COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD)

Twenty-third session
Geneva, 23 to 27 March 2020

Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2019 to implement the outcomes of the WSIS

Submission by

Internet Society

This submission was prepared as an input to the report of the UN Secretary-General on "Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels" (to the 23rd session of the CSTD), in response to the request by the Economic and Social Council, in its resolution 2006/46, to the UN Secretary-General to inform the Commission on Science and Technology for Development on the implementation of the outcomes of the WSIS as part of his annual reporting to the Commission.

Flow of information for the follow-up to the World Summit on the Information Society

Ref: Internet Society's Annual Contribution in 2019
(Written in accordance to Report Template)

Part One: **An executive summary of activities undertaken by all stakeholders, progress made, and any obstacles encountered.**

The Internet Society (ISOC) has been actively involved in supporting the implementation of the Internet-related targets, recommendations and commitments of the World Summit on Information Society (WSIS) since its inception. We believe that significant progress has been made toward the vision of a people-centered, inclusive and development-oriented Information Society but that there is more work to be done. Our work in promoting an open, globally-connected, secure and trustworthy Internet has shown the importance and effectiveness of a collaborative approach notably in the following areas: Connectivity in remote and rural areas, Building Trust of Digital Communications (Encryption, Internet of Things), and Improving Routing Security. Collaboration between stakeholders is a key pillar to deliver sound Internet-related initiatives and policies.

Part Two: **A brief analytical overview of trends and experiences in implementation at the national, regional and international levels and by all stakeholders, highlighting achievements and obstacles since WSIS, and taking into account the follow-up and review of the 2030 Agenda for Sustainable Development. This could include information on the facilitation process of implementation, monitoring and cooperation among stakeholders.**

Although great progress has been made to achieve the WSIS goals over the past decade, there are still challenges to be overcome.

The Internet Society believes that everyone, everywhere should have the choice and opportunity to reap the benefits that the Internet offers for sustainable-economic development. However, today, nearly 50% of the world's population remains off-line[1]. And once people are connected to the Internet, there is still a need to ensure it is secure and trustworthy. Given the Internet's role as a horizontal enabler for development, this digital divide presents a major challenge to fulfilling other related development goals, such as those formulated in 2030 Agenda for Sustainable Development.

Connecting the unconnected
In 2019, ISOC continued its work in developing technical, policy, and regulatory frameworks that help communities all over the world connect themselves. Our work has shown that connecting the next billion(s) depends on various factors: the existence of sustainable local organisations, the availability of technological capabilities, and the existence of an Enabling Regulatory and Policy Environment[2] that favours the implementation of community networks, local access networks, and better exchange of traffic and network interconnection in countries.[3]

After nearly four decades, the Internet development and network infrastructure built and operated on traditional business models have not yet reached many remote, rural, and underserved areas. Community networks are a complimentary option to traditional State-based and market-based models

1 International Telecommunications Union (2019), Measuring digital development: Fact and figures 2019. Available at: https://www.itu.int/en/mediacentre/Pages/2019-PR19.aspx

2 Internet Society (2016). A Policy Framework For Enabling Internet Access. Available at: https://www.internetsociety.org/resources/doc/2016/a-policy-framework-for-enabling-internet-access/ .

3 Internet Society (2018) Community Networks in Latin America: Challenges, Regulations and Solutions. Available at: https://www.internetsociety.org/resources/doc/2018/community-networks-in-latin-america/.

internetsociety.org
@internetsociety
Quai de l'île 13
Geneva, CH-1204 Switzerland
Tel: +41 (43) 4334 80 22
Fax: +41 (43) 4334 80 22
11710 Plaza America Dr, Suite 400,
Reston, VA 20190 USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

used to provide connectivity. By working in/with underserved and isolated communities, we have demonstrated that communications infrastructure built, deployed, and operated by local groups to meet their own communication needs can empower people. These networks, known as "Community Networks" bring connectivity to those otherwise excluded because of geography, topography, size, or income level, and enable local development, and lead to local business development.4 We can see that community networks reduce digital divides, empower people, and provide opportunities.

During the past three years, the Internet Society has supported and helped deploy several community network projects across 4 regions, from the rural village of El Cuy in Patagonia (Argentina)[5] and the mountainous region of Tusheti in Georgia,[6] to the artic indigenous community of Inuvik in Canada[7]. We have also organized workshops and events on community networks to exchange knowledge and expertise, and to support capacity building of practitioners, including four regional Summits on Community Networks in Africa[8], Asia-Pacific, Latin America and Europe, and the Third Indigenous Connectivity Summit to be held in November 2019.

