



# Internet Governance

*Asia-Pacific Perspectives*

Edited by **Danny Butt**  
Foreword by **Nitin Desai**

# Internet Governance

*Asia-Pacific Perspectives*

*Edited by* **Danny Butt**  
*Foreword by* **Nitin Desai**



Asia-Pacific Development  
Information Programme



ELSEVIER  
*A division of*  
Reed Elsevier India Private Limited



# APDIP

The Asia-Pacific Development Information Programme (APDIP) is an initiative of the United Nations Development Programme (UNDP) that aims to promote the development and application of new Information and Communication Technologies (ICTs) for poverty alleviation and sustainable human development in the Asia-Pacific region.

## UNDP ASIA-PACIFIC DEVELOPMENT INFORMATION PROGRAMME

Regional Centre in Bangkok  
3rd Floor, United Nations Service Building  
Rajdamnern Nok Avenue, Bangkok 10200, Thailand  
Tel: +66 2 288 1234; 288 2129  
Fax: +66 2 280 0556  
E-mail: [info@apdip.net](mailto:info@apdip.net)  
Website: [www.apdip.net](http://www.apdip.net)

All UNDP-APDIP documents on Internet Governance are available at: <http://igov.apdip.net>.

The analysis and recommendations of this publication do not necessarily reflect the views of the United Nations Development Programme nor do they necessarily reflect the views of the institutions with which the authors are affiliated.



ELSEVIER

17A/1, Lajpat Nagar IV,  
New Delhi-110 024  
Tel: +91 11 2644 7160  
Fax: +91 11 2644 7156  
Website: [www.asiaelsevier.com](http://www.asiaelsevier.com)

ISBN-13: 978-81-312-0110-7  
ISBN-10: 81-312-0110-4

Academic Press, Butterworth-Heinemann, Digital Press, Elsevier, Focal Press, Morgan Kaufmann, North Holland, Pergamon are the Science and Technology Imprints of Elsevier.

© UNDP-APDIP 2005

Printed and bound in India

# Table of Content

## Foreword

The Working Group on Internet Governance <i>Nitin Desai</i>	v
--	---

## Abbreviations

x

## Introduction

The Open Regional Dialogue on Internet Governance <i>Danny Butt</i>	1
--	---

## PART I: PERSPECTIVES ON GOVERNANCE 7

### Chapter 1

The Legacy of the Working Group on Internet Governance <i>Peng Hwa Ang</i>	9
---	---

### Chapter 2

Strengthening the Voice and Participation of Developing Countries in Internet Policy-making <i>Mohamed Sharil Tarmizi</i>	19
---	----

## PART II: INTERNET GOVERNANCE ISSUES 35

### Chapter 3

Internet Governance in the Asia-Pacific Region <i>UNDP-APDIP</i>	37
---	----

### Chapter 4

Internet Governance and Socio-cultural Inclusion <i>Danny Butt and Norbert Klein</i>	66
---	----

### Chapter 5

Governing Internet Use: Spam, Cybercrime and e-Commerce <i>Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell</i>	89
--	----

### Chapter 6

Development and the Regulation of Access Technologies: Wireless and VoIP <i>Fuatai Purcell, Samudra Haque and Onno Purbo</i>	105
---	-----

## PART III: INTERNET GOVERNANCE – COUNTRY REPORTS FROM THE REGION 113

### Chapter 7

Country Reports: China, Indonesia, India, Pakistan and Thailand	115
Internet Policy Priorities in China	120
Internet Policy Priorities in India	123
Internet Policy Priorities in Indonesia	126
Internet Policy Priorities in Pakistan	129
Internet Policy Priorities in Thailand	132

Contributors	136
--------------	-----

Acknowledgements	139
------------------	-----

## Governing Internet Use: Spam, Cybercrime and e-Commerce

—*Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell*

Developmental approaches to the Internet are often focussed on getting people connected to the Internet and providing them with tools to send text and audiovisual content across it. This is usually the extent to which we understand that there is a “digital divide”. However, from a governance perspective, the physical connections are in some ways the easiest to address. It is when use of the Internet grows that its nature as a relatively unified global platform creates a whole series of new challenges for public policy that lay outside of the easy control of nation-states. As WGIG noted, the coordination required due to the global nature of the Internet is not well defined, but may require “international legal frameworks, coordination mechanisms or cooperation structures to promote effective and consistent handling of these issues”.<sup>93</sup> This chapter explores three related dimensions of global Internet use and the challenges raised by them: spam, security and e-commerce.

The Internet is used for many activities that were not envisaged by the designers of the key technical protocols for information transfer that underpin it. In some cases, such as spam, the lack of easy-to-use authentication mechanisms can be attributed to the large installed base of mail servers – any new solution would have to maintain some level of interoperability with existing protocols. For other issues, such as e-commerce, many of the issues relate less to technology and more to the increase in cross-border transactions that the Internet facilitates, sometimes with little regard for policy attempts to regulate markets.

And in general, the “disembodied” nature of e-commerce and email – where there is no clarity about which physical location or human initiates an electronic communication – combines with the scale of digital communication to raise difficult security issues. If a user in Samoa interacts with a server in China to transact with an Australian company, it may be difficult for legal authorities to track the people whose behaviour they must regulate. Despite these difficulties, Internet use continues to grow in the region and addressing the issues of Internet use remains central to increasing participation in the Information Society, so the need to address these issues is crucial.

