IGF 2020 Messages

Trust

Version 1: 17 November 2020

Note: this is a living document being put out for public comment. A final version will be published 3 weeks after IGF ends. For any questions or feedback regarding the IGF 2020 Messages, please write to igf@un.org.

Messages related to Overarching Policy Question 1

What building blocks are essential to ensuring a functioning, stable and resilient Internet and online world both now and, robust enough to continue working well into the future, regardless of the constantly evolving environment and changing threat landscape?

- COVID-19 turns our lives upside down and restrictions to control the spread of the pandemic limit us in our most normal daily activities. The e-solutions that allow us to continue to work or study from home, require a secure and stable connectivity to a reliable Internet.

- Users and nations must be able to trust on a well-protected and fortified Internet infrastructure.

- Countries that establish a national emergency telecommunications plan are better positioned to manage disaster responses more effectively during times of crisis, like COVID-19. Disaster response strategies should ensure coordination and alignment across all levels of government. – Federal, state, local, tribal and territorial partners are important for developing a cohesive, meaning response to national disasters, even when infrastructure isn't impacted such was the case with the COVID-19 crisis.

- The COVID-19 pandemic is an opportunity to assess and identify gaps and bottlenecks in the digital infrastructure, and start preparing action plans for

affordable and reliable connectivity, ensuring sufficient bandwidth through each leg of the network, and expanding connectivity to those not yet connected or not yet well-connected.

- The Internet was explicitly designed to encourage global interconnectivity and oblivious to international borders. It was and continues to be a core goal to get as many people, devices and networks as possible connected in a global network of networks.

- The current situation with large parts of the workforce working from home, as an abrupt and unforeseen measure to fight covid, creates new security risks and increases existing ones, because employees connect to their home networks instead of the well protected company network. This requires special efforts to strengthen their cybersecurity readiness. Improved and continuous capacity building, education and training contributes to the creation of a culture of cybersecurity.

- The fast growth in IoT home devices raises concerns about security and privacy implications for their users. Guidelines, publications and recommendations need to be published in a user-friendly format and use a language with less jargon and technical terminology.

Messages related to Overarching Policy Question 2

What can stakeholders do, ranging from government models to concrete initiatives to create an Internet that is a safe and secure online space for all, supported by the respect for human rights and the protection of our children, minimise the risks and potential harm to users, and eradicate discrimination?

- Online channels are critical to communicate and ensure that citizens have access to important information in times of crisis. The digital transformation of governments needs to continue and where possible accelerated.

- Digital transformation within the government sector is critical to ensuring citizen access to important information during times of crisis.

- Fact-checking requires local and international cooperation, and the skills and resources to cope with an avalanche of information, a variety of sources and diversity in languages. On top, adequate fact-checking is being hindered by political pressure, and financial and legal threats.

- Fact checking will remain ineffective if there's no trust in the fact checkers. Government involvement in fact checking initiatives can strengthen or undermine this trust.
- Bots are important, innovative and compelling tools to automate tasks in the fight against disinformation, and save resources that can be concentrated on tasks where human oversight is needed. Transparency is crucial to avoid that bots limit essential

rights, such as freedom of expression and access to information, and has many layers: the inner working of the tool, the used criteria and their effects, but also who is deploying the tool and their objective.

- Education, media literacy and a public dialogue that fosters respect for facts and science are central in combating misinformation online, as is restoring trust in journalism, and more transparency in how social media companies (and their algorithms) handle information.

- Stakeholders, researchers and developers from academia and business in particular, should partner to develop technical tools to address disinformation and fake news online, for example, how to apply AI and machine learning to recognise hate speech.

- Combating fake news is a shared ánd individual responsibility, every user has to remain vigilant when encountering information and hold themselves accountable when sharing or helping to spread information on social media, and not hide behind the technology or shift all responsibility on social media. The debate and awareness raising on tackling disinformation and hate speech cannot be postponed and should be strengthened. Training young people's skills to critical thinking should start from an early age.

- Academics and specialists in behavioural science and mental health must amplify their research into the positive and negative impact of online activities, including the influence of gaming on children's development and wellbeing, so that their findings can guide policy making and industry practice.

- Technology can be a solution as well as part of a problem. The digital world creates opportunities for children to learn, play, develop their potential and protect their rights, but is also full of dangers that can harm or undermine their rights.

- The protection of children online requires a careful balance that manages the risks while maximizing the opportunities. A successful approach should involve children, parents, educators, industry, and policymakers ensure cyberspace is as safe and empowