Contribution ID: 239caa2b-1f06-4915-ab2f-fd72a826fe09
Date: 12/12/2024 14:21:26

Targeted consultation on Internet Governance

Fields marked with * are mandatory.

Background

The European Commission is launching a targeted consultation on its stance on Internet governance in preparation for the critical milestones foreseen in 2025 (WSIS+20) and in response to the request from the Council to develop “an EU strategy on the multistakeholder governance of the Internet to set out a common position to uphold in international fora with a view to ensuring an open, free, affordable, neutral, global, interoperable, reliable and secure Internet”.

The aim is to gather input from stakeholders across governments, business, technical experts, and civil society organisations—to inform and strengthen the EU’s position. This consultation aims to refine the EU’s vision for a free, secure, and open internet while safeguarding its core values of data protection, human rights, and the rule of law in the digital space. Your insights and participation are essential to help direct the future of internet governance.

Internet governance is a system of processes, policies, and standards that shape how the internet functions and evolves. The internet is inherently decentralised, involving governments, international organisations, technical experts, businesses, and civil society organisations. The EU believes that supporting this multistakeholder approach is vital to keeping the internet free, secure, efficient, equitable, and respectful of human rights, especially in the face of rapid technological advancements.

However, the multistakeholder model of internet governance has been and is under increasing pressure in global forums, such as the recently adopted Global Digital Compact (GDC) and the upcoming World Summit on the Information Society (WSIS+20). Some governments are pushing for more centralised, state-controlled approaches, citing national

security, data privacy, and digital sovereignty concerns. While these concerns are valid, that shift risks breaking the internet into isolated national networks, undermining global connectivity, innovation, and the principles of a free, open, and accessible internet. The growing politicisation of internet standards and infrastructure—driven by market competition and geopolitical tensions between superpowers —adds to the complexity. The upcoming discussions on the future of the internet governance is an opportunity to examine the challenges and opportunities and seek solutions to ensure that it is future proof.

Against this background, the EU must clearly articulate its expectations for the outcome of WSIS+20 and make a compelling case for why a multistakeholder governance model is essential for supporting the internet's open and global nature. The EU's leadership in sustaining this model is crucial for protecting its digital interests and ensuring the global internet stays stable and open. Together with its core values—data protection, human rights, fundamental freedoms and the rule of law—the EU can secure international recognition of its digital policies and regulatory frameworks.

Privacy Statement

Before proceeding with the questionnaire please take a moment to review the privacy statement:

Targeted_consultations_privacy_notice.pdf

About you

* Full name

Tatiana Tropina

* Email address

tropina@isoc.org

* Which institution/organisation(s) do you represent?

Internet Society

* Which stakeholder group best represents you?

Technical community

* In which country are you based?

Netherlands

1. Introduction

1. According to the institution/organisation that you represent, what are the most important benefits of the open, free, global, interoperable, reliable, and secure Internet?

Maximum 3 selection(s)

- [ ] a. Possibility to connect with other users worldwide
- [ ] b. Opportunity to freely express one's opinions
- [ ] c. Greater access to information worldwide
- [ ] d. Greater participation to democratic processes and decision-making
- [ ] e. Greater transparency and accountability of government
- [ ] f. e-Government and cutting red tape
- [ ] g. Possibility of association
- [ ] h. Business and commercial opportunities
- [ ] i. Learning and development
- [x] j. Other

Other. Please elaborate:

Internet Society strongly believes that all the benefits of the Internet are extremely important. The Internet, as a global technical infrastructure, is a resource that enriches and transforms our lives and our society for the better. The WSIS Declaration of Principles 2003 states that "the usage and deployment of ICTs should seek to create benefits in all aspects of our daily life." We are concerned that this question aims at creating a hierarchy of the benefits by asking to pick "the most important" ones. The answers would depend on the perspective of a particular stakeholder. Yet the benefits are interrelated, and many of them are indivisible, as the technical building blocks that allow the Internet to exist and thrive don't distinguish among applications or services.

2. According to the Member State/institution/organisation on whose behalf you are responding, what are the biggest threats and challenges to an open and resilient internet? Please pick your top three responses.