---

<sup>93</sup> WGIG Background Report, <http://www.wgig.org> para. 106

## e-Commerce

Some cross-border issues are most visible in e-commerce. e-Commerce is the process of exchanging products, services and information using computer networks including the Internet (Turban *et al*, 2002), as well as automated business processes, automated services and online buying and selling. Many studies were conducted since then and research found that e-commerce can benefit organizations of all sizes, and is particularly important for the small business sector (Bright, 1997; Rommel, 1997; Huff & Yoong, 2000). Despite this high potential, SMEs in many developing countries are still reluctant to infuse e-commerce into their business processes. New technologies provide tremendous potential for SMEs, especially the suppliers of cultural goods (e.g., handicrafts,) and services in the in the Pacific Small Island Developing States (SIDS) (UN 2005) to access global markets. However, there is need for greater access to computers and the Internet – especially low-cost broadband – and for the creation of the enabling legal framework to facilitate e-commerce.

While numerous studies have explored the issues of e-commerce adoption by SMEs, nearly all such studies have been conducted in developed and highly populated developing countries. One of the functions of WSIS is to address more specifically the situation of Pacific Small Island Developing States (SIDS) in relation to Information Society issues.

Table 6 below summarizes the findings of research undertaken by Fuatai Purcell on the key challenges and barriers to e-commerce adoption by SMEs in Samoa.

**Table 6 : Summary of the issues that impact e-commerce adoption by SMEs in Samoa**

Existing e-commerce activities and opportunities		Reported challenges and barriers to adoption	
Activities	Opportunities	Challenges	Barriers
Email	Allows SMEs with possibilities not previously available e.g. online selling	Lack of awareness of the perceived benefits of e-commerce	Poor telecommunication infrastructure
Search for information	Cheaper and faster method of communication	High costs of computer hardware and Internet costs	Monopoly
Can order online but payment is done manually by vendor going to the bank to check credit card details, etc.	Empowerment through increased knowledge and skills	Lack of skills of SMEs to use computers and the Internet	Affordability
Only 5% of SMEs have Internet access	SMEs will significantly contribute to the economy	SMEs owners are also managers	Lack of an enabling environment
Only 5% of SMEs with Internet access have a website	Added value to existing products and services	Most tourist operators in rural villages have limited knowledge of the English language	Lack of initiatives to enable capacity building
Most SMEs with websites are in the tourism sector	Government deregulation strategy increases the number of SMEs	Lack of skills to upgrade websites i.e. changing photos of products, etc.	Cheaper alternatives e.g. open source software systems
Most SMEs with websites are owned by foreigners	Better ways of managing customers relationships		Trust and security of cyberspace

The Samoan situation brings to light a number of difficulties faced by SMEs that are not reducible to regulatory or financial issues. Purcell's research suggested that there were no fully integrated e-commerce systems used by SMEs in Samoa. A fully integrated e-commerce is where the selling and buying of goods and services are all conducted online. When SMEs and ISPs participating in this study were asked how payments were made when customers ordered their goods or services online, they explained that:

- For local customers, they (SMEs) receive orders through email, then they deliver the orders and collect the cash.
- For overseas customers, there are two forms of payments:
  - Customers email their credit card details, then SMEs verify the details with the bank, or
  - SMEs email the customers their bank account details, after which the customer makes the payment and faxes or emails the payment confirmation.

Greenturtle Holidays, for example, is an SME that uses the first type of payment (above) for overseas customers. The following paragraph appears at the bottom of the booking form:

"Once your itinerary is prepared from the above information, one of our reservations staff will email you our quotation. On your approval of itinerary and quotation, we will request a 50 percent deposit for your confirmed reservations. Just email us your credit card details (we advise you to break up the numbers in two separate emails for security reasons) and we will process this deposit and will confirm all your bookings with you by email. The balance of your payment is due one month prior to your arrival in Samoa"<sup>94</sup>

### Transaction systems and credit cards

Almost all business-to-consumer (B2C) e-commerce systems require use of a major credit card, but this brings a number of issues for a variety of Asia-Pacific countries. Firstly, credit cards may not be available in countries like Iran due to trade embargos. The dominant credit card companies are located in the United States, and therefore they cannot legally do business in Iran. Secondly, due to credit card fraud, many businesses increasingly exclude purchases made by credit cards with billing addresses in countries like Indonesia, which have had a high level of credit card fraud. Finally, and most important, in the Pacific, developing country SMEs are unlikely to have freehold title or other tradable assets that can be used for security for trading banks. Most of the lands they own are customary land which cannot be transferred for cash – altering this situation would have significant cultural and economic effects, with a significant risk of increasing inequality over the long term.

Branches of overseas-owned banks also cannot process credit card applications in Samoa because there is no central credit risk management in place. This means that if a person applies for a credit card, the bank has no way of knowing if this person owes money to other banks or

---

<sup>94</sup> <http://www.greenturtleholidays.com/bookings/samoa/tanumatiu.html>

companies. It is a manual process of bank staff using the telephone to call other banks or utility companies. The issue of debt management has also been raised by the acting CEO of SamoaTel. He explained that debt management was one of the key issues they face. They disconnect as much as they connect new phones, especially in the rural villages.

Moreover, SMEs do not trust payment online. Quite often this is based on incorrect information or a lack of experience. As one SME owner explained:

“I do not like online payment by customers because what if the customer tells me that payment has been made and I have not yet received it? Do I supply the goods or not? If someone else got the money by other means, who is responsible? How would I find out who got the money? It is much easier if they make the payment to my bank account. When I check my bank account and the money is there, then I send the goods.”

### Trust and security

The question of trust brings with it questions related to security. As noted above, when so many transactions become largely automated or exist in uncertain physical locations, it can be difficult to tell who the people might be on the other end of the communication and transaction. However, this is not simply a question of providing more and better security, even if this was technically possible. As WGIG note, “the transactional certainty obtained through authenticating the parties to a transaction needs to be balanced with legitimate privacy needs and rights of users to ensure that data used in the authentication process is not used illegally or in an unauthorized fashion by third parties.”<sup>95</sup>

Part of the challenge in addressing security is in the speed of response required to match the instantaneous nature of online transactions, and the rapid spread of information about security vulnerabilities. For this reason, the first line of defence is often in information security, and is often relatively informal and loosely networked. Examples include CERTs, which are “typically made up of technical experts who are in communication with other CERTs to share knowledge and best practices and to warn of impending attacks... Because a standardized approach to information security may undermine the level of network security, security requires a holistic approach, with each participant undertaking measures appropriate to their role, understanding that there may be principal spheres of influence, and that collaboration on many levels will be required.”<sup>96</sup>

As WGIG notes, the guiding principle of security is that there can never be perfect security, but that all stakeholders must be able to find a level of security that is proportional to their level of investment and which does not create unnecessary burdens.

---

<sup>95</sup> WGIG Background Report paras 153-4.

<sup>96</sup> Ibid. para 137.

## Security: an example from Pakistan

The interlocking nature of technology and policy issues related to security are illustrated by the example of Pakistan. In 2000, Pakistan came up with a forward-looking ICT policy and made strategic interventions to dramatically increase bandwidth, reduce process and rapidly increase the ingress of ICT in the government and the private sector. Demand for the Internet spread rapidly as it started to be used for more than chat and email. Bandwidth also increased rapidly with costs dropping precipitously.

All this was happening without the requisite oversight on network capacity, stability and security. The monopoly service provider at that time (the market has since been deregulated) had one point of entry and the international bandwidth was brought in via one undersea fibre with no redundancy. The ambition of the government to deploy pornographic content blocking on the core gateway router by putting up access control lists (which turned out to be a futile exercise) added to the vulnerability. The total bandwidth coming into Pakistan was less than 250 Mbps. Finally, the total lack of any security awareness and training in the staff manning the Internet Exchange set the stage for trouble.

A childish exercise by Pakistan-based hackers to deface Indian sites was met by an equally immature response by the Indian hackers in devising the 'yaha virus'. This was originally a Denial of Service (DoS) attack on all .gov sites. This rapidly escalated to a Distributed Denial of Service (DDoS) attack in different strains of the virus. The attacks were routed via Korea, China and other countries to mask the originating sites.

This attack was accompanied by different varieties of attacks (fragmented packets, etc.) which coupled with the overloaded core router handling the pornographic access lists brought the complete network down. The attacks collapsed web servers, choked the domestic bandwidth, overloaded the router and consequently flooded the international bandwidth. These attacks continued intermittently for several months as the Pakistanis tried desperately to address the multiple threats. The national network went down for hours and days at a time.

Finally several mitigation measures were put in place: important web sites were also hosted outside Pakistan, powerful core routers, proper attack mitigation schemes and redundant networks were implemented, and there was re-training for critical staff. This episode forced Pakistan to take a long hard look at information security – not only the government but also the banking and corporate sector, and take steps to create more reliability and availability in their systems.

## Recent trends in security attacks<sup>97</sup>

With time there is an increased level of sophistication in the cyber-attacks and a downward trend in the average level of competence of the attacker, due to the spread of attack tools that can be used by malicious "script kiddies" with little sophisticated programming knowledge.

---

<sup>97</sup> Based on Information from the CERT® Coordination Center.

## Trend 1 – Automation; speed of attack tools

Automated attacks commonly involve four phases:

- scanning for potential victims,
- compromising vulnerable systems,
- propagating the attack, and
- coordinated management of attack tools distributed across many Internet systems.

This automation has allowed tools like Code Red to self-propagate to a point of global saturation in less than 18 hours.

## Trend 2 – Increasing sophistication of attack tools

Attack tool developers are using more advanced techniques than before. They use anti-forensic techniques that obfuscate the nature of attack tools. Some also become polymorphic tools that evolve to be different in each instance. Increasingly, they can execute on multiple operating system platforms, and use common protocols like HTTP to become difficult to distinguish from legitimate network traffic.

## Trend 3 – Faster discovery of vulnerabilities

The number of newly discovered vulnerabilities reported to the CERT/CC continues to more than double each year. It is difficult for administrators to keep up to date with patches. Subsequent reviews of the existing code for examples of the new vulnerability class often lead, over time, to the discovery of examples in hundreds of different software products. Intruders are often able to discover these exemplars before the vendors are able to correct them.

## Trend 4 – Increasing permeability of firewalls

Firewalls are often relied upon to provide primary protection from intruders.

