SUBMISSION: HIGH-LEVEL PANEL ON DIGITAL COORDINATION CONSULTATION

Note: in this submission, the Internet Society includes first a preamble, which summarises the overarching issues, values and challenges which our organization believes to be most critical to digital cooperation now and its development in the future. This preamble thus applies to the HLPDC's work as a whole as well as the priority consultation areas of principles and values, mechanisms and methods, and mapping areas and challenges in an overarching and cross-cutting manner. The preamble followed by specific responses to relevant questions from the consultation areas.

Preamble

The Internet Society recognises the significance that the Internet and other digital technologies have not only in our lives, but also for our economies, our development, and our digital futures. We believe **the only way in which we will realise this positive potential is if the Internet remains open, globally-connected, secure, and trustworthy for everyone, everywhere.**

First and foremost, the values that underpin governance responses to digital issues should derive from our collective understanding of the Internet as a technology. Ill-informed or overhasty policy responses or recommendations, no matter how laudable their intentions, could break this technology.

The Internet connects people because of its open, distributed, and interoperable design. Each network that connects to the Internet then also becomes part of the Internet. Together these networks are richer, more reliable, and more valuable than any would be alone. And of necessity, they gain that value without the requirement for pre-existing contract or careful geography-based controls on connection. Attempts to impose such controls are, in effect, attempts to break the Internet.

Similarly, the Internet works at multiple layers. The layers that provide connectivity, for instance, work without attending to the content they are carrying. This kind of separation of responsibility is a hallmark of modern network design, and the Internet relies on it. Policies that do not respect these technical distinctions – policies that might mix issues of content and network neutrality, for instance – are damaging to the Internet. We are more likely to avoid such mistakes when we involve all stakeholders.

All stakeholders have to work together to address digital issues, **in a truly multistakeholder fashion**. Just as the Internet is a network of networks that depends on the collaborative, voluntary action of networks holding it together, no stakeholder can alone address digital issues properly. Unilateral action will only result in stakeholders putting the Internet at more risk. But while we believe the Internet can be best protected through the valuable collective shield that multistakeholder collaboration among and between stakeholders can proffer, we are also aware of the need to carefully design such collaborative approaches to prevent policy failure, wasted resources, and – more importantly – breaking the Internet.

Keeping these risks and opportunities in mind, we believe the HLP can benefit from the lessons already learned by other existing policy processes, including the Internet Governance Forum (IGF) and the Global Commission on the Stability of Cyberspace (GCSC). Key challenges for the HLP to address include, for instance, improving the ways in which values of diversity, openness, transparency, and inclusiveness can be brought to the fore in its own processes, and the need for more clearly defining its mandate, objectives, and terms of reference. **We notably encourage the Secretariat of the HLP to open its working process** by organising for example a physical meeting between the panel members and the various stakeholder groups. We also request that all submissions to the HLP be published on online, for better transparency.

In terms of topics, as outlined in further detail below, we invite the HLP to consider becoming a champion within the UN environment and elsewhere for proposed norms that are produced by the Global Commission on Cyber Stability (GCSC), and other multistakeholder entities that have been developing **cyber stability principles by consensus**. In particular, there is an opportunity for the HLP, in cooperation with the GCSC, to bring the proposed norm to protect the public core[1] in to UN governance, thereby shepherding a new area of protection of the Internet for the world.

The Internet Society has over twenty years of experience in helping, in a multistakeholder, collaborative manner, the Internet community to maintain and grow the Internet to what it is today. In this time, it has gathered valuable lessons on what works, when it comes to digital governance, and what doesn't[2]. Our key message to the HLP is **the importance of ensuring the Internet remains open, globally-connected, secure, and trustworthy for everyone, everywhere.**

[1] https://cyberstability.org/research/call-to-protect/
[2] https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

Responses to specific questions from the HLPDC:

I. Values & Principles:

a) What are the key values that individuals, organizations, and countries should support, protect, foster, or prioritize when working together to address digital issues?

The Internet Society believes that the values that should underpin any work on digital issues should derive from our collective understanding of the Internet as an enabling technology that should be and remain open, globally-connected, secure, and trustworthy for everyone, everywhere.

