2011 STRATEGIC OBJECTIVES AND ACCOMPLISHMENTS
Despite Africa’s growing regional infrastructure, the majority of its cross-border Internet traffic exchange still relies on routing via Europe and North America. Consider a typical example: an Internet packet being transmitted from Nairobi, Kenya to Kigali, Rwanda. Although the two cities are separated by only a few hundred kilometres, the packet must go first to Europe, and then on to its destination. This routing system occurs throughout the region and is clearly inefficient, but of even greater concern is that such cross-border and regional communications depend entirely on global connectivity.

Participants in the Africa Peering and Interconnection Forum (AfPIF), an annual conference organised by the Internet Society, work to address this and related issues that have delayed Internet development across the continent, notably in the area of creating Internet exchange points (IXPs). At the second AfPIF conference, held in Accra, Ghana in August 2011, nearly 100 Internet engineers gathered for discussions and collaboration.

There are signs that this major component of the Society’s global outreach effort is having its intended effect: while much of the dialogue at the first AfPIF focused on fundamental issues involving peering and IXPs, in 2011 attendees were focusing on more strategic challenges, such as attracting ISPs, optimizing investment, and finding ways to help local IXPs drive down Internet costs and function more effectively.
Before Paulos Nyirenda left for Nairobi, Kenya, to attend the first Africa Peering and Interconnection Forum (AfPIF) in August 2010, he had a problem: traffic routed from the Malawi Internet exchange point (IXP) wasn’t going beyond South Africa. It gave Nyirenda – coordinator at SDNP Malawi, a government program dealing with Internet and information services – a huge headache. The eight ISP members of the Malawi IXP were eager to find a solution. Nyirenda had questions for other IXP operators in the region that he hoped to answer at the conference: Was the problem unique to Malawi? Could network operators from South Africa help solve it?

“At the end of AfPIF, I was able to identify that the problem was at the South Africa Internet Exchange [SAIX] operated by Telkom South Africa [SA], and I was able to devise ways to solve the problem,” Nyirenda said.

Nyirenda’s situation demonstrates the challenges that faced attendees of the first AfPIF conference in 2010. Last year’s meeting focused on increasing interconnection among African networks and especially IXPs because they’re a key factor in the Internet’s development in Africa. They’re also likely to attract investment from content providers.

Dr Nii Narku Quaynor of Ghana has been referred to as “the father of the Internet in Africa,” and is credited with establishing some of the first Internet connections on the continent. To an extent, Quaynor views his work as a “liberation struggle” to free Africa from technological and economic colonialism.

AFPIF: GROWING AFRICA’S INTERNET INFRASTRUCTURE

Photos © Nyani Quarmyne / Internet Society
By the end of 2011, there was agreement among key content providers, access providers, and Contingency Planning Exchange vendors to undertake a follow-up event to drive operational scale and deployment further and showcase progress toward joint goals. Moreover, the Internet Society announced plans for World IPv6 Launch, in which major ISPs, home networking equipment manufacturers and web companies around the world would come together to permanently enable IPv6 for their products and services.

Another front in the Society’s effort to advance the health of the Internet was the launch of the Deploy360 Programme. This initiative is designed to provide a free, open resource for organisations involved in deploying IPv6, DNSSEC and other new standards and technologies.

In the fourth quarter of 2011, the Deploy360 web portal launched, offering hands-on technical resources and educational articles, operational best practices, case studies, and in-depth deployment information. The team is continuing to work with content creators and has established a review panel for vetting newly featured deployment content.

For over a decade the Internet technical community has recognized that the limited number of addresses available in the version of the Internet Protocol most widely deployed today, IPv4, threatens to increase costs and limit functionality for Internet users everywhere as the Internet continues to grow. The Internet Society served as a catalyst to accelerate full adoption of IPv6, the next version of the protocol with enough addresses to enable the Internet to grow indefinitely, by organising World IPv6 Day.

On 8 June 2011, more than 1,000 organisations around the world, including some of the most popular websites, joined forces for a global-scale 24-hour “test flight” of IPv6. Nearly 400 participating organisations enabled IPv6 on their main services for 24 hours, demonstrating that major websites are well positioned for the move to a global IPv6-enabled Internet, enabling its continued rapid growth.

A key goal of this effort was to expose potential issues with IPv6 use under real-world (but controlled) conditions. In rare cases, users experienced impaired access to participating websites during the trial; however, the vast majority of users were able to access services as usual. A secondary goal was to increase awareness of IPv6 deployment among various audiences, including industry leaders, policymakers, and the general public.

With the help of key partners Akamai, Facebook, Google, Limelight Networks, and Yahoo!, as well as Members, Chapters, and Regional Bureaus, the Internet Society generated a significant amount of media coverage, including stories from CNN, Bloomberg, Spanish outlets, Le Temps, Wall Street Journal – Europe, Business Week, the Financial Times, ABC (Australia), Fiji Times, Lanka Newspapers of Sri Lanka, Straits Times of Singapore, The Australian, and the Times of India, and many others.
A MORE STRATEGIC APPROACH TO LEADERSHIP DEVELOPMENT

Create a pool of leaders capable of operating at the intersection of Internet policy, technology, and the Internet Model throughout our activities.