However, technologies are being designed to bypass typical firewall configurations; for example, IPP (the Internet Printing Protocol) and WebDAV (Web-based Distributed Authoring and Versioning). Certain aspects of “mobile-code” (ActiveX controls, Java, and JavaScript) make it difficult for vulnerable systems to be protected and malicious software to be discovered.<sup>98</sup>

## Trend 5 – Infrastructure attacks

Infrastructure attacks are attacks that broadly affect key components of the Internet. They are of increasing concern because of the number of organizations and users on the Internet and their increasing dependence on the Internet to carry out day-to-day business. Their impact

---

<sup>98</sup> See [http://www.cert.org/reports/activeX\\_report.pdf](http://www.cert.org/reports/activeX_report.pdf)

includes DoS, compromise of sensitive information, spread of misinformation, and significant diversion of resources from other tasks.

Cross-border transactions make regulation of security issues extremely difficult. While this may, in some cases, provide opportunities for trade and commerce, it also allows for the illegal use of resources whose effects weigh most significantly on minority cultures with few financial resources. The spate of unsolicited email which is an annoyance to the worker with a broadband connection in a highly-developed city becomes an expensive and critical issue for less developed communities in a low bandwidth situation.

## Cybercrime

The above security breaches are usually criminal in nature, but they only cover a small proportion of the broad spectrum of cybercrime. The most common crimes include:

- **Hacking** – recreational hacking can lead to unauthorized modification of programs and data, or damage to intangible property; criminal hacking may be involved in fraud or espionage, or blackmail; political hacking may seek to convert websites with a public presence to unauthorized political messages. Mhacking is undertaken by company insiders.
- **Denial of Service** attacks prevent or hinder access to information on particular sites.
- **Viruses** and Trojan horses cause malicious damage to usually untargeted computers without a human directly attacking them.
- **Fraud** and scams such as ‘phishing’, where a website masquerades as another.
- **Pornography**, especially child pornography.
- **Hate sites** or those that seek to encourage violence against other groups.
- **Intellectual Property** violations such as piracy.
- **Cyber-stalking** where email or instant messaging is used to harass or threaten an individual (particularly women).

These crimes range from the extremely serious through to the relatively victimless, and different nations and cultures have different interpretations as to which of these are criminal. Some activities may raise conflicts between different national systems (e.g., IPR). Existing laws and arrangements are not enough to address the challenges posed by these crimes and criminals, and new laws are required to be framed in every jurisdiction. However, if we only focus on national legislations, then we face the problem that the very idea of jurisdiction based on geographic boundaries is difficult to apply to the Internet which does not easily recognize geographical distinctions. The WGIG Background Report noted that “to avoid the creation of ‘cybercrime havens’, it will be necessary to ensure that criminalization of specific conduct committed in cyberspace, should be put in place on a global level, while respecting the diversity of cultures and legal systems”.<sup>99</sup> In practice, this will be quite difficult.

Security issues such as cybercrime ranked as the highest concern among respondents to the ORDIG survey on Internet governance priorities for the Asia-Pacific. While the scale of the

---

<sup>99</sup> WGIG Background Report, para 137.

problem is severe, caution should be used with respect to legislation to address the issue, and its side-effects on freedom of speech and cultural diversity should also be considered.

For example, according to Wong, Malaysia's Computer Crimes Act allows that "any police officer arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against this Act. Further to this, the Act also allows police officers above the rank of Inspector to conduct search[es] at premises without warrant, should the officer believe that delays may effect them obtain[ing] necessary evidence."<sup>100</sup> While, as Wong points out, the legislation's broadness also introduces many opportunities for errors in procedure, preventing successful prosecution, there are also grave human rights consequences to such significant changes to due process being implemented under legislation brought about for the laudable purposes of curbing a new threat. Analogies can be drawn to the United States' Digital Millennium Copyright Act, which used technical change as a justification for the imposition of new legislation that conflicts with free speech principles and consumer rights such as fair use, and has drawn ire from civil society groups supportive of cultural diversity.<sup>101</sup>

International cybercrime conventions also pose dangers in its globalization of particular definitions of crime, neglecting that each country has a legal system which is in some ways culturally specific. It is important that governments using model legislation and critically assess its relevance for their own needs. Civil society has a strong role to play in this process of signalling the limitations of Internet policies from a cultural and social perspective.

## Spam

It is an accepted fact that spam is a problem around the world, and it is the area of cybercrime that affects most people using the Internet every day. It is a problem that makes itself felt even more strongly in economies that are comparatively new to the Internet, such as several economies throughout the Asia-Pacific region, where the rapidly developing Internet infrastructure has not been accompanied by a corresponding development of policy and governance systems at an ISP and government level. Further, user awareness tends to lag far behind the norm in more developed economies, thus making users far more vulnerable when exposed to the seamier side of the Internet – scams, identity thefts, viruses – and spam.

ISPs and email providers in large parts of the Asia-Pacific region often find their meagre resources stretched to the limit dealing with high levels of spam, with little or no budget available to invest in new resources just to deal with the ever-increasing levels of spam. There is always the danger that when a new virus is released "in the wild" and begins to propagate, traffic spikes may overload their mail server infrastructure, causing it to slow down or even completely stop functioning.

Representatives cutting across government and industry from around the Asia-Pacific region have strongly expressed their views on the threat that the Internet economy in their countries

---

<sup>100</sup> Wong, C. Y. 2002. *Malaysian Law and Computer Crime*, Sans Institute, 4 April 2005, <<http://www.securitydocs.com/library/1268>>.