In addition, we advocate for key recommendations to develop policy and regulatory enabling environments that boost connectivity and unleash the potential of Community Networks and IXPs, beyond several national, regional and international fora. In particular at OECD Going Digital Summit (March 2019), WSIS Forum (April 2019), Arctic Council (May 2019), and African Union ICT Ministerial (October 2019). Finally, in 2019, we have co-sponsored the publication of *Innovations in Spectrum Management – Enabling community networks and small operators to connect the unconnected*, which provides examples from domestic successful regulatory changes, and sets key recommendations to policymakers on innovative licensing models to provide affordable access to spectrum.

Internet Exchange Points (IXPs) are another a key part of the Internet ecosystem, and represent a vital way to increase the affordability and quality of connectivity in local communities. Better national and regional connectivity helps strengthen overall Internet growth, allowing for fewer dependencies on outside networks and for greater network resiliency, redundancy, and more opportunities for users and businesses. In our experience, IXPs are most successful when they enjoy the support of a broad array of local stakeholders who work together to build and sustain the infrastructure. Indeed, the ideal model based on best practice is for stakeholders to work among themselves to develop, govern, and manage the IXP on a non-profit basis. In some cases, there may be policy barriers to the establishment of an IXP and we encourage governments to consider steps to remove those barriers and so that a vibrant local interconnection ecosystem that is anchored around the IXP(s) can emerge. In October 2019, the IXP community in Africa celebrated the addition of a 46th IXP member, the Lubumbashi IXP in Democratic Republic of Congo (DRC). This achievement illustrates the importance of bottom-up stakeholder processes and the commitment for many years of various local stakeholders in providing local training, capacity building and equipment donations.

Strengthen Global Routing Security

Shared connectivity and trust are the enablers of a trustworthy and secure Internet for everyone based on interconnectivity and unhindered data exchange. Internet security, stability and resilience require a community-wide effort. The security of the global routing system is crucial to the Internet's continued growth and to safeguard the opportunities it provides for all user. That is why, in 2019, ISOC has continued to promote a set of visible, baseline practices for network operators to improve the security of the global routing system. We call this MANRs: Mutually Agreed Norms for Routing Security (MANRS). We are especially proud of the 2019 launch of the MANRs Observatory which is a free online tool that anyone can use to see the state of routing security and resiliency of the Internet.

4 Internet Society (2018) Unleashing Community Networks: Innovative Licensing Approaches. Available at: https://www.internetsociety.org/resources/2018/unleashing-community-networks-innovative-licensing-approaches/.

5 See: https://www.internetsociety.org/blog/2019/07/in-patagonia-a-new-community-network-in-the-village-of-el-cuy/

6 See: https://www.internetsociety.org/blog/2016/06/how-you-can-help-connect-the-planet/.

7 See: https://www.internetsociety.org/resources/doc/2019/2018-indigenous-connectivity-summit-community-report/

8 See: https://www.internetsociety.org/news/press-releases/2019/summit-seeks-to-connect-communities-in-africa-to-the-global-internet/

MANRS has historically focused on measuring companies' and organizations' commitments to take action to strengthen global routing security. It is a global initiative that provides crucial fixes to reduce the most common routing threats faced by network operators and IXPs. The deployment of the MANRS Observatory in 2019 gives the ability to note how many routing leaks happen on the Internet, whether there is a downwards trend in such failures, and whether the efforts of MANRS (and other routing security efforts such as route signing) appear to make any difference.

Beyond MANRS, ISOC advocates for the importance of security and trust in the components and operations that make up the Internet's infrastructure. The adoption and implementation of industry and community-wide norms of behavior that protect the public core, including in the international security community, is an important objective in that context. In particular, ISOC continued its work in the Global Commission on the Stability of Cyberspace (GCSC), and has contributed to the global norm development around Cyber and International Stability. ISOC's sees the need to weigh in on discussions around privacy, identification, and encryption in various policy-oriented forums and to speak out against Internet shutdowns, lending our technical expertise to communities impacted by government mandated disruptions of Internet access.

Promote Trust

Trust is the key issue in defining the future value of the Internet. The Internet Society's policy agenda on trust is guided by the "Policy Framework for an Open and Trusted Internet." This document underscores the challenge that diminishing trust presents to the Internet. And, it provides a blueprint for addressing the complexities of establishing the solid foundation of trust required to realize the Internet's full potential.

