Academy of ICT Essentials for Government Leaders

Module 5

Internet Governance

Ang Peng Hwa

APCICT ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

The Academy of ICT Essentials for Government Leaders Module Series

Module 5: Internet Governance

Contact:
United Nations Asian and Pacific Training Centre for Information
and Communication Technology for Development (UN-APCICT/ESCAP)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, IncheonCity
Republic of Korea

Tel: 82 32 245 1700-02
Fax: 82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

ISBN: 978-89-97748-02-0

Design and Layout: Scand-Media Corp., Ltd.
Printed in: Republic of Korea

FOREWORD

The world we live in today is inter-connected and fast-changing, largely due to the rapid development of information and communication technologies (ICTs). As the World Economic Forum fittingly states, ICTs represent our "collective nerve system", impacting and connecting every fabric of our lives through intelligent, adaptive and innovative solutions. Indeed, ICTs are tools that can help solve some of our economic, social and environmental challenges, and promote more inclusive and sustainable development.

The increased access to information and knowledge through development of ICT has the potential to significantly improve the livelihoods of the poor and marginalized, and promote gender equality. ICTs can serve as a bridge connecting people from different countries and sectors in the region and beyond by providing more efficient, transparent and reliable means and platforms for communication and cooperation. ICTs are essential to the connectivity that facilitates more efficient exchange of goods and services. Success stories from Asia and the Pacific region abound: e-government initiatives are improving access to and quality of public services, mobile phones are generating incomes and professional opportunities for women, and the voices of the vulnerable are louder than ever through the power of social media.

Yet, the digital divide in Asia and the Pacific is still seen to be one of the widest in the world. This is evidenced by the fact that the countries of the region are placed across the whole spectrum of the global ICT Development Index ranking. Despite the impressive technological breakthroughs and commitments of many key players in the region, access to basic communication is still not assured for all.

In order to complete the bridging of the digital divide, policymakers must be committed to further realizing the potential of ICTs for inclusive socio-economic development in the region. Towards this end, the Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) was established as a regional institute of the United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP) on 16 June 2006 with the mandate to strengthen the efforts of the 62 ESCAP member and associate member countries to use ICT in their socio-economic development through human and institutional capacity development. APCICT's mandate responds to the Declaration of Principles and Plan of Action of the World Summit on the Information Society (WSIS), which states that: "Each person should have the opportunity to acquire the necessary skills and knowledge in order to understand, participate actively in, and benefit fully from, the Information Society and the knowledge economy."

In order to further respond to this call to action, APCICT has developed a comprehensive information and communication technology for development (ICTD) training curriculum, the *Academy of ICT Essentials for Government Leaders*. Launched in 2008 and based on strong demand from member States, the *Academy* presently consists of 10 stand-alone but interlinked modules that aim to impart essential knowledge and expertise to help policymakers plan and implement ICT initiatives more effectively. Widespread adoption of the *Academy* programme throughout the Asia-Pacific attests to the timely and relevant material covered by these modules.

ESCAP welcomes APCICT's ongoing effort to update and publish high quality ICTD learning modules reflecting the fast-changing world of technology and bringing the benefits of ICTD knowledge to national and regional stakeholders. Moreover, ESCAP, through APCICT, is promoting the use, customization and translation of these *Academy* modules in different countries. It is our hope that through their regular delivery at national and regional workshops for senior- and mid-level government officials, the acquired knowledge would be translated into enhanced awareness of ICT benefits and concrete actions towards meeting national and regional development goals.

Noeleen Heyzer

Under-Secretary-General of the United Nations
and Executive Secretary of ESCAP

PREFACE

In the effort to bridge the digital divide, the importance of developing the human resource and institutional capacity in the use of ICTs cannot be underestimated. In and of themselves, ICTs are simply tools, but when people know how to effectively utilize them, ICTs become transformative drivers to hasten the pace of socio-economic development and bring about positive changes. With this vision in mind, the *Academy of ICT Essentials for Government Leaders* (*Academy*) was developed.

The *Academy* is the flagship programme of the United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT), and is designed to equip government officials with the knowledge and skills to fully leverage ICT for socio-economic development. The *Academy* has reached thousands of individuals and hundreds of institutions throughout the Asia-Pacific and beyond since its official launch in 2008. The *Academy* has been rolled out in over 20 countries in the Asia-Pacific region, adopted in numerous government human resource training frameworks, and incorporated in the curricula of university and college programmes throughout the region.

The impact of the *Academy* is in part a result of the comprehensive content and targeted range of topics covered by its eight initial training modules, but also due to the *Academy's* ability to configure to meet local contexts and address emerging socio-economic development issues. In 2011, as a result of strong demand from countries in the Asia-Pacific, APCICT in partnership with its network of partners developed two new *Academy* training modules designed to enhance capacity in the use of ICT for disaster risk management and climate change abatement.

Adhering to APCICT's "We D.I.D. It In Partnership" approach, the new *Academy* modules 9 and 10, like the initial modules 1 to 8, were Developed, Implemented and Delivered in an inclusive and participatory manner, and systematically drew upon an extensive and exceptional group of development stakeholders. The entire *Academy* has been based on: needs assessment surveys from across the Asia-Pacific region; consultations with government officials, members of the international development community, and academics and educators; research and analysis on the strengths and weaknesses of existing training materials; and a peer review process carried-out through a series of APCICT organized regional and sub-regional workshops. These workshops provided invaluable opportunities for the exchange of experiences and knowledge among users of the *Academy* from different countries. The result is a comprehensive 10-module *Academy* curriculum covering a range of important ICTD topics, and indicative of the many voices and contextual nuances present across the region.

APCICT's inclusive and collaborative approach to development of the *Academy* has also created a network of strong partnerships to facilitate the delivery of ICTD training to government officials, policymakers and development stakeholders throughout the Asia-Pacific region and beyond. The *Academy* continues to be rolled out and adopted into training frameworks at the national and regional levels in different countries and regions as a result of close collaboration between APCICT and training institutions, government agencies, and regional and international organizations. This principle will continue to be a driving force as APCICT works with its partners to continuously update and further localize the *Academy* material, develop new *Academy* modules to address identified needs, and extend the reach of *Academy* content to new target audiences through new and more accessible mediums.

Complementing the face-to-face delivery of the *Academy* programme, APCICT has also developed an online distance learning platform called the APCICT Virtual Academy (http://e-learning.unapcict.org), which is designed to enable participants to study the material at their own pace. The APCICT Virtual Academy ensures that all the *Academy* modules and accompanying materials are easily accessible online for download, dissemination, customization and localization. The *Academy* is also available on DVD to reach those with limited or no Internet connectivity.

To enhance accessibility and relevance in local contexts, APCICT and its partners have collaborated to make the *Academy* available in English, Bahasa Indonesia, Mongolian, Myanmar language, Russian, Tajik and Vietnamese, with plans to translate the modules into additional languages.

Clearly, the development and delivery of the *Academy* would not have been possible without the commitment, dedication and proactive participation of many individuals and organizations. I would like to take this opportunity to acknowledge the efforts and achievements of our partners from government ministries, training institutions, and regional and national organizations who have participated in *Academy* workshops. They not only provided valuable inputs to the content of the modules, but more importantly, they have become advocates of the *Academy* in their countries and regions, and have helped the *Academy* become an important component of national and regional frameworks to build necessary ICT capacity to meet the socio-economic development goals of the future.

I would like to extend heartfelt acknowledgments to the dedicated efforts of the many outstanding contributors who have made Module 5 possible, with a special note of gratitude to module author Ang Peng Hwa. I would also like to thank the more than 7,500 participants that have attended over 80 *Academy* workshops in over 20 countries, as well as online trainings. Their invaluable insight and feedback have helped to make sure that the *Academy* has had a lasting impact.

I sincerely hope that the *Academy* will help nations narrow ICT human resource gaps, remove barriers to ICT adoption, and promote the application of ICT in accelerating socio-economic development and achieving the Millennium Development Goals.

Hyeun-Suk Rhee

Director
UN-APCICT/ESCAP

ABOUT THE MODULE SERIES

In today's "Information Age", easy access to information is changing the way we live, work and play. The "digital economy", also known as the "knowledge economy", "networked economy" or "new economy", is characterized by a shift from the production of goods to the creation of ideas. This underscores the growing, if not already central, role played by ICTs in the economy and in society as a whole.

As a consequence, governments worldwide have increasingly focused on ICTD. For these governments, ICTD is not only about developing the ICT industry or sector of the economy but also encompasses the use of ICTs to engender economic as well as social and political growth.

However, among the difficulties that governments face in formulating ICT policy is that policymakers are often unfamiliar with the technologies that they are harnessing for national development. Since one cannot regulate what one does not understand, many policymakers have shied away from ICT policymaking. But leaving ICT policy to technologists is also wrong because often technologists are unaware of the policy implications of the technologies they are developing and using.

The *Academy of ICT Essentials for Government Leaders* module series has been developed by the UN-APCICT/ESCAP for:

1. Policymakers at the national and local government level who are responsible for ICT policymaking;

2. Government officials responsible for the development and implementation of ICT-based applications; and

3. Managers in the public sector seeking to employ ICT tools for project management.

The module series aims to develop familiarity with the substantive issues related to ICTD from both a policy and technology perspective. The intention is not to develop a technical ICT manual but rather to provide a good understanding of what the current digital technology is capable of or where technology is headed, and what this implies for policymaking. The topics covered by the modules have been identified through a training needs analysis and a survey of other training materials worldwide.

The modules are designed in such a way that they can be used for self-study by individual readers or as a resource in a training course or programme. The modules are standalone as well as linked together, and effort has been made in each module to link to themes and discussions in the other modules in the series. The long-term objective is to make the modules a coherent course that can be certified.

Each module begins with a statement of module objectives and target learning outcomes against which readers can assess their own progress. The module content is divided into sections that include case studies and exercises to help deepen understanding of key concepts. The exercises may be done by individual readers or by groups of training participants. Figures and tables are provided to illustrate specific aspects of the discussion. References and online resources are listed for readers to look up in order to gain additional perspectives.

The use of ICTD is so diverse that sometimes case studies and examples within and across modules may appear contradictory. This is to be expected. This is the excitement and the challenge of this newly emerging discipline and its promise as all countries begin to explore the potential of ICTs as tools for development.

Supporting the *Academy* module series in print format is an online distance learning platform—the APCICT Virtual Academy—with virtual classrooms featuring the trainers' presentations in video format and presentation slides of the modules (visit http://e-learning.unapcict.org).

In addition, APCICT has developed an e-Collaborative Hub for ICTD, or e-Co Hub (http://www.unapcict.org/ecohub), a dedicated online site for ICTD practitioners and policymakers to enhance their learning and training experience. The e-Co Hub gives access to knowledge resources on different aspects of ICTD and provides an interactive space for sharing knowledge and experiences, and collaborating on advancing ICTD.

MODULE 5

The Internet raises significant challenges for public policy and sustainable human development, both internationally and for individual nations. Hence, the ongoing development of international policies and procedures to govern the use and operation of the Internet. However, although the Asia-Pacific region has the biggest share of global Internet users, it is under-represented in forums that develop Internet-related policies. There are a number of issues and specific challenges related to Internet Governance in the regional context. Governments of emerging economies need to understand these issues if they are to have a voice in the global information network.

Module Objectives

This module aims to:

1. Describe the ongoing development of international policies and procedures that govern the use and operation of the Internet; and

2. Provide an overview of the issues and specific challenges related to Internet Governance in the regional context.

Learning Outcomes

After working on this module, readers should be able to:

1. Describe the development of international policies and procedures governing the use and operation of the Internet;

2. Discuss key issues in Internet Governance from the perspective of developing countries; and

3. Outline the first steps towards better governance of the Internet in their respective countries.

TABLE OF CONTENTS

List of Case Studies

List of Figures

Acronyms

ACPA	Anti-Cybersquatting Consumer Protection Act
ACTA	Anti-Counterfeiting Trade Agreement
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
ccTLD	Country Code Top-Level Domain
CoE	Council of Europe
CSC	Common Services Centre (India)
DEC	Digital Equipment Corporation
DNS	Domain Name System
ESCAP	Economic and Social Commission for Asia and the Pacific (UN)
EU	European Union
FOSS	Free and Open Source Software
GAC	Government Advisory Committee
GNSO	Generic Names Supporting Organization
GPS	Global Positioning System
gTLD	Generic Top-Level Domain
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEN	International Consumer Protection and Enforcement Network
ICRA	Internet Content Rating Association
ICT	Information and Communication Technology
ICTD	Information and Communication Technology for Development
IDN	Internationalized Domain Name
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
MDG	Millennium Development Goal
OECD	Organisation for Economic Co-operation and Development
PPP	Public-Private Partnership
RIAA	Recording Industry Association of America
RIR	Regional Internet Registry
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top-Level Domain
UDRP	Uniform Dispute Resolution Process
UK	United Kingdom
UN	United Nations
USA	United States of America
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society

List of Icons

 Case Study

 Questions To Think About

 Something To Do

 Test Yourself

1. THE PROBLEM AND SCOPE OF INTERNET GOVERNANCE

This section aims to provide a brief history of and context for Internet Governance, and briefly outline the scope of Internet Governance.

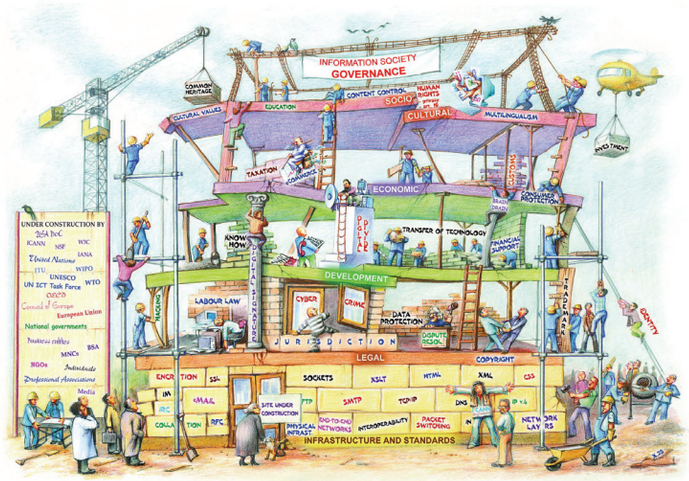
1.1 Introduction

It is often assumed that the new medium of communication called the Internet cannot be regulated. This is understandable as its first users said loudly and often that the Internet is an invention designed to survive a nuclear attack, circumvent blockages by routing around them, cross multiple international boundaries and therefore be censor-proof. Being censor-proof means that its contents are difficult if not impossible to police and therefore the users are difficult to regulate.[1]

Now, more than 10 years after the Internet was made publicly available, we know that these notions about the Internet are myths and that the Internet can be regulated. In fact, it is the more developed countries that have more regulations on the Internet while the least developed countries have very few or no rules governing the Internet. The lack of rules can result in developing countries becoming a haven for those who engage in acts of mischief using the Internet, such as spam and scams.

