COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD)

Twenty-second session
Geneva, 13 to 17 May 2019

Submissions from entities in the United Nations system and elsewhere on their efforts in 2018 to implement the outcome 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 22nd 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

- Annual contribution -

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

For the past 13 years, 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). Significant progress has been made toward the vision of a people-centered, inclusive and development-oriented Information Society. Our work over the past year has shown the importance and effectiveness of a multistakeholder approach notably in the following areas: Connectivity in remote and rural areas, Internet of Things and Routing Security.

Collaboration between stakeholders is indeed a key ingredient of any 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. For instance, today, roughly 50% of the world's population remains off-line. 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.

Innovating to connect the world

After more than 25 years of Internet development and network infrastructure built and operated on, traditional business models have not yet reached many remote, rural, and underserved areas. Reaching not just the next billion but the last billion requires a renewed approach. Community-powered networks based on innovative and sustainable resource models provide a way to further extend the Internet. In 2018, the Internet Society placed a specific focus on those communities in countries and regions that are characterized by vulnerabilities as a result of geography, small populations, higher exposure to global economic disruptions and frequent natural disasters.

People in the hardest-to-reach places in the world, when empowered, equipped and trained, have connected themselves to the Internet. Known generally as "community networks", initial successes with these approaches can inspire and guide other efforts to connect similarly challenged locations. Built using new policies, partnerships, and ways of working, these successes can influence and inform policy and decision makers, industry, and communities around the world. While these networks are often small in scope, usually serving communities under 3,000, some serve more than one village or community. For example, guifi.net, a community network located predominantly in Spain, and with nodes in Africa, Asia, Latin America, and Portugal, is estimated to serve more than 50,000 people.

During the past two years, ISOC supported and helped launch 10 community network projects across 4 regions, in Argentina, Georgia, India, Mexico, Kenya, Kyrgyzstan, Pakistan, South Africa and Zimbabwe. ISOC also organized several workshops and events on community networks to exchange knowledge and expertise, and to support capacity building of practitioners, including the Third Summit on Community Networks in Africa in September 2018 and the second Indigenous Connectivity Summit in October 2018, in Inuvik, Northwest Territories.

Finally, ISOC published a policy brief, "Unleashing Community Networks – innovative licensing approach," offering recommendations to policymakers on innovative licensing models to provide meaningful access to spectrum.

Securing the Internet of Things

An insecure and untrusted Internet will not realize its potential to empower people, communities and economies. Yet ensuring online security is an enormous, multifaceted endeavor which no one organization or effort can tackle. Informed by our work on the 2017 Global Internet Report, in 2018 we've worked with the aim to make security a built-in feature for the rapidly growing Internet of Things (IoT).

The Internet and its users face an increasing risk of cyber threats because more insecure consumer devices connect to the Internet every day. The number of devices and systems that make up this Internet of Things is expected to reach 20.4 billion by 2020—more than 2.5 times the global population. While this is a well-known problem, not enough is being done to strengthen the security and privacy of consumer IoT.

This year, ISOC focused on promoting the Online Trust Alliance's (OTA) IoT security and privacy principles in the production of their devices and services. The adoption of those principles protects the network, its users, and critical information infrastructure from cyber threats.[1]

ISOC has also published the policy brief on IoT Security for Policymakers in order to inform regulators, policymakers, and anyone interested in the development and implementation of policy tools regarding IoT security.

Strengthening the global routing system

For a long time, the reliability of the Internet's core has relied on informal chains of trust that span continents. As Internet connections become more abundant and more critical to everyday life, and as attacks on the Internet's infrastructure increase, security must become an integral and formal part of network operations.

To address this issue, ISOC is promoting a set of recommendations —already adopted by some network operators— that improve the security and resilience of the Internet's routing system. The Mutually Agreed Norms for Routing Security (MANRS), mitigates many of the risks facing the Internet's core today, including route hijacking, traffic detouring, and address spoofing - which is a root cause of Distributed Denial of Service (DDOS) attacks. Making MANRS an anchor point of network operations continues the established and successful approach of the Internet community adapting and evolving how it works in the face of new circumstances and challenges. Today, more than 25 Internet Exchange Points (IXPs) and 115 Network Operators are part of the initiative. ISOC also signed several Memorandums of Understanding with key partners in different parts of the globe to enhance routing security including NIC.BR, the Latin American and Caribbean Internet Exchange Association *(LAC-IX), Latin America and Caribbean Network Information Centre (LACNIC)*, Asia Pacific Network Information Centre (APNIC), ISP Association of Bangladesh, Internet Service Providers Association of India (ISPAI) and RedCLARA.