<sup>101</sup> Electronic Frontier Foundation. 2003. *Unintended Consequences: Five Years under the DMCA*, Electronic Frontier Foundation, [http://www.eff.org/IP/DMCA/unintended\\_consequences.php](http://www.eff.org/IP/DMCA/unintended_consequences.php). Accessed 3 April 2005.

faces from spam at international forums such as the WSIS Thematic Meeting on Spam, and the WGIG. Based on the ORDIG survey, there appears to be a near-unanimous consensus that spam and viruses are serious threats, and that countries in the Asia-Pacific region lack the resources, know-how and policies to effectively mitigate these threats. This threat is magnified by a lack of comprehensive cybercrime, anti-spam and data protection laws.

Even in highly developed economies with world class Internet infrastructure, with some of the highest levels of broadband penetration in the world, have their own dimensions to the spam problem. This has, however, led to several poorly secured personal computers, running without the latest operating system and anti-virus security updates, and without a proper firewall or other means of security – making them highly vulnerable to viruses and hackers – getting connected to the Internet on a continuous basis. Further, Internet providers in these economies may lack a comprehensive framework of policies and standard operating procedures to deal with spam issues, and soon find themselves overrun by spammers.

While this chapter can only give a brief overview of the economic, technical and social aspects of spam, we also suggest measures to mitigate the spam problem. The word “mitigate” has been carefully chosen to avoid suggesting that there exists a solution to the spam problem, any more than there is a solution to pollution and global warming. The most that can be achieved is to mitigate the effects of spam and enable various stakeholders in the spam problem to cope with it and reduce it to acceptable levels. However, coordinated approaches such as the OECD anti-spam Toolkit exist, where legislative and technical measures are backed by initiatives for international cooperation against spam, and campaigns to educate and empower users, giving them access to secure computing resources and sensitizing them on net abuse issues.

Like other security issues, spam is an international problem, and therefore requires international cooperation and communication in order to help resolve spam issues on a continuous and proactive basis. It poses unique public policy challenges because, as WGIG note, “legal, policy and regulatory frameworks at the national level are complementary with the development and implementation of technological solutions to spam: technical work can affect the context for policy decisions, [while] protecting legitimate use of email can conflict with anti-spam requirements”<sup>102</sup>.

### *Economics of spam*

Spam exploits the recipient-pays nature of email, coupled with the comparatively negligible cost of sending vast quantities of email. Almost all the costs are borne by the receiving site, and finally by the user who receives the spam in his mailbox – the costs of receiving, storing and downloading spam, and the costs of hiring administrators and buying or developing filters to block spam. These costs far outstrip the costs incurred by the spammer, whose expenses are limited, at the most basic level, to the cost of an Internet connection and software to send bulk email.

It is also much easier for senders of bulk email to achieve economies of scale, as they can ramp

---

<sup>102</sup> WGIG Background Report para 136.

up the volume of email sent out by orders of magnitude with a comparatively low corresponding expansion in their bulk emailing infrastructure. Thus, a spammer finds that nearly all the costs of his advertising campaign are unwillingly subsidized by several parties completely unrelated to him, such as the ISPs and bandwidth providers. Inevitably, the increased costs faced by ISPs to deal with spam are passed on to their users, so end-users are unintentionally paying higher costs, so that they can receive spam.

Contrast this with the sender-pays model of traditional marketing tactics like telemarketing and bulk postal mail, or media advertising where the sender bears nearly all the costs of transmission, and where receiving these communications does not normally incur any costs. In fact, newspapers and free-to-air channels are typically heavily subsidized by revenues derived from carrying advertising.

It should be noted that legitimate senders of bulk email, who maintain contact with their customers and carry out bulk marketing over email, also find that the recipient-pays nature of email works in their favour. Their costs are far lower when using bulk email than when they use traditional sender-pays methods of marketing such as bulk postal mail.

In their constant quest to remain anonymous and undetected by ISP spam filters and law enforcement, and to ramp up their rate of sending spam, several spammers now seek to gain unauthorized access to third party computing resources, such as poorly configured open relays and open proxy servers, as well as deliberately compromised hosts such as virus-infected PCs and hacked servers. These server compromises, combined with techniques such as rapidly cycling through a huge list of compromised servers, or infecting thousands of PCs around the world with viruses, create a “zombie army” or “botnet” of hijacked machines that are coordinated to send out spam, perpetrate DDoS attacks and, as a measure of self perpetuation, further swell the zombie army’s ranks by infecting and compromising even more machines.

This horizontal scaling tactic can be a nightmare for email and spam filter administrators and law enforcement officials investigating anti-spam cases, as they make spammers a rapidly moving, hard-to-detect target. Using these techniques, spammers can illegally harness virtually unlimited resources, namely the computing power and bandwidth of thousands of innocent people around the world in order to send out their spam.<sup>103</sup> Many people have had the experience of receiving an email from someone saying that “you have a virus” when in fact the offending email had been sent by someone completely different.

### *The challenges of authentication*

Various sender authentication schemes are being suggested, and in some cases, aggressively promoted by their sponsors, as solutions to effectively put an end to forgery of email, and hence to phishing (identity theft) and spam, but they are all under various, but very early, stages of development at the time of writing, and will require substantial engineering analysis to refine them before they start to have a tangible effect on reducing the amount of forged spam. Further, spammers may well change tactics and send non-forged spam, but using

---

<sup>103</sup> An excellent technical presentation to the North American Network Operator Group (NANOG) on botnets, by John Kristoff, is available at <http://www.nanog.org/mtg-0410/pdf/kristoff.pdf>.

disposable “throwaway” domains that are registered several hundreds at a time, at less than US\$ 10 per domain, and using cheap hosting services that cost around US\$ 10 a month.

