LAYER 9 TECHNOLOGIES

Bridging Technology and Policy

Contribution from Layer 9 Technologies to the International Telecommunication Union Council Working Group on International Internet Public Policy Issues 2024 Open Consultation on:
CWG-Internet: Online Open Consultation

www.layer9.tech
contact@layer9.tech

Contribution by Layer 9 Technologies

Robustness, Reliability, Security, and Accessibility: No "one size fits all solution."

Purpose

Layer 9 Technologies is pleased to submit this contribution to the upcoming International Telecommunication (ITU) Council Working Group (CWG-Internet) on International Internet Public Policy Issues 2024 Open Consultation (Open Consultation) for the upcoming Open Consultation meeting on 3 October 2024.

Action Required

Discussion and consideration during the 3 Oct Open Consultations and the subsequent meeting of the CWG-Internet.

References

Provided in response footnotes.

Contribution from Layer 9 Technologies to the International Telecommunication Union Council Working Group on International Internet Public Policy Issues 2024 Open Consultation on:

CWG-Internet: Online Open Consultation

Layer 9 Technologies is pleased to submit this contribution to the upcoming International Telecommunication (ITU) Council Working Group (CWG-Internet) on International Internet Public Policy Issues 2024 Open Consultation (Open Consultation) for the upcoming Open Consultation meeting on 3 October 2024.

Addressing Internet Development

Internet development is an ongoing process in which many organizations, multilateral, multistakeholder, and otherwise, have been involved for a very long time. This development ranges from the very core technical work done to create the technologies underlying networks, to capacity building to enhance technical and other skills needed to build and grow the Internet, to the resources needed to extend and expand more Internet networks. Most importantly, when looking at how relevant multilateral and multistakeholder processes can address aspects related to Internet development, new multilateral work or initiatives should not duplicate existing efforts but rather should cooperate with those existing efforts to find and fill gaps that can be best dealt with in a multilateral framework. Given the number of multistakeholder efforts involved in governing and maintaining the Internet, finding better methods of working together on common goals of Internet development is a critical part of the effort for the models of governance.

To understand how to build cooperation between the multilateral efforts and the multistakeholder efforts in addressing the open issues in Internet development requires an openness and willingness to work with the world's many different stakeholders. This necessitates opening the doors of meetings, sharing goals and methods, and accepting the differing approaches those methods may take. It also requires building on the

opportunities and possibilities available within the Internet Governance Forum (IGF) environment for mutual understanding, coordination, and cooperation. The ITU is perfectly situated to offer a link among the many ways in which multilateralism and multistakeholderism have been and are being implemented. The key is to identify ways and methodologies by which cooperation and collaboration between the multilateral and multistakeholder worlds can be improved.

This is not a new idea as all the key documents coming from various stakeholder engagements, including the WSIS "Tunis Agenda"[1], "Our Common Agenda"[2], the "Global Digital Compact"[3], and the "Summit of the Future in 2024"[4] all point in the direction of a cooperation among state-based multilateral models and stakeholder based multistakeholder models. One potential way to improve the efficiency of addressing global Internet development and reduce duplication would be for the CWG-Internet to be more open to the various stakeholder communities, thereby facilitating the exchange of multiple views inherent in multistakeholder organizations.

Strengthening the Internet

In order to identify "the challenges and opportunities, good practices, and favorable policy environments to strengthen the Internet", a reasonable first step would be to come to agreement on what "strengthen the Internet" actually means. For the purposes of this response, we will define "strengthen the Internet" as:

> *Actions and initiatives aimed at enhancing the overall robustness, reliability, security, accessibility, and functionality of the global Internet infrastructure and ecosystem*.

