

Part III: Internet Governance Issues – Critical Internet Resources

Critical is defined as “of essential importance, indispensable”. In the context of the Internet, it is difficult to define what is indispensable. Imagine losing your phone. Or imagine your computer crashing. You could replace your SIM, handset or computer within days if not hours. In this situation, what is the most critical resource for you? For most people, it will be the data.

Water, power, road and cyber networks can all be classified as critical infrastructures. The Internet, however, is structurally and operationally quite different from the other three. It is a vast body encompassing stakeholders from all sectors: the public, industry and business, academia, governments and civil society. The underlying skeleton of this body lies in the hands of a multifarious amalgam of stakeholders. Each stakeholder contributes to building the skeleton in the form of physical infrastructure, i.e. cables, optical fibres, satellite, routers and other hardware. This includes filling out the flesh on the skeleton in the form of content and applications to facilitate communication, commerce and networking. Each aspect is as critical as the other and at the same time as varied.

What is critical?

The criticality of the resources is different for different users. In a survey conducted by Paul Wilson, Director General of Asia Pacific Network Information Centre (APNIC), the users were asked to name the resources they felt was most critical for the Internet. The spread shows that most users term applications such as Email, WWW, Search, Communications and Commerce as critical resources of the Internet. It is closely followed by Infrastructure such as Connectivity, Devices, Internet Exchange Points, Routing and Ubiquity. The

administration of the Internet which includes resources such as DNS, IP Addresses and Standards is cited by 22 per cent of the users surveyed as a critical resource. Only 6 per cent cite environmental features, such as availability of electricity, as a critical resource for the Internet.

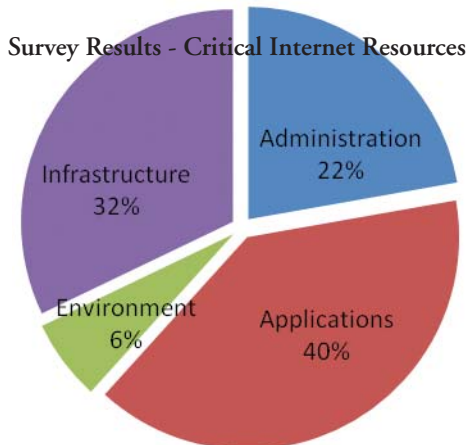
Widely accepted critical elements required to keep the Internet running are IP addresses, the Domain Name System (DNS), sufficient bandwidth and security against Denial of Service (DoS) attacks. Most of these terms are rather technical and they may not seem critical by the common users as is evident from the smaller section of the pie chart above. However, the fact is that a seemingly unrelated event such as Pakistan blocking YouTube may block a user’s access to YouTube in Europe, Southeast Asia or anywhere else in the world!

News stories like those above are not uncommon. Disruption due to natural or man-made cause can result in downtime for the entire globe. Quoting Eric J. Sinrod, an attorney from the United States of America, “*Problems in Cyberspace can Cause Real World Hurt*”¹. For example the Taiwan earthquake in 2006 knocked out the Internet services in Phillipines, Singapore and Malaysia. These countries rely heavily on the Internet for day-to-day commerce, defense systems, medical systems, government transactions etc. “You don’t realize until you miss it how heavily you rely on technology,” said Andrew Clarke, a sales trader in Hong Kong. “Stuff you took for granted has been taken away...”

How do we secure Critical Internet Resources?

The Internet is a global entity. The management, security and administration of the various critical resources lie with multiple stakeholders. Root servers and policies in Internet issues are managed at a global cooperation level, the allocation of IP addresses are done by regional agencies; such as Asia Pacific Network Information Centre (APNIC) and the DNS is managed by ICANN broadly.

Rajesh Aggarwal, Additional CEO of NIXI, highlights a few issues related to India’s IT policies and its capacity to ensure security of critical Internet resources. He says, “India has a light regulatory framework, with independent Telecom Regulatory Authority of India (TRAI) and positive court rulings, which has resulted in a vibrant telecom



Source: Paul Wilson, quoted from CircleID, http://www.circleid.com/posts/critical_internet_resources/

sector. Prices are market driven and competitive when compared with global scenario". "However," he also points out, "as compared to the developed countries the broadband availability in India is still largely limited to a 256k connection, whereas for the developed world, 1-2MB lines are becoming commonplace. Though the market is fairly competitive we still have a long way to go to create systems to ward off massive DoS attacks".