We believe that the Internet empowers users with certain abilities. These abilities underpin the social value that the Internet provides to people. As we look to the future, these abilities must remain at the heart of the Internet experience for everyone, everywhere.

The ability to connect

The Internet was designed to ensure anywhere to anywhere connectivity. All Internet users, regardless of where they live, should have the ability to connect to any other point on the Internet, without technical or other impediments. This ability to connect people is essential to the Internet's value as a platform for innovation, creativity and economic opportunity.

The ability to speak

The Internet's value as a medium for self-expression is dependent on the ability of its users to speak freely. Private, secure and – when appropriate – anonymous communications ensure that Internet users can express themselves in a safe and secure manner. All Internet users should have the means to communicate and collaborate without restriction.

The ability to innovate

The growth of the Internet is the direct result of the open model of Internet connectivity and standards development. Any individual or organisation should have the ability to develop and distribute new applications and services, free of governmental or private sector restrictions, for anyone to use.

The ability to share

The Internet enables sharing, learning and collaboration. The ability to share has given rise to the open development of the key components of the Internet, such as the Domain Name System (DNS) and the World Wide Web. Fundamental to this ability is the concept of fair use, and the freedom to develop and use open source software.

The ability to choose

User choice and competitive communications markets result in the availability of better, cheaper, and more innovative Internet-related services. An Internet access environment characterised by choice and transparency allows users to remain in control of their Internet experience.

The ability to trust

Everyone's ability to connect, speak, innovate, share and choose hinges on trust. The security, reliability and stability of the network, applications and services is critical to building online trust.

These values should be at the heart of any discussion or decision about digital priorities and issues.

b) What principles should guide stakeholders as they cooperate with each-other to address issues brought about by digital technology?

The Internet, a globally-connected network of networks, by its very nature has a number of important characteristics (described below). As stakeholders cooperate to address issues "brought about by digital technology," it is first important to consider whether the issues being faced are really a product of digital technology, or rather, a product of human behaviour (perhaps, in some cases, enabled by technology). Second, it is vital that any action to address those issues does not have the consequence of altering those important characteristics which have been the foundation of social and economic growth in digital economies:

Global reach, integrity

The Internet's routing, naming and addressing service ensures it is truly global. An Internet user can reach websites, email addresses, smart phones or any other Internet connected devices and is able to trust that the information received is the information requested.

General purpose

The Internet has no inherent limitations on the applications and services it supports. The Internet supports more than the World Wide Web and email.

Supports innovation without requiring permission

"Permissionless innovation' is crucial to the Internet's success; it removes the barriers to entry. From the World Wide Web to social networking, from BitTorrent to Bitcoins, many of the applications that billions of Internet users use every day were only possible because of this permissionless innovation.

Accessible

There are no limitations on who can access the Internet; all that is required is a connection. Anyone can use their connection to create and share content, but also to attach entirely new networks such as small, local community networks.

Based on interoperability and mutual agreement

The Internet is a network of networks. It works because those networks can communicate with each other, based on open standards for the technologies that support it and through the agreements made between network operators.

Collaboration

The various stakeholders who support the operations of the Internet collaborate to ensure the Internet continues to work, grow and develop. This spirit of collaboration exists even among competitors in the private sector and between stakeholder groups that might not otherwise collaborate (for example, between the technical community and civil society). Collaboration when needed, competition when possible.

Technology, reusable building blocks

The Internet is comprised of numerous technologies that together create the Internet as we know it today. However, each individual technology, or building block, may be used for purposes for which it was not initially developed. There should be no restrictions on the functions of the technologies that comprise the Internet being used for future innovations.

No permanent favourites

The Internet has no favourites. In the 1990s, Netscape and Mosaic were among the most popular browsers on the Internet. Before Facebook and Twitter, MySpace was the dominant social network. Today, more people access the Internet with a mobile device instead of a desktop computer. New technologies and applications often replace older ones, and this is part of the natural evolution of the Internet.