2011 marked a watershed for the Internet Society’s progress on its vision to establish itself as the “Learning Community for All Things Internet.” To sharpen our focus in this area — and our ability to have an impact — we brought together, at an organisational level, several programmes that had operated somewhat independently in the past.

Our new structure integrates the Next Generation Leaders (NGL), ISOC Fellowship to the IETF, and Internet Governance Forum (IGF) Ambassadorship programmes into a single new functional group, the department of Internet Leadership Programmes (ILP). This consolidation brought resources from across the organisation into one department, allowing us to further leverage existing programmes and materials, and also extend our activities.

The organisational change described at left was managed in a challenging environment of increased demand for ISOC leadership courses, driven by our ongoing outreach and marketing efforts. Amongst our efforts in response to demand, we expanded the NGL eLearning curriculum to two languages (French and English), with planned expansion to Spanish planned for 2012. We also received over 600 applications from around the world for 50 e-learning slots in 2011, and we completed and released two courselets, including “History of the Internet,” that leverage content from the eLearning curriculum.

In addition, ILP piloted Fellowships to the World Bank infoDev Global Forum as an NGL experiential component, and conducted application and selection processes for the Fellowships to the Organisation for Economic Co-operation and Development Technology Foresight Forum and the IGF. Based on demand, ILP continued to work on repackaging selected NGL course materials for use by broader audiences, such as Chapters and self-guided individuals. The team also explores potential partnerships to provide customized programmes to regional or national bodies.

http://www.internetsociety.org/leaders
INTERNET SOCIETY FELLOWS TO THE IETF INCREASE PARTICIPATION ON A GLOBAL SCALE

Six members of an Internet Society Fellowship programme took part in the 81st meeting of the Internet Engineering Task Force (IETF). The Internet Society Fellows to the IETF programme, which operates under the aegis of the Internet Society’s Internet Leadership programme, began in 2006 and is today an established Internet Society activity. Through a competitive process, the Internet Society selects Fellows from a talented pool of applicants from around the world. Fellows infuse IETF meetings with their diverse experience and local expertise about how the Internet works in their communities.

“Since the inception of the Fellows to the IETF programme, the Internet Society has selected and supported 57 engineers from more than 25 developing and emerging economies,” said Toral Cowieson, senior director of Internet leadership at the Internet Society. “Having these engineers engaged in this critical standards work helps ensure representation of a broad range of viewpoints and the ongoing development of globally relevant and effective Internet standards.”

As in prior years, each first-time Fellow was assigned a mentor to assist them in networking with others with similar Internet technology interests and to advance specific standards work. These Fellows will continue to participate in the IETF’s standards development process and will bring back to their local communities the knowledge and expertise they gained from their IETF experience.
Strengthen the Internet Society’s efforts at the regional level, and through Chapter and Member activities so they are maximally effective in realizing the organisation’s mission and goals.

The town of Chanderi, in the state of Madhya Pradesh, is a microcosm of how a wireless network helps connect a region’s individuals and institutions.

In this rural town of 20,000, the Internet Society, in partnership with the Digital Empowerment Foundation (DEF), held “Wireless for Communities” (W4C) community workshops and deployed a wireless network. Since then, the network has introduced previously unavailable Internet connectivity to more than 50 local panchayats (governments at the village or small-town level), teachers and students at 11 local schools, the telehealth facility at a local public health center, and even the town’s first-ever cybercafé.

In 2011, ISOC and DEF continued their W4C collaboration in locations throughout the country, including Baran, Rajasthan, and Tura, Meghalaya. Programme workshops were delivered in local languages; but even more significantly, since the aim is to achieve wireless connection “by the community for the community,” the workshops were targeted not for Internet engineers and technicians, but rather the community at large.
The Internet Society’s Trust and Identity initiative recognises that in order to be trusted, the Internet must provide channels for secure, reliable, private, communication between entities that can be clearly authenticated in a mutually understood manner.

A trusted Internet takes into account security, transaction protection, and identity assertion and management. Given the network dependence on unique numbers and the escalating amount of geolocation data being gathered, privacy represents a significant and growing concern.