Contact information for such disposable domains is invariably bogus, and the domains are often bought using stolen credit cards. These domains and their associated web hosting are then disposed of after a few days, and the spammer moves on to send out more spam using a different combination of domains and web hosting. Additionally, it has been noted that the stolen cards used by spammers are increasingly being obtained from phishers, identity thieves who pretend to be banks or online merchants and try to cheat gullible people into disclosing their identity and credit card information.

We thus see the spam problem has developed new levels of complexity, starting from over a decade ago when most spammers were small-time, individual operators to the current situation, where well-coordinated organized spam is the norm.

Technical measures to curb spam can only serve, to a limited extent, to mitigate the spam problem, as they typically try to mitigate the symptoms (block incoming spam) rather than address the actual cause (target the spammers). Regulatory measures take much longer to implement, and it is only right that they be put in place prudently, with a conservative approach that limits regulation to minimal levels, backed with an efficient and well trained enforcement mechanism (judiciary, law enforcement, etc.). Any proposed measures to mitigate spam must keep in mind the desirability of destroying the economic advantage that spammers have and exploit. These measures must ensure that both the spammer, and the person or organization that hires the spammer to send out an advertisement using spam email, are equally liable.

**Table 7: Percentage of messages estimated to be spam in 2004 (courtesy Messagelabs) <sup>104</sup>**

% of Spam Month													
Country	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Average 2004
Australia	30.9%	24.9%	24.6%	30.9%	30.7%	40.2%	44.8%	46.0%	45.3%	58.1%	64.7%	33.6%	44.5%
China	0.0%	0.0%	8.0%	28.4%	51.5%	45.5%	47.6%	47.6%	48.9%	51.8%	67.5%	93.7%	47.8%
Hong Kong	37.7%	19.9%	18.6%	20.4%	27.6%	33.2%	40.4%	43.1%	45.1%	51.9%	66.2%	72.1%	44.5%
India	14.4%	11.6%	13.0%	21.0%	31.4%	26.2%	25.9%	31.4%	38.5%	56.9%	39.2%	55.4%	34.4%
Indonesia			0.0%	8.8%	8.8%	8.6%	9.1%	10.0%	9.0%	9.7%	13.6%	9.7%	9.4%
Macau			38.8%	35.1%	45.9%	43.7%	44.7%	45.0%	54.9%	47.9%	48.3%	58.7%	47.0%
New Zealand	10.8%	29.2%	26.0%	31.5%	29.0%	33.0%	36.1%	38.2%	64.3%	46.8%	45.8%	40.9%	
Singapore	45.4%	41.7%	37.8%	40.0%	54.9%	51.2%	49.6%	52.7%	46.4%	34.0%	40.1%	41.7%	45.1%
South Korea	57.1%	54.5%	59.7%	51.3%	72.1%	64.0%	64.9%	73.0%	79.7%	70.3%	64.3%	64.8%	
Sri Lanka	25.1%	36.4%	30.3%	32.2%	41.2%	41.1%	40.1%	48.3%	46.3%	41.8%	50.1%	43.3%	39.1%
Thailand	52.9%	54.0%	58.4%	65.4%	87.2%	80.3%	79.0%	74.3%	74.2%	66.3%	72.0%	68.3%	68.9%
Average	37.0%	26.4%	24.6%	28.6%	33.2%	39.3%	43.9%	45.9%	45.5%	54.9%	64.4%	63.5%	44.6%

<sup>104</sup> These statistics are provided courtesy of Messagelabs, a provider of email security and management services, based on spam and virus statistics gleaned from analyzing over 100 million messages a day across a userbase of over 10,000 businesses based across 12 countries. - <http://www.messagelabs.com>

### *Challenges to the technical solutions*

Spam, and the control of spam, is a major cost centre for ISPs, and one that is not going to earn them a single cent in profit by itself. It is however a necessary cost, as it saves the ISP significant amounts of money and goodwill in terms of customers who have a better online experience as they get less spam, and in terms of other ISPs who note the proactive stance of an ISP against spam, and refrain from blocking mail from it.

The costs of receiving, storing and downloading spam, the opportunity costs of hiring administrators solely to do spam filtering, when their talents could be devoted to other tasks within the company, are all high. Another cost that tends to get factored in is the cost of terminating services to a paying customer because the customer is a spammer. However, these are necessary costs, due to the associated savings in bandwidth, server infrastructure and, most of all, in retention of customers who would otherwise shift to another ISP just because it offered better filters, and had a reputation as a spam-free ISP.

Users whose Internet connectivity is a slow and expensive dialup, who find it difficult to even download their email, may not be prepared to download software updates for programs installed on their PC, even if they could, even if they have installed legal and licensed software on their PCs that makes them eligible to download these updates. For example, a new installation of Windows XP, with the latest service packs and other updates, may take a few hours even on a fast broadband line. It may be practically impossible to download all these updates, amounting to several hundred megabytes, over an expensive and unreliable dialup, even if the user is prepared to stay up all night, when Internet access is likely to be faster and less congested than during daytime, to download the required updates, paying telephony and ISP bandwidth charges on a per hour or per byte basis. Such users can order a CD with the necessary updates from their software manufacturer or vendor, but given the rapid spread of viruses, they may find their PCs infected, and abused as a vector to send out thousands of spam emails (probably with their email address, and email addresses from their address book, spoofed into the front line of the spam), before the CD reaches them.