Further, to support an Internet that is open, globally-connected, secure, and trustworthy (see our response to question 1a), the Internet Society and other colleagues[3] involved in global discussions such as the G20 believe in the central importance of:

- **Meaningful access**, which requires significant investments in expanding affordable and high-quality Internet access for everyone, also through alternative access strategies like community networks.

[3] The Call for G20 Leaders is available at: https://g20openletter.org/

- **Trust**, founded on user trust, technologies for trust, trusted networks and a trustworthy ecosystem. All stakeholders have a positive role to play in nurturing a trusted and open Internet. We need to work to secure core aspects of Internet infrastructure, to protect the confidentiality and integrity of the data that flows over it, and to ensure the right policies are in place to support the technologies, networks and actors that make the Internet work. We do this through collective responsibility and collaboration.

Finally, effective and sustainable solutions to digital issues are best achieved through **multistakeholder collaboration** among and between stakeholders. While the nature of such collaborative approaches is discussed in more detail in the next question, the Internet Society believes that in order for the HLP, specifically, to be able to meaningfully collaborate with other stakeholders in the digital arena to address issues brought about by technology, it must show and practice a clear dedication to the values of openness, transparency and accountability. This includes not only the scope of issues to be covered by the HLP, but to how participation in the panel is shaped and how more communities can be involved in what it is attempting to achieve.

c) How can these values and principles be better embedded into existing private and/or public activities in the digital space?

The Internet Society believes that the only way to effectively address digital issues is to involve all stakeholders, public, private, academic, technical, civil society, etc. Just as the Internet is a network of networks that depends on the collaborative, voluntary action of networks working together, no stakeholder alone is equipped to address digital issues properly. Unilateral action will only result in stakeholders putting the Internet at greater risk of.[4] This approach needs to open, decentralized, and distributed. It is not the traditional multilateral way of doing things, but it is the Internet way – the only one that can work effectively in the digital space. We therefore believe it to be crucially important that multistakeholder, collaborative approaches be adopted in private and public activities, as discussed in the previous question.

Multistakeholder approaches to digital governance has proven to be the most effective collaborative model for addressing digital and Internet policy challenges, especially if such approaches continue to recognize the open, decentralized and distributed nature of the Internet's operation. For example, the Canadian Multistakeholder Process on Enhancing the Security of Internet of Things (IoT) brought a wide range of stakeholder groups, including government, academia, public interest, and

[4]See: Sullivan, A. (2018). *We won't save the Internet by breaking it* (blog). The Internet Society. Available at: https://www.internetsociety.org/blog/2018/11/we-wont-save-the-internet-by-breaking-it/

industry representatives together to develop recommendations for a set of norms to secure IoT in Canada.[5]

To ensure the continued security, stability and resilience of the Internet, governance structures and principles must be developed in an environment of strong and equal cooperation among stakeholders, each contributing a perspective informed by their respective roles and responsibilities. Some **values that are important to multistakeholder[6] approaches** include:

- **openness and transparency**, meaning that all interested and informed stakeholders should be able to participate in governance processes that have an impact on them. To enable such participation, processes, panels and working methods need to be open and transparent, and stakeholders must be clear about their interests and affiliations.

- **diversity and inclusiveness**, meaning that diverse stakeholder groups should be represented along with diverse stakeholder interests and, naturally, regional, gender, and linguistic diversity. Special measures should be taken to ensure the participation of stakeholders that might find it difficult to dedicate sufficient funding and capacity-building efforts to participate meaningfully (e.g., marginalized communities, women, small business entities, and/or civil society participants from developing and/or Global South regions);

- **consensus-based**, meaning that any decisions and processes should be developed and reached through accountable processes that are based on consensus and that can benefit from the collective expertise of a range of stakeholders.

- **pragmatic and evidence-based approaches**, meaning that: discussions and debates about digital policy issues must be informed by and depend upon objective, rigorous and empirical information and data, and consider the intended and unintended consequences of policy choices on the Internet and its users.