Maximum 3 selection(s)

- [ ] a. Cybersecurity threats targeting internet infrastructure
- [ ] b. Cybersecurity threats targeting online users
- [ ] c. Unequal access to the internet for users across the globe
- [ ] d. Disinformation and misinformation
- [ ] e. Censorship including cancelling, deplatforming, banning, etc
- [ ] f. Violation of human-rights online
- [ ] g. Insufficient privacy protection, particularly personal data

- [ ] h. Rise of digital authoritarianism and state control over the internet, e.g. internet shutdowns
- [ ] i. Centralised, state-centric models versus the current decentralised, multi-stakeholder structure
- [ ] j. Lack of investment in critical internet infrastructure
- [x] k. Other

Other. Please elaborate:

In our 2030 Strategy, we committed to addressing two global challenges affecting people across the world, each as important as the other: global inequality in access to the Internet, with 2.6 billion people remaining unconnected, and the lack of trust in the Internet (https://www.internetsociety.org/resources/doc/2024/2030-strategy/).

Some of the most significant threats and challenges to an open and resilient Internet we identify in the context of the WSIS+20 review—Internet shutdowns, fragmentation, and threats to encryption technology—relate to the responses suggested to this question. However, we would like to offer our view on these issues as we are concerned that the proposed wording of answer options might aim to create a hierarchy and frame the challenges in a way that only certain solutions would be acceptable to address them.

1) Internet shutdowns are a major concern, as they have become an increasingly common tactic for governments to restrict connectivity at national and sub-national levels, often primarily for political reasons. According to the Internet Society's Pulse platform, there were 135 Internet shutdowns from January to December 2024, with ten incidents ongoing at the time of writing. The Internet Society believes Internet shutdowns harm societies, economies, and the technical infrastructure of the global digital economy. Internet shutdowns constitute a significant risk for many businesses and investors, including those building infrastructure or developing services.

2) Another significant threat is Internet fragmentation, where the Internet is carved up along political, economic, and technological boundaries in a fundamental contradiction to the original principles of the globally connected Internet, where data flows freely and securely across the world. A growing number of government and corporate decisions around the world have the potential to adversely impact the open and interoperable global Internet, often with unintended consequences.

3) We are also concerned about threats to encryption technology, which is essential for protecting the personal security of billions of Internet users worldwide and the national security of countries globally. Many governments are considering laws and regulations that could weaken encryption, significantly jeopardizing security and safety on the Internet. As more people connect to the Internet, it is important for everyone involved to take steps to keep it safe. This includes protecting against security threats, exploitation, personal privacy harms, online gender-based violence, discrimination, and other abuses of human rights.

Lastly, the most serious threat to an open and resilient Internet is the risk that the WSIS+20 review outcomes will undermine the multistakeholder model of Internet governance. The multistakeholder model is key to addressing all the above-mentioned challenges, and reaffirming the commitment to it should be the utmost priority in the WSIS+20 review.

3. According to the institution/organisation that you represent, is the EU is doing enough to address the above-mentioned challenges and threats?

- ○ Yes
- ◉ No

Please pick the top three actions that you consider should be carried out.

Maximum 3 selection(s)

- ☐ a. Step up EU internal coordination with the Member States to increase its international leverage
- ☐ b. Strengthen EU action to protect the open internet on the international stage by bridging the digital divide
- ☐ c. Reinforce EU actions to protect human rights online
- ☐ d. Ensure equitable access to the Internet
- ☐ e. Promote internet freedom, counteract internet shutdowns and censorship
- ☐ f. Support the greater involvement of stakeholders from the Global South in internet governance
- ☐ g. Increase participation of EU stakeholders in the international Internet governance institutions
- ☐ h. Advocate to strengthen internet governance institutions (ICANN, IETF, IGF)
- ☐ i. Step up the efforts of the EU technical community in standardisation
- ☐ j. Foster internet technologies that are compliant with EU principles and norms and enable users' choice, protect their privacy, and increase their security
- ☑ k. Other

Other. Please elaborate:

To address the above-mentioned challenges, the EU should strengthen and reinforce its support for the multistakeholder model, which over the years has shown continuous success in addressing various threats to the open, globally connected, secure, and trustworthy Internet.

The Internet was built to support and promote innovation. It will continue to stay open, globally connected, secure, and trustworthy in the future if we ensure that we protect what the Internet needs to exist, thrive, and stay healthy. We need to recognize and preserve what Internet Society defines as "critical properties' of the Internet and its enablers, which have been a constant foundation for the success of the Internet from the beginning. Any Internet-related regulatory proposals in the EU must be assessed from the perspective of supporting and preserving these critical properties. The Internet Society developed an Internet Impact Assessment Toolkit — a collection of practical tools that can be used for such assessments of how legal and regulatory proposals can impact a healthy Internet (https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit).

We would also like to note that the answer to the following question (Question 4) does not specify which of the two governance models the respondents consider crucial for the open and secure global Internet. We

want to emphasize that our answer to Question 4 refers to the importance of the multistakeholder model, which we consider crucial.