It is not the quantity of rules and laws that stifle use of the Internet. If that were the case, the United States of America (USA) would be the most stifling for the Internet while a place like Lao PDR, which is still struggling with infrastructure issues, would be thriving on the Internet. What matters is that rules governing the Internet should be made based on a sound understanding of the legal and technical issues and through international cooperation. This module aims to clarify these issues and to show how international cooperation in Internet Governance might be achieved.

Figure 1. Information society governance: An overview



Source: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1190.

1 Peng Hwa Ang, *Ordering Chaos: Regulating the Internet* (Singapore, Thomson, 2005).

1.2 History and Technical Background of the Internet

Historical and technical developments

The Internet was invented not to create a communication network that would survive a nuclear attack but to enable physicists to share computers to solve computational-intensive problems. Computers at the time were large expensive equipment spread over far-flung locations.[2] The method of connecting the computers used a protocol invented in the 1960s that did not depend on the technology in the network. This is counter-intuitive because one would think that to send messages from one location to another one should use good equipment and technology. Instead, the protocol made it possible to send computer messages and transactions into packets and then re-form them at the receiving end. If the message was not received clearly or well, it was re-sent. Such a method of transmission meant that the network or pipe did not need to have "intelligence". All that was needed were routers to point the messages where to go, and the messages would then find their way through the "stupid network". This "Internetworking protocol" was better at helping messages cross different networks than the protocol used for the telephone.

The superiority of the Internetworking protocol was highlighted from the 1970s when telephone companies began to put more intelligence into their networks.[3] Although the International Telecommunication Union (ITU), which was the United Nations (UN) agency set up to coordinate global telecommunications, did develop some of the protocols and standards, the difference in perspectives was to lead to a clash that ultimately swung in favour of the Internetworking protocol over the telephone companies' protocol.

History of Internet Governance[4]

It should be kept in mind that protocols and standards are very important in the technology world because whoever controls these can dictate, if not control, the direction the technology will take. In the case of the Internet, the protocol that came to be used to knit the different networks is now called Transmission Control Protocol/Internet Protocol (TCP/IP). Invented by Vinton G. Cerf and Bob Kahn in 1974, this communication protocol was so critical to the network's functioning that any network that used TCP/IP came to be referred to as the Internet.

For the purposes of this module, the most interesting principle of the protocol is that there was no direct control of the communication flowing over the network; there only had to be control over the address to which the communication was to be delivered. The issue of an address meant that there had to someone who had to ensure that there would be no clash of addresses. The global addressing system used numbers to designate the networks. Some person or agency has to ensure that no two addresses use identical numbers, that is, there must be a central directory to eliminate such conflicts. Thus it came to be that Jon Postel, who obtained all his degrees from the University of California at Los Angeles but then crossed town to the University of Southern California to be director of the Information Sciences Institute, became the "God of the Internet", as *The Economist* called him. He resolved such conflicts to keep the network growing.

---

2 Katie Hafner and Mathew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York, Simon and Schuster, 1998).

3 David S. Isenberg, "The Dawn of the Stupid Network", *ACM Networker* 2.1, February/March 1998, pp. 24-31, http://www.isen.com/papers/Dawnstupid.html.

4 Any book that touches on the history of the Internet would be a good resource. Two such books are Hafner and Lyon's *Where Wizards Stay Up Late*, and Jack Goldsmith and Tim Wu's *Who Controls the Internet: Illusions of a Borderless World*. A reliable online resource is The Internet Society's *Histories of the Internet* at http://www.isoc.org/internet/history.

As the number of networks grew, it became more and more difficult to remember the numbers for each of them. So in 1983, Postel and Paul Mockapetris proposed giving names to the numbers. For example, instead of typing 64.233.161.18, one would type google.com to get to a search engine. This was the equivalent of giving names to a telephone numbering system. Thus was born the Domain Name System (DNS).

The DNS would also create some legal problems of its own. This will be discussed in a subsequent section. For now, it is important to understand the DNS to understand the problem.[5]

The DNS is a hierarchical system of using a "tree-like" structure to organize information about networks and computers. It resembles a postal address: just as one puts the street address in front and the country name at the end, so the top level domain (TLD) name is at the end and the more specific network address is in front. So when a computer looks up an Internet address, it looks from the right to the left, asking each server about the name to its left.

When they were first implemented in January 1985, there were six TLDs:

COM – for commercial organizations
EDU – for educational institutions
NET – for network providers
ORG – for non-profit organizations
MIL – for the US military
GOV – for the US government[6]

Since then, more generic TLDs (gTLDs) have been added.[7] Probably the most significant for our current purpose is the creation of country-code TLDS (ccTLDs). These codes resemble but are not identical to the ISO 3166-1 alpha-2 two-letter country codes for countries and dependent territories that are used in international commerce.[8] The USA also has a two-letter ccTLD (US). But because of its historical dominance and first-mover advantage, a gTLD without a country-code, especially a COM, is taken to be from the USA or else to have a more global ambition.

The availability of ccTLDs means that governments can have a greater say in the way the domain names are decided. So yahoo.fr, for example, would be subject to the rules that the administrator of the DNS in France would impose. Thus, in a famous case, a French court decided that Yahoo could not sell Nazi memorabilia on its website targeted at the French audience. The French court could intervene and impose such a decision because the domain name—yahoo.fr—was registered in France. Yahoo subsequently renamed its website for French-language users as fr.yahoo.com. Read as an address, the new website address is in the COM domain space, on Yahoo and on a server labelled FR. The new address does mean that Yahoo can defy French law although there would be no sound commercial reason for it to do so. Indeed, Yahoo has renamed all of its foreign sites so that the addresses end in COM.

From the mid 1990s, there had been calls to have more gTLDs introduced. Some wanted more specialized TLDs; others saw a financial opportunity in running a gTLD. For more than a decade, fewer than 20 gTLDs were established. Finally, in June 2011 in Singapore, Internet Corporation for Assigned Names and Numbers (ICANN) agreed to implement the recommendation that gTLD applications be fully open—what has been described as dot-anything. This means that there can be be gTLDs for brands, cities and names. The vote was not without controversy.

5 See Wikipedia, "Domain Name System", http://en.wikipedia.org/wiki/Domain_name_system for a more detailed account of the DNS.

6 See Wikipedia, "Generic Top-level Domain", http://en.wikipedia.org/wiki/Generic_top-level_domain for a more detailed account of the TLD system.

7 For a definitive list, see http://data.iana.org/TLD/tlds-alpha-by-domain.txt. A more reader-friendly list is available at Wikipedia, "List of Internet Top-level Domain", http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains.

8 See "ISO 3166-1 alpha-2", http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2 for more details about ISO 3166-1 alpha-2.

A major point of contention was that besides a deposit of USD 5,000, an evaluation fee of USD 180,000 had to be included as part of the application to run a new gTLD. The fee, it was felt by some, could deter applications from developing countries. Also, there was no such fee for those who obtained the gTLDs earlier.[9] The Government Advisory Committee (GAC)[10] to ICANN commented in a May 2011 communiqué that the fees be reduced and that the annual fee of USD 25,000 be waived for three years for applications from developing countries and needy applicants.[11]

ICANN identified four "Overarching Issues" related to the introduction of new gTLDs: (1) trademark protection; (2) potential for malicious conduct; (3) security and stability/root zone scaling; and (4) TLD demand and economic analysis.[12]

Trademark protection arises because companies feel compelled to register their companies' name with a TLD. With the rule of first-come-first served, their trademark could be shut out if they do not register early. Registration, however, incurs expenses. Since that vote, business associations on both sides of the Atlantic have criticized the proposal.[13]

Malicious conduct may enter the Internet as those who are new to running a gTLD may not have the financial resources or technical capacity to secure their domains from attacks. The stability and security of the DNS may then be compromised.[14]

On the economic front, the major issue is whether there should be a separation of the registry that runs the TLD, and the registrars that sells the domain names. The registry of a new gTLD, so it is argued by some, may not generate enough profits to keep themselves going especially in their early stages. Also registrars may not be as motivated to work with a new gTLD compared with a more established one because more marketing effort would be needed with a new entrant. Therefore, allowing the registry also to market, essentially vertical integration of the registrar function, would make the business more viable.

On the other hand, vertical integration would mean that the established registries, such as those running .com, .net and .org, would also be able to sell domain names directly. This would increase market concentration and the market power of the incumbents in the domain name industry.

ICANN commissioned two studies and both recommended that vertical integration not be prohibited but that rules be established to regulate such integration.[15] The European Commission and the US Department of Justice, however, sent strongly worded letters to ICANN to "reconsider"[16] and have a "more thorough examination".[17] Vertical integration between registries and registrars is therefore on hold for now.

---

9 The Berkman Center for Internet and Society, *Accountability and Transparency at ICANN: An Independent Review: Appendix C: The Introduction of New gTLDs* (2010), Harvard University, pp. 12-13, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixC_gTLDs.pdf.

10 ICANN receives input from governments through the GAC. The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. GAC issues communiqués after its meetings to report its activities and recommendations. For more information see https://gacweb.icann.org and http://www.icann.org/en/committees/gac/.

11 GAC, "GAC Comments on the Applicant Guidebook (April 15th, 2011 version)", 26 May 2011, http://www.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf.

12 ICANN, "New gTLD Draft Applicant Guidebook: Analysis of Public Comment", 18 February 2009, http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf.

13 Kevin Murphy, "UK-US corporate world slams 'dot-brand' domain plans", *The Register*, 1 September 2011, http://www.theregister.co.uk/2011/09/01/icann_generic_domain_plan_slammed_by_corporates/.

14 ICANN, "New gTLD Draft Applicant Guidebook".

15 ICANN, "Public Comment: CRAI Report on gTLD Registries and Registrars", 24 October 2008, http://www.icann.org/en/announcements/announcement-24oct08-en.htm; and Steve Salop and Joshua Wright, "Vertical Integration Between Registries and Registrars—The Economic Pros and Cons", presentation made in Sydney, Australia on 22 June 2009, http://syd.icann.org/files/meetings/sydney2009/presentation-vertical-separation-22jun09-en.pdf.

16 European Commission, "Removal of vertical integration between registries and registrars for new and existing gTLDs", http://www.icann.org/en/correspondence/eu-to-icann-17jun11-en.pdf.

17 Lawrence Strickling. "Cross-Ownership Issues for Registries and Registrars", US Department of Commerce, 16 June 2011, http://www.icann.org/en/correspondence/strickling-to-dengate-thrush-16jun11-en.pdf.

Meanwhile, GAC raised concerns over how its views would be incorporated into the guidelines for the formation of new gTLDs. In March 2007, the Committee developed the "GAC Principles Regarding New gTLDs" that state, among other things, that the new gTLDs should respect national, cultural, geographic and religious sensitivities.[18] This "morality and public order standard", as it became known, was criticized by both civil society members and some within GAC. In an explanatory memorandum in November 2008, ICANN had said that such morality and public order standards would be restricted to three areas:

- Incitement to violent lawless action;
- Incitement to or promotion of discrimination based upon race, color, gender, ethnicity, religion or national origin; and
- Incitement to or promotion of child pornography or other sexual abuse of children.[19]

But GAC itself questioned the appropriateness of the phrase "morality and public order" in March 2011.[20] ICANN in November 2010 followed up with another explanatory memorandum further clarifying the meaning intended and also changing the title to "limited public interest" objection.[21] The objection procedure, however, required that governments pay a fee to object and, as the subject matter of objection was defined, limited what government could object to.[22] So in April 2011, ICANN followed up with yet another explanatory memorandum, this time removing the phrase "limited public interest" altogether and substituting it with "GAC and Government Objections; Handling of Sensitive Strings; Early Warning". Governments may now raise objections on any subject matter without being compelled to comply fully with the procedure; it would suggest that there is no need to pay any fees.[23] Given the history of the process for objections, it looks like this is still a work in progress.

Another work in progress is the fine-tuning of the rules concerning internationalized domain names (IDNs). They are, in theory, the best way for the non-English using community to access the Internet. With the domain name in their native language, conceptually, such users should have the experience of being at home on the Internet. IDN had been proposed and shown to be technically capable of being implemented back in the late 1990s. But it was only in May 2010 that the first IDN ccTLD was able to be installed in the root zone.[24] Before that, some countries, notably China, had been selling domain names with Chinese characters but only through its .CN registry.

The IDN has been treated as a type of gTLD by ICANN in its gTLD Applicant Guidebook.[25] Many working in the IDN arena feel that the misfit can pose many problems.[26] The biggest concern is over "confusingly similar" names, which would allow complainants to block the registration of the names. A Generic Names Supporting Organization (GNSO) IDN Working Group had reported in March 2007 that there was support for confining "confusingly similar" to

18 GAC, "GAC Principles Regarding New gTLDs", 28 March 2007, Clause 2.1, http://www.icann.org/en/topics/new-gtlds/gac-principles-regarding-new-gtlds-28mar07-en.pdf.

19 ICANN, "New gTLD Program Explanatory Memorandum: Morality and Public Order Objection Considerations in New gTLDs", 29 October 2008, http://www.icann.org/en/topics/new-gtlds/morality-public-order-draft-29oct08-en.pdf.

20 "GAC Communiqué—Nairobi", 10 March 2010, https://gacweb.icann.org/download/attachments/1540146/GAC_37_Nairobi_Communique.pdf?version=1&modificationDate=1312226773000.

21 ICANN, "New gTLD Program Explanatory Memorandum: Limited Public Interest Objection (Morality and Public Order Objection)", 12 November 2010, http://www.icann.org/en/topics/new-gtlds/explanatory-memo-morality-public-order-12nov10-en.pdf.

22 GAC, "GAC Comments on the Applicant Guidebook (15 April 2011 version)", 26 May 2011, http://www.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf.

23 ICANN, "GAC and Government Objections; Handling of Sensitive Strings; Early Warning", 15 April 2011, http://www.icann.org/en/topics/new-gtlds/gac-objections-sensitive-strings-15apr11-en.pdf.

24 See Wikipedia, "Internationalized Domain Name", http://en.wikipedia.org/wiki/Internationalized_domain_name for a more detailed account.

