Briefing Note 5

January 2010

Internet Governance

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

APCICT Briefing Note No. 5
Internet Governance

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 road map 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 of nine core modules 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 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

Series Editor: Christine Apikul

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.

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. Control in the conventional sense may be too strong a word but 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 is 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 the 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 Internet has run well. The issue that causes discomfort is that ICANN is an American company under the authority of the US Department of Commerce. That is, the US Government can tell ICANN what to do. Given that governments all over the world have used the Internet infrastructure to deliver essential services in education, health and government services, it raises the question of whether the US Government can somehow stop the Internet from being used in a country that for some reason finds itself at odds with the US. It would be more reassuring if there were no instance in which a country was cut off from the Internet. Unfortunately, there was one case.

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, it meant that Iraq did not exist in cyberspace just before the war began in 2003. 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. This is the issue that China has mentioned repeatedly as the control of the “critical Internet resources.”

2. The Origins of the Internet Governance

The issue of Internet Governance traces back to the 1998 plenipotentiary meeting of the International Telecommunication Union (ITU) in Minnesota where the idea of a summit on the information society was mooted. There were a few motivations behind the summit. The dotcom boom was in full flow. The Arab countries were concerned that for all their oil wealth, they might be left behind in the information-based economic wealth that was being created. The Chinese saw the matter partly as a resource issue – that because US universities such as the Massachusetts Institute of Technology and Michigan State University had each been given more IP addresses than China, and the IP addresses were limited, it was possible that large parts of the Chinese population would not be able to access the Internet. (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 was insufficient capacity especially in developing countries to address the issue. It was therefore 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 the Final Report, which was 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.*

Several important points should be noted about the definition. Internet Governance is not merely 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 thought of 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 rejected the attempt by then ITU Secretary-General 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 root zone server.
2. **Use and abuse issues** of the Internet, such as spam, network security and cybercrime; these were issues that were specific to the Internet.
3. **Issues related to Internet but with wider impact**, which would encompass such issues as competition policy, e-commerce and intellectual property rights; these issues spilled over from the Internet to the offline world.
4. **Development aspects** of Internet, which had been a motivating force behind the WSIS in the first case. The Final Report recommended that Development be a priority that cuts across all the issues. It 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 the Final Report added should be transparent and democratic, and with multilateral (i.e., many countries’) participation.

The WGIG Final Report also gave two key recommendations. First, 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 to deny decision-making to this forum was to avoid the protracted negotiations that would inevitably accompany the discussion. The forum, in short, was to be a 'talk-shop'.

Second, the Final Report recommended that "oversight of the Internet" be "internationalized" based on the WSIS principles that such oversight be democratic, transparent and with multilateral (involving many countries) and multi-stakeholder (government, business, civil society) participation. In short, ICANN should not be in the hands of the US Government but be placed in an international body.

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 at least theoretically, 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 various international bodies that were involved in Internet Governance and that national governments should aim to implement "Internet-friendly national policies."

3. Implementing Internet Governance

The WGIG Final Report was intended to resolve the question of defining Internet Governance and so it is short on details how to go about resolving the issues outlined. The Final Report does not contain a road map or a plan of action. First, it should be noted that regulation does not mean only using 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 the website with a privacy protection policy they are comfortable with before transacting on the site.
3. ***Social norms – through expectation, encouragement, or embarrassment***
   On the Internet, there are areas where there are social norms in place. Posts on discussion boards, for example, are expected to be relevant (on-topic).
4. ***Law – government and private sanctions and force, including self-regulation***
   Law will always lag fast-changing technology, as it should be because of the rapid pace of change. Self-regulation would be a good mode of regulation because being industry-specific, it should be able to adapt to change more quickly than legislation passed by Parliament. However, not all the 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. That is, given the competing priorities, what steps in Internet Governance should be taken. The following is a suggested road map that could 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 about the order outlined 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 is worthwhile because doing so benefits not only 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 such as areas as 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 that of liability for third-party content. That is, to what extent a website host should be liable for content posted by its 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; what is acceptable in one part of the world may be objectionable in another. To merely allow everything on the Internet through would mean upsetting existent laws. On the other hand, it is impossible in practice to apply existent laws for the Internet because that would require an army of censors. Current best practice is to filter rather than block content. That is, content may be available for some groups but not available for other.

Another issue in content regulation is that of online defamation. Given the ease with which this can occur, the traditional law of 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 as well as Trojan horse that surreptitiously collect sensitive data such as 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 to extend the existent intellectual property law to the digital era. There are new areas, such as whether the domain names should be linked to trademarks. That is, should it be automatically the case that a company should 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 is fairly narrow and for practical purposes 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 to all third-party countries.

6. Illegal Content

Contents globally accepted as illegal are child pornography and consumer fraud. There are international ‘sweeps’ where law enforcement 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.

7. Development

There is a whole sub-field on information and communication technology for development or ICTD. 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 is to computerize government services. Such e-government implementations have been shown to increase efficiency and reduce corruption.

8. The Future of the Internet Governance Forum

The mandate for the IGF ends 2010. Much of the action in the IGF is now happening in the parallel sessions and not the plenary sessions. Often, issues have some technical dimension that must be grasped before policy can be made. The parallel sessions are able to bring together a small, diverse and motivated group of stakeholders called Dynamic Coalitions to address the issues. Any interested person or organization may join these Dynamic Coalitions.

Recently, China stated that it would not support the continuance of the IGF beyond 2010 because a ‘talk-shop’ is not enough to solve problems, the main one being on the Internet “there is a monopoly that exists.” The IGF, however, was never intended to change Internet Governance arrangements. The strongest complaint would be that the IGF has not helped social and economic development in developing countries, which was a major motivation behind the WSIS. However, this is not the basis of the complaint by China. There appears to be political backroom manoeuvrings because in 2005 at WSIS 2, China suddenly dropped its demand that ICANN be internationalized after a direct appeal by the US Government. It is possible that China is seeking some bargaining chips with the USA. In 2005, the USA had opposed the formation of such a forum; now, however, the USA wants the forum to continue.

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, they show the need for countries to be aware of the issues in Internet Governance. The mandate for the IGF ends 2010. Much of the action in the IGF is now happening in the parallel sessions and not the plenary sessions. Often, issues have some technical dimension that must be grasped before policy can be made. The parallel sessions are able to bring together a small, diverse and motivated group of stakeholders called Dynamic Coalitions to address the issues. Any interested person or organization may join these Dynamic Coalitions.

Recently, China stated that it would not support the continuance of the IGF beyond 2010 because a ‘talk-shop’ is not enough to solve problems, the main one being on the Internet “there is a monopoly that exists.” The IGF, however, was never intended to change Internet Governance arrangements. The strongest complaint would be that the IGF has not helped social and economic development in developing countries, which was a major motivation behind the WSIS. However, this is not the basis of the complaint by China. There appears to be political backroom manoeuvrings because in 2005 at WSIS 2, China suddenly dropped its demand that ICANN be internationalized after a direct appeal by the US Government. It is possible that China is seeking some bargaining chips with the USA. In 2005, the USA had opposed the formation of such a forum; now, however, the USA wants the forum to continue.

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, they show the need for countries to be aware of the issues in Internet Governance.

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.

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.

Contact information:

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