4. According to the institution/organisation that you represent, how important is the type of governance model for an open and secure global internet (multistakeholder model versus state-centric)?

Very important

5. According to the institution/organisation that you represent, is there sufficient knowledge in the EU of the impact of internet governance on the open and secure global internet?

No

2. Coordinating and engaging EU Internet governance stakeholders

6. According to the institution/organisation that you represent, is there sufficient participation and coordination between EU stakeholders in the internet governance area?

No

7. According to the institution/organisation that you represent, how can the EU enhance participation and coordination among its internet governance stakeholders?
Please pick your preferred top three options.

Maximum 3 selection(s)

- [ ] a. Increase coordination between the national and European authorities through common positions ahead of key policy milestones
- [ ] b. Create networks of technical experts to represent common EU interests in standardisation fora
- [x] c. Increase funding for national and regional initiatives, such as the national IGFs and EURODIG
- [ ] d. Increase connections between national and regional initiatives with international ones on internet governance especially the IGF
- [x] e. Empower underrepresented groups such as youth, seniors, digital rights, and civil society organisations for active involvement in the field of Internet governance
- [x] f. Other

Other. Please specify:

We would like to highlight that all the proposed options offer a good way forward to enhance participation and coordination, but with some caveats. Any increased coordination (option 1) between the national and European authorities should improve transparency and input mechanisms from the multistakeholder community.

With regard to the creation of technical experts' networks (option 2), the EU should foster the participation of technical experts and the technical community, not only in standardization forums. The knowledge and expertise of the technical community are crucial to ensure that any Internet-related regulation or other actions proposed and taken by the EU preserve an open, globally connected, secure, and trustworthy Internet.

We would also like to elaborate on our answers to Questions 5 and 6. The questions related to knowledge and coordination are very important, thus, we would have appreciated more context on what Question 5 refers to because it might mean the EU Institutions, stakeholders, citizens, media, or something else. While there is sufficient knowledge of the impact of Internet governance on the open and secure global Internet in the technical community and some of the EU institutions, we would welcome efforts to increase awareness, knowledge-sharing, and capacity-building within the EU institutions and various stakeholders.

In our answer to Question 6, in addition to having more context, we would have appreciated an opportunity to explain our answer. We answered “no” even though some stakeholders are well-coordinated. Yet enhancing this coordination and building upon existing mechanisms, especially learning from the multistakeholder governance mechanisms, is crucial.

8. According to the institution/organisation that you represent, what are the main barriers to effective multi-stakeholder participation in internet governance? Please pick your preferred top three options.

Maximum 3 selection(s)

- [ ] a. Power imbalances expressed in varying interest, influence, and stake
- [x] b. Ways of engagement that overlook the various levels of expertise, interest and influence of different stakeholder groups that vary depending on the topic
- [ ] c. Technical expertise and knowledge gaps
- [ ] d. Geopolitical tensions and bloc-thinking
- [x] e. Lack of inclusivity
- [ ] f. Coordination difficulties and separate siloed discussions on specific issues risk creating incompatible and even conflicting outcomes
- [ ] g. Legal and regulatory differences
- [ ] h. Resources limitations
- [x] i. Other

Other. Please specify:

Both multilateral and multistakehodler processes present numerous challenges. It is crucial to focus on improvements to ensure that these processes are as effective as possible.

The multistakeholder approach to Internet governance has grown from the Internet's own DNA and is what allows it to thrive. The multistakeholder processes have already proven to be extremely effective, and we have great examples over the past decades. While the barriers put forward in the answer options still exist (for instance, inclusivity and knowledge gaps, among others), these issues are well-known to the multistakeholder community. The community has been making a lot of efforts to solve them, for example, working on more inclusivity and building technical expertise.

The main barrier to multistakeholder participation arises when a particular process is not open to stakeholders (or not inclusive enough), is not transparent, or does not provide opportunities for meaningful participation for non-governmental stakeholders. This barrier mainly concerns various multilateral fora and can exist due to various factors, some of which are outlined in the proposed answer options, such as lack of inclusivity, geopolitical tensions, resource limitations, and others.

A true multistakeholder process involves all the stakeholders by design. In some cases, in multilateral processes, mere consultations without meaningful participation, where stakeholders' contributions are not taken into account, do not meet the definition of "a multistakeholder approach", even if there are attempts to label them as such. The NETmundial+10 outcome document outlines best practices on how to improve multilateral processes and make them more inclusive to ensure meaningful participation. Therefore, we suggest putting efforts into implementing these recommendations.