Of course, the Internet, being a global interconnection of over 100,000 independently operated networks without a single control point or jurisdiction, fundamentally relies upon voluntary cooperation, collaboration, and trust. The challenges and opportunities, good practices, and favorable policy environments to strengthen the Internet must therefore take

[1] See https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[2] See https://www.un.org/en/common-agenda
[3] See https://www.un.org/techenvoy/global-digital-compact
[4] See https://www.un.org/en/summit-of-the-future

this fundamental reliance into account. While much can be done in a local context, i.e., strengthening the Internet from the perspective of individual networks, from a global perspective, the best ways to "strengthen the Internet" have historically been via focusing on facilitating and incentivizing that cooperation, collaboration, and trust and discouraging actions that impede or obstruct the evolution of the standards, processes, and structures that have made the Internet a critical part of today's economies and social interactions.

While the Internet operates, grows, and evolves via mutual agreement to abide by voluntary standards, protocols, and conventions, the independent networks that make up the Internet are subject to myriad physical, regulatory, political, economic, and social constraints, thereby precluding simplistic, "one size fits all"-style prescriptions. Fortunately, there has been wide acceptance of this reality as exemplified by the utilization of the multistakeholder model of Internet governance, the use of subsidiarity where possible, and the reliance upon existing, limited scoped bodies to formulate the Internet's best practices, recommendations, standards, and conventions.

Strengthening the Internet can therefore be seen as requiring not only local action, implemented by impacted stakeholders within a particular community, to enhance the robustness, reliability security, accessibility, and functionality of the individual networks and their components that make up the Internet but also global action by the global multistakeholder community, to reinforce and evolve the structures that facilitate and support the coordination, collaboration, and trust required to enable the Internet's component networks to interoperate.

Robustness

Enhancing the overall robustness of the Internet would include local measures to improve, expand, and diversify both the Internet infrastructure and the infrastructures upon which the Internet fundamentally relies. These latter infrastructures include the electrical grid, telecommunications facilities, and robust and enforced rule of law mechanisms and governance structures which, while critical, won't be further discussed in this response as they are best discussed by others.

In the Internet infrastructure context, numerous existing organizations such as the various regional and national Network Operator Groups (NOGs)[5], Peering and Interconnection Forums (PIFs)[6], Internet Governance Forums (IGFs)[7], as well as venues such as Internet Exchange Points (IXPs)[8] and colocation facilities can all provide avenues in which coordination, collaboration, and technical capacity-development occur and where trust can be built.

From a more global perspective, measures taken by stakeholders to reinforce the confidence in the multistakeholder model of Internet governance, evolving it in light of lessons learned over the last three decades, should continue. Enhancing the robustness of the Internet's governance structures would involve improving and evolving the resiliency, inclusiveness, transparency, and effectiveness of the mechanisms used to manage the Internet's resources and policies, with those improvements being done in the

[5] NOGs are collaborative forums that bring together network operators, engineers, and other professionals involved in the management and operation of Internet networks and facilitate the exchange of technical knowledge, best practices, and operational experiences among members. A list of Asia Pacific NOGs can be found at https://www.apnic.net/community/support/network-operator-groups/, European NOGs at https://labs.ripe.net/nogs/, and examples of regional, national, or local NOGs would include NANOG (https://nanog.org/), CHI-NOG (https://chinog.org/), Middle East NOG (https://www.menog.org/), etc.

[6] PIFs are specialized gatherings focused on discussing, negotiating, and optimizing the peering and interconnection arrangements between Internet Service Providers, content delivery networks, and other network operators. These forums facilitate the direct exchange of traffic between networks, helping to reduce latency, improve performance, and lower costs. Examples of PIFs and organizations that support them would include https://www.afpif.org/afpif2024/, https://www.ripe.net/meetings/regional-meetings/capif/, https://pif.ng/, https://www.carpif.net/, etc.

[7] IGFs, global, regional and national, are multi-stakeholder platforms that bring together representatives from governments, the private sector, civil society, the technical community, and academia to discuss public policy issues related to the Internet. IGFs are designed to facilitate open and inclusive dialogue on the development, management, and governance of the Internet, ensuring that diverse perspectives are considered in decision-making processes. Examples of national and regional IGFs include: African IGF (AfIGF, https://afigf.africa/), European Dialogue on Internet Governance (EuroDIG, https://www.eurodig.org/), Brazil IGF (Fórum Brasileiro de Governança da Internet - FIBGI, https://forumdainternet.cgi.br/), etc.