25 ICANN, "gTLD Applicant Guidebook", 30 May 2011, http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.

26 Panel at the Asia Pacific Regional Internet Governance Forum, 16-18 June 2011, http://2011.rigf.asia/transcript/04.pdf.

names that were visually or typographically confusingly similar.[27] Such a rule is necessary to prevent what is known as an IDN homograph attack[28] where a second language is inserted into the first language. An example, cited in Wikipedia, is using the Cyrillic C to replace the Latin C in Citibank.com. Because the gTLD approach is a dot-anything approach, such mixture of languages has been permitted.

Another issue is that the gTLD Applicant Guidebook at 2.2.1.1.3 says that "confusion based on any type of similarity (including visual, aural, or similarity of meaning) may be claimed by an objector."[29] Given that some languages, such as Chinese or Indian, have tones, the guideline would enable one registrant to potentially block other registrants with similar sounding tones in the domain name.

At this time in late 2011, both issues have yet to be fully resolved.

There is one more technical issue to discuss. This concerns the root server. When a computer looks up an address, it looks from right to left. As the gTLD is to the right of a Web address, the first place the computer should look up is the extreme right. So for www.google.com, the computer should look up .com. Here, the modern DNS code has "inserted" an implied code: all Internet domain names actually end with a dot or full-stop (".") that goes to a server called the root server. There are 13 root organizations, called root server operators, running servers labelled A to M. The A server functions as the master server, communicating with the B to M servers several times a day so that the information is current. In practice, much of the information is stored in other servers around the globe for redundancy, to minimize traffic on the Internet and to speed up access. This entire area is called the Root Zone.[30] Because the Root Zone is critical to the running of the Internet, there is even a server that is hidden from hackers called the hidden server. The hidden and A master servers are both physically located in the USA.

This raises the question of what happens to a country's Internet if the country is at war with the USA. Can the US Government, for example, delete that country from the root zone file so that it disappears off the Internet?

Before the war in Iraq, the IQ domain name disappeared from the Internet. The IQ domain was not operated by any of Saddam Hussein's cronies but by Palestinian Arabs living in Texas. The domain name operators, the Elashi brothers and their business partners, were arrested and charged in 2002 for illegally exporting computer parts to Libya and Syria. Coincidentally or otherwise, the IQ domain name system was shut off just before the war. On 28 July 2005, between the time the report of the UN-appointed Working Group on Internet Governance (WGIG) was completed and before it was translated into the official United Nations languages, the IQ domain name was given to the Iraqi government. The reason was that it was only at that time that there was a stable and functional Iraqi government.

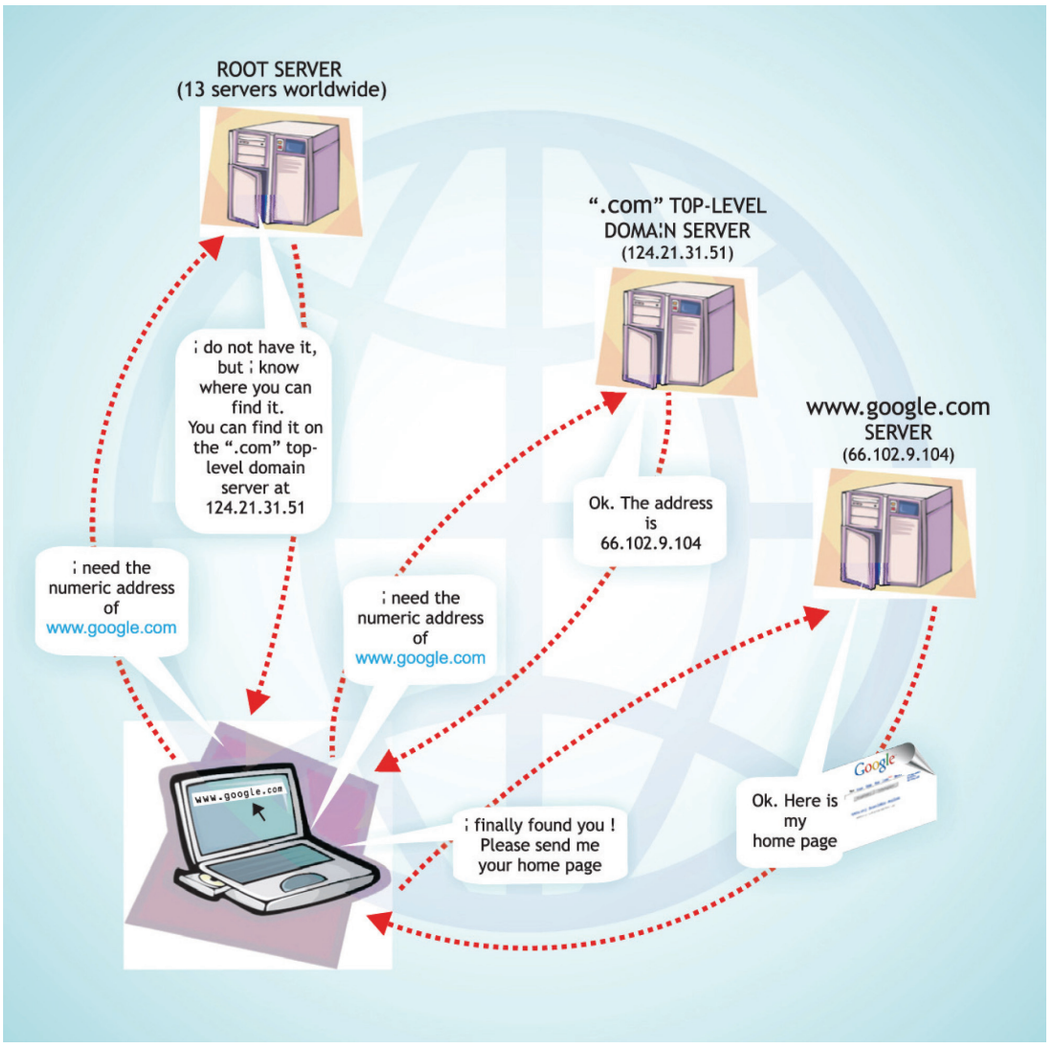
27 GNSO, "Outcomes Report of the GNSO Internationalized Domain Names Working Group", 22 March 2007, http://gnso.icann.org/drafts/idn-wg-fr-22mar07.htm.

28 See Wikipedia, "IDN Homograph Attack", http://en.wikipedia.org/wiki/IDN_homograph_attack for more details.

29 ICANN, "gTLD Applicant Guidebook", 30 May 2011, pp. 2-8, http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.

30 Wolfgang Kleinwächter, "De-Mystification of The Internet Root: Do We Need Governmental Oversight?", in *Reforming Internet Governance*, William J. Drake, ed. (New York, UN ICT Task Force, 2005), pp. 209-225, http://www.wgig.org/docs/book/WGIG_book.pdf.

Figure 2. Locating a website on the Internet



Source: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1175.

Control over the root zone is seen as the key issue in Internet Governance. There are other related concerns, however. Some countries have been concerned about the issue of the distribution of Internet Protocol (IP) addresses. Due to the haphazard and unplanned way that the Internet has developed, some US universities have more IP addresses than some countries. The issue is not just the basis on which the IP addresses are distributed but also whether the IP addresses can be exhausted. Under the Internet Protocol version 4 (IPv4) system in use, there are 4,294,967,296 unique IP addresses. Because the global population is far greater than this number, there is the possibility of running out of IP addresses. To some extent, the issue has been ameliorated by more efficient use of the IP address system and the introduction of Internet Protocol version 6 (IPv6), which has 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 (340 trillion trillion trillion) unique IP addresses.[31]

The issue of Internet Governance came to the fore during the 2003 World Summit on the Information Society (WSIS). While many countries wanted to address the issue of Internet Governance, the USA was of the view that there was insufficient capacity especially in developing

31 OECD, "Governments and business must tackle Internet address shortage together, says OECD", May 2008, http://www.oecd.org/document/29/0,3343,en_2649_201185_40542045_1_1_1_1,00.html.

countries to address the issue. Thus, it was decided that a working group be appointed by the United Nations Secretary-General to report on the issue. The WSIS Declaration of Principles states:

> 50. International Internet governance issues should be addressed in a coordinated manner. We ask the Secretary-General of the United Nations to set up a working group on Internet governance, in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005.[32]

The WGIG, as the committee was called, consisted of 40 persons tasked with a fact-finding mandate, that is to determine what Internet Governance is all about, what the issues are, and who should be doing what. It is to the report of the WGIG that we next turn.

Question To Think About

How important is Internet Governance to your country?

Test Yourself

1. Why was the Internet invented?
2. It is often said that the Internet has no “centre”. Is that true?
3. How does the DNS organize the Internet?
4. What is the difference between an IP address and a domain name?
5. What are the practical differences between IPv4 and IPv6?

32 WSIS, Declaration of Principles – Building the Information Society: A global challenge in the new Millennium (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/dop.html.

2. MULTILATERAL AND MULTISECTORAL GOVERNANCE OF THE INTERNET

This section aims to give an overview of the WGIG Final Report, the political tension around the most contentious aspects of Internet Governance, and the rise of the Internet Governance Forum.

A legitimate concern in Internet Governance is that the recommendations not undermine the functioning of the Internet. Thus, WGIG adopted several guiding principles for its work, namely, that the Internet should continue to be stable and secure, that its architecture and development of standards remain open and decentralized, and that names and numbers continue to be managed competently.

2.1 Definition

The definition of Internet Governance began with some controversy. In his address to the WGIG, then ITU Secretary-General Yoshio Utsumi, in his role as WSIS Secretary-General, wanted a narrow definition of Internet Governance. He said:

> [M]any of the issues that could fall under the wider political concept of "Internet Governance" have already been extensively debated during the first phase of WSIS and agreed principles and actions have been stipulated in the final documents of the first phase. There is wide agreement among governments, as stated in Hammamet, that these issues should not be reopened. Therefore, there is no need, for instance, to discuss such issues as free flow of information, countering spam, network security, regional root servers, privacy protection or misuse of information and communication technologies (ICTs). Instead, we should focus on the core activity of the management of Internet resources by ICANN [Internet Corporation for Assigned Names and Numbers], in particular top-level domains, which is where important issues remain unresolved.[33]

The Working Group did not accept that narrow view but adopted instead a broader definition of Internet Governance:

> 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.[34]

The definition was succinct, especially when compared with others that were offered.[35] The definition is significant in several ways. First, it rejects the narrow view of Internet Governance as referring simply to the functions of ICANN that the ITU felt were equivalent to what it was

33 Yoshio, Utsumi, "Welcome Speech", a statement to the First Meeting of the Working Group on Internet Governance, Geneva, Switzerland, November 2004, pp. 23-25, http://www.wgig.org/docs/Utsumi.pdf.

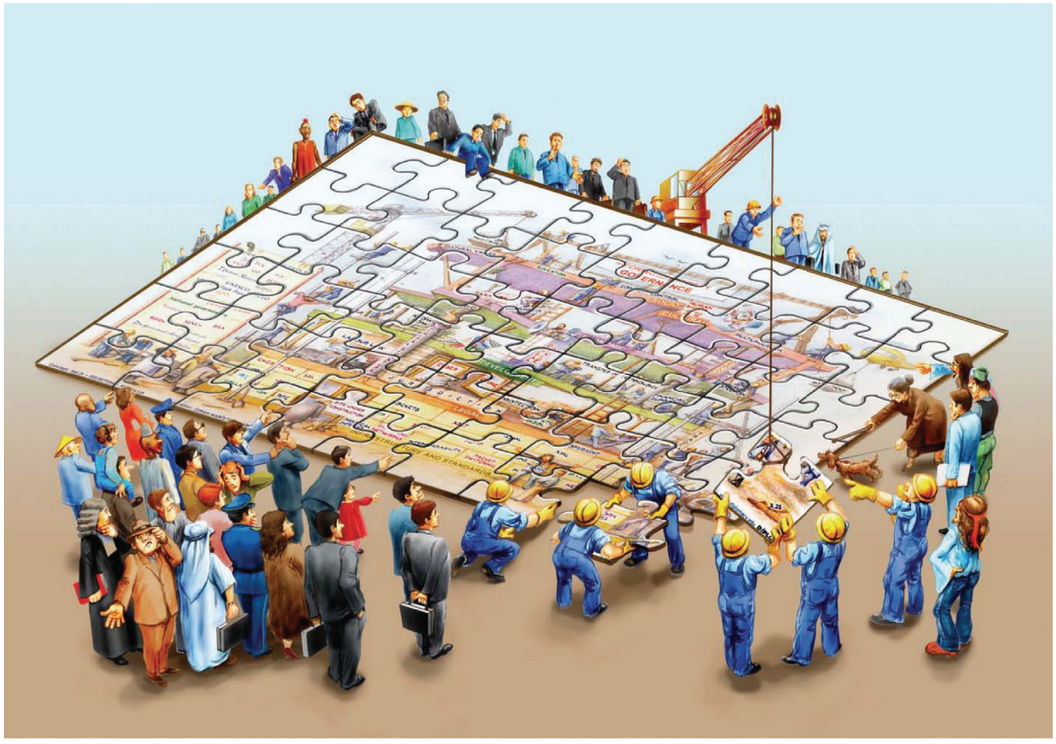
34 WGIG, Report of the Working Group on Internet Governance, June 2005, p. 4, http://www.wgig.org/WGIG-Report.html and http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695%7C0.

35 WGIG, Background Report, June 2005, http://www.wgig.org/WGIG-Report.html and http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1661|1662|1663|1664.

already doing. Second, the definition covers important public policy issues such as spam, privacy, cybercrime, security and development of the Internet—issues that did not sit comfortably with the structure of the ITU. Third, the definition included the private sector and civil society in a multi-stakeholder approach that the ITU could not incorporate easily into its meetings because the ITU membership consisted of telephone companies, which in many countries were government-linked business entities. The definition also implied that Internet Governance was more than just laws passed by governments. It included social norms and rules that had been developed by the Internet community. This gave recognition to civil society, which had played a role in the development of the Internet.

The definition, coupled with statements made in the WSIS Declaration, implied that the Internet Governance process should be multi-stakeholder (involving government, private and public sectors), multilateral (involving many countries), and transparent and democratic (respecting the wishes of the majority). It underlined the importance of process in Internet Governance.

Figure 3. Multilateral and multisectoral participation in Internet Governance



Source: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1188.

2.2 Recommendations

The Working Group also made several recommendations. The first was a forum for all stakeholders to address Internet-related issues. The forum was to be a low-cost structure with no decision-making power. Its aim was to be a venue for stakeholders to discuss issues and share best practices. The first Internet Governance Forum met in Athens in 2006. The second meeting was in Rio de Janeiro, Brazil. The third meeting was in December 2008 in Hyderabad, India.