As noted in question Ib), it is also important for the HLP to illustrate its commitment to demonstrating these values of multistakeholder participation. This extends beyond the scope of its work to issues of representation, how it ensures diversity and inclusiveness and makes special provision to potentially marginalised communities, and clarity and transparency about how it will use the submissions made by stakeholders in these processes.

[5] See: Canadian Multistakeholder Process: Enhancing IoT Security, available at: https://iotsecurity2018.ca/
[6] https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

II. Methods & Mechanisms

a) How do the stakeholders you are familiar with address their social, economic, and legal issues related to digital technologies? How effective or successful are these mechanisms for digital cooperation? What are their gaps, weaknesses, or constraints? How can these be addressed?

Multistakeholder approaches are not unique to Internet governance. They are indeed a popular organizing principle and practice in other topics with cross-border and global relevance, including sustainable development, environmental protection, and human rights.[7] Where the Internet and digital cooperation is concerned, multistakeholder governance approaches have been almost intrinsic to the technologies involved. Since all control on the Internet is distributed as a feature of the technical design, no actor or single group on the Internet – not industry, not governments – can solve the challenges alone.

Distributed operation is what makes the Internet robust. That feature presents security challenges that are different than what's found in other kinds of technology. Therefore, the only way to stay on top of evolving challenges around cybersecurity is by using the collaborative and distributed approach to decision-making – what allowed the Internet to thrive in the first place. The value of this kind of collaboration has been specifically recognised in regional and national frameworks or guidelines for securing the digital economy (e.g. the *OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity*; the Internet Society-Commission of the African Union Internet infrastructure security guidelines for Africa).

However, multistakeholder approaches to digital policy challenges and governance are not without challenge or fault,[8] and may face increasing challenges as a result of the growing dependency of the Internet to countries' economic and social prosperity. That said, they still offer the tools and means to enable better digital cooperation which serves the values and principles detailed in the questions above.[9]

---

[7] Van der Spuy, A. (2017) *What if we all governed the Internet? Advancing Multistakeholder Participation in Internet Governance.* Paris: UNESCO. Available at: https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf.
[8] Ibid.
[9] The Internet Society. *Why Multistakeholder Approach works*. Available at: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.

Example of a Collaborative Governance Process in Action: the Canadian Multistakeholder Process on Enhancing IoT Security

The Internet Society has led a collaborative process in Canada to develop a shared-responsibility approach and policy recommendations to strengthen IoT security. The Canadian Multistakeholder Process: Enhancing IoT Security[10] has been carried out in partnership with the Canadian government (Innovation, Science and Economic Development, ISED), CIPPIC[11], CANARIE[12], and the Canadian Internet Registration Authority (CIRA)[13]. The group has convened over a dozen in-person and virtual meetings over the past nine months to address the security risks posed by IoT devices. Participants have included representatives from the government, academia, technical sector, public interest groups, university students, and others. Including all of these voices and encouraging their participation has led to a more robust and well-rounded understanding of the state of IoT security in Canada, and the role each stakeholder group can play in enhancing security.

This group self-divided into three working groups focused on Consumer Education, Labeling, and Network Resiliency. Each group has worked both independently and in tandem to create recommendations and frameworks for improving the security of IoT devices.

The Labeling and Consumer Education groups have worked particularly closely to create a shared responsibility framework, an outline of what a security label in Canada might look like, and a framework for how consumers could be made aware of and interact with that label.

Among other outcomes in development, the Network Resiliency working group has supported the efforts of CIRA to create an open-source, secure home gateway prototype[14], designed with the challenges of IoT devices in mind, which it believes will help mitigate some of the risks to networks from IoT devices. This prototype would allow users to connect all of their IoT devices to a gateway or firewall that would then connect to the Internet. After assigning each device a unique network password, the gateway operates by analyzing outbound traffic from IoT devices using Manufacturer's Use Description (MUD)[15] and configuration information provided by users. If the traffic flows do not conform to what is expected by the gateway, the device is isolated from other devices and the network, helping to prevent it from being used as part of a botnet.