[8] IXPs are physical infrastructure locations where different Internet Service Providers, content delivery networks, and other network operators connect and exchange Internet traffic. The primary purpose of an IXP is to facilitate the efficient exchange of data between networks, which can help improve Internet performance, reduce costs, and enhance the overall resilience and redundancy of the Internet. There are over 1100 IXPs around the world. Examples of IXPs would include DE-CIX (Deutscher Commercial Internet Exchange, https://www.de-cix.net/), NYIIX (New York International Internet Exchange, https://www.nyiix.net/), APE (Auckland Peering Exchange, https://www.nzix.net/), Bangkok IX https://bknix.co.th/en/, Ghana Internet eXchange http://www.gixa.org.gh/, etc.

multistakeholder environment via the existing ICANN[9], Regional Internet Registry (RIRs)[10], and Internet Governance Forum processes.

Reliability

In one sense, enhancing Internet reliability involves ensuring that the Internet is consistently available, robust, and able to withstand disruptions, whether caused by technical failures, cyber-attacks, natural disasters, network shutdowns (man-made), or human errors. That is, that the Internet infrastructure can be relied upon despite various natural and/or man-made interruptions. In another sense, enhancing Internet reliability speaks to ensuring that the information and resources made available via the Internet can be relied upon.

In the case of infrastructure disruption and within a local context, many of the organizations and venues that participate in enhancing Internet robustness are also engaged in enhancing Internet reliability. Indeed, most of the solutions aimed at improving Internet robustness improve reliability and vice versa. Support and participation in those organizations and venues would facilitate improved coordination and collaboration, which would be supportive of strengthening the component networks that comprise the Internet.

More globally, Internet infrastructure reliability may be enhanced by increased cooperation and collaboration among stakeholders, harmonization of policies that impact the use and operation of the Internet globally, and consistent treatment globally of Internet infrastructure in the context of policy and regulation, in particular, limiting policies and legislation that encourage or lead to fragmentation of the Internet.

Perhaps more critically, Internet availability is largely at the discretion of the states in which the Internet operates. The increased activities by state-based and/or state-sponsored actors involved in cyber-espionage and cyberwarfare attacks risks significant degradation of Internet reliability, not just for the attackers and their targets, but also, due to the Internet's interconnected and interdependent nature, other users and resources globally. To date, multilateral efforts at establishing treaties, conventions, or norms of behavior to

[9] Internet Corporation for Assigned Names and Numbers, https://www.icann.org/

[10] The five regional Internet registries are AfriNIC (https://afrinic.net/), APNIC (https://www.apnic.net/), ARIN (https://www.arin.net/), LACNIC (https://www.lacnic.net/), and RIPE-NCC (https://www.ripe.net/). More information on the RIRs can be found at https://www.nro.net/.

limit these activities such as the UN GGE[11] and UN OEWG[12] have made significant progress and it is clear that further cooperation and collaboration by nation-states, with participation by other stakeholders, will be helpful for further improvement in this area.

Enhancing the reliability of information and resources available via the Internet, is significantly more challenging, particularly considering AI-facilitated "deep fake" technologies and state-based and stage-sponsored actors' proliferating use of those technologies. Increased use of technologies such as "content credentials"[13], digital signatures, and end-to-end encryption may be helpful, but ultimately, just as is the case with information in the non-digital world, no single solution exists that will ensure that what is found on the Internet can be relied upon. This suggests that the least worst approach to enhancing the reliability of information and resources available via the Internet is via capacity building and education on the realities of the Internet today.

Security

It is increasingly obvious, even to the most technically naïve, that "Internet security" is an oxymoron. From "surveillance capitalism"[14], to multi-terabit per second denial of service attacks, to increasingly sophisticated AI-enabled phishing campaigns, to increased use of the Internet by state-based, state-sponsored, and organized crime actors to compromise systems all over the Internet, trust in and on the network is degrading at an ever-accelerating rate.