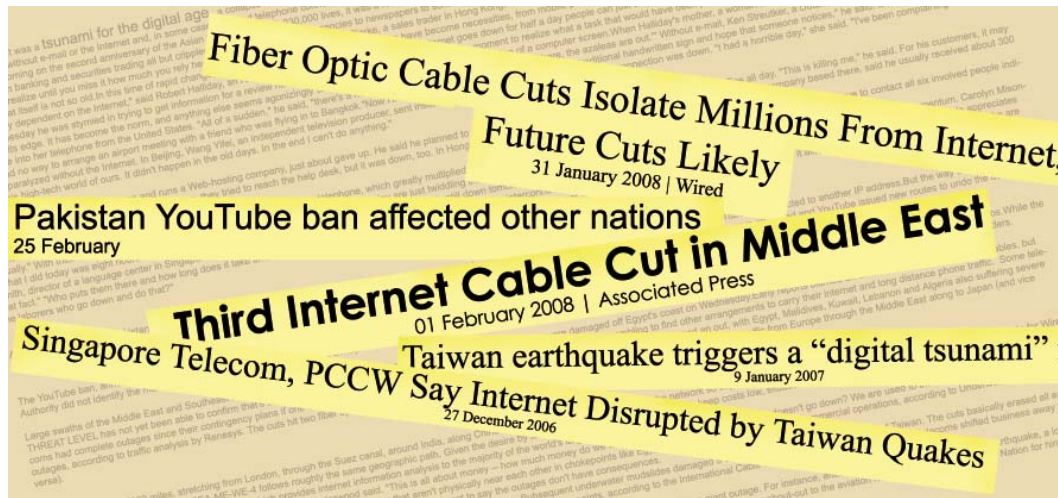
Early this year, India faced a communications crisis which had a similar outage of Internet services as a DoS attack would. Due to the severance of multiple communication cables which connect India to the world, there was a 60 per cent cut in the Internet services. This is a very unusual situation where accidents have actually caused large-scale outage. However, a situation such as this is a good touchstone of the security of critical Internet resources of a country.

There are two factors which can contribute to such a major outage. The first is that since most Internet Service Providers (ISPs) get their bandwidth from only one of the seven operational cables, if the cable is down, it will completely shut down that ISP. A simple solution to this, as suggested by S N Gupta, telecom expert and currently Chief Regulatory and Government Affairs, India and SAARC, BT Global Services could be that each ISP hedges its connectivity by dividing its bandwidth amongst multiple cables. This ensures that the ISP remains operational even if there is an outage on one of its lines.

The second factor is that most of our communication is routed through international channels since website hosting is still very expensive in India, and most of the popular websites are hosted abroad. This further implies that a breakdown in international Internet communication, such as in case of an earthquake or accidents, effectively shuts down communication within the country as well. One part of the solution is that Government has to come up with plans to promote content hosting within India. Another part is ensuring that traffic emanating from India and destined within India must remain within India. This issue is being addressed by NIXI. Their objective is that all ISPs of the country should join NIXI exchange points at various locations and declare their regional routes to them. Therefore, all data whose origin and destination are within India are routed within the country itself and not through international servers.

IP Addresses and Domain Name Systems

From homing pigeons to emails, everyone needs an address to identify the destination of a piece of communication. IP addresses are the Internet equivalent of the same. Domain Name Systems (DNS) are the descriptive names that are assigned to IP



addresses. The Internet could not have been as ubiquitous as it is today if it hadn't been for the DNS. Think of the number of phone numbers you remember and compare it to the number of people whose numbers are stored on your phone. Therefore, losing your phone will also mean losing the contact numbers. The DNS gets past this dependence on a single storage point to remember hundreds of numbers by associating a descriptive name such as www.google.com to them. This domain name will be recognised on any machine anywhere in the world as long as it has Internet connectivity.

The IP addresses are obviously the backbone of the Internet but like the city of New Delhi, the Internet is also running out of new addresses for the next billion who want to occupy this space. The present system is a 32-bit number called Internet Protocol

version 4 (IPv4). However, these addresses are running out. At present, it is said that 75 per cent of all the addresses (approximately 4.5 billion) have already been allocated. The Internet is growing at an exponential rate. In India alone, we are looking at an expansion of another 20 million broadband connections. This spells a

scarcity of IP address in the near future. The solution to this issue is being presented in the form of 128-bit addresses termed as IP version 6 or IPv6. Writing for Technology Review in 2004, Simson Garfinkel wrote that there will exist "roughly 5,000 addresses for every square micrometer of the Earth's surface"ⁱⁱ. This enormous magnitude of available IP addresses will be sufficiently large for the indefinite future, even though mobile phones, cars and all types of personal devices are coming to rely on the Internet for everyday purposes.

These issues among many others need to be discussed on a multiparty forum. On the 29th of July 2008, we are going to hold such a forum at the eINDIA2008 event at Pragati Maidan, New Delhi. We invite you all lend your voices.

Write to us and contribute to the upcoming articles

- August – Cybercrime
- September – Privacy & Data Protection
- October – IPv4 vs IPv6

Write to us at response@i4donline.net

References

- <http://www.mondaq.com/article.asp?articleid=62212>
- <http://www.technologyreview.com/Infotech/13426/?a=f>

For eINDIA2008 participation contact Sulakshana Bhattacharya at sulakshana@eindia.net.in