The second recommendation of the WGIG had to do with oversight of the Internet. The Working Group recommended the internationalization of oversight based on the WSIS principles that such oversight should be multi-stakeholder, multilateral, transparent and democratic. While observing that such oversight should not interfere with the day-to-day operations of the Internet, the Working Group implicitly suggested that the US government should give up its sole oversight authority over ICANN.

Although the WGIG Report found ICANN to be the most transparent among international agencies involved with the Internet, it also pointed out issues with ICANN. The first is that ICANN does not offer any timetable as to when gTLDs will be created. Having such a timetable is useful for those suggesting gTLDs and for those who may have comments to make regarding the gTLDs being proposed. Second, it was found that the least transparent part of ICANN is the GAC, the forum at which governments give their inputs. The major governance issues, however, are that first, ICANN is a US company with a sole-sourced contract, not a contract awarded based on tender in accordance with best practice. Second, ICANN is under the US Department of Commerce with a memorandum of understanding signed between them.

The US government has given two reasons for its continued oversight of ICANN: (1) to ensure the stability and security of the Internet; and (2) to avoid censorship of the Internet by other governments.[36] Both reasons are debatable. The first suggests that the expertise for the continued running of the Internet does not exist outside of the USA. The second reason runs counter to the de facto censorship of the domain name space when the XXX domain name space, which was intended to be used for pornography sites, was approved and then recalled and rejected. Although this was a decision made by ICANN, a private company, the recall was apparently initiated by a US lobby group and supported by a US government appointee.[37]

But so what if the USA behaves as if it owns the Internet? One might look at two similar technologies where there is international tension over US dominance. The first is the global positioning system (GPS), a military-controlled service made available for civilian use. The Europeans have developed a parallel system called Galileo to ensure that a positioning service would be available should the US cut off the availability of the GPS.[38] The second technology where there is US dominance is the Joint Strike Fighter Program. The total cost of the 10-country program is estimated at more than USD 40 billion, with partner countries contributing more than USD 4 billion. The source code for the computer program that is essential to operate the plane is in the hands of the USA. Initially, there was resistance to sharing the source code even with the United Kingdom (UK), which had contributed USD 2.5 billion, the biggest share among the partners. After the UK threatened to pull out of the project and abort the planned purchase of 150 planes, the US government signed an agreement to allow the UK to retain "operational sovereignty" over the planes.[39]

In summary, having a parallel system adds to the cost of developing both systems. In the case of the GPS, the Galileo system promises to be more accurate than the American system. In the case of the Joint Strike Fighter Program, the US reaction will give pause to cooperation on similar programs in the future.

36 See, for example, the letter by US Congressman Edward Markey as chairman of the Subcommittee on Telecommunications and the Internet in "Markey, Committee Members Comment on Possible Changes to Internet Watchdog Agency", Office of Congressman Markey, 6 May 2008, http://markey.house.gov/index.php?option=content&task=view&id=3342&Itemid=125.

37 Milton Mueller, "XXX Puzzle Pieces Start to Come Together: And the Picture is Ugly", *CircleID*, 17 August 2005, http://www.circleid.com/posts/xxx_puzzle_pieces_start_to_come_together_and_the _picture_is_ugly.

38 Directorate-General Energy and Transportation, "Galileo FAQ", http://ec.europa.eu/dgs/energy_transport/galileo/faq/index_en.htm.

39 BCC, "Joint Strike Fighter Deal Agreed", 12 December 2006, http://news.bbc.co.uk/2/hi/uk_news/politics/6173143.stm.

The third WGIG recommendation was that international cooperation among the various organizations and agencies involved in Internet Governance should be improved. Among the inter-governmental organizations are the ITU, the World Intellectual Property Organization (WIPO) and the United Nations Educational, Scientific and Cultural Organization (UNESCO). Among the Internet institutions are ICANN, the Internet Society, the Internet Engineering Task Force, the World Wide Web Consortium (W3C) and the Regional Internet Registries (RIRs). The WGIG recommendation indicated that there were many other agencies besides the ITU that are involved in Internet Governance. In short, the ITU had not proven itself to have a distinctive claim on Internet Governance.

The fourth WGIG recommendation is for regional and national coordination of policies. This recommendation calls for a closer working relationship between ccTLDs and governments and the shaping of "Internet-friendly" policies. It also recommends that governments set up Internet "steering committees" to guide national Internet Governance. In particular, the committees are supposed to look at the following issues:

- Administration of root zone files and root server system of the DNS
- IP addressing
- Interconnection costs
- Internet stability, security and cybercrime
- Spam
- Freedom of expression
- Meaningful participation in global policy development
- Data protection and privacy rights
- Consumer rights
- Multilingualism

These issues have been grouped into four clusters, as follows:

Physical infrastructure – This is the cluster that discusses the more politically charged issues such as the ICANN-related issues concerning IP addresses, domain names and the root zone server. Also included in this category would be the issue of financing charges.

Use and abuse of the Internet – In this cluster are such issues as spam, network security and cybercrime. Addressing these issues should increase the use of the Internet while minimizing its misuse.

Issues related to the Internet but with a wider impact – Policies that affect the Internet may also have an impact beyond the Internet itself. Key areas where this is apparent are competition policy, e-commerce and intellectual property rights.

Development aspects of the Internet – Keeping in mind that development is one of the driving forces behind WSIS and therefore the Internet Governance debate, development is an issue that cuts across the discussions. The Digital Solidarity Fund has been started to facilitate the use of information and communication technology for development (ICTD). Development in this context should be aligned with the Millennium Development Goals (MDGs).

These four categories of issues will be discussed in subsequent sections of this module.

Something To Do

1. List policies regarding the Internet that exist in your country.

2. Trace (or briefly narrate) how these policies regarding the Internet developed in your country.

Developing countries face two issues with respect to Internet Governance: (1) how to have effective and meaningful participation in Internet Governance arrangements; and (2) how to build capacity to address the issues.

The WSIS Summit in Tunis responded to the WGIG Report by leaving Internet Governance arrangements more or less as they were with the caveat that national governments have the sole authority over their ccTLDs. This allowed anyone who wanted to claim victory to do so.

Conclusion

The WGIG Report is an excellent summary of key governance issues regarding the Internet. It also offers a model for the Internet Governance process. The Report embraces government, private sector and civil society as key stakeholders in Internet Governance. The WGIG process itself was a model of openness and transparency. However, the WGIG Report is neither a road map nor a plan for action.

Test Yourself

1. What is the definition of Internet Governance as espoused by the WGIG? What is the significance of the definition?

2. What are the key recommendations of the WGIG?

3. What are some lessons regarding Internet Governance that may be drawn from the WGIG Report?

3. DIMENSIONS OF INTERNET GOVERNANCE I — USE OF THE INTERNET

This section aims to describe various modes of regulating the Internet.

Knowing the issues, how does one go about putting in place rules and policies for the Internet? Is it possible to regulate the Internet?

In fact, within limits, it is possible to apply some rules to the Internet to encourage its use and enhance its utility.

3.1 Modes of Regulation

There are four modes of regulation, as follows:

- Law – Through government and private sanctions and the use of force, including self-regulation, especially when it is delegated by the government;
- Social norms – Through expectation, encouragement or embarrassment;
- Market mechanisms – Usually addressing price and availability; and
- Architecture – What technology permits, dissuades or prohibits.[40]

Architecture

The term “architecture” refers to the design of the technology so that certain behaviours are encouraged or discouraged. For example, to discourage speeding, one could put more traffic police on the road or one could install speed bumps. In Singapore, roads in residential estates are made winding to slow down drivers and also to beautify the estate. Similarly, manufacturers have put in locks and blocks to make it difficult to copy songs and videos.

With regard to the Internet, some people believe that the very design of the Internet empowers greater freedom of expression. This implies that those who would like to regulate content would find it very challenging to do so. In the Republic of Korea, instead of attempting to pinpoint and catch hackers and those who use botnets to attack the Internet, the security agency has developed a “honeynet” to fool the botnets into accessing the false network.

Market mechanisms

This mode of regulation usually deals with pricing and availability of goods and services. Regulations that use market mechanisms as a regulatory tool would include rules of fair play, clear contractual terms, and fostering competition in the marketplace. At the basic level is the notion of trading, of buying and selling.

40 Lawrence Lessig, *Code 2.0* (New York, Basic Books, 2007).

Trading privacy on the Internet, such as by giving one's e-mail in exchange for the right to read or receive content, is an example of using a market mechanism as a form of regulation. The idea is that if one values one's privacy more than the right to read or receive content, then one would not surrender one's e-mail address. In the USA, private companies such as Trust-e have sprung up to offer users privacy protection. In contrast, the European Union (EU) believes that privacy should be governed not by private agreement between an individual and a company but by law.

Social norms

Using social norms as a regulatory mechanism assumes that social pressure can dictate a person's behaviour. Netiquette, or etiquette on the "Net", is an example of the use of social norms as a regulatory mechanism. Netiquette requires, among others, that posts to a forum should be relevant or on-topic, and that after someone has said "you're welcome" to your "thank you", there is no need for a further response.

The use of social norms is easier when there is a social group involved because the group then functions as the monitoring and enforcement agency. Those who break the norms may be expelled from the social group. Such a sanction can be powerful when membership in the social group is considered important.

Laws, including self-regulation

Laws are manifestations of policies and are made by the parliament or national assembly. In general, one should be careful about passing laws in a fast-changing environment such as technology. Here, there is a first-mover disadvantage. For example, Utah's Digital Signature Act, which was the first of its kind in the world, was very quickly made obsolete because new technologies emerged that made its technology-specific approach dated. Singapore and the USA, which came out with the first laws to immunize network operators (in the case of Singapore) and other intermediaries (in the case of the USA), soon found that other countries had taken their laws and modified them, arguably in superior ways.

Probably the best advice is that laws should lag and not lead technology, and that one should always adopt a multi-stakeholder approach with wide consultation before the laws are passed. It must be borne in mind that the Internet is still at a relatively early phase of development.

Self-regulation

The Internet industry has tended to talk of self-regulation as a way of allowing greater flexibility in the passage and enforcement of laws. Originally, self-regulation meant industry regulating industry, not the person or company regulating him/herself or itself. In practice, self–regulation was often delegated power, with the ultimate power to sanction still in the hands of the government. That is, the government allowed industry to take the lead in regulating the sector in question. Advertising is an area where governments, especially in developed countries, have tended to use self-regulation. Recalcitrant offenders who disregard the decisions of the industry can find the government pursuing legal action against them for misleading or offensive advertising.

Self-regulation, however, needs a motivated private sector. It seems to work in advertising because using government edict to approve advertising will slow down this fast-paced sector and very likely stifle creativity. The Internet industry favours self-regulation less. Some in the industry have even complained that self-regulation means that the industry is doing the work of government.

Questions To Think About

1. To what extent are the four modes of regulation used in your country?
2. Which mode or modes of regulation would not work well in your country and why?
3. Which mode or modes would work best and why?

3.2 Suggested Road Map

Since the definition of Internet Governance is broad in scope, the following is suggested as a road map to develop a policy framework. The road map covers the range of issues and indicates milestones so that one has a benchmark to determine the efficacy of the rules and policies being developed. The road map is robust to the extent that it has been "tested" against real world developments.[41]

When the road map was developed in 1996, many countries did not have even basic rules governing electronic evidence. Today, there are few countries without the basic rules. However, the framework is still applicable in that it guides refinement of the rules and policies surrounding the Internet.

Roughly in descending order of importance, the issues to be addressed are:

1. Access and Service Provision
2. Electronic Commerce
3. Content Regulation
4. Security
5. Intellectual Property Rights
6. Privacy

It is essential to address access and cost issues first because doing so would make the Internet more widely available. The availability of access would then throw up a plethora of issues related to mapping the online world to the offline world. For example, if someone commits banking fraud using the Internet, are the rules of evidence updated so that the person may be prosecuted based on evidence collected online? There is a commercial incentive to resolve these fundamental issues in reconciling offline laws with the online world. Issues in content regulation and security will arise because of the tension between what is available and can be done on the Internet versus what is available and can be done in the offline world. Many countries have given up on regulating content on the Internet except to protect the young, which is defined as those below 12 years old. There is some urgency in resolving content regulation and security issues because there are potential users who shy away from the Internet because they do not want, for example, pornography accessed at home or their computer hacked by others. Intellectual property rights and privacy protection gain greater importance as use of the Internet becomes more widespread.

41 See Peng Hwa Ang, *Ordering Chaos* (footnote 1) for a fuller discussion.

Access and service provision

The issues to be addressed under this heading are related to providing affordable access to the Internet. These issues are:

- How to manage technical standards in a networked environment.
- How to ensure interconnection and interoperability of computer systems and networks.
- How to regulate pricing and service quality of information services.
- Clarifying the responsibilities and liabilities of access and service providers, such as protecting access and service providers from liability for third-party content.

The issue of immunity is important because without it, e-commerce could be stifled.

Questions To Think About

In many countries, the law on defamation means that anyone who injures another person through a false statement would have to compensate the injured person. In some countries, the amount of compensation may depend on whether the false statement was made knowingly or not. In other countries, it does not matter whether the false statement was made unknowingly. In your country, to what extent would your laws tolerate erroneous statements made on (a) a book review site, (b) a hotel review site, and (c) an auction site? Would an Internet service provider in your country be held liable if it is found to be transmitting the erroneous statements?

Electronic commerce

From a commercial point of view, electronic commerce or e-commerce has many advantages. A firm that opens an e-commerce business opens a 24-hour store that eliminates the middle person and opens new markets. e-Commerce may also make a business more efficient because it automates business.

e-Commerce, however, is not for all businesses. e-Commerce may not work for businesses that sell expensive items such as furniture because customers usually want to test these items before purchasing them. Also, in some cultures shopping is a leisure activity that e-commerce will detract from.

It is worthwhile to try to address e-commerce issues because doing so also resolves a host of problems that are obstacles to the greater use of the Internet. The following should be addressed:

- Legally recognize the electronic environment
- Admit electronic evidence
- Recognize e-transactions
- Recognize digital signatures and digital certificates
- Clarify the rights, responsibilities and liabilities of various parties, as well as dispute resolution mechanisms
- Encourage electronic payment mechanisms and their use
- Empower the police to enforce law in electronic commerce
- Clarify taxation in electronic commerce

It will probably be necessary to pass an act along the lines of what has been called an e-commerce or e-transactions law. Such a law would prepare the environment for e-commerce.

Recognizing Electronic Evidence

In many countries, the recognition of electronic evidence in its various forms became necessary with the wide public availability of the Internet from the mid-1990s. For example, rules of evidence had to be amended when digital signatures were invented. In Singapore, the rules were amended in the Electronic Transactions Act in 1996. In India, they were amended in the Information Technology Act 2000. In short, the new laws updating the offline world to cope with the online world are of fairly recent origin.