Locally, efforts to encourage end users and organizations to practice better "cyber hygiene" to improve Internet security have had limited success and what success has been achieved will likely be severely challenged in a world of AI-augmented attacks. Further, end users will have little ability to affect change where attacks target the vast and frequently unappreciated inter-relationships and dependencies in software and services on the Internet and their maintainers[15]. Historically and today, "security" has not been prioritized

[11] See https://disarmament.unoda.org/group-of-governmental-experts/

[12] https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021

[13] For example, see https://contentauthenticity.org/

[14] Zuboff, Shoshana. "Surveillance Capitalism and the Challenge of Collective Action." *New Labor Forum* 28, no. 1 (January 2019): 10–29. https://doi.org/10.1177/1095796018819461.

[15] For example, the "xz" vulnerability (see https://pub.layer9.tech/papers/240408-ebersman-xz-vuln.pdf)

over new features in software or services, either during development or in purchase decisions, and the Internet facilitates remote and frequently untraceable attacks leveraging the resulting vulnerabilities. Over the long-term, it may be that recent efforts such as "Secure by Design"[16] and "Secure by Default"[17] will improve the Internet security situation, but ultimately, a change in the economics of Internet security will likely be necessary. In the near-term, best practice would be to minimize exposure, be hyper vigilant, and take proactive steps to ensure software and systems are as protected and up to date as possible. However, in the face of the increased sophistication and availability of attackers' tools, the ease in which those tools can be deployed, and the challenges defenders face in minimizing risk, it seems enhancing Internet security will be increasingly challenging.

The most common paradigm for Internet security today is largely based on a multilayered, risk-based approach that focuses on threat detection, mitigation, and response. To date, multilateral efforts at coordinating and enhancing cybersecurity have not been particularly successful. Multistakeholder collaborative efforts and industry organizations embodied in

[16] See https://www.cisa.gov/securebydesign

[17] See https://www.ncsc.gov.uk/information/secure-default

initiatives such as FIRST[18], CERTs[19], CSIRTs[20], ISACs[21], CTA[22], M3AWG[23], etc., tending towards being operational and reactive arguably having had more success.

Enhancing Internet security from a global perspective may require a paradigm shift, moving from the current paradigm to a more holistic approach. For example, recent work done in the realm of Cyber Public Health[24] draws parallels to public health practices that focus on preventing widespread disease and promoting general well-being. While traditional Internet security paradigms emphasize defending specific systems and networks against targeted threats, the cyber public health paradigm broadens the focus to consider the overall health

[18] The global Forum of Incident Response and Security Teams, see https://www.first.org/

[19] CERTs are teams established to handle and respond to computer security incidents, such as malware attacks, data breaches, and other cybersecurity threats. operating at a national or regional level, serving multiple organizations within their jurisdiction, CERTs provide a wide range of services, including incident analysis, coordination of responses among affected parties, and dissemination of security information to prevent future incidents. Examples of CERTs would include CERT Coordination Center (CERT/CC, https://www.cert.org), CERT-EU (Computer Emergency Response Team for the EU Institutions, https://cert.europa.eu), JPCERT/CC (Japan Computer Emergency Response Team Coordination Center, https://www.jpcert.or.jp/)

[20] CSIRTs are specialized teams that focus on responding to security incidents and managing security incidents at an organizational or sector-specific level. Like CERTs, CSIRTs tend to have a narrower focus, typically on specific organizations or sectors and their internal security needs. CSIRTs are generally established by individual organizations, governments, or industries to handle incidents that specifically affect their network or domain. They work on incident detection, containment, recovery, and providing post-incident analysis to prevent recurrence. Examples of CSIRTs would include Cisco PSIRT (https://tools.cisco.com/security/center/home.x, Product Security Incident Response Team), DFN-CERT Services GmbH (https://www.dfn-cert.de/, serving German Research and Education networks), Microsoft Security Response Center (https://msrc.microsoft.com/, handling security incidents related to Microsoft products and services)

