

Internet Governance

United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT)

Bonbudong, 3rd Floor Songdo Techno Park 7-50 Songdo-dong, Yeonsu-gu, Incheon City Republic of Korea Telephone: +82 32 245 1700-02 Fax: +82 32 245 7712 E-mail: info@unapcict.org http://www.unapcict.org

Summary

The Internet raises significant challenges for public policy and sustainable human development. Hence the ongoing development of international policies and procedures to govern the use and operation of the Internet. Internet Governance, however, is more about governance than the Internet, and there are a number of political issues concerning international Internet policy, the use and abuse of the Internet, as well as the deployment of the Internet to help achieve social and economic development. Governments need to understand these issues if they are to have a voice in the global information network. The first section of this briefing note provides a brief history of and context for Internet Governance. The next section gives an overview of the report developed by the Working Group on Internet Governance, the political tension around the most contentious aspects of Internet Governance, and the rise of the Internet Governance Forum. In the final section, a roadmap is suggested to guide policymakers in developing a plan of action for addressing Internet Governance issues at the local, regional, and global levels.

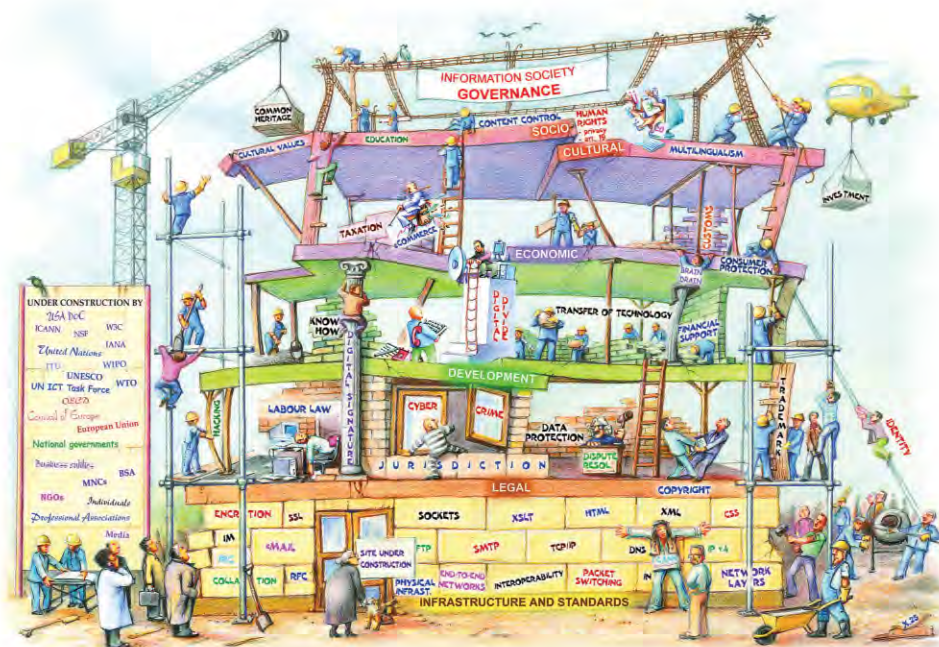
This briefing note is drawn from the fifth module of the Academy of ICT Essentials for Government Leaders (Academy). The Academy is a comprehensive ICT for development training curriculum that aims to equip policymakers with the essential knowledge and skills to fully leverage opportunities presented by information and communications technology (ICT) to achieve national development goals and bridge the digital divide. More information on the Academy is available at <http://www.unapcict.org/academy>.

Author: Peng Hwa Ang



Module 5 - Internet Governance

Discusses the ongoing development of international policies and procedures that govern the use and operation of the Internet.



Internet Governance

Module 5: Internet Governance, p.57 [Source: DiploFoundation, <http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1190>]

The APCICT Briefing Note Series aims to provide at-a-glance information on key information and communication technology for development (ICTD) agendas for high-level policymakers and stakeholders. The series includes: 1) highlights of conventional research papers, assessment and survey reports and publications; 2) policy considerations drawn from the Academy modules; and 3) key challenges and lessons learned based on analyses of best practices and case studies.

1 Introduction: What Is The Big Deal About Internet Governance?

Contrary to common misperception, the Internet has one point of 'control' called the Root Zone System. This Root Zone may be imagined as a master directory of directories of telephone numbers. Every computer that accesses the Internet must have an assigned number called an Internet Protocol (IP) address. It is analogous to a postal code or a phone number; the numbers tell the sender where the letter, call or data are to be sent. This master directory or Root Zone is

needed to ensure that no two recipients have the same address. Management of the entire Root Zone System is in the hands of a US company called Internet Corporation of Assigned Names and Numbers (ICANN). As its name suggests, ICANN gives out names and numbers. The names are for country codes. So .CN is for China, .IQ for Iraq, .SG for Singapore, and so forth. Without an assigned IP address, a computer does not exist in cyberspace. This role of ICANN is therefore critical to the functioning of the Internet.