[10] https://iotsecurity2018.ca/
[11] Samuelson-Clushko Canadian Internet Policy and Public Interest Clinic https://cippic.ca/
[12] https://www.canarie.ca/about-us/
[13] https://cira.ca/
[14] https://static.ptbl.co/static/attachments/191684/1540208530.pdf?1540208530
[15] MUD is a specification being created by the IETF (Internet Engineering Task Force). This specification will allow the gateway to receive information regarding what typical data traffic patterns coming from IoT devices ought to look like. If patterns deviate from the MUD, the gateway can limit the device's access. In cases where there are no MUD files, there would be secondary repositories that could be referenced.

For the HLP, in particular, to meaningfully address the social, economic, and legal issues related to digital technologies, it could learn valuable lessons from the Canadian multistakeholder IoT working group, as well as other similar groups.

Furthermore, to ensure its legitimacy in the broader digital governance area, the HLP needs to carefully design a process – and a panel – which serves as a strong example of not only process, but also how diverse interests and stakeholders can be fairly and adequately represented in a collaborative initiative to address digital policy challenges.

We believe that **properly defined terms of reference, along with a more representative panel** appointed in consultation with the global digital policy community, will go a long way towards ensuring the HLP's continued legitimacy and efficacy in the field. However, additionally, the HLP will need to be highly selective in the issues it decides to tackle (being mindful of other places where those issues might already be being addressed, and cognisant as to what is relevant and urgent) and very clear in what outcomes and impact it would have.

b) Who are the forgotten stakeholders in these mechanisms? How can we strengthen the voices of women, the youth, small enterprises, small island states and others who are often missing?

The Internet Society believes in the values of diversity and inclusiveness, and recognizes that some stakeholders have fewer opportunities to participate in digital governance mechanisms that affect them. This is why we believe special measures should be taken to ensure the participation of stakeholders that might find it difficult to dedicate sufficient funding and capacity-building efforts to participate meaningfully.

We also note that there may be categories of organisations and individuals that may be missing from these mechanisms, simply because they are unaware that they exist or because they do not value them. Addressing these groups is also imperative. With regards to the HLP, the **current lack of representation of the Internet technical community** should specifically be addressed.

We also believe that inclusiveness does not mean that all stakeholders have to be involved in all governance mechanisms, but rather that they must have the opportunity to use their voices as interested stakeholders when needed. Further, it is important that those voices are taken into consideration and where their ideas are not followed, a clear explanation is given. Ultimately, inclusiveness is a basis of legitimacy in collaborative decision-making, along with other important values discussed above.

c) What new or innovative mechanisms might be devised for multi-stakeholder cooperation in the digital space?

Like other forms of collaborative governance, instances of multistakeholder cooperation in the digital space are not formulaic, and indeed highly dependent on the governance issue to be addressed and the stakeholders involved. There is, therefore, no single multistakeholder approach. Existing and new mechanisms must be flexible enough to continuously adapt to meet the specific needs of particular digital policy dilemmas.

Some of the Internet governance community's experiences over the past decade and more have illustrated the importance of such agility. For example, the Internet Governance Forum (IGF) and its community have established and carefully developed foundation for collaborative governance mechanisms. As a multistakeholder platform that facilitates the discussion of public policy issues pertaining to the Internet, the IGF was probably the first organization founded explicitly on the principle of multistakeholder collaboration as a creature of the World Summit on the Information Society (*Tunis Agenda*). However, the Internet Society is not alone in recognizing that the IGF is in need of change. **Today the IGF needs to be reformed** in order to serve as the main forum for setting the global agenda on Internet governance issues and increase its value to stakeholders.

The IGF example illustrates both the promise of multistakeholder collaboration to deal with digital issues as well as the importance of regularly evaluating processes, outcomes and goals to ensure that they remain legitimate, relevant, and transparently on track.

We believe the challenges faced by multistakeholder collaborative mechanisms such as the IGF are intrinsic to the process, and will be evident in most other mechanisms to enable broader and more inclusive cooperation in the digital space. Reinventing the process will not necessarily solve the problem; rather, we need a commitment to values and a willingness to continuously evolve and reform when needs be to remain fit for purpose.