[21] Information Sharing and Analysis Centers (ISAC) are organizations designed to gather, analyze, and share information related to cybersecurity threats, vulnerabilities, and incidents within a specific industry or sector. ISACs play a critical role in enhancing the cybersecurity posture of their members by facilitating the exchange of threat intelligence and best practices among organizations facing similar risks. Examples include Financial Services Information Sharing and Analysis Center (https://www.fsisac.com/), Maritime and Port Security Information Sharing and Analysis Organization (https://www.mpsisao.org/), European Energy Information Sharing and Analysis Centre (https://www.ee-isac.eu/)

[22] Cyber Threat Alliance, see https://www.cyberthreatalliance.org/

[23] Messaging, Malware, and Mobile Anti-Abuse Working Group, see https://www.m3aawg.org/

[24] See, for example, Rice, M., Butts, J., Miller, R., Shenoi, S., "Applying public health strategies to the protection of cyberspace." International Journal of Critical Infrastructure Protection, vol. 3, no. 3-4, 2010, pp. 118-127, https://doi.org/10.1016/j.ijcip.2010.07.002, Charney, Scott. "Collective Defense: Applying the Public-Health Model to the Internet." IEEE Security & Privacy, vol. 10, no. 2, 2012, pp. 54–59, https://ieeexplore.ieee.org/document/6051417, Shostack, Adam. "Public Health & Cyber Public Health." Technical Report 22-01. CyberGreen Institute, 2022. https://cybergreen.net/technical-report-22-01/. See also: https://cybergreen.net/cyber-public-health/.

and resilience of the Internet ecosystem and the digital population at large. While the traditional Internet security paradigm focuses on protecting individual entities from specific threats, the cyber public health paradigm takes a broader view, emphasizing the collective security of the entire Internet ecosystem. By promoting proactive measures, community-wide collaboration, and widespread education and awareness, the cyber public health paradigm seeks to create a safer, more resilient digital environment for all users.

Accessibility

Enhancing the accessibility of the Internet is multifaceted, encompassing gaining access to the data transmission and reception facilities the Internet provides, ensuring that the information carried over the Internet can be reached, and that the information can be understood in preferred languages and scripts. Solutions to improving accessibility will necessarily require contributions from many stakeholders, including governments, private companies, technical communities, and civil society.

With respect to gaining access to the Internet, the key considerations, which are frequently characterized by the concept of the “Digital Divide”, are the availability of robust and reliable infrastructures as discussed previously as well as affordability. These two considerations can be at odds; robust and reliable infrastructure can be expensive, which can negatively impact affordability as network operators recover their costs. Increased use of community networks and shared resources can ameliorate some of the costs, but ultimately there will need to be investment in infrastructure, including broadband, fixed wireless, mobile, satellite, and new technologies aiming at increasing ubiquitous Internet access.

Investment in infrastructure is nearly always local in nature, deploying new hardware or services to meet a specific location’s needs. Historically, it is unsurprising that increasing access to Internet infrastructure has focused on areas with the highest potential for return on investment. This has resulted in concentrations of easy access and areas in which access is challenging at best. Increased availability of lower cost satellite and wireless technologies may help alleviate “have vs. have not” situations and, assuming a friendly regulatory regime, finally make progress in addressing “Digital Divide”.

Issues related to accessibility of information on the Internet range from questions related to content control, i.e., topics such as privacy, content appropriateness and moderation, censorship, filtering, and shutdowns as well as questions relating to enabling those with various disabilities to access Internet content.

In terms of content control, given the architecture of the Internet, there has long been an aphorism in the network operations world of "my network, my rules." Traditionally, what information, service, or resource is allowed to be sourced or transit through a particular network operator's network is at the discretion of that network operator. Operationally, this has translated into individual networks blocking access to or filtering traffic from sites that the network operator deems poses a risk or otherwise violates the network's terms of service. Legislative or regulatory requirements can modify this behavior to force traffic to flow, albeit potentially at some economic cost or in terms of increased risk to network reliability or security. However, legislative and regulatory requirements more frequently have the opposite impact, requiring the limitation of resources, e.g., blocking websites that house information deemed inappropriate or blocking Internet access wholesale to prevent certain behaviors. In these cases, if they are truly necessary, great care must be taken to minimize "collateral damage", e.g., over-filtering, unintentionally blocking non-related resources, casting non-objectionable content in an inappropriate light, causing negative economic impact to regions or even nations, etc.