3. Transforming global stakeholder organisations for inclusive, effective, and sustainable Internet governance

9. Is the institution/organisation you represent familiar with or does it participate in the work of the following Internet governance institutions/fora (pick up to 3 answers):

Maximum 3 selection(s)

- [ ] a. EURODIG
- [ ] b. Internet Governance Forum (IGF)
- [ ] c. Internet Corporation for Assigned Names and Numbers (ICANN)
- [ ] d. Internet Engineering Task Force (IETF)
- [ ] e. All the above
- [ ] f. None of the above
- [x] g. Other

Other. Please specify:

We are familiar with all of the institutions and organizations listed in the answer options. However, we would have appreciated more background information provided on how the selection of these organizations was made and on what grounds. For example, the list doesn't include various standards-development organizations, such as the World Wide Web Consortium (W3C) and the European Telecommunications Standards Institute (ETSI). It also doesn't mention the Number Resource Organization (NRO) and Regional

Internet Registries (RIRs), even though they manage Internet resources under fairly open and multistakeholder processes with strong participation from their communities. Notably, the intergovernmental organizations dealing with Internet Governance are also absent.

10. Noting the fast-paced evolution of the internet and building on your analysis of the current IG institutions (ICANN, IETF, IGF), does the institution/organisation you represent consider that there is a need for changes or improvements to their mandates, governance, or functioning?

- ○ Yes
- ◉ No
- ○ I do not know

4. Emerging technologies: anticipating the governance of the future Internet

12. What are the key governance challenges associated with emerging technologies such as those underpinning Web 4.0 according to the institution /organisation you represent? Please choose your top three replies.

Maximum 3 selection(s)

- ☐ a. Uncertain definition of the scope
- ☐ b. Lack of common global standards
- ☐ c. Lack of a common institutional framework
- ☐ d. Balancing public and private interest
- ☐ f. Identifying the right balance between innovation and regulation
- ☐ g. Potential far-reaching implications for society
- ☐ h. Risk of deepening digital divide
- ☑ i. Other.

Other. Please specify:

The background description of this consultation states that “the EU must clearly articulate its expectations for the outcome of WSIS+20 and make a compelling case for why a multistakeholder governance model is essential for supporting the Internet’s open and global nature”.

We are concerned that this consultation contains questions related to the vague and undefined concept of Web 4.0. This concept appears to include just an application, a set of services that don’t create a new Internet. On the contrary, Internet architecture, by its very nature, facilitated innovation and will continue to do so if its critical properties and its multistakeholder model of governance are preserved. This model has also been crucial in addressing various technical and governance challenges related to the development of technologies in the last few decades. The key challenge in the WSIS+20 review and beyond is to reaffirm the commitment to this model. This model will also be crucial in addressing any governance aspects of

future applications and technologies.

We also want to note that it would be helpful to have a more detailed background information of substance about the technologies in question. Without specifying the technology, the question about governance challenges might produce various answers based on different understanding of those who respond to this survey.

13. Is the institution/organisation you represent familiar with alternative (blockchain-based) domain name spaces?

- (●) Yes
- ( ) No

14. If yes, what will be their impact on the traditional DNS infrastructure and its governance (multiple answers possible) according to the institution/organisation you represent?

- [ ] a. Increased offer of domain names for consumers possibly leading to lower prices
- [ ] b. Greater freedom for internet users due to immutable and resistant to tampering nature of alternative domain names based on blockchain solutions
- [ ] c. Increased competition and innovation in the domain name space
- [ ] d. Consumer confusion linked to possible identical domain names (name collision) in the traditional DNS and in the alternative (blockchain based) DNS spaces
- [ ] e. Lower protection for intellectual property rights due to the absence of collective governance mechanisms for alternative domain name spaces
- [ ] f. Lower protection for consumers against harms due to the absence of collective governance mechanisms for alternative domain name spaces
- [x] g. Other

Other: Please specify:

The impact of these systems on the traditional DNS infrastructure is likely to be very minimal because the alternative blockchain-based domain name spaces are not likely to be successful. None of them are yet available in typical operating systems or web browsers, nor are they likely to be at any time soon. Additionally, none of the alternative blockchain-based domain name spaces have shown any ability to come close to the scale of transactions necessary for usage in production Internet connectivity. They may be used by small groups of people seeking alternative solutions and willing to put the time into configuring their systems, but it is not clear how any of these alternatives could be used in large-scale consumer usage.

We would also like to note that the question is asked about the impact on the traditional DNS infrastructure

and its governance, but some of the proposed answer options consider the impact on the consumer side, protection of IP, and other broader (perceived) issues. Therefore, it is not entirely clear what kind of information is gathered for the purpose of this consultation and why.