There is no disputing that ICANN has run the Root Zone System well in the sense that the Internet has run well. There is concern, however, that companies that manage such systems may be beholden to or otherwise unduly influenced by the governments of countries in which they operate. For example, a government may put undue pressure on systems management companies to limit, or totally prohibit another country's access to the internet. This is especially worrisome as more and more essential government services, such as education and health, are delivered online. The possibility that one government can somehow prevent the use of the Internet by another country is disquieting for many governments and users. There is in fact an actual instance of a country being cut off from the Internet. In

2002, the domain name .IQ was in the hands of a Palestinian living in Texas who was charged for unauthorized sale of computer parts. In the process, the .IQ domain name was taken back by ICANN. That is, there was no one to turn on the computer servers for .IQ. Coincidentally or otherwise, this meant that Iraq did not exist in cyberspace just before the 2003 war between Iraq and a US-led coalition. The .IQ domain name was not available until July 2005, just days before the Working Group on Internet Governance was to issue its report recommending that every sovereign government should have the right to control its own country-code domain name. It is with reference to this that China has repeatedly called attention to control of “critical Internet resources” as an important concern.

2 The Origins of Internet Governance

The issue of Internet Governance goes back to the 1998 plenipotentiary meeting of the International Telecommunication Union (ITU) in Minnesota, USA where the idea of a summit on the information society was mooted. There were several motives behind the summit. The dotcom boom was at its height. Some countries were concerned that for all their natural resource wealth, they might be left behind in the information-based economic wealth that was being created. Some countries also viewed the information-based economic wealth being created as a resource management issue - believing that the allocation of limited IP addresses was not in accordance with projected population needs. In the early years, for instance, a few well-known universities received more IP addresses than that received by many countries. (The universities have since returned the unused IP addresses. Also, a new IP addressing system called IPv6 has been introduced.) The ITU itself, many of whose members had thought the Internet was a fad, was keen to have some role in the governance of the Internet.

The 2003 World Summit on the Information Society (WSIS) came close to failure over the issue of Internet Governance. While many countries wanted to address Internet Governance, the USA was of the view that there is insufficient capacity especially in developing countries to address the issue. It was decided that a working group be appointed by the UN Secretary-General to report on the issue. The Working Group on

Internet Governance (WGIG) concluded its work with an 80-page Background Report that reflected the inputs of many interested parties, and a Final Report edited by the entire Group. The Final Report defined Internet Governance thus:

Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.



Participants engaging in discussion at the second UN-APCICT/ESCAP Training of Trainers (TOT) workshop on the Internet Governance in Seongnam, Republic of Korea (March 2009)

Several important points should be noted about the definition. Internet Governance is not merely a law passed by a government. It also encompasses the principles, policies, rules, processes, and procedures for administration by government. Other public policy issues such as spam, privacy, and cybercrime were included. The private sector and civil society were to be considered as stakeholders in Internet Governance. This meant that Internet Governance was not the traditional government-to-government arrangement that was prevalent in international agencies. The sweep of the definition implied a rejection of the attempt by the ITU Secretary-General at the time to limit Internet Governance to “ICANN-related issues” only.

2.1 The Four Clusters of Issues

The WGIG Final Report outlined the issues in Internet Governance and divided them into four clusters:

1. **Physical Infrastructure**, which encompasses ICANN-related issues such as IP addresses, domain names, and the root zone server.
2. **Use and abuse** of the Internet, such as spam, network security, and cybercrime;
3. **Issues related to the Internet but with wider impact**, such as competition policy, e-commerce, and intellectual property rights; and

4. **Development aspects** of the Internet, which had been a motivating force behind the WSIS in the first case.

The second cluster refers to issues specific to the Internet while the third cluster refers to issues that spill over from the Internet to the offline world. As for the fourth cluster of issues, the WGIG Final Report recommended that development be considered a priority that cuts across all the issues. Internet Governance was to be placed within the context of the Millennium Development Goals. This meant that there should be effective and meaningful participation in Internet Governance arrangements, which in turn means capacity building to address the issues. A Digital Solidarity Fund had been created but very little money for what is needed has been donated.

These issues need to be worked on in a process that, according to the Final Report, should be transparent and democratic, and with multilateral (i.e. involving many countries’) participation.