In the context of improving Internet accessibility for those with disabilities, significant efforts have been made in various Internet-related standards organizations such as the Internet Engineering Task Force (IETF)[25] and the World Wide Web Consortium (W3C)[26] to facilitate technological enhancements that will allow the differently abled to access Internet content. The challenge then becomes ensuring software and services in use on the Internet make use of those technological enhancements. Addressing these challenges require concerted efforts by the multistakeholder community to prioritize the implementation of these technological enhancements within the appropriate software and services.

As Andrew Grove, former CEO of Intel, said "How well we communicate is not determined by how well we say things but how well we are understood." Making Internet access ubiquitous and information on the Internet accessible is largely meaningless if it is not

[25] See https://www.ietf.org

[26] See https://www.w3.org/

possible to understand the information accessed. Meaningful access includes local content that relies on languages/scripts other than English. Multilingualism is a priority area as was discussed in the Report of the Nineteenth Meeting of the Council Working Group on International Internet-related Public Policy Issues.[27] Work is being done on a global basis and is supported by multiple stakeholder groups, but the work needs further support and encouragement. This is one area in which the ITU, given its reach and scope, can assist by spreading the word, encouraging suppliers, and enabling capabilities. Cooperation with ICANN's Universal Access Steering Group (UASG)[28] would be a good contribution that could lead to indications of other areas where the special capabilities of the ITU could be leveraged.

Fortunately, recent improvements in automated translation systems have made such translations less comical and more usable. This, along with increased availability of resources over the Internet in local scripts via the domain name system (i.e., "internationalized domain names" or IDNs) and deployment of software and systems that support non-ASCII characters has started to help remove some of the barriers to those for which English is not the primary language. Continued investment by the software and system industry and even private-public incentivization of these efforts could facilitate an Internet where people can converse and be understood in ways that are most comfortable for them.

Functionality

As has been demonstrated historically, enhancing Internet functionality has been well served by embracing the "permissionless innovation" the Internet facilitates.[29] The Internet can be seen as a substrate upon which applications and other platforms can be built and scaled up to a global population. Keeping that substrate simple with minimal regulatory overhead provides a growth medium in which new functionalities can be developed, deployed, and revised quickly and cost-effectively.

---

[27] See https://www.itu.int/md/S24-RCLINTPOL19-C-0007/en

[28] See https://uasg.tech/

[29] Thierer, Adam. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Arlington, VA: Mercatus Center at George Mason University, 2014.

However, history has also shown that this approach cannot be absolute: for example, the realities of the Internet today require care to ensure new functionalities are secure as any insecurities can put the Internet at risk. Careful deliberation within relevant multistakeholder communities is necessary to ensure an acceptable balance is met between innovation and the constraints on that innovation.

More pragmatically, the Internet is defined by voluntary standards, cooperation, and collaboration. For a new functionality to be accepted, that functionality must "scratch an itch", that is, address a need, felt by a significant portion of the multistakeholder Internet community, resulting in a "pull" for that functionality. Efforts to "push" new functionality, that is, to mandate its use, have largely been ineffective.

Take, for example, the deployment of IPv6. While this deployment has, to date, been slow (after starting in 1998 and depending on how measurement is done, current IPv6 deployment can be seen to be between 36-38%[30] and over 45%[31] of Internet traffic at the time of this writing), this can largely be attributed to a perceived lack of need. When sufficient IPv4 resources were available, there was little incentive or pressure to undertake the non-trivial costs and potential challenges transitioning to IPv6 were presumed, rightly or wrongly, to imply. However, as IPv4 addresses became more scarce, network operators began to more actively deploy IPv6, both internally and customer-facing (i.e., allowing their customers to communicate over IPv6).