In 2011, the Society continued to make progress on network confidence in a range of areas. Several research programmes within the Trust and Identity initiative worked to ensure that trust is a primary design element at every layer of the Internet’s architecture, and in some cases worked to redesign or improve existing elements to meet emerging requirements. Specifically, the Society:

• Established clear leadership in the realm of online privacy, making contributions to OECD and APEC privacy guidelines, leading regional stakeholder discussions, and partnering with W3C to advance identity options in the browser
• Catalysed delivery of software to promote inter-federation among identities providers through ongoing support for the development of the TERENA/REFEDS hosted PEER project, and also prepared for a second software release and public listing service for federation meta-data
• Shaped and contributed to multiple stakeholder responses to the U.S. government’s proposed National Strategy for Trusted Identities in Cyberspace, in part through ISOC participation in the Kantara Initiative
• Initiated a multiple stakeholder examination of the Identity Ecosystem and committed to a coordinating role in advancing collaboration among the key parties involved on related technical, policy, and governance solutions

In 1993, The New Yorker magazine offered its readers a prescient message on the topic of Internet privacy and security. Peter Steiner’s cartoon of one computer-using dog explaining to another, “On the Internet, no one knows you’re a dog,” seemed both absurd and funny at the time. But almost 20 years later, it serves as a shorthand insight into one of the most serious and difficult challenges presented by the Internet.

Unfortunately, on today’s Internet, ‘horror stories’ about online privacy and trust are so commonplace, they’ve almost lost the ability to shock. Identity theft is one of the more well-known threats, but a variety of other scenarios are equally troubling, including the abuse of social media to harass, rumour-monger, destroy reputations, and worse.

The underlying theme is that each of us can still be vulnerable to not only criminals, but also to a wide variety of other individuals intent on doing mischief or harm — and who can still rely on a certain amount of anonymity in interacting.

Enhance network confidence by actively promoting and supporting developments that engender user trust in networked environments.

Network Confidence

http://www.internetsociety.org/networkconfidence

In 1993, The New Yorker magazine offered its readers a prescient message on the topic of Internet privacy and security. Peter Steiner’s cartoon of one computer-using dog explaining to another, “On the Internet, no one knows you’re a dog,” seemed both absurd and funny at the time. But almost 20 years later, it serves as a shorthand insight into one of the most serious and difficult challenges presented by the Internet.

Unfortunately, on today’s Internet, ‘horror stories’ about online privacy and trust are so commonplace, they’ve almost lost the ability to shock. Identity theft is one of the more well-known threats, but a variety of other scenarios are equally troubling, including the abuse of social media to harass, rumour-monger, destroy reputations, and worse.

The underlying theme is that each of us can still be vulnerable to not only criminals, but also to a wide variety of other individuals intent on doing mischief or harm — and who can still rely on a certain amount of anonymity in interacting.

Enhance network confidence by actively promoting and supporting developments that engender user trust in networked environments.
The story of the Tunisian uprising and its widespread implications perfectly illustrate why engagement and public policy have become key issues for the Internet Society. Driven by the conviction that all people should be able to fully enjoy the benefits of access to knowledge, information, and communication, worked on a number of fronts to promote policies that support an open and sustainable Internet for all. Amongst other policy actions, in 2011 the Society:

- Released a statement opposing the US Protect-IP Act (PIPA) and Stop Online Piracy Act (SOPA)
- Supported the upcoming World Conference on International Telecommunications by launching a variety of relevant web resources dedicated to WCIT and the International Telecommunication Regulations treaty
- Deepened engagement with the IETF and ISOC Members and Chapters
- Marked UN Human Rights Day (9 December 2011) with a statement highlighting the importance of an open, global, and accessible Internet to basic human aspirations for freedom and social development
- Co-organised, with the World Intellectual Property Organisation, three workshops on issues around copyright laws and protections

Advance, validate, and defend the Internet model, based on the Internet’s open architecture and open governance arrangements.

Internet policy may seem a dry, technical subject. But the historic events in the Middle East throughout 2011 proved otherwise.

In fact, Internet Society Board of Trustees Member Khaled Koubaa, a Tunisian national, has seen firsthand how freedom of expression — a central focus in Internet policy — can impact lives, and even entire cultures. Since 1997, he has played a leadership role in the development of policies allowing for more openness of the Internet in Tunisia and across the Arab region, despite opposition and censorship from the government.

Prior to the Tunisian uprising that evolved rapidly into the region-wide Arab Spring, the flow of online information was controlled and censored by Tunisia’s Ben Ali regime. The government basically owned and controlled the country’s Internet ecosystem and censored a broad swath of website content. Indeed, many of the country’s “cyber-activists” risked severe punishment at the hands of the secret police whenever they tried to circumvent these controls.

Then, in December 2010, 26-year-old Mohamed Bouazizi self-immolated in protest outside Tunisian government offices. Only a decade before, the government would have quickly moved to censor news of such a protest. But instead, Bouazizi’s act of defiance and the protests that followed were captured on mobile phones, and transmitted via social media sites across Tunisia.

Enabled and empowered by the Internet, Tunisians used Facebook, Twitter and YouTube to distribute the voices of activists and protestors. In doing so, they set in motion a series of events that in less than a month toppled the country’s repressive, decades-long regime and introduced a level of personal freedom unknown to millions of people. Moreover, the protest and the means of sharing information amongst the protestors — was soon echoed in Egypt, Libya, Yemen, and almost a dozen other countries in the region, fundamentally changing the relationships between tens of millions of people and their governments.