The WGIG Final Report also gave two key recommendations. The first recommendation was that there should be an international forum for all stakeholders to discuss Internet-related issues. Such a forum should be low-cost and have no decision-making powers. The reason for denying decision-making to this forum was to avoid the protracted negotiations that would inevitably accompany the discussion. In short, the forum was to be a ‘talk-shop’.

The second recommendation was that “oversight of the Internet” be “internationalized” based on the WSIS principle that such oversight be democratic, transparent, and with multilateral (involving many countries) and multi-stakeholder (government, business, civil society) participation. In short, systems management companies critical to the functioning of the internet should be governed by an international body, and not subject to potential pressure from a sovereign government.

The US Government was against both recommendations. At the second World Summit on the Information Society held in Tunisia (it should be noted that this is the first time ever that there has been two summits on one issue; by definition, there should only be one summit), the bargaining led to the following outcomes:

- ICANN should be allowed to continue in its present form;

- The Internet Governance Forum (IGF) will be established; and
- Country-code top-level domains (cc-TLDs) will be placed entirely under the control of national governments.

This last point meant that theoretically at least, the .IQ situation where the Iraq domain name was removed from cyberspace would not be repeated.

The Final Report also recommended better coordination among the international bodies involved in Internet Governance, and the implementation by national governments of “Internet-friendly national policies.”



Multilateral and multisectoral participation in Internet Governance Module 5: Internet Governance, p. 20
 [Source: DiploFoundation, <http://textus.diplomacy.edu/textus/bin/env/scripts/Pool/GetBin.asp?IDPool=1188>]

3 Implementing Internet Governance

The WGIG Final Report was intended to resolve the question of defining Internet Governance. Thus, it is short on details regarding how to go about resolving the issues outlined. The WGIG Final Report does not contain a road map or a plan of action.

It should be noted that regulation of the Internet can be done not just through laws. There are four modes of regulation:

1. Architecture-what technology permits, dissuades or prohibits

Technology may be used to regulate conduct. For example, software encryption is being used to attempt to defeat online piracy.

2. Markets-price and availability

Market forces may be used in certain instances. An example may be privacy protection. In the USA, users are encouraged to ‘shop’ around for a website with a privacy protection policy that they are comfortable with before transacting on the site.

3. Social norms-through expectation, encouragement, or embarrassment

On the Internet, there are areas where social norms are in place. For example, posts on discussion boards are expected to be relevant (on-topic).

4. Law-government and private sanctions and force, including self-regulation

Laws will always lag behind fast-changing technology. Self-regulation would thus be a good mode of regulation. Being industry-specific, it should be able to adapt to change more quickly than legislation passed by Parliament. However, not all conditions for self-regulation exist. Perhaps the most serious objection is that the industry for the most part is unwilling to self-regulate.

4 Suggested Road Map

While the WGIG Final Report places heavy emphasis on process, it does not give as much guidance on the ‘what’ of Internet Governance. Given competing priorities, what steps in Internet Governance should be taken? What follows is a suggested road map that may be used as a plan of action. This road map has been ‘tested’ in the sense that where there have been regulations, they have covered the areas outlined and in the sequence shown below.

I. Access and Service Provision

Obtaining affordable access while maintaining quality are key issues. Where possible, competition among Internet Service Providers should be encouraged to lower prices.

II. Electronic Commerce

Addressing e-commerce issues not only benefits the business community but also overcomes a host of problems in going online. By this time, most countries would have their legal systems set up to enable e-commerce. However, many countries have not fully resolved issues in areas like taxation and the rights and responsibilities of various parties online. With the increase in the use of social networking sites, an issue that has come to the fore is liability for third-party content-that is, the extent to which a website host should be liable for content posted by users where there are hundreds of thousands of such posts everyday, making it impractical for a

person to scan all posts.

III. Content Regulation

The issues in this area go beyond censorship. The fundamental issue is reconciling conflicting cultural values in information content, since what is acceptable in one part of the world may be objectionable in another. To allow everything on the Internet would mean upsetting existent laws. On the other hand, it is impossible in practice to apply existent laws to the Internet because doing so would require an army of censors. The current best practice is to filter rather than to block content. That is, content may be available to some groups but not available to others.

Another issue in content regulation is online defamation. Given the ease with which this can occur, the traditional law on defamation will need some modification. For example, some form of mediation may be useful.

IV. Security

The US Government will be putting greater emphasis on this in the near future. Broadly speaking, the issues here encompass the protection of computer systems against hackers, as well as the prevention of online crime. Among the issues to be addressed are scams and Trojan horses that surreptitiously collect sensitive data like passwords. Developing countries will need to work on security issues as well because tightening security in the US will have the unintended consequence of driving hackers to attack systems that are less secure, which would be in developing countries.