Mechanisms only go so far – more crucially, the HLP should consider whether those participating are the right people, whether what they decide will be accepted and followed outside their scope of influence, and how to demonstrate that their work is effective in addressing digital issues.

III. Illustrative Action Areas

The Panel plans to explore, among others, the following areas where greater digital cooperation is required:

- **inclusive development and closing the digital gap**
- **inclusive participation in the digital economy**
- **data**
- **protection of human rights online, particularly of children, women and marginalized communities**
- **human agency and voice/participation in shaping technological choices and architecture**
- **digital trust and security**
- **building the capacity of individuals, institutions and governments for the digital transformation.**

a) What are the challenges faced by stakeholders (e.g. individuals, Governments, the private sector, civil society, international organizations, the technical and academic communities) in these areas?

While the Internet Society commends the HLP for identifying a diverse range of issues that would benefit from greater digital cooperation, we believe it is important for the HLP to keep its scope narrow and focused to one area where there is an easily identifiable multistakeholder governance gap and general agreement that the HLP is the best (or one of the better) places to practically address that digital issue or, importantly, to promote consensus. In this regard, perhaps the HLP could consider how to take forward the work of the Global Commission on Cyber Stability, namely how to promote the acceptance of the proposed norm to protect the public core across the Internet governance space. (Please see below for further details.)

As to the challenges in addressing the issues identified above, we strongly believe in the need to ensure that everyone, everywhere, can reap the benefits that the Internet and other digital technologies offer for sustainable and economic development. To do so, these issues need to be addressed in a manner that respects the core values and principles of the Internet as a global, resilient and interoperable network of networks. Further, the open and inclusive process for developing Internet protocols and standards, the impartial stewardship of Internet naming and addressing resources, and the decentralized cooperation and collaboration of network operators around the globe — must be kept front of mind in developing responses to any digital policy issue.

The challenges faced by stakeholders in the digital issues listed therefore have to be addressed in a manner which places the importance of the Internet's technical development, the protection of its technical characteristics, and its public core, at the centre of any governance response.

b) What are successful examples of cooperation among stakeholders in these areas? Where is further cooperation needed?

We believe multistakeholder approaches must be designed and tailored to specific governance dilemmas. As a result, it is difficult to highlight specific successful examples, although in addition to the IGF (see question II c) above), we believe the Global Commission on the Stability of Cyberspace (GCSC) offers various positive examples of cooperation.

The GCSC is a multistakeholder group of experts and interested parties established in 2017 to promote stability in cyberspace by developing proposals for norms, policies and initiatives to enhance international security and stability. Despite the challenge of its mandate, the GCSC is delivering robust results in advancing proposed international norms, working in an open, bottom-up and multistakeholder fashion and building on existing mechanisms at intergovernmental level. A recent outcome of the GCSC includes the "Singapore Norm Package"[16].

As a further example, from the area of digital security, as a consequence of the Internet Society (ISOC) - Commission of the African Union (AUC) Internet Infrastructure Security Guidelines for Africa, the AUC has issued a call for participation in a new Africa-wide Cyber Security Collaboration and Coordination Committee, a multistakeholder group that would advise policymakers of the AUC on regional strategies and capacity building, and facilitate information sharing across the region.

c) What form might cooperation among stakeholders in these areas take? What values and principles should underpin it?

As noted above, the global Internet community has over two decades of experience in creating, improving, deploying and coordinating the Internet. While many lessons can be drawn from these experiences, a critical element of our success thus far is a commitment to a collaborative, multistakeholder governance approach. The HLP can thus do well to learn from these lessons – also in the ways in which it appoints, selects, manages, and constitutes its own participants, processes and governance mechanisms.

To avoid potentially compromising the Internet's technical core functions and processes, digital policy debates would benefit greatly from being informed by the experience and insight of those who have been directly responsible for developing and operating it. The principles that have

[16] https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

promoted and sustained the development of the Internet since its inception — the open and inclusive process for developing Internet protocols and standards, the impartial stewardship of Internet naming and addressing resources, and the decentralized cooperation and collaboration of network operators around the globe — are the Internet technical community's critical contribution to these debates.