[1] OTA IoT Security and Privacy Principles, see: https://otalliance.org/initiatives/internet-things

Also, to provide policymakers with an overview of challenges related to routing security and key considerations around the routing ecosystem, the Internet Society launched a Policy Brief on this topic.

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.

The Internet and Extra-Territorial effects of laws
As new Internet policy approaches and regulations are developed, ISOC has flagged the extra-territorial effects of laws and their unintended consequences. The Internet has fundamental characteristics that have made it a global enabler of social and economic progress. These characteristics rely on the underlying source of the Internet's strength, even though applications that run above it often change, the underlying source of the Internet's strength does not vary. ISOC's Concept Note on Extraterritorial effects of laws aims to reflect on an approach to avoid rule-setting and decision-making that will constrain the Internet around the world.

Promoting collaborative governance
The Internet Society has also been developing initiatives and positive new approaches to multistakeholder policy formulation which we see as a foundation for an Internet that serves its users.

In 2018, ISOC acted to expand the endorsement of the Internet multistakeholder model by key governments and intergovernmental organizations in all regions of the world, and to promote a collaborative governance approach for Internet policy development. For example, ISOC participated in the Inter-American Telecommunication Commission (CITEL), Africa Telecommunication Union, Asia Pacific Telecommunity (APT) the International Telecommunication Union's Plenipotentiary Conference 2018, the G20 working groups such as the W20 and the C20 and other arenas. ISOC has also put significant effort in a long-term strengthening of the Internet Governance Forum (IGF).

Through multistakeholder channels, the Internet Society has been able to provide information and expert advice to assist policymakers and improve the public policy development process on issues such as information security, privacy, critical infrastructures, Internet economy and innovation.

Philippines Department of ICT Sets the Multistakeholder Model into Action

In 2018, ISOC joined an initiative with the Philippines Department of ICT (DICT) to co-develop the country's National ICT Ecosystem Framework (NIEF) in a multistakeholder fashion. The NIEF, which succeeds the Philippine Digital Strategy, will guide the course of ICT use and development, as well as the priority areas for government, until 2022. Having formalized our partnership in a Memorandum of Understanding, signed in July by DICT's Secretary, ISOC pledged to support the DICT in embedding the multistakeholder approach not only in the framework's development but in its implementation. The engagement effort was complemented by an Internet Governance training workshop to broaden understanding among civil servants of the principles that underpin the architecture and continued evolution of the Internet. Through DICT's commitment to putting the multistakeholder model into action, the Philippines joins a growing number of countries around the world demonstrating that making sound decisions in a rapidly evolving, globalized yet decentralized digital landscape begins with policymaking processes that are open, inclusive, and accessible to everyone in the ecosystem.

Canadian Multistakeholder Process: Enhancing IoT Security

In 2018, ISOC 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. Taking this process as an example, ISOC is also working in different countries in Africa, Europe and Latin America to promote IoT Security. Our goal is that more governments will see these examples as inspiration for their own Internet policy development processes.

Personal Data Protection Guidelines for Africa

In 2014, the African Union (AU) members adopted the African Union Convention on Cyber Security and Personal Data Protection. To continue facilitating the implementation of the Convention, the African Union Commission (AUC) invited ISOC to jointly develop the Privacy and Personal Data Protection Guidelines for Africa, which were released in May 2018. The guidelines were created with contributions from regional and global privacy experts, including industry privacy specialists, academics and civil society groups. It emphasizes the importance of ensuring trust in online services, as a key factor in sustaining a productive and beneficial digital economy. They also offer guidance on how to help individuals take a more active part in the protection of their personal data, while recognizing that in many areas, positive outcomes for individuals depend on positive action by other stakeholders.

In January 2018, the 32nd Ordinary Session of the Executive Council endorsed the decision to create an Africa Cyber Security Collaboration and Coordination Committee (ACS3C) upon the recommendations in the guidelines in order to advise the AUC and policy makers on the Cyber strategies.