V. Intellectual Property Rights

In many countries, the issue is the need to extend current intellectual property law to the digital era. There are new areas, such as whether domain names should be linked to trademarks-that is, should a company be entitled to the same name online as it has offline? Intellectual property rights are defined and in the past there has been a balance between the rights-holders and society. The tendency is for the rights-holders to push their case. Many academics are in favour of less restrictive copyright rules because of the larger social benefits of encouraging innovation.

VI. Privacy

For many countries, privacy is a new word.

On the Internet, the scope of this concept is fairly narrow and for practical purposes privacy refers to the use of personal information by the collector of the data. The European Union's Data Protection Directive requires non-EU countries that handle data from the EU to have 'adequate' data protection. The Directive has yet to be given full force in all third-party countries.

VII. Illegal Content

Child pornography and consumer fraud are content that are globally accepted as illegal. There are international 'sweeps' where law enforcement groups in some 40 countries cooperate to sweep the Internet for such content. Simultaneous raids have been conducted to arrest offenders, particularly in child pornography cases. Such sweeps require offline laws before these online counterparts can be effective.

Spam, despite its nuisance factor, is not illegal in many countries. At the IGF, there is a loose grouping of interested stakeholders who are looking into the issue.



"Better hold up, George - this is a copyright notice."

5 Development

Information and communications technology for development or ICTD is a whole sub-field by itself. There are many ICTD applications in government services, agriculture, education, health and business, and with varying success. The cost of hardware continues to decline, making access more affordable. One area that governments can work on is computerizing government services. e-Government implementations have been shown to increase efficiency and reduce corruption.

6 The Future of the Internet Governance Forum

The first IGF mandate ended in 2010 and was extended by the UN General Assembly for another five years over the reservations of some countries. Privately, many countries wondered about the utility of the IGF because the results were not perceived as tangible. Even the Dynamic Coalitions, which were groups that met in parallel tracks during the IGF, have not delivered much by way of concrete results in such areas as spam and network security.

Some countries feel that the IGF is not capable of tackling the perceived "monopoly" over the Internet by a few nations. Despite these reservations, many countries went along with the renewal of the IGF's mandate in December 2010 in the UN General Assembly because there is no clear alternative.

Yet the future form of the IGF remains a major item of discussion. A number of countries have proposed an International Code of Conduct on Information Security as an agenda item for the UN General Assembly. The main objection to the Code is that it intentionally omits the private sector and civil society as stakeholders. The Code therefore seems to go against the consensus built during the two WSIS meetings and the five IGFs that Internet governance should be a multi-stakeholder, and not a purely governmental arrangement.

The political dimension of Internet Governance especially at the international level therefore continues to dominate. At the local level, the need for development is as strong as ever. Together, these aspects demonstrate the requirement for countries to be aware of the issues in Internet Governance.



Participants engage in workshop on Internet Governance, co-organized by the Indonesian Ministry of Communication and Information Technology, and the University of Indonesia in collaboration with UN-APCICT/ESCAP in Bali, Indonesia. (April 2009)

UN-APCICT/ESCAP

APCICT, a regional institute of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), was established and inaugurated on 16 June 2006 in Incheon, Republic of Korea. The role and mission of APCICT is to strengthen the efforts of the 62 ESCAP member and associate member countries to use ICTs in their socio-economic development through building the human and institutional capacity for ICT. In pursuance of this mandate, APCICT's work is focused on three inter-related pillars-Training, Advisory Services and Research. The Briefing Note Series is part of the research pillar. Also under the research pillar is a Case Study Series that provides analyses and compilations of best practices and case studies on different aspects of ICTD and capacity building in the Asia Pacific region.

<http://www.unapcict.org>

ESCAP

ESCAP is the regional development arm of the United Nations and serves as the main economic and social development centre for the United Nations in Asia and the Pacific. Its mandate is to foster cooperation between its 53 members and 9 associate members. ESCAP provides the strategic link between global and country-level programmes and issues. It supports Governments of countries in the region in consolidating regional positions and advocates regional approaches to meeting the region's unique socio-economic challenges in a globalizing world. The ESCAP office is located at Bangkok, Thailand.

<http://www.unescap.org>

This work is released under the Creative Commons Attribution 3.0 License.

To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/>

The opinions, figures and estimates set forth in this publication are the responsibility of the authors, and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations.

The designations used and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Mention of firm names and commercial products does not imply the endorsement of the United Nations.