Automated attempts to delete spam before it reaches the end user carries with it the danger that valid and non-spam email, such as an enquiry from a new client, may be rejected as spam, possibly losing large amounts of money for the company as a result of their not getting the new client's business. This does indicate the need for a more fine-grained and conservative approach to spam filtering, an approach that necessarily costs the business more in terms of money, and/or time and effort on the part of the corporate email administrator.

### *Asia-Pacific ISPs*

ISPs in several Asian countries have at their disposal abundant bandwidth and state-of-the-art data centres, but there is often a corresponding lack of anti-spam policies and procedures. This causes a migration of spammers to their service, from ISPs that have comparatively better enforced anti-spam policies. A real world analogy would be criminals who shift their base of operations to a country with less stringent law enforcement and no extradition treaties with countries where they risk being arrested. Similarly, an ISP with a lax or complacent attitude

towards spam attracts not just local spammers but, in several cases, spammers from other countries who find it convenient to move their operations abroad. In keeping with current industry trends across the economy, several spammers are known to be outsourcing their spamming to spammers based in Asian countries.

Besides lax enforcement policies at ISPs, it has been alleged that some cash-strapped ISPs find that spammers are an attractive source of revenue, and have been known to provide “bulk hosting” services, that is, a service that is specifically geared towards hosting of spammer websites and spam sending servers, in addition to a commitment to ignore any spam complaints directed towards them. Such contracts between ISPs and spammers are colloquially known as “Pink Contracts”.

This is again a question of opportunity cost, however, as ISPs hosting such contracts will inevitably find that their reputation among other ISPs is diminished, and that ISPs and blocklist providers around the world start to block email and other traffic from their networks because of the spam. They may also face action taken by their “upstream” ISPs, that is, larger ISPs from whom they buy international connectivity and bandwidth, and who may exert pressure on customer ISPs to enforce their anti-spam policies, or start to restrict available connectivity by “null routing” IP addresses on customer ISPs that are shown to be a consistent source of spam or other net abuse. Null routing is a common method of blocking IP addresses at the router level, cutting blocked IP addresses off from the Internet.

It is also important that ISPs are easy to contact through the established channels and procedures. It is a standard best practice of network administration for IP addresses and domains to have complete and up-to-date records in the WHOIS database maintained by the domain registrars and RIRs.

### *Spam Filtering*

Most of the issues with spam are best addressed by attempts to stop outgoing spam from ISP networks. However, the other side of the anti-spam equation is the filtering of incoming spam. While filtering of inbound email is quite common at ISPs, the importance of filtering outbound email is quite often underestimated and, consequently, ISPs neglect the mitigation of outbound spam, to the detriment of the Internet at large.

ISPs and email providers have three options when deploying spam filtering.

- Outsourcing all the spam filtering, and/or their email hosting, to third party providers of spam filtered email such as Outblaze, Postini or Messagelabs.
- Purchasing and installing a commercial spam filter package such as Brightmail or Sophos PureMessage on their mail system, and working with the software’s manufacturer to customize it to their needs.
- Using an Open Source spam filtering program such as Spamassassin or ASSP, and then customizing it to their needs themselves, with input from other users of that package provided by asking questions on mailing lists and discussion boards.

In these options, the costs of doing this specialized task entirely inhouse, and dedicating staff to it versus the costs of deploying a commercial anti-spam package or outsourcing spam filtering to a third party vendor will vary from provider to provider, and must be balanced before making a decision on how spam filtering must be implemented in the organization or ISP.

Even rudimentary spam filters, when set up on a mail server, will result in a drastic drop in the volumes of spam reaching the users' mailboxes. Finding and rejecting spam reliably, with a bare minimum of false positives, gets harder as the ISP's user base increases in size, or if there is a requirement to block a larger percentage of spam, so that more complex spam filtering strategies have to be evaluated.

Spam filtering is a task that can be accomplished at two levels – at the acceptance stage, where spam filters running on an ISP's inbound mail gateways filter spam coming in to all the ISP's users. And after the email has been delivered to the users' mailboxes, using "block sender" or "move to trash" filters setup by the user in his email program, as well as desktop anti-spam programs that automatically filter the users' email when he downloads it onto his PC.

Economies of scale, as well as the fact that the ISP's mail gateways make a natural chokepoint/ single point of entry that all the incoming email (and thus, all the incoming spam) to that ISP's users has to pass through, makes it much more efficient for an ISP to filter spam at their mail gateways, so that blocking a single spam source that is sending spam to thousands of the ISP's users means that the spam is blocked from all the ISP's users by the application of a single filter. ISP-wide spam filtering also lets an ISP track "trends" in spam so that a persistent spam source can be blocked, or addressed by other means, such as those detailed in the section about cooperation between ISPs

Desktop filtering software such as Norton Internet Security and McAfee Viruscan, as well as free alternatives such as AVG Grisoft and Avast, serves as an additional layer of protection for the ISP's users, and such software helps protect users' systems and data from any spam or viruses that manages to escape the ISP's anti-spam defences. In a situation where the ISP does not filter spam, or is not very good at filtering spam, desktop spam and virus filters become an even more important protection for end users of email. This is not an efficient solution by itself, as spam that has been delivered to the user's mailbox before being filtered out during download has already been delivered, and the ISP and the user have already borne the costs of receiving the spam.