Internet Society Beyond the Net & Chapterthon Grants
Finally, the Internet society supports a collaborative approach to addressing Internet issues by empowering its members and stakeholders to take action. Since 2015, ISOC's Beyond the Net Grants have contributed towards the WSIS goals in multiple ways: more than 460,000 people have gained access to the Internet and 41,000 received Internet skills training.

Furthermore, the recently created Global Chapters marathon – "Chaptherton" - is an initiative specifically focused on empowering ISOC Chapters. In 2017 the programme supported 30 Chapters from all 6 regions to improve education through the use of the Internet. The ISOC's Chapterthon on Digital Schools programme was recognized as the winner of a 2018 World Summit on the Information Society (WSIS) Prize under the category "International and Regional Cooperation," awarded by the ITU. In 2018, ISOC's Chapterthon on the Internet of Things invited Chapters to focus on IoT Security on their IoT related projects. More than 40 projects from just as many countries were competed in the Chapterthon.

(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.

In light of the challenges mentioned above (see Part One and Two), ISOC is committed to working in 2019 on the following areas.

Expand Access and Connectivity
In 2019, ISOC will continue its work by developing technical, policy, and regulatory frameworks that will help communities of the world connect themselves. The Internet community—a global, self-sustaining community of industry, governments, technical experts, policy makers, and the community members themselves—is needed to complete this work. ISOC expects to hold a global summit for this community by the end of 2019.

ISOC will also continue to support and develop Internet exchange points (IXPs) by providing equipment, building capacity, and promoting best practices to scale the technical operations of at least 10 IXPs in Africa. One of the goals is that 80% of African Internet traffic remains in Africa.

Finally, we will continue to focus on training and skills development iniatives, in collaboration with other capacity-development organizations and continue to support forums like the African Peering and Interconnection Forum (AfPIF) and the Indigenous Community Summit (ICS), including ensuring evolution towards becoming true community events.

Strengthen Global Routing Security

In 2019, ISOC will continue its campaign to promote MANRS. MANRS has historically focused on measuring companies' and organizations' commitments to take action to strengthen global routing security. 2019's goal is doubling the number of MANRS members by the end of the year. ISOC plans to engage the community in discussions with the aim of establishing a governance model that supports a sustainable MANRS community.

Beyond strengthening the community, the deployment of the MANRS Observatory in 2019 will give 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 will work within various communities to create the technical and policy building blocks that allow trust infrastructure to be developed, promoted, and implemented. ISOC plans to assess potential deployment issues for new standards security protocols such as Transport Layer Security (TLS) 1.3, and Domain Name System (DNS) over TLS and HTTPS. To reach communities such as network operators, ISOC will use the Deploy360 Programme channels to report on these issues and to drive deployment of trust technologies.

In addition, ISOC will continue to advocate 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.

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 will prioritize improving the security posture of producers of Internet of Things (IoT) devices. The goal is to make IoT security a differentiator for consumers. The Online Trust Alliance's (OTA) trust framework will be used as a cornerstone of an expanded IoT-focused effort.

Beyond IoT security, the idea is to approach the critical issue of trust from many dimensions. ISOC will continue to be a home for the Network and Distributed System Symposium (NDSS). NDSS is a top academic conference on network and systems security, with a unique open-publication policy. This conference not only attracts top researchers from around the world, but shares contributions in a way that promotes diffusion of information to industry and beyond.

In addition, ISOC will continue its work in the Global Commission on the Stability of Cyberspace (GCSC), and contribute 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.

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.

The "*2017 Internet Society Global Internet Report: Paths to Our Digital Future"* underscored that emerging trends (such as IoT) have the potential for great benefit, but also carry with them risks to the Internet itself. Similarly, the upcoming *Global Internet Report* looks at how consolidation—including growing forces of concentration, vertical and horizontal integration, and fewer opportunities for market entry and competition—might influence the Internet's fundamental technical properties, shape the role of Internet stakeholders including governments, and affect Internet users themselves.

During the upcoming year, based on issues raised in the soon to be released 2018 *Global Internet Report*, ISOC will improve its understanding of how consolidation at all layers of the Internet could shape not just the ways in which the Internet is used by people around the world, but its future technical evolution in the next three to five years.