In 2019, ISOC prioritized improving the security posture of producers of Internet of Things (IoT) devices. IoT introduces incredible opportunities for the digital transformation of industries, governments and societies at large. However, the IoT industry has rushed to release products and services into the market following more of a cost-benefit rationale than security/privacy considerations. This introduces various levels of risk to both users and the Internet itself – from unwitting surveillance and data compromise to physical risk (e.g., smart locks) to security cameras used as part of a botnet to attack the Internet. The goal of the Internet Society is to make IoT security a differentiator for consumers. The Online Trust Alliance's (OTA) trust framework as well as the Minimum standards for tackling IoT security will be used as a cornerstone of an expanded IoT-focused effort. ISOC is the main facilitator of the IoT Policy Platform. This project aims at harmonizing global efforts to promote security among manufacturers, retailers, policymakers, regulators, and consumers trying to make good choices, we can take greater strides towards a safer connected future for all.

ISOC also released its policy brief for IoT Privacy for Policymakers (September 2019) and supported the publication of The economics of security of consumer-grade IoT products and services (April 2019).

ISOC has also intensified its advocacy activities around the importance of encryption technologies for the development of digital economies and societies. Encryption is a crucial tool for information security and communications confidentiality in critical systems employed by industry, trade and financial services, digital government services, and health care systems among others. Encryption helps keep Internet users (either individuals or corporations in the public in the private sector) safe online by protecting the integrity and confidentiality of their data and communications in web browsing, online banking transactions. It also helps secure critical public services like electricity, elections, and transportation.

In 2019, The Internet Society and more than 30 organizations have signed an open letter calling on the G7 leaders to do just that – prioritize digital security – and not to require, coerce, or persuade device manufacturers, application, and service providers to: modify their products or services or delay patching a bug or security vulnerability to provide exceptional access to encrypted content; turn off "encryption-on-by-default"; cease offering end-to-end encrypted services; or otherwise undermine the security of encrypted services.

Research and Policy for Emerging Challenges

As a global infrastructure, the Internet is also shaped by economic and policy forces. A key part of the Internet Society's work is to understand and anticipate how these various factors might affect the Internet's future, and work to ensure changes do not undermine the key attributes that have allowed the Internet to thrive over the past three decades.

Our Global Internet Report 2019 confirms that technology in general and the Internet in particular are driving interdependence as a result of forces of concentration and consolidation that operate in and across the Internet. By failing to investigate trends in and across the application, services, and access layers of the Internet, most existing work on these trends lacks a comprehensive understanding of the very characteristics which not only enable people to benefit from using the Internet on a daily basis, but which have also helped certain companies leverage their size to gain digital dominance.

***Part Three:* A brief description of:**

(a) Innovative policies, programmes and projects which have been undertaken by all stakeholders to implement the outcomes. Where specific targets or strategies have been set, progress in achieving those targets and strategies should be reported.

The Internet Society, since its inception, has been working with partners globally to address a wide range of issues in order to promote an open, globally-connected, trustworthy and secure internet for everyone.

National Multistakeholder Processes: Enhancing IoT Security

ISOC has partnered with Innovation, Science and Economic Development (ISED), the Canadian Internet Registration Authority (CIRA), CANARIE, and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) to convene stakeholders in order to develop recommendations for a set of norms (or policy) to secure the Internet of Things in Canada. ISOC has held several meetings in a year-long process to promote a collaborative approach to address the growing set of challenges in IoT Security as we move towards a world of smart homes and cities. Policymakers should work together with experts from a variety of fields in their communities to prevent IoT devices from causing harm to consumers and the networks to which they connect. Following the Canadian experience, ISOC is also working in different countries, namely Senegal, France and Uruguay, to promote similar multistakeholder processes to develop recommendations on IoT Security. Our goal is that more governments in all regions will see those examples as inspiration for their own Internet policy development processes.

(b) Future actions or initiatives to be taken, regionally and/or internationally, and by all stakeholders, to improve the facilitation and ensure full implementation in each of the action lines and themes, especially with regard to overcoming those obstacles identified in Part Two above. You are encouraged to indicate any new commitments made to further implement the outcomes.

Earlier in 2019, the Internet Society laid out a 5-year Strategic roadmap to achieve an open, globally connected, secure and trustworthy Internet for everyone. Beginning in 2020[9], the Internet Society will embark on a way forward in order to build, promote, and defend the Internet. Working with our global community, the Internet Society will focus on extending the Internet to communities that do not have it and need it the most, promoting the Internet model of networking as the preferred model, promoting the deployment of technologies and protocols that secure the interconnection of independent networks, and promoting among governments sound policy formulation that support the growth of independent networks and trust technologies such as encryption that are foundational for trust on the Internet.

[9] The Internet Society's Action Plan 2020 is not concluded. We are committed to submit an addendum by early December, once the plans are approved by our Board of Trustees