## **National and international cooperation in the Asia-Pacific region**

### *Network Operator Group meetings*

ISPs should consider attending anti-spam workshops organized by Messaging Anti-Abuse Working Group (MAAWG) and Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE), as well as network operator group (NOG) events. NOGs are conferences operated on a cooperative basis by senior and well-known members of the network operator community

in the region, with close coordination and support from the RIRs, where ISPs and network operators from around the region gather to discuss current and emerging operational trends in networking, security and spam, as well as to teach the skills they have acquired to their peers from other networks. ISPs attending such an event can take away with them a great deal of practical and operational knowledge, benefiting from the experience of their peers from other ISPs, as well as expert technologists in several fields of network operations, from DNS administration and routing to network security and anti-spam.

ISPs and network operators in South Asia can consider attending South Asian Network Operators Group (SANOG) besides attending Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT). SANOG is a smaller NOG that is focused on the needs of South Asian economies that are currently at an earlier development stage in their Internet infrastructure and economy, compared to other Asian economies such as Singapore or Japan.

### *Regional CERTs*

As discussed above, CERTs play a crucial role in information security. In the Asia-Pacific region, there exists APCERT, an umbrella association of several regional CERT bodies that are active in incident response and handling. Some other countries in the Asia-Pacific region do have CERTs in place, but their role needs to be expanded, and stabilized in order to concentrate their focus on handling systems and network security issues. CERTs can also work with local and international law enforcement authorities to quickly notify the responsible ISP in cases where illegal and/or harmful content, such as child pornography, or a virus' command and control centre, are located on a particular ISP in their region of coverage.

### *Regulator and Government level*

At a regulatory and government level in the Asia-Pacific region, international organizations such as the Asia-Europe Meeting (ASEM) and APEC, as well as the ITU and OECD can facilitate cooperation, with substantial inputs from ISPs, eminent experts, and anti-spam organizations. International pacts and agreements such as the London Action Plan and the Seoul-Melbourne Anti-spam Agreement; that bring together regulators, ISPs and other stakeholders from different countries in the region will also help foster cooperation in the fight against spam, and provide a sounding board for countries that wish to introduce anti-spam legislation. International cooperation between multiple agencies at the regulatory and law enforcement levels is essential to fight spam, given its international nature, and the criminal aspects of spam, so that a spammer may be based out of the United States, have their web server hosted in China and have their payments processed by a payment gateway provider in the Caribbean.

### **User education**

Education can play an important role in suppressing local spam industries, where people advertise email marketing services. Such services typically sell CDs with "ten million email addresses", all of dubious provenance, and most of which do not exist at all, having been randomly generated by the spammer. These CDs also ship with bulk mailer software that may forge headers, and abuse open relays and proxies to send out spam. Users of such spam software

thus unknowingly violate local laws against computer crime and hacking, even if there are no specific anti-spam laws in their country. As ignorance of a law is not normally regarded as a valid excuse for breaking the law, this may result in innocent people, whose only crime is that they believed the glib claims of a spammer and wanted to promote their business on the Internet, go to jail or have to pay heavy fines.

Developing countries have a major advantage when it comes to running education and awareness building campaigns, due to the way people access the Internet: often, users have limited Internet access at home, so they connect to the Internet at work or school, or use one of several commonly available community access points, such as cyber cafés or public libraries.

## Conclusions

As a general rule, solutions to security and spam issues need much further development in the region, as evidenced by the high rates of dissatisfaction with governance in these areas in the ORDIG survey. Some solutions are short-term in scope and implementation, and can be rapidly implemented by local ISPs and NGOs, with the assistance and cooperation of their peers from developed economies. The equally necessary efforts on developing comprehensive legal and regulatory frameworks, and on maintaining high-level channels for cooperation, can proceed at a government-to-government level, at a slower pace, with regular inputs from ISPs, NGOs and other stakeholders in the problem.

Developing economies often lack a proper legislative and regulatory framework, and there is an urgent need to help them develop and build such a framework, and facilitate cooperation between law enforcement bodies in different countries. ISPs in developing economies must be convinced of the need to filter spam coming into their users' mailboxes, crack down on spam originating from their network, and develop policies that prevent their networks being used for spam and cybercrime.

In spam, cybercrime, and e-commerce, implementing local solutions to the challenges of Internet use depends on creating awareness, and building up a large pool of people who are aware of the issues involved and their solutions – trained email administrators, Internet savvy users who refuse to be drawn into the schemes touted to them by phishers and scam artists, people with expertise in online sales and business models, financial services personnel who understand e-commerce, local organizations which educate users and work with ISPs to facilitate better interaction between ISPs and the user community, and policy makers with an understanding of the interaction between technology and policy.

Developing economies are rich in human resources – talented personnel who are aware of the issues involved, and who will benefit enormously from training and interaction with their peers in tackling these problems. Deployment of local personnel and low cost open source software solutions involve comparatively low amounts of monetary investment. Moreover, such soft investments injected into a developing country's Internet economy are directed towards long-term capacity building and development of a trained pool of local expertise, both of which contribute to improving the operational stability of the Internet and its use in those regions.