14th October 2019

HIGH-LEVEL PANEL ON DIGITAL COORDINATION: THE AGE OF DIGITAL INTERDEPENDENCE
REPORT

TOWARDS IMPLEMENTATION: RESPONSES AND RECOMMENDATIONS FROM THE INTERNET SOCIETY

The Internet Society appreciates the opportunity to comment on the report of the Secretary-General's High-Level Panel on Digital Cooperation, *The Age of Digital Interdependence* (June 2019).

The Internet Society has supported the Panel's efforts from the beginning of its work, although we have expressed concerns about the lack of transparency in its composition, and the need for clarity in its mandate. We are encouraged to see that the Panel has drawn inspiration from various stakeholders' contributions worldwide, and we hope this approach will continue as the Secretary-General turns to the challenging task of implementing the Report's recommendations.

In this submission, we specifically examine the recommendations that are relevant to our own priorities and mission. While the Report addresses technologies in general, our submission focuses on the Internet as the driving force of many of the changes the Panel was mandated to address.

Suggestions for Chapter 2 – Leaving No One Behind
(including Recommendations 1A and 1C)

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.

We have observed 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[1] that favours the implementation of community networks, local access networks, and better exchange of traffic and network interconnection in countries.[2] The capacities and capabilities of relevant regulators is crucial – as is also highlighted in the Panel's report more generally.

In relation to Chapter 2, *Leaving No One Behind*, and particularly its Recommendation 1C, we suggest that the Secretary General take into account collaborative approaches that involve local infrastructure development in/with communities – like community networks – which proffer the most effective ways of addressing barriers like those posed by geography, socio-economic realities.

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. We agree with the Panel that 'what works in one country may not work in another' when it comes to developing policy, and when looking at connectivity solutions. Each community must find the right solution for sustainable development.

[1] 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/.
[2] 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

From the rural village of El Cuy in Patagonia (Argentina)[3] and the mountainous region of Tusheti in Georgia,[4] to the artic indigenous community of Inuvik in Canada[5], we can see that community networks reduce digital divides, empower people, and provide opportunities. 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.[6]

Suggestions for Chapter 3 – Individuals, Societies and Digital Technologies (including Recommendation 4)

In Section 3.2., *Trust and Social Cohesion*, the Panel argues that trust among states and in multilateral processes has deteriorated, hence 'the world is suffering from a "trust deficit disorder"'. We think it is important to highlight that declining trust is not just a factor or a consequence of technology *per se.* We observe that it is experienced more generally as a result of broader societal and geopolitical developments.

Today, policymakers are facing an important challenge: how to fully embrace the digital revolution while simultaneously ensuring the safety, security and trust of citizens. Some are doing so in rather protectionist ways that restrict access to content or impede the use of social media networks, for example. Others have imposed data localisation measures to retain Internet traffic to their own borders. And even more have taken steps to ban key trust technologies, like encryption, because they believe these technologies hamper law enforcement agencies' ability to combat crime or terrorism.

These developments are harming trust itself: without encryption and other trust technologies, there would be no secure banking or communications confidentiality, for instance. These policies result in the opposite of what is actually needed: they further damage user trust, remove opportunities and stifle innovation.[7]

The Internet Society has a different approach to building trust. We see it as depending on four interrelated features, including:

- user trust, namely how and why Internet users – including government, private sector and citizens – trust the Internet, and how to build that trust;
- technologies for trust, including the technical building blocks for establishing and maintaining trusted networks, applications and services;
- trusted networks, because the Internet's strength is that it is an ever-evolving collection of interconnected networks with distributed ownership and control. Trust is the glue that keeps networks connected and exchanging data; and a
- trustworthy ecosystem, encompassing issues pertaining to how the Internet is governed and how it deals with Internet issues.