This demand for IPv6, particularly with mobile devices, has encouraged equipment vendors and many, if not most, Internet Service Providers to add IPv6 support to their products and services, and they have been doing so for years. Today, lack of IPv6 support is largely limited to legacy or resource constrained systems and within enterprise networks that see no reason to absorb the costs in replacing those legacy systems or training their network operators in the use and management of IPv6. Since it seems likely that all significant Internet resources will be reachable by IPv4 for the foreseeable future, the position of these network operators is understandable: IPv6 has limited pull for those operators, and mandates, i.e., efforts to push IPv6, typically encounter resistance since IPv6 generally does not address an issue the legacy, resource constrained, or enterprise network operators believe they experience.

[30] See https://stats.labs.apnic.net/ipv6, "World, IPv6 Capable, IPv6 Preferred"

[31] See https://www.google.com/intl/en/ipv6/statistics.html

Ignoring subjective evaluations of fairness in historical address allocations, in today's Internet, failure to transition to IPv6 may ultimately be self-correcting. With the increased scarcity of IPv4 addresses and the continuing demand for those addresses being driven by network and cloud computing operators who have continued requirements to grow their IPv4-based networks, the price of IPv4 address space has unsurprisingly followed a market-based supply/demand curve. This has resulted in some network operators, typically of large legacy networks that obtained their addresses in the earliest days of the Internet, choosing to voluntarily consolidate their use of IPv4 and/or transition to IPv6, enabling the sale of the IPv4 addresses they had used within their networks. The resulting proceeds are then used to fund their network consolidation or transition.

Alternative mechanisms to increase the pull of IPv6, such as increased or particularly desirable Internet resources that are only available over IPv6, may be possible. However, this seems unlikely as it would essentially block some portion of Internet users, i.e., those who only have IPv4 Internet access available to them, from gaining access to those resources. The next best alternative would be for increased capacity building and training, particularly in dispelling myths about IPv6 deployment challenges and the benefits of having an Internet that is connected by IPv6.

Ultimately, full acceptance of IPv6, like any other Internet technology, depends on whether Internet network operators and users find sufficient value in the technology to make the change.

Promoting International Multistakeholder Cooperation

While this open ITU Council Resolution 1336 consultation is appreciated, the fact that the CWG-Internet remains closed to non-state actors may not be seen as supportive of promoting international multistakeholder cooperation.

Multiple international instruments (e.g., Our Common Agenda, the Global Digital Compact, and the Summit of the Future in 2024) have called for the introduction of multistakeholder methods and outreach. Considering that Our Common Agenda, the Global Digital Compact, and the Summit of the Future in 2024, followed by the 20-year review of WSIS in 2025 all make specific reference to the inclusion of stakeholders, it may be the fact that the

ITU CWG-Internet remains closed to stakeholders will limit the degree to which the ITU could meet this requirement for openness.

Recently, NETmundial+10[32] suggested an approach for enhancing the multistakeholder model and for bringing it and the multilateral models into closer cooperation. Adding consideration of those recommendations to widening the experiments that ITU is already engaged in may enhance the efforts of the participating states in dealing with their governance issues and concerns.

Active and open participation in the multistakeholder model, while the ITU maintains its multilateral responsibility of "working towards harnessing innovation and connecting everyone to ensure a better future for all,"[33] is a necessary condition for promoting multistakeholder cooperation in achieving progress in meeting the challenges and opportunities that are the goals of this consultation and for providing good practices and policy environments that strengthen the Internet by enhancing the overall robustness, reliability, security, accessibility, and functionality of the global Internet infrastructure and ecosystem.

[32] See https://netmundial.br/netmundial-10-multistakeholder-statement-strengthening-internet-governance-and-digital-policy-processes

[33] https://www.itu.int/en/about/Pages/default.aspx

About Layer 9 Technologies

Layer 9 Technologies, LLC is a consulting and advisory firm providing a broad range of services and expertise in Internet governance, technology policy, corporate strategy, business and operational transformations, and creation of new organizations.

With cumulatively over a century of experience in Internet technology and governance, information security, and business & program management, Layer 9 Technologies helps bridge the gap between technology and policy and brings in expertise that supports decision making and resolving policy problems.

Visit www.layer9.tech or email contact@layer9.tech for more information.