Media pluralism & Internet governance: A post WCIT view

Rohan Samarajiva

CEPS, Brussels

March 20, 2013

LIRNEasia
www.lirneasia.net

This work was carried out with the aid of a grant from the International Development Research Centre, Canada and the Department for International Development, UK

IDRC CRDI DFID Department for International Development Canada

Media pluralism in developing world

- Increasingly dissenting views have shifted to online “newspapers,” YouTube, Facebook, Twitter, etc.
- Most entities that value their independence from their governments keep their websites abroad and do not rely on country TLD
- China and Iran at forefront of trying to create national Internets to improve their ability to control dissenting views

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

(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.







Renesys 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

SPNP is not only impractical; it is harmful to media pluralism in developing world

- The advertising-based business model of the OTTs is what makes it possible for independent voices to flourish
- No guarantee that dissenting media can flourish even under present arrangements, but SPNP will make it much, much harder