Something To Do

Describe regulations for enhancing or enabling e-commerce in your country. If there are no such regulations, list what you think might be appropriate regulations to enhance or enable e-commerce in your country.

Content regulation

Some users cite objectionable content as a reason for not subscribing to the Internet. However, what is objectionable varies among individuals. Resolving this issue therefore requires balancing competing interests. The major benefit of not having any filtering is the unlimited availability of content. Sometimes, the filters “overblock” so that innocuous content is also blocked.

The following are the issues in content regulation that need to be addressed:

- How to block objectionable materials on the Internet, principally for the sake of children.
- How to protect national interests against undesirable foreign materials.
- How to reconcile conflicting cultural values in information content.

Illegal Content: Global Coordination

Due to cultural differences, it is difficult to arrive at a universal agreement regarding what is objectionable. There is, however, greater agreement on what is illegal, which is typically that which causes harm. Child pornography comes to mind.

Global coordination by enforcement agencies has acted as a check to the spread of child pornography. Law enforcement agencies have cooperated to conduct occasional sweeps. As recently as the late 1990s, much of the images of child pornography were scanned from the offline world. But with the Internet, there are images of live abuse of children transmitted over webcam. To stop such abuse, police agencies target those who download child abuse images. A number of high profile coordination campaigns were conducted in 1998 (Operation Cathedral) and 1999 (Operation Ore) that led to hundreds of arrests in many countries.

For more information refer to WGIG, Background Report, June 2005, p. 34, para. 141, http://www.wgig.org/WGIG-Report.html and http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1661|1662|1663|1664.

Security

This issue has gained greater significance as Internet worms, viruses and Trojan horses have become ever more sophisticated.

ILoveYou Virus

The most damaging computer virus ever written spread so quickly that agencies such as the US Pentagon, Central Intelligence Agency and UK Parliament had to shut down their e-mail system to get rid of it. The virus spread quickly because it replicated itself on e-mail addresses that were resident in users' Microsoft Outlook address book. Because the e-mails came from acquaintances, users clicked open the message and spread the virus.

Despite the immense cost of disinfecting computer systems the world over, the author of the virus got away scot-free even though he was identified. When the virus was released in May 2000, there was no law in the Philippines, where he lived, against the release of a computer virus. In June 2000, the Philippine e-Commerce Law, which had been in the works, was passed. It includes provisions to criminalize the spread of computer viruses.

Source: Peng Hwa Ang, "Policing Asia's Internet", *Asian Wall Street Journal*, 7 September 2000, p. 8.

In essence, the security issues are:

- How to protect against breaches of security in computer systems and networks.
- How to prevent crime in the digital environment.

Module 6 in the *Academy of ICT Essentials for Government Leaders* module series is on Information Security and Privacy.

Intellectual property rights

The digital world makes it possible to make perfect replicas of the first copy. There is no degradation of quality, as happens in the analog world. However, the ease with which perfect copies may be made also means that it is easy to breach intellectual property rights.

A modern intellectual property rights regime should therefore address the following issues:

- How to extend the current copyright regime to include digital works.
- How to acquire, protect and manage rights in the digital environment.
- How to prevent piracy of copyrighted work.

Music Piracy

Music is probably the most widely pirated content globally. While sales of the iPod and other music players have continued to climb, sales of music compact discs have declined for several years. Fuelling the piracy is the widespread sharing and downloading of songs through peer-to-peer software.

Contrary to a widespread misconception, those who share songs online can be traced and prosecuted. The misconception probably arose because with peer-to-peer software such as BitTorrent and LimeWire, users are downloading the songs from other individuals. Thus, one person can pass on a song to many others in a viral-marketing fashion.

Music owners have fought back, with the most aggressive being the Recording Industry Association of America (RIAA). The RIAA has prosecuted students, knowing that they are a financially impoverished group, to set an example for others. Some reports suggest that the RIAA has even urged students to drop out of school to work in order to pay the settlement.

Something To Do

Identify laws and other measures to protect copyright in your country. Assess how effective they are in a digital environment (i.e. in light of developments in digital technology).

Privacy

The strongest privacy regime is the EU's Data Protection Directive, which demands that third parties have an "adequate level" of data protection before they can process data from the EU. But its implementation has been delayed by the reluctance of the US Government to have a similar regime. The US has offered the creative alternative of a "safe harbour" provision in which those who comply with the Directive would be considered to be in a safe harbour and deemed to be in compliance with the Directive.

The Organisation for Economic Co-operation and Development (OECD) has also developed privacy guidelines that attempt to strike a less demanding posture on privacy compared with the EU's position on privacy.[42]

The main issue in privacy regulations is how to regulate use of personal information by public and private institutions.

42 OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.

Meeting the EU Standard

The EU's position on privacy is well thought out. Part of its novel approach is the requirement that data from the EU cannot be passed to another country for processing unless that country has the same level of protection of the data as the EU. In practice, there are exemptions, such as for aeroplane flights. But the EU policy has had the effect of forcing many countries to update their data protection laws to meet the EU standard.

There is no question that the EU standard imposes some business costs. So understandably, business associations try to meet the bare minimum of the standard where possible.

The US has safe harbour provisions negotiated in part by the US Government although ostensibly it was done by the private sector. The US safe harbour provision means that those companies whose data protection standards meet the self-regulatory safe harbour standards would be able to receive and process data from the EU.

In Australia, the Government attempted to update its privacy laws to bring it to a level "adequate" for the EU. However, apparently because of lobbying by business, the provisions were watered down and some safeguards are lacking.

There is therefore a balance to be struck between business interests and the EU standard of privacy protection.

The European Commission's webpages on data protection at http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm have links to resources and more information on privacy.

Conclusion

The approaches to Internet-related issues outlined above are based on international norms because the Internet is international in scope and no country can be isolated from the rest of the international community. Moreover, it is essential to consult stakeholders, such as industry and civil society, widely, both to educate the community and to be educated about the issues.

Something To Do

Decide whether the ranking of the six categories of issues above is appropriate for your country context. If you feel that the given ranking is not appropriate for your country, propose how these categories of issues should be ranked in terms of degree of importance in your country and justify your proposal.

Test Yourself

1. What are the four modes of regulating the Internet? What are their limitations with respect to regulating the Internet?

2. The suggested road map for regulating the Internet is just that—a suggested guide. What are the suggested steps within this road map?

4. DIMENSIONS OF INTERNET GOVERNANCE II — ABUSE OF THE INTERNET

This section aims to raise awareness of the more common abuses of the Internet and the actions that can be taken to address these.

4.1 What's Special about the Internet

Some have commented that the Internet is merely a reflection of the offline world and that therefore no special rules are needed for it. However, this misses several special features of the Internet.

First, the Internet makes it easier to be anonymous. To be sure, it is possible for law enforcement to trace users. But doing so requires special effort and resources. The strength of anonymity is that it affords open and frank communication on such matters as medical conditions. However, anonymity may also be a cloak for criminals.

Second, there is a culture of anarchy and lawlessness on the Internet that is probably best illustrated by John Perry Barlow's "Declaration of the Independence of Cyberspace":

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[43]

This declaration was of course a hopelessly unrealistic "pipedream" that reflected a misunderstanding of laws: laws do not govern a place but people in the place. As long as there are people, there will always be a need for laws to spell out rights and to act as a social lubricant to minimize human friction.

Third, as we are beginning to learn, the Internet is a powerful tool for networking. This capacity, which is best illustrated in social networking sites such as MySpace and Facebook, is now known as Web 2.0. With Web 2.0, hitherto small niche groups may gather and become sizeable communities globally. An example is barefooters.org, the members of which walk barefoot except on formal occasions. In 1999, there were just 400 of them worldwide. By 2007, they numbered 2,000 spread across several countries. On a global basis, they command a large enough group of users to have their own logo.

In a similar way, the Internet enables those who are bent on mischief to gather and make trouble, as discussed below.

43 John Perry Barlow, A Declaration of the Independence of Cyberspace, 8 February 1996, http://homes.eff.org/~barlow/Declaration-Final.html.

4.2 Abuses of the Internet

Child pornography

Initially, child pornography consisted of the conversion of hardcopy content to softcopies. But as the technology was exploited, it became possible to have porn-on-demand in which child pornography was produced on demand.[44]

International cooperation has been necessary to crack down on criminal groups promoting child pornography. Two examples of such international cooperation were the simultaneous multi-country raids by Interpol during Operation Cathedral in 1999 and Operation Ore in 2002 that broke up the child pornography networks.[45] International cooperation is possible because child pornography is one of the few areas where there is near universal agreement that it is a criminal act.

Consumer fraud

The Internet has shown that offline laws sometimes need to be changed to cope with the new economy. Auction laws are one example. In many Commonwealth countries, auctions require the physical presence of someone with an auctioneer's licence. At first glance, such a law appears very old-fashioned. It would mean, for example, that eBay auctioneers would have to be checked in terms of whether they have a license. The rationale for the law, however, became clear very quickly once the law was liberalized to allow e-auctions: auction fraud became the most frequent variety of online fraud.[46]

Consumer fraud is another area where there is near universal agreement that it should be stopped. Cracking down on such frauds can only enhance the utility of the Internet. Since 1996, there has been an annual sweep of the Internet for consumer fraud. The number of countries involved in the sweep has been growing.

Consumer Annual Sweep

Almost 40 countries have banded together to address consumer fraud online under the International Consumer Protection and Enforcement Network (ICPEN). The Network holds an annual International Internet Sweep Day to scour the Internet for websites that exaggerate claims. In particular, the sweeps target online frauds and scams.

It should be noted that such sweeps work only as well as the offline laws offering consumer protection. It is therefore the more developed countries that are more active in such sweeps.

More details about ICPEN and its activities are available at http://www.icpen.org.

44 Ethel Quayle and Max Taylor, *Child Pornography: An Internet Crime* (New York, Brunner-Routledge, 2003).

45 Peng Hwa Ang, *Ordering Chaos* (see footnote 1).

46 Ibid.

Question To Think About

How effective are the laws against child pornography and consumer fraud in your country?

Spam, scams, malicious code, phishing

An issue that has seen the gradual strengthening of political and commercial will is spam, or unsolicited bulk commercial e-mail. This is because spam wastes bandwidth. More important, it can pose a significant security threat, as spam today can carry malicious code and allow phishing, which is "the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication."[47]

Because of its roots in the university, the Internet began with an open and trusting culture. In the early days when users (who were often based in US universities) posted messages to their e-mail lists, many would leave their phone number after their signature, which was an indication of the veracity of what they had just posted. Today, with mass availability of the Internet, indicating one's phone number in an e-mail message would attract all manner of attacks.

The first spam was probably sent by a marketing representative of Digital Equipment Corporation (DEC), which made the mini-computers for the Internet. It was a commercial message advertising a product presentation. Users complained and, unlike today where the spammers are not so easily traced, action was taken against the spammer.[48]

While the most widely recognized form of spam today is e-mail spam, the term is applied to similar abuses in other media over the Internet such as instant messaging, Usenet newsgroup, Web search engine, blogs, wikis, mobile phone messaging and games. Internationally, e-mail spam is defined as "unsolicited bulk e-mail": the e-mail is part of a larger collection of substantively identical e-mails the sending of which the recipients have not consented to receive. Spam therefore is an issue of consent, not content.[49] This means that legislation targeted at spam should address consent, not content.

Spam Spam When Will It End

The problem with spam is that unlike traditional advertising, much of its costs are borne by the receiver, not the sender. Various studies suggest that the bulk of e-mail traffic consists of spam.

The "first generation" of spam consisted of annoyances that users and system administrators could filter out most of the time. It is the newer generation of spam that is alarming. Increasingly, spam now carries malicious software code that is run without the user knowing it. The computer can then be turned into a "bot" controlled by the spammer to send out spam. In some instances, the spam may carry code to retrieve passwords and other sensitive data.

47 Wikipedia, "Phishing", http://en.wikipedia.org/wiki/Phishing.

48 Brad Templeton, "Reaction to the DEC Spam of 1978", http://www.templetons.com/brad/spamreact.html.

49 Spamhaus, "The Definition of Spam", http://www.spamhaus.org/definition.html.

The sophistication and scale of these operations suggest a level of organization often associated with criminal gangs.

The first law aimed at containing spam was the American CAN-SPAM Act of 2003. Its full name is: Controlling the Assault of Non-Solicited Pornography and Marketing Act. The Act empowers legal action by private citizens and has been used to prosecute known spam operators in the USA. An evaluation of the Act was conducted in 2005 and no significant changes were made to it. However, the level of spam in the US is such that the country ranks number one or number two for spam globally. China and the Republic of Korea also rank high.

It would appear that spam thrives with the greater penetration of the Internet, as in the case of the Republic of Korea, and where there are weak laws and enforcement, as in China.

It is a cat-and-mouse game, with spammers developing ever more sophisticated methods of dealing with spam when their previous methods are defeated. Various coalitions, taskforces and groupings of interested stakeholders have been formed over the years, most after 2003, to address the issue. At this time of writing at the end of 2011, the most active group is the Messaging Anti-Abuse Working Group (MAAWG), which has a full-time executive director and an office in San Francisco, USA. Unlike the previous groupings, which tended to focus exclusively on e-mail spam, the MAAWG adopts a holistic perspective, also looking at spam in other new media such as short message service (SMS) and social network sites.[50]

Cyberbullying, cyberstalking, identity theft, Internet addiction

The harms in this cluster result from online use. That is, they are more likely to arise when one spends more time online. Cyberbullying is harassment of a minor by another minor using the Internet and other electronic means of communication. Often, it involves the sending of humiliating and insulting messages. If the harassment is done by an adult, it is cyberharassment.

Cyberstalking is the use of the Internet and other electronic means of communication to stalk the victim. It often follows from offline stalking but it can also be a prelude to offline stalking.

Identity theft involves the use of personal details for some benefit or to avoid some obligation. Common examples include the use of the victim's personal details to obtain a credit card.

The harm from these mischiefs can be serious, as in the case of the cyberstalker who killed the female victim he was stalking. The solution lies in passing laws to combat them.

In the case of Internet addiction, which is the excessive use of the Internet to the detriment of school or office work, the Republic of Korea has a novel counselling service to address the issue.

