wholesale pricing for traffic carried on such telecommunication networks.*

**42D Accounting---rate principles**

**42DA Terms and conditions**

**42E 6.2**

*The following provisions may apply where the terms and conditions of international telecommunication service arrangements are established through accounting---rate principles, established pursuant to national regulation. These provisions do not apply to arrangements established through commercial agreements.*



# But SPNP\* not buried

- Possibly, the WCIT debates shifted the goal posts and legitimated efforts to apply government pressure on OTTs to make payments to telcos
  - ETNO is keeping up the pressure
  - More governments than Togo may be tempted to think of another source of revenue
    - And the attendant benefits

\* Sending party network pays

# A story that illustrates the issues

- Once upon a time, there was a sleepy old railway company, serving a sleepy old town. The tracks were old, the rolling stock had been paid for, and the customers were regular. The money was not great, but neither was it bad. The engineers working for this company led a quiet life. They would occasionally talk about how good it would be to have new business and new investment, but that was just talk.
- Then came change, in the form of big amusement park that attracted large numbers. The trains were now crammed full at peak times, and sometimes one could not even board the train. It was clear that major new investments would have to be made to accommodate the qualitatively higher traffic volumes and expectations. It was not in the interest of the amusement park to have grumpy customers who had been tortured by a sub-optimal transport system. It was definitely not in their interest to have their potential customers unable to make the journey at all.

# The story continued

- The first reaction of the engineers running the trains was to seek government intervention in the form of compulsory levies and taxes and even actions to limit demand. The amusement park fought back. The battle continues.
- Parallel to this confrontation, there were those on both sides who sought common ground. Could the “big data” capabilities of the amusement park, used for marketing and for smoothening the peaks and valleys of demand for its attractions, be mobilized to better manage the demand for the trains? Could the amusement park take over parts of the ticketing and reception interfaces (the stations) of the system? Could there be joint ventures?

# Implications if SPNP is implemented

- Internet take-up will stall, especially in markets with limited purchasing power
- It will be easier to pull the kill switch

(Copyright: Thinkstock)

If you think the most vulnerable regions are autocratic regimes or civil war zones, think again. Many countries or regions are at severe risk of disconnection. Here's why.

### Related



Weighing up the web's impact



System failure in cyber warfare?



Becoming biohackers

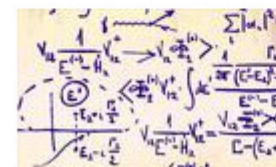


How many phone calls does it take to kill the internet? It seems like an odd question to ask about a network once thought to be strong enough to withstand a nuclear attack. However, first-strike mushroom clouds aren't the biggest threat to the internet anymore. Just ask the citizens of [Libya](#), [Egypt](#) and [Syria](#): nations whose connections have been recently severed, albeit temporarily.

But if you think that the internet's most vulnerable regions correspond to autocratic regimes or civil war zones, think again. Following the Syrian blackout in late 2012, Renesys, a consultancy that specialises in monitoring and mitigating risks to connectivity, [created a map](#) ranking every country's "risk of internet disconnection". They found resilience has little to do with the presence or absence of jackbooted thugs: Belarus is at "significant risk" of internet disconnection, while China – which blacked out the entire province of Xinjiang for ten months in 2009 and 2010 – is rated at "low risk".

How can this be? Renesys simplified the question of global internet resilience by tracking one metric: the number of so-called "frontier" internet service providers (ISPs) that a country has. A frontier ISP is one that maintains connections or gateways to the global internet at large, not just to its own domestic network. "Not all ISPs have or need connections to the outside world," says Jim Cowie, chief technology officer and co-founder of Renesys. "Comcast, for example, only sells internet service in the United States."

It's this number of international gateways, then, that captures how difficult it would be to snuff out a country's internet pulse. Disable them, and the global web goes dark. The more gateways there are, the more difficult it will be to neutralise all of them.



# Renesisys sees limited number of frontier ISPs as the key

- But think of Bangladesh and Pakistan where all ISPs have to go through government-sanctioned gateways from which governments collect around 50% rent

# Were the Americans wrong?

- To refuse to sign because of spam provisions
  - Is this the camel's head in the tent? One man's spam is another man's content
- What was wrong with Resolution 3?

### To foster an enabling environment for the greater growth of the Internet

The World Conference on International Telecommunications (Dubai, 2012),

*recognizing*

- a) the outcome documents of the Geneva (2003) and Tunis (2005) phases of the World Summit on the Information Society (WSIS);
- b) that the Internet is a central element of the infrastructure of the information society, which has evolved from a research and academic facility into a global facility available to the public;
- c) the importance of broadband capacity to facilitate the delivery of a broader range of services and applications, promote investment and provide Internet access at affordable prices to both existing and new users;
- d) the valuable contribution of all stakeholder groups in their respective roles, as recognized in § 35 of the Tunis Agenda for the Information Society, to the evolution, functioning and development of the Internet;
- e) that, as stated in the WSIS outcomes, all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized;
- f) Resolutions 101, 102 and 133 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference,

*resolves to invite Member States*

1 to elaborate on their respective positions on international Internet-related technical, development and public-policy issues within the mandate of ITU at various ITU forums including, *inter alia*, the World Telecommunication/ICT Policy Forum, the Broadband Commission for Digital Development and ITU study groups;

2 to engage with all their stakeholders in this regard,

*instructs the Secretary-General*

1 to continue to take the necessary steps for ITU to play an active and constructive role in the development of broadband and the multistakeholder model of the Internet as expressed in § 35 of the Tunis Agenda;

2 to support the participation of Member States and all other stakeholders, as applicable, in the activities of ITU in this regard.