Examples of collaborative security also show why multistakeholder collaboration offers strong measures for digital trust. One example is the Mutually Agreed Norms for Routing Security

[3] See: https://www.internetsociety.org/blog/2019/07/in-patagonia-a-new-community-network-in-the-village-of-el-cuy/
[4] See: https://www.internetsociety.org/blog/2016/06/how-you-can-help-connect-the-planet/.
[5] See: https://www.internetsociety.org/resources/doc/2019/2018-indigenous-connectivity-summit-community-report/
[6] Internet Society (2018) *Unleashing Community Networks: Innovative Licensing Approaches*. Available at: https://www.internetsociety.org/resources/2018/unleashing-community-networks-innovative-licensing-approaches/.
[7] Internet Society (2016). *A Policy Framework for an Open and Trusted Internet*. Available at: https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/.

(MANRS)[8], a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats. It demands collaboration among participants (specifically network operators and Internet exchange points (IXPs)) and shared responsibility for the global Internet routing system. It consists of a vibrant community of security-minded organisations committed to making the global routing infrastructure more robust and secure.

Another relevant regional example of collaborative security towards a trusted ecosystem is the *Internet Infrastructure Security Guidelines for Africa*, a joint initiative of the Internet Society and the African Union Commission (AUC).[9] The principles offer valuable guidance for the implementation team to 'deepen cooperation and information-sharing among the experts who comprise national governments' CERTs'.

In Chapter 3, *Individuals, Societies and Digital Technologies,* particularly Recommendation 4, we see the potential value of developing a Global Commitment on Digital Trust and Security. However, we suggest that the Secretary General builds on the approach to Trust described above, grounded on collaborative and bottom-up approaches.

Suggestions for Chapter 4 – Mechanisms for Global Digital Cooperation (including Recommendation 2, and Recommendations 5A and 5B)

In our previous contribution, we emphasize that existing digital cooperation mechanisms need to be improved and that collaborative approaches are the best way where technology is concerned. Therefore, we appreciate the Panel's call for mechanisms to 'become more holistic, multi-disciplinary, multistakeholder, agile and able to convert rhetoric into practice'.

While we agree with the overall idea of the six general gaps identified by the Panel, it is important to stress that:

- When digital technology and digital cooperation issues do become a priority in political agendas, they often focus on problems rather than opportunities. The risk is that they be used to justify more interventionist regulatory approaches that may impact negatively technology and society.

- Barriers to participation in various digital cooperation arrangements are not unique to this environment. They tend to reflect 'offline' realities. It is important that policymakers therefore focus on the root causes of the problem.

- There is a need for better cooperation between and among stakeholders, and to reduce overlapping efforts.

- Rather than creating new Internet governance mechanisms, we believe it is important to strengthen existing ones.

[8] See: https://www.manrs.org.
[9] See: https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/.

The Internet Governance Forum Plus Model

The Internet Society has been closely following and supporting the IGF since its inception. While the Panel's proposal for an IGF Plus is interesting, it also raises some questions.

We believe that now is the time to strengthen the IGF rather than reinventing new mechanisms. The objective should be to deliver more tangible outcomes, while not transforming the IGF into a negotiating body. The IGF could have a useful "dispatch function", i.e. identifying where issues can be further discussed in other relevant fora.

The Panel suggests that new mechanisms such as an *Advisory Group, a Help Desk and a Cooperation Accelerator* be created to better operationalize the IGF. We would recommend furthering the discussion with the IGF community to better understand and define these functions, in detail.

Another proposal that has caught our attention is the idea that the IGF Plus could provide 'multi-stakeholder and multilateral legitimacy' at the same time. In trying to be both, an IGF Plus may arguably be forced to make unreasonable compromises in negotiating outcomes, and might not, at the end, do either very well. We recommend clarifying this ambiguity and putting in place safeguards to ensure the IGF remains entirely multistakeholder.

The multistakeholder approach to governing the Internet has indeed demonstrated its value over the past years. Processes such as the NETmundial meeting, the WSIS+10 Review High-Level Event, and the successful transition of the IANA functions, are clear illustrations of this value. They can be used as a source of inspiration to further develop the IGF Plus concept.

In order to serve as the main forum for setting the global Internet governance agenda, the IGF also needs to increase its value to all stakeholders, and to enhance government and private sector engagement. This should be one of the key drivers of the Implementation Team, working in collaboration with all stakeholder groups.

The Internet Society is looking forward to pursuing the dialogue around the future of the IGF.