5. Internet security and resilience

15. Facing a growing number of cybersecurity threats, what does the institution /organisation you represent see as the most pressing challenges to ensure the security and resilience of the open and global Internet in the next years?

- [x] a. Possible fragmentation of the open and global Internet
- [x] b. Insufficient deployment of advanced security features
- [x] c. Possible vulnerabilities of the global routing system
- [x] d. Availability and reliability of crucial Internet functionality in case of major incidents or in case of crisis
- [ ] e. Other

16. Please briefly explain the choices above:

We consider all of the challenges mentioned in the answer options important. The first challenge— Internet fragmentation (Option 1)—is an overarching concern, which we have already elaborated on in our previous answers. With regard to other choices, we would like to highlight the following:

Option 2: Insufficient deployment of advanced security features.

In our Internet measurement work, which is available online in the Internet Society Pulse platform (https://pulse.internetsociety.org/), we track statistics around advanced Internet security technologies. Technical community stakeholders, such as the IETF, constantly develop and deploy advanced security features that, if widely adopted, can increase the security of our networked interactions (for example, HTTPS, which protects web transactions with encryption). The wide adoption of these features can sometimes take quite a long time, leaving certain data flows and individuals vulnerable. However, advancing technical protections online should be done by the technical community, rather than mandated by regulations as both trust and flexibility are an integral part of Internet security and resilience, as much as developing the innovations themselves.

Option 3: Possible vulnerabilities of the global routing system.

We have long championed increased global routing security at the Internet Society. This includes our support in 2014 of the creation of Mutually Agreed Norms for Routing Security (MANRS), a global, community-driven initiative to improve the security and resilience of the Internet's global routing system. Initially created by a small group of network operators who recognized the need to join forces to improve the system, MANRS has grown from nine original operators to a community of hundreds participants within a decade. In 2024, we successfully transitioned the secretariat and MANRS Observatory to our partner organization, Global Cyber Alliance.

We also recognize various initiatives emerging in addition to these efforts, including the ones by the US government. Like any process to improve security, this is a constant work in progress. Routing security is

also an illustrative example of challenges in the development and deployment of advanced security features.

Option 4: Availability and reliability of crucial Internet functionality in case of major incidents or in case of crisis.

The technical Internet infrastructure is resilient enough to weather crises such as failures of physical infrastructure (e.g., damage to submarine cables). Still, efforts to enhance the resilience of the physical infrastructure are crucial. What we consider the most pressing challenge in the context of the availability of critical Internet functionality is non-technical shutdowns when governments restrict connectivity primarily for political reasons. These shutdowns undermine the resilience and security of the whole network and its users, who, for example, are not able to install recent security updates.

17. According to the institution/organisation you represent, are the current policy instruments and approaches available at the EU level (coordination at EU level and cooperation with international partners, supporting EU-based critical infrastructure (such as the EU-based public DNS resolver DNS4EU) for the benefits of EU citizens and the global Internet, fostering deployment of important security standards, …) adequate with respect to these challenges?

- ○ Yes, fully adequate
- ◉ Yes, partially adequate
- ○ No

18. According to the institution/organisation you represent, how can the EU contribute better to enhance the security and resilience of its internet infrastructure and the overall Internet for the benefits of its citizens and the global Internet?

Internet Society appreciates the EU's efforts to support the open, globally connected, secure, and trustworthy Internet and its multistakeholder governance model. We also value and respect the intent to ensure that EU citizens stay safe and secure through the development of the EU-based critical infrastructure as a part of the global Internet. However, some of the EU initiatives, such as previous proposals for NIS2, eIDAS, and a current proposal on combatting CSAM, despite best intentions, can have profound unintended consequences for the global, open, secure, and trustworthy Internet.

We would like to reiterate that the EU efforts should preserve what makes the Internet an essential global tool and a space for innovation, growth, and transformation. Any Internet-related regulatory proposals in the EU must be assessed from the perspective of supporting and preserving what we call the Internet's "critical properties"—the properties that define the Internet Way of Networking and underpin the growth and adaptability of the Internet—and its enablers.

It is crucial to include various stakeholders early in the discussions to properly assess regulatory and governance initiatives. In particular, the technical community has a strong foundation of expertise based on a common understanding of the characteristics the Internet needs to exist and thrive. Technical community experts, together with other stakeholders, can provide valuable input and ensure that the EU initiatives benefit EU citizens while maintaining an open, globally connected, secure, and trustworthy Internet.

Contact

CNECT-IG-CONSULTATION@ec.europa.eu