50 See http://www.maawg.org/ and http://en.wikipedia.org/wiki/MAAWG for more details on the organization.

Addressing Internet Addiction

Internet addiction is gaining notice as a compulsive disorder like compulsive gambling. Those so addicted can spend 17 to 18 hours on the Internet. Countries that have reported more Internet addicts include China, Japan, the Republic of Korea and Taiwan. That many cases of Internet addition are in Asia raises the question of the extent to which cultural factors impact on this compulsive behaviour. More research is being conducted to determine whether the disorder is a manifestation of other compulsive disorders.

The Wikipedia entry on "Internet Addiction Disorder" (http://en.wikipedia.org/wiki/Internet_addiction_disorder) gives a reasonably balanced account of the arguments for and against the phenomenon being a true addiction.

Something To Do

Make a quick informal assessment of the level of awareness of spam, scams, phishing, cyberbullying, cyberstalking, identity theft and Internet addiction in your organization, in your government and in your society as a whole. Cite evidence or justification of your assessment.

Political will

Battling these negative uses of the Internet requires political will. First, the acts in question must be illegal in a country. In some countries, consumer protection laws are so weak that enforcement is impossible or ineffective. Second, there must be the political will to cooperate internationally. The Nigerian 419 scam, for example, continues because of practically non-existent enforcement by the Nigerian government. The result is a low level of trust in Nigerian e-commerce.

Advance Fee or Nigerian 419 Fraud

It is unfortunate that Nigeria, which is at the bottom of global corruption indices, is associated with a common online fraud named after a provision in its criminal code against obtaining property under false pretences. The Nigerian 419 scam is an advance-fee fraud where the victim is made to send money in expectation of obtaining a larger return.

The typical e-mail to the victim comes from someone with funds that he cannot access without help. The funds are supposedly from an inheritance due to the child of a deposed ruler, a dormant bank account, or even some bribes. Anyone who takes the bait will be asked to send more and more money to resolve some unexpected difficulty.

Because of the sums of money involved, these operations are often professionally organized with the collusion of government officials. Some of those who have gone to Nigeria to investigate have gone missing or been murdered.

Wikipedia's entry on "Advance-Fee Fraud" (http://en.wikipedia.org/wiki/Advance-fee_fraud) summarizes the history of the scam and also details its variants.

4.3 Sanctions

Any discussion of governance must touch on the issue of enforcement of rules. Without enforcement, rules are treated as ideals at best; at worst, they are treated with cynicism as something to be flouted. This section touches on how sanctions might be applied to enforce agreed rules regarding the Internet.

Cybercommunity norms: Netiquette and community-administered sanctions

Cybercommunities may have their own netiquette customs, norms and rules of conduct. In such instances, the most severe form of community-administered sanctions would be social isolation and expulsion. This happened in the well-known case of the "toading" of Mr. Bungle who committed online rapes against two players in a game. He was isolated and eventually had to leave the game.[51]

A Rape in Cyberspace

Online communities existed before the advent of the Internet. The communities were smaller in number and communication was text-based. This applied also to online multi-user dimension online games, which can be regarded as the predecessor of modern multi-player games such as World of Warcraft. In one of these games, LambdaMOO, a player by the name of Mr. Bungle used a program that allowed him to make it appear as if the text was coming from another player. Among the actions that Mr. Bungle described were sexual acts between the avatar he controlled and another avatar that he had made to appear as if he was controlling. The actions, which went on for hours, violated the community norms.

A few days later, LambdaMOO users met online to discuss the actions to be taken against Mr. Bungle. After the meeting, one of the master programmers of the community decided unilaterally to terminate Mr. Bungle's account. Since then, LambdoMOO users have instituted a program to temporarily remove a disruptive user from their community.

However, such community sanctions are rare because it is often difficult to get agreement that the action is wrong, and agreement about the degree of "wrongness" and the amount of the sanction. Also, the sanction of social isolation may not be sufficiently severe for some people. In short, community sanctions work but in a limited way.

Self-help

In some cases, it is possible for the offended party to resort to self-help. Copyright owners, for example, have a history of using self-help in suing those who infringe on their copyright and indeed the enforcement regime is often set up that way. This means that much of the work in investigating and enforcing the legal action is undertaken by the copyright owners themselves and not the police even though copyright rules come under criminal provisions.

51 Julian Dibbell, "A Rape In Cyberspace", *The Village Voice*, 23 December 1993, http://www.juliandibbell.com/texts/bungle_vv.html.

In 2000, the Sydney Olympic Committee hired a private company called Copyright Control Services to patrol the Internet for unauthorized sites disseminating news about the Olympics. The reason is that the rights for the broadcast of the results had been sold to the highest bidder for USD 200 million and any unauthorized leaks would have undermined the successful bidder. The 60 or so persons who "patrolled" the Internet were successful in stopping large-scale unauthorized broadcasts. A Russian television station, Moscow TV6, did attempt to argue for freedom of expression when it put out an Internet video feed. But Moscow TV6 had to halt its unauthorized broadcast because they were told that if they continued, the video feed to the TV station would be stopped.[52] Since then, there have been patrols for both summer and winter Olympics.

International law

There has been talk of developing international law to enable the investigation and prosecution of cybercrimes. In essence, such a law would create a uniform code to define, prosecute and enforce the rules against cybercrimes. There is international cooperation but few countries are involved.

The Council of Europe Convention on Cybercrime is a regional effort at such a code. Because Europe is sufficiently diverse, the Convention could have wider application. The Convention also balances the need for enforcement with freedom of expression.

Council of Europe Convention on Cybercrime

To be effective in cyberspace, law enforcement agencies have to consider the ease with which the Internet allows the crossing of borders and jurisdictions. This means that unless law enforcement agencies come together to agree on some universal rules, it will be difficult to go after criminal types.

The Internet community, however, is wary of law enforcement. On the Internet there is a culture of "almost anything goes" where freedom of expression is celebrated. There is also the concern that as the Internet is still in its emergent stage, laws that are passed for enforcement could stifle its development.

The Council of Europe Convention on Cybercrime attempts to address these concerns. The Council of Europe (CoE) consists of nearly all of the countries in Europe. It has more member states than the EU, which is a different organization. The CoE develops treaties that member states may or may not ratify, while the EU promulgates declarations that its member states must pass into domestic law.

Because of the large number of countries (nearly 50) involved, the development of the cybercrime treaty raised many issues. But because the CoE is a regional organization, the closer cultural and physical proximity means that the diplomatic tensions inherent in the discussion of these issues were minimized. Also, the nature of treaties means that countries may agree on the text but may not opt-in, or they may opt-in selectively. This ability to opt-in leaves the decision-making power regarding laws in the hands of the national parliament. In contrast, the rules made in the Parliament of the EU have to be implemented as law in national legislation.

52 CNN, "Violators caught as Olympic video monitored on Internet", 22 September 2000.

The CoE rules therefore strike a balance between the diverse concerns. The Convention on Cybercrime underwent several rounds of international review, with inputs from organizations such as the American Civil Liberties Union regarding potential free expression conflicts. The Convention lays down guidelines for countries intending to implement cybercrime laws. It came into force in July 2004. There is a provision for international cooperation, which means that non-CoE countries may join the Convention. Indeed, in January 2007 it came into force in the USA.

For more information see CoE, "Cybercrime: a threat to democracy, human rights and the rule of law", http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.

Question To Think About

To what extent is your country involved in international cooperation to address abuses of the Internet?

Conclusion

There is no question that the very capabilities of the Internet that make it such a powerful medium are also why it can be used for darker purposes. There is no doubt that there is a need to regulate some of these more sinister uses of the Internet.

Because of the difficulties in getting agreement on a definition of what is universally offensive, there is limited success in addressing some of the harm and mischief found on the Internet. The most notable successes are in consumer fraud and child pornography.

International agreement is necessary first for the institution of the laws and then for their enforcement. The Council of Europe Convention on Cybercrime may be the foundation for future agreement and cooperation.

Test Yourself

1. What difficulties do law enforcement agencies face in checking criminal abuse on the Internet?

2. What does the global community accept to be cybercrimes that should be checked?

3. What are some new crimes that have emerged as a result of the Internet?

4. What are some sanctions against these crimes that may be applied through the Internet?

5. ISSUES OVERLAPPING WITH THE OFFLINE WORLD

This section aims to raise awareness of the overlap of the Internet with the offline world in key areas concerning the government and the economy, and with respect to content. It also aims to increase awareness of the need for an appropriate regulatory response.

The Internet is having an impact on the offline world. Should the offline world be modified so that it more closely resembles the online world? Or should offline rules be applied to the online world? The answer of course lies somewhere in between.

5.1 Competition Policy

As far as possible, access to the Internet should be competitive. This means the liberalization of the telecommunications sector, particularly if the sector is monopolistic or is in fact, a monopoly. Liberalization in this sector has been shown to improve the quality of service while prices are lowered. Low pricing has been shown to increase Internet penetration. And in the case of broadband, lower pricing changes Internet use pattern. Game theory says one should have at least three players in order to have effective competition.

Liberalization of Telecom and the Cost of Internet Use

It has been said that one reason for the rise of the Internet in the USA was the liberalization of the telecommunications sector. The Internet, after all, does depend on long-distance telecommunications connection. Competition in that sector brought prices down. The impact of liberalization is most apparent in the USA, which started the telecommunications liberalization movement: it is cheaper to host a website in the USA than in most other countries. This leads to a virtuous cycle where the scale economies in turn allow prices to be kept low.

Research has shown that telecommunications demand is fairly elastic. That is, a drop in price of X per cent leads to an increase in use of more than X per cent. Studies have shown that allowing competition in the local loop of telecommunications will result in greater Internet penetration.

France, Japan and the Republic of Korea have increased broadband penetration through pro-competition policies. The Republic of Korea has the highest broadband penetration in the world. It has had the policy of allowing free entry into the facility-based telecommunications sector since the 1980s. The cases of France and Japan are more instructive as penetration rates were not very high up to about 2005. Since then, pro-competition policies have pushed down prices and the broadband penetration has jumped.

From the mid-1980s to the mid-1990s, many books and papers discussing the benefits of liberalizing the telecommunications sector came out. The liberalization of the Internet sector is an extension of the ideas explored in the telecommunications sector. See Emanuele Giovannetti, "The IT Revolution, the Internet, and Telecommunications: The transition towards a competitive industry in the European Union", in *The Internet Revolution: A Global Perspective*, E. Giovannetti, M. Kagami and M. Tsuji, eds. (Cambridge University Press, 2003), pp.124-142.

5.2 Censorship and Freedom of Expression

Censorship by government and the private sector exists all over the world. As discussed earlier, the issue is balancing the local interests with the international norm of imposing little or no censorship of the Internet. Wholesale blocking of sites is frowned upon by the Internet community. The most practical and acceptable solution lies in some element of filtering by the user. Software filters installed by the user are acceptable. But it has been found that parents are not often as savvy as their children in installing and using the filters.

Voluntary Self-Rated Filtering

In 1999, the Bertelsmann Foundation put together a team to develop a system of filtering Internet content that would be free and culturally sensitive and that would also not infringe on the right to free speech. That team included researchers, regulators as well as free speech advocates. The final output was the formation of the Internet Content Rating Association (ICRA).

The group knew the ideal outcome: a parent would click on their country name, then click on a filtering system (say, one established by the Catholic church), and then sites deemed not appropriate would be filtered out. Under the filtering system, sites would label themselves for language, violence and nudity, and whether there is objectionable (but not illegal) content such as alcohol. There were some 40 labels altogether.

In the end, however, ICRA did not come close to its lofty goal. First, there was opposition from the civil libertarians, such as the Center for Democracy and Technology in the USA. News sites that initially agreed to self-label changed their minds when they felt that they would be perceived as succumbing to a censorship regime. Second, to accommodate free speech concerns, the websites had to be self-labelled. This hindered the development of a critical mass of websites that labelled themselves. Without that critical mass of websites, filter-users would have to stop using the filters every so often. Third, the filters would have worked best had they been embedded in the browsers. At the time that the ICRA method was ready to roll, the browser war was over and Microsoft had won. Until then, both Netscape and Microsoft were adding features to their browsers. In fact, the Microsoft browser of 2000 did have a crude filtering system. Finally, as has been experienced in other similar labelling systems such as the V-chip in the USA that was supposed to filter violent television content, there is no actual demand from consumers or consumers do not act on their verbal agreement on the need for such a filtering scheme.

In 2007, the ICRA was folded into the Family Online Safety Institute.

As the author was directly involved in ICRA as a Board member, the above is recounted in detail for the first time. The book *Ordering Chaos* has some details about ICRA in the chapter titled "Censorship and Content Regulation of the Internet".

Another approach has been to install server-level filters that are sold as a special value-added service to users. A fee is paid for updating and maintaining the list of blocked sites. This is a filter that the average user would find practically impossible to bypass. The disadvantage, however, is that sometimes there is over-blocking and it is difficult to "un-block" a site that has been wrongly blocked.

Something To Do

1. Describe steps in content regulation that are being taken in your country, if any.

2. If the government of another country requests your government to block a site for content that is illegal in that other country, what should your government do? Make a recommendation and justify it.

5.3 Defamation

With much greater freedom of expression on the Internet comes a greater chance of online defamation. In general, addressing defamation requires balancing competing interests: the individual's interest in reputation and societal interest in encouraging greater freedom of expression. On the Internet, there is also the additional complication of conflicting cultural values in the weight given to individual and societal interests.

One of the most instructive cases involved Joseph Gutnick, a businessman in Melbourne, Australia. Barron's magazine, owned by the Dow Jones company, had defamed Mr. Gutnick in an article. The magazine had 14 subscribers in Australia of which five were in the state of Victoria and that was enough for the Australian High Court to assert jurisdiction.[53] Barron's had 1,700 online subscribers who paid with an Australian credit card. And the question became: If Gutnick won the case, did it mean that all publications would have to watch what they published using as a yardstick the country with the toughest libel laws? Fortunately, the High Court decided that the monetary compensation that Mr. Gutnick could claim would be limited to the damage to his reputation in Melbourne, not globally.[54] The Court seemed to have taken note of the actual damage that the defamatory article may have had, something that Commonwealth courts have not tended to do.

53 David Fickling and Stuart Millar, "How Diamond Joe's libel case could change the future of the internet", *The Guardian*, 11 December 2002, http://www.guardian.co.uk/technology/2002/dec/11/media.newmedia.

54 High Court of Australia, Dow Jones & Company Inc v Gutnick, [2002] HCA 56, 10 December 2002, http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.

Something To Do

Advise Y, who is a citizen of your country, in the following situations:

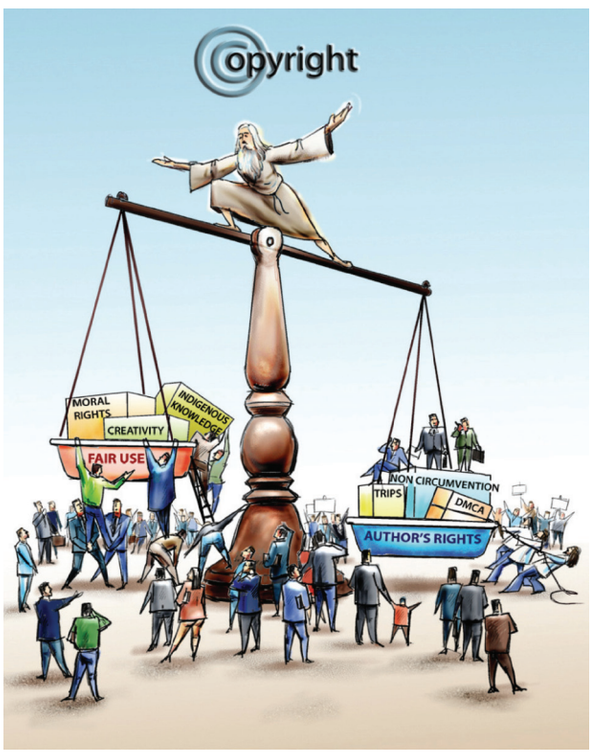
Situation 1:
W's blog in your country defames Y. Would it make any difference if the blog were popular or unpopular? What if there were 200 posts defending Y?

Situation 2:
What if an online news organization in the USA defames Y's company. Should there be "global liability" for Internet defamation?

The Internet has compelled another change in Internet laws: the need for an immunity provision for third-party content. That is, website and forum hosts should not be held liable for content posted by others provided the host acts "reasonably" after being given notice of the defamatory content. In most jurisdictions, "acting reasonably" means removing the defamatory content within a specified period of days.[55] This has also been called a notice-and-take-down provision.

5.4 Copyright and Other Intellectual Property Rights

Figure 4. A balancing act in copyright



Source: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1181.

55 Peng Hwa Ang, *Ordering Chaos* (see footnote 1).

A major contentious area in intellectual property rights is the treatment of domain names as trademarks. Multinational companies, international brands and famous personalities have tended to hold the view that their name should only be used by them as a domain name. In the USA, where many international brands originate, the Anti-cybersquatting Consumer Protection Act (ACPA) of 1999 makes it easier for such companies and individuals to take over domain names that are confusingly similar to their trademark or name and if the domain name owner has acted in bad faith. Most other countries, however, do not have a similar law. Many countries, such as Australia and Canada at the ccTLD level, check that the registrant has some connection to the domain name being registered. And when disputes do arise, the preference is for the Uniform Dispute Resolution Process (UDRP) created by ICANN because it is cheaper than using the courts. But US courts using ACPA can and have overruled the UDRP result.[56] This has in turn led to "reverse domain hijacking" where companies, typically the larger ones, attempt to take away domain names of owners by making false claims of bad faith.[57]

The WIPO Arbitration and Mediation Center, which has a procedure to handle domain name disputes based on the UDRP, reported a record 2,696 cybersquatting cases in 2010.[58] With the new gTLDs coming onstream, the number of complaints is expected to grow.

A more recent contention concerns the liability of intermediaries on the Internet. Websites that allow users to post comments and reviews may host content that breach copyright and other civil rules. Under conventional law, such websites would ordinarily be held liable for the violation even though they may not have originated the content. From about the mid-1990s, laws were amended so that intermediaries enjoyed some form of immunity from liability provided they responded "reasonably".[59] The Anti-Counterfeiting Trade Agreement (ACTA) that was finalized in April 2011, however, runs counter to that trend.

ACTA was intended to address the piracy of digital content. Both the process and outcome of ACTA, however, have been criticized for several reasons. A group of prominent academics issued a coordinated statement criticizing ACTA.[60] First, although the negotiating countries constitute the vast majority of the world's intellectual property rights, they are a small group of countries: Australia, Canada, the EU, Japan, the Republic of Korea, Mexico, Morocco, New Zealand, Singapore, Switzerland and the USA. Second, the Agreement was negotiated in secrecy until towards the end.[61] In general, discussions of the law concerning intellectual property rights should be held in an open and transparent manner because of the need to balance competing interests such as consumer protection, business competition, privacy and freedom of expression. Third, there are provisions that pin liability for copyright violations on intermediaries such as Internet service providers (ISPs).[62]

At the time of writing at the end-September 2011, even some countries that had been involved in the negotiations were not ratifying the agreement.[63]

56 See Wikipedia, "Cybersquatting", http://en.wikipedia.org/wiki/Cybersquatting for more details.

57 See Wikipedia, "Reverse Domain Hijacking", http://en.wikipedia.org/wiki/Reverse_domain_hijacking for more details.

58 WIPO, "Cybersquatting Hits Record Level, WIPO Center Rolls out New Services", 31 March 2011, http://www.wipo.int/pressroom/en/articles/2011/article_0010.html.

59 Peng Hwa Ang, *Ordering Chaos* (see footnote 1).

60 Axel Metzger and Rita Matulionyte, "Opinion of European Academics On Anti-Counterfeiting Trade Agreement", February 2011, http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_11021 1_DH2.pdf.

61 European Parliament, "Resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations", http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0058+0+DOC+XML+V0//EN.

62 See Wikipedia, "Anti-counterfeiting Trade Agreement", http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement for more detail.

63 Intellectual Property Watch, "Still A Long Way To Go For Anti-Counterfeiting Trade Agreement", 8 September 2011, http://www.ip-watch.org/weblog/2011/09/08/still-a-long-way-to-go-for-anti-counterfeiting-trade-agreement/.

Questions To Think About

1. Should domain names be treated as trademarks? Why or why not?

2. How would you balance the interests of your country and those of copyright holders, who may be from a more developed country?

5.5 Privacy

As observed earlier, privacy rules are here to stay. The question is: Which model should be used to regulate privacy? There are essentially two models with vastly different paradigms. In the EU model, privacy is a human right. It cannot be bought, sold or traded away and it deserves comprehensive legislation. In the US model, privacy is a legal right that can be contracted away. For example, in exchange for one's e-mail address, one may be able to read some documents or have some service done. Legislation is not comprehensive but fragmented across industry.

On the Internet, both paradigms are very similar in implementation and outcome. Of course the European model has more sanctions, which does add to costs.

Which mode a country chooses will be most influenced by its culture and history. The European model, however, has the potential to be adopted globally if the Data Protection Directive is enforced.

Posing an increasing concern is the ease in which data that are collected online are retained, sometimes indefinitely. The search engine, Google, for example, has kept all its research results from the day that it started. Social network sites too sometimes make it difficult for users to remove content. The classic example is of social network site users who lose their jobs after an embarrassing photo of them appeared on a site. The special concern with social network sites is that the information can be tracked to the individual. Data protection laws can limit data collection and retention to an extent through purpose limitation clauses. It has been suggested that there should be an expiration date on information uploaded to the Internet.[64]

Questions To Think About

1. In your country, to what extent is privacy recognized as a legitimate user demand?

2. Is your country likely to follow the EU model or the US model of privacy regulation? Why do you think so?

64 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton, Princeton University Press, 2009).

Conclusion

The process of regulation should be transparent, multi-stakeholder and democratic. That is, the process should be consultative, involving all of the stakeholders. Regulation should explore all four modes of regulation—market, social norms, architecture and government regulation (including self-regulation because to be effective, self-regulation requires delegated power from the government).

Test Yourself

1. What is the relevance of competition policy to Internet access?
2. To what extent can censorship on the Internet be tolerated or allowed, if at all?
3. Can an Internet user defame someone else online and get away with it?
4. Should defamation law be modified to adapt to the Internet?
5. What are the major contentious issues regarding copyright and other intellectual property rights on the Internet?
6. What are the two approaches to privacy and data protection and how are they different?

6. DEVELOPMENT DIMENSION: THE DIGITAL DIVIDE

This section describes how the Internet can be used for social and economic development, as well as the limits of ICTD.

National development was one of the motivations for the WSIS, which eventually led to the debate on Internet Governance. However, development is a large issue that will take many decades to address. The hope for ICTs, including the Internet, is that they will help accelerate the development process.

6.1 ICT for Development

To be effective, ICTD must encompass the following: (1) Governance and Empowerment, (2) Infrastructure, (3) Economic Development, and (4) Social Development. Without proper governance, funds could be squandered away. Without empowerment, users do not feel they can change their situation. Without infrastructure such as electricity or a telecommunications line, it would be impossible for the Internet to be sustainable.

The WSIS has helped to establish the Digital Solidarity Fund. The MDGs are a good guide to how the Fund should be spent. The MDGs are:

1. Eradicate extreme poverty and hunger
2. Achieve universal primary education
3. Promote gender equality and empower women
4. Reduce child mortality
5. Improve maternal health
6. Combat HIV/AIDS, malaria and other diseases
7. Ensure environmental sustainability
8. Develop a Global Partnership for Development

Module 1 of the *APCICT Academy of ICT Essentials for Government Leaders* module series discusses the link between ICTs and the MDGs.

Internet for the Village

As a powerful and modern technology, the Internet has the potential to widen income inequalities between those who use it and those who do not. One of the most dramatic illustrations of the disparity may be found in India. There, the latest in modern technology may be found—in the large cities. But in the rural areas of India are places that the Indians call “media dark”—where television is not available.

To spread the use of the Internet and address some social ills, the Indian government in 2007 rolled out a national e-governance project called the Common Services Centre (CSC) Scheme in which 600,000 villages in India will share 100,000 centres. In essence, these are Internet kiosks.

Previously, deployment of Internet kiosks did not have a high rate of success. In fact, the first wave of such kiosks had a success rate of only 3 per cent, with success in this case being measured by sustainability after a year. Learning from the experience of the first wave, the second wave had a success rate of 30 per cent. That is a tenfold increase but it still meant a 70 per cent failure rate. The CSC Scheme would be the third wave. It would be rolled out based on the latest research of what applications would be useful for the villagers as well as transformative of their lives.

For example, the Indian government will allow access to land titles because in the villages corrupt officials sometimes cheat the villagers of their land. CD-burning and digital-photo printing have also been found to be revenue generators. In Chennai, a private initiative has found that putting examination papers online is transformative: The villagers have a low pass rate for major exams. But when they practise with the examination papers available online, their pass rate jumps. The confidence that comes with passing the exam is empowering.

The CSC Scheme is an imaginative idea. Besides using the Internet to solve social problems (such as illegal land grabbing) and narrowing the digital divide, it is also aimed at providing some employment. The operators of the Internet kiosks in the villages are to be private sector entrepreneurs. In theory, this means that the cost to the national government will be low, while state governments are expected to contribute in cash or kind and the involvement of the private sector would augment the financial outlay.

The Scheme is being rolled out. As of 30th September 2011, a total of 96,733 CSCs have been rolled out in 33 States.[65] This means the target of 100,000 CSCs by June 2011 had not been met. The Department of Information Technology, which oversees the project, has put out a booklet of some success stories of village level entrepreneurs earning a reasonable to good income of between INR 5,000 (USD 100) and INR 25,000 (USD 500) per centre.

For more information see Department of Information Technology “Common Service Center Scheme”, Government of India, http://www.csc-india.org.

6.2 Limits and Barriers

At this stage, it should be borne in mind that there are limits to the utility of ICTD. For example, using ICTD assumes that “better information equals better decisions”, which may not necessarily be the case. Also, many ICT applications are a means for providing or processing information, not a means of communication when communication often yields much more robust results for development. There are also obstacles beyond the control of any one person. Language may be a barrier. Corruption is also a barrier.

Cost is still a major consideration. However, the costs may be reduced. First, there is the increasing availability of cheaper hardware. Second, there is the availability of software under the free and open source software (FOSS) movement. It should be noted that FOSS applications may not be cheap because they require maintenance and sometimes some other parts of a software programme needed to connect to, say, a printer, may not be available and would need to be specially written.

65 Department of Information Technology, “Common Services Centers”, http://www.mit.gov.in/content/common-services-centers, last updated on 10 October 2011.

6.3 Applications of ICTD

There are many well-known and well-tested applications of ICTD. As previously pointed out, most of them are in the form of information delivery. Such applications may be found in agriculture, education, health services and tourism. Often it is true that better information in these sectors leads to a better outcome. For example, knowing what to plant when would be helpful for farmers.

Beyond information, communication would be even more helpful. For example, after planting it would be helpful to know how to combat the pests that have attacked the plants. It is in making possible better communication that ICTD holds much promise.

Particularly promising is the development and promotion of e-government services. Examples of e-government services include visa applications, taxes, land titles, driving licences and even simply the availability of application forms online. To get started, the government offices have to be computerized. The outcome of computerization is an increase in the efficiency of government. For example, putting government tenders online has been shown to save money. With computerization the process becomes more transparent, which reduces corruption. Computerization also builds an IT economy, making an IT career for technicians and software programmers possible. Computerization coupled with use of the Internet makes it possible for greater consultation of citizens on significant public issues. This in turn will result in greater empowerment of the citizens, which is a start in the virtuous cycle of development. (Module 3 in the *APCICT Academy of ICT Essentials for Government Leaders* module series discusses e-Government Applications.)

The greater transparency afforded by e-government services has often been said to lead to greater democracy. This is not necessarily the case. In fact, e-government services make it possible for more control by the central government. It makes it easier for a central government to know what is going on at the delivery end of the service. But to that extent, it makes for more responsive government service at the local level and thereby reduces corruption.[66]

Conclusion

Development was one of the motivations for the WSIS, which led to the formation of the WGIG. But development was not given sufficient attention in the WGIG Final Report and it is often overlooked in the Internet Governance debate. The international community can of course do much by way of funding ICTD projects. A public-private partnership (PPP) is the more sustainable mode as it shares funding costs while structurally making projects more likely to succeed. (The use of PPP for funding ICTD projects is discussed in Module 8 of the *Academy of ICT Essentials for Government Leaders* module series.) But there is much that national governments can and should do to use ICTD. The cost of access needs to be lower. For example, the cost of registering a domain name could be lowered. Then there needs to be the political will to foster a legal environment that is friendly to ICTD. The use of ICTD, particularly as a tool for communication, has never been more promising.

66 R. Kluver, “The Architecture of Control: A Chinese Strategy for e-Governance”, in “The Internet and Governance: The Global Context”, *The Journal of Public Policy*, vol. 25, No. 1 (2005), pp. 75-97.

Test Yourself

1. How might the Internet be used to help achieve development goals?

2. What are some limitations and barriers to the use of the Internet in achieving development goals?

7.0 INTERNET GOVERNANCE: LOOKING AHEAD

This section lists outstanding Internet Governance issues that the Internet Governance Forum cannot and will not resolve and that require the attention of governments.

The five-year mandate of the Internet Governance Forum ended in 2010. A lot of the planning for the Forum has gone into the plenary sessions. The benefits of having the Forum are evident. Conceptually, it was to have provided an opportunity to discuss significant issues and allow smaller countries to raise issues. In practice, it has raised awareness of Internet Governance issues and helped improve understanding of the importance of process in Internet Governance.

Much of the real action in Internet Governance had been happening in the parallel sessions where planning was decentralized to the parties proposing the sessions. Some of the dynamic coalitions in particular had been active in pursuing the interests of their respective groups. The dynamic coalitions have met with varying success. For example, the parallel session on spam had been very active in organizing meetings to resolve the issue but then appeared to have stopped.

The issues raised in the WGIG Final Report are thorny and do not lend themselves to easy resolution. For example, the political issue of international oversight of ICANN and the DNS has been papered over. The US Government can claim “victory” in the sense that ICANN is still in its hands. In the background are rumbles that even though ccTLDs are in the hands of national governments, there is nothing to physically stop the US Government from unilaterally cutting off a government from control of its ccTLD. There are practical restraints but no physical restraints, which means that the possibility still exists, albeit remote, of a country being cut off from the Internet.

The other significant clusters—on use of the Internet, issues related to the Internet but with wider impact, and development aspects of the Internet—do not lend themselves to easy resolution. What the Internet Governance Forum can do is to help highlight the best practices to resolve them. Building capacity for Internet Governance will therefore also be an ongoing issue that all governments need to address.

The debate that led to the WGIG Final Report has raised awareness of the significance of Internet Governance issues. As the issues will take time to resolve, governments have to build their capacity to address the issues and participate in the international debate about them. Such capacity-building is necessary because Internet Governance is not just an international affair. Many of the issues in Internet Governance are local, with ICTD being the most significant for local government. For that reason, local and national governments have a key role to play in Internet Governance.

SUMMARY

This module on Internet Governance discusses the following:

Internet Governance is more about governance than the Internet. It covers some political issues concerning international policy regarding the Internet, the use and abuse of the Internet, as well as the deployment of the Internet to help achieve social and economic development.

Contrary to common misperception, the Internet does have a central control point in an area called the root zone system. This root zone system is under the control of a US Government-backed entity called ICANN.

The WGIG was established by the United Nations to resolve the tension around the political dimension of Internet Governance. In the horse-trading after the WGIG report, it was accepted that a lightweight Internet Governance Forum would be held but that the root zone system would still be in the hands of ICANN with the proviso that only national governments can control and run their respective ccTLDs.

Internet Governance should be multilateral and multisectoral. That is, no one country or entity should have the decisive say on governing the Internet. Instead, the process, whether at the national or international level, should be democratic. At the international level, participation in Internet Governance must be extended to all countries; at all levels, governance must be extended to the private and civil society sectors.

As with life in the offline world, the Internet may be regulated through four modes: law, social norms, market mechanisms and architecture. Because enforcement of the law is not always viable on the Internet, governments have to be creative in approaching Internet regulation.

Self-regulation is a form of delegated government regulation. It is often recommended as a preferred form of regulation of the Internet but there are limitations and costs to its applicability.

A road map for regulating the Internet to encourage its diffusion while containing harm was proposed.

The Internet has given new life to some old criminal conduct and also created some new offences. One of the difficulties in enforcement is the definition of a crime.

Two areas where there is practically universal agreement are child pornography and consumer fraud. Enforcement agencies do cooperate to prosecute these offences.

Spam, scams, malicious code and phishing are generally accepted to be offensive but not all countries have laws against them.

There is even greater disparity in regulations and actions against cyberbullying, cyberstalking, identity theft and Internet addiction.

The Internet Governance Forum has sparked the creation of “dynamic alliances” where groups interested in addressing a particular problem can meet to discuss best practices and common actions.

Just as regulations have to be creative, sanctions on the Internet also have to be creative.

In the end, international cooperation is essential to defeat criminal conduct on the Internet.

Internet Governance issues do spill over to the offline world. Examples include competition policy, censorship and freedom of expression, defamation, copyright and intellectual property rights, and privacy.

One of the motivations for the study of Internet Governance was the concern that developing countries would be left behind in the information economy. So the use of ICTD is an important part of Internet Governance.

There are limitations and barriers to the use of ICTD.

There are also success stories that can be replicated.

ICTD can help improve real world governance by improving transparency, for example.

The political tension in Internet Governance has not been resolved, and building capacity for Internet Governance remains an ongoing issue that all governments need to address.

ANNEX

Further Reading

Ang, Peng Hwa. *Ordering Chaos: Regulating the Internet*. Singapore: Thomson, 2005.

Butt, Danny, ed. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP, 2005. Available from http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

Cukier, Kenneth Neil. Who Will Control the Internet? *Foreign Affairs,* (November/December 2005). Available from http://www.foreignaffairs.org/20051101fa comment8460 2/kenneth-neil-cukier/who-will-control-the-internet.html.

Drissel, David. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs,* vol. 19, No.1, (March 2006), pp. 105-120.

Kapur, Akash. *Internet Governance: A Primer*. Bangkok: UNDP-APDIP, 2005. Available from http://www.apdip.net/publications/iespprimers/eprimer-igov.pdf.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance*. Available from http://www.wgig.org.

Wu, Tim, and others. On the Future of Internet Governance. *American Society of International Law Proceedings of the Annual Meeting*, vol. 101. Available from http://ssrn.com/abstract=992805.

Glossary

IP Address	Internet Protocol address: a unique identifier corresponding to each computer or device on an IP network. Currently there are two types of IP addresses in active use. IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 (which uses 32 bit numbers) has been used since 1983 and is still the most commonly used version. Deployment of the IPv6 protocol began in 1999. IPv6 addresses are 128-bit numbers.
Registrar	A body approved ("accredited") by a registry to sell/register domain names on its behalf.
Registry	A company or organization that maintains a centralized registry database for the TLDs or for IP address blocks (e.g. the RIRs, see below). Some registries operate without registrars at all and some operate with registrars but also allow direct registrations via the registry.
RIRs	Regional Internet registries. These not-for-profit organizations are responsible for distributing IP addresses on a regional level to Internet service providers and local registries.
Root servers	Servers that contain pointers to the authoritative name servers for all TLDs. In addition to the "original" 13 root servers carrying the Internet Assigned Numbers Authority-managed root zone file, there are now large number of Anycast servers that provide identical information and which have been deployed worldwide by some of the original 12 operators.
Root zone file	Master file containing pointers to name servers for all TLDs.
WHOIS	A transaction oriented query/response protocol that is widely used to provide information services to Internet users. While originally used by most (but not all) TLD Registry operators to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services, including RIR WHOIS look-ups for IP address allocation information.

As noted in the section entitled “About The Module Series”, this module and others in the series are designed to have value for different sets of audiences and in varied and changing national conditions. The modules are also designed to be presented, in whole or in part, in different modes, on- and off-line. The module may be studied by individuals and by groups in training institutions as well as within government offices. The background of the participants as well as the duration of the training sessions will determine the extent of detail in the presentation of content.

These “Notes” offer trainers some ideas and suggestions for presenting the module content more effectively. Further guidance on training approaches and strategies is provided in a handbook on instructional design developed as a companion material for the *Academy of ICT Essentials for Government Leaders* module series. The handbook is available at: http://www.unapcict.org/academy.

Using the Module

Each section of the present module begins with a statement of learning objectives and ends with a set of “Test Yourself” questions. Readers may use the objectives and questions as a basis for assessing their progress through the module. Each section also contains discussion questions and practical exercises that may be accomplished by individual readers or used by trainers. These questions and exercises are designed to enable readers to draw on their own experience to benchmark the content and to think reflectively on the issues presented.

Case studies are an important part of the module content. These are intended for discussion and analysis, particularly in terms of the extent to which the key concepts and principles presented in the module work in real-world cases. In the case of Internet Governance, the issues are at once international and national or local. A lot of the work is at the local and national levels, particularly in the use of ICT, including the Internet, for development. Trainers may encourage participants to cite other cases and examples from their own experience to substantiate the module discussion.

Structuring the Sessions

Depending on the audience, time available and local settings and conditions, the content of the module can be presented in different structured time capsules. There may be senior government officials who need to be given some updates and information about Internet Governance. The training programme should therefore have sessions as brief as an hour or two. The full training programme takes a minimum of 1.5 days. The module has been designed with the first three sections heavy on background and theory, and the remaining sections on applications.

For a one- to two-hour session

Condense sections 1 and 2, focusing on the issues and the outcomes reached at the WSIS and WGIG. Include ICTD from section 6.

For a three-hour session

Condense sections 1 and 2 as above. Depending on the attendees, combine sections 3, 4, 5 and 6 with a view to either:

Developing a legal framework, in which case stress sections 4 and 5; or
Using ICTD, in which case stress sections 5 and 6.

For a full day session (six hours)

Cover sections 1, 2 and 3 in the morning. In the afternoon, discuss sections 4, 5 and 6 using exercises and questions for discussion. This is to keep the energy level high after lunch. Wrap up with section 7.

For a 1.5-day session

Although there are seven sections, they are of varying length. You should be sensitive to the aims of the group and what they hope to get out of the training. Sections 1 and 2 are heavy on background. If the group is not interested in that but in the outcome, then focus on the outcome. In general, it is more likely that the participants will want more practical skills. The discussions and sharing of information should prove useful in reinforcing the training.

For a three-day session

Discuss sections 1 and 2 on Day 1. Depending on how the group responds, it may be possible to go into section 3. On Day 2, cover sections 3, 4 and 5. On Day 3, discuss sections 6 and 7. Pacing is important. Participants should be encouraged to bring their own experience to the classroom to share. In particular, participants should be encouraged to use section 6 to address the digital divide issue in their respective countries. Section 7 provides an opportunity to wrap up the entire session.

About the Author

Ang Peng Hwa is Professor and Director of the Singapore Internet Research Centre at the Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore. Also a lawyer by training, he teaches media law and policy. His research is in the area of Internet Governance. His 2005 book, *Ordering Chaos: Regulating the Internet*, argues that the Internet can be, is being and should be regulated.

In 2004, he was appointed by the United Nations Secretary-General to the Working Group on Internet Governance to prepare the report for the 2005 meeting of the World Summit on the Information Society. He later helped co-found the Global Internet Governance Academic Network where he served as inaugural chair. He currently serves as chairman of the Asian Media Information and Communication Centre.

UN-APCICT/ESCAP

The United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT/ESCAP) is a subsidiary body of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). UN-APCICT/ESCAP aims to strengthen the efforts of the member countries of ESCAP to use ICT in their socio-economic development through human and institutional capacity-building. UN-APCICT/ESCAP's work is focused on three pillars:

1. Training. To enhance the ICT knowledge and skills of policymakers and ICT professionals, and strengthen the capacity of ICT trainers and ICT training institutions;
2. Research. To undertake analytical studies related to human resource development in ICT; and
3. Advisory. To provide advisory services on human resource development programmes to ESCAP member and associate members.

UN-APCICT/ESCAP is located at Incheon, Republic of Korea.

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 nine 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

The Academy of ICT Essentials for Government Leaders

http://www.unapcict.org/academy

The *Academy* is a comprehensive ICT for development training curriculum with currently ten modules that aims to equip policymakers with the essential knowledge and skills to fully leverage opportunities presented by ICTs to achieve national development goals and bridge the digital divide. Below are the short descriptions of the ten modules of the *Academy*.

Module 1 - The Linkage between ICT Applications and Meaningful Development

Highlights key issues and decision points, from policy to implementation, in the use of ICTs for achieving the MDGs.

Module 2 - ICT for Development Policy, Process and Governance

Focuses on ICTD policymaking and governance, and provides critical information about aspects of national policies, strategies and frameworks that promote ICTD.

Module 3 - e-Government Applications

Examines e-government concepts, principles and types of applications. It also discusses how an e-government system is built and identifies design considerations.

Module 4 - ICT Trends for Government Leaders

Provides insights into current trends in ICT and its future directions. It also looks at key technical and policy considerations when making decisions for ICTD.

Module 5 - Internet Governance

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

Module 6 - Information Security and Privacy

Presents information on security issues and trends, and the process of formulating an information security strategy.

Module 7 - ICT Project Management in Theory and Practice

Introduces project management concepts that are relevant to ICTD projects, including the methods, processes and project management disciplines commonly used.

Module 8 - Options for Funding ICT for Development

Explores funding options for ICTD and e-government projects. Public-private partnerships are highlighted as a particularly useful funding option in developing countries.

Module 9 - ICT for Disaster Risk Management

Provides an overview of disaster risk management and its information needs while identifying the technology available to reduce disaster risks and respond to disasters.

Module 10 - ICT, Climate Change and Green Growth

Presents the role that ICTs play in observing and monitoring the environment, sharing information, mobilizing action, promoting environmental sustainability and abating climate change.

These modules are being customized with local case studies by national *Academy* partners to ensure that the modules are relevant and meet the needs of policymakers in different countries. The modules are also been translated into different languages. To ensure that the programme stays relevant and addresses emerging trends in the ICTD, APCICT regularly revises the modules and develops new modules.

APCICT Virtual Academy (http://e-learning.unapcict.org)

The APCICT Virtual Academy is part of the multi-channel delivery mechanism that APCICT employs in the implementation of its flagship ICTD capacity building programme, the *Academy of ICT Essentials for Government Leaders*.

The APCICT Virtual Academy allows learners to access online courses designed to enhance their knowledge in a number of key areas of ICTD including utilizing the potential of ICTs for reaching out to remote communities, increasing access to information, improving delivery of services, promoting lifelong learning, and ultimately, bridging the digital divide and achieving the MDGs.

All APCICT Virtual Academy courses are characterized by easy-to-follow virtual lectures and quizzes, and users are rewarded with APCICT's certificate of participation upon successful completion of the courses. All *Academy* modules in English and localized versions in Bahasa and Russian are available via the Internet. In addition, plans for more content development and further localization are underway.

e-Collaborative Hub (http://www.unapcict.org/ecohub)

The e-Collaborative Hub (e-Co Hub) is APCICT's dedicated online platform for knowledge sharing on ICTD. It aims to enhance the learning and training experience by providing easy access to relevant resources, and by making available an interactive space for sharing best practices and lessons on ICTD. e-Co Hub provides:

- A resources portal and knowledge sharing network for ICTD
- Easy access to resources by module
- Opportunities to engage in online discussions and become part of the e-Co Hub's online community of practice that serves to share and expand the knowledge base of community of practice that serves to share and expand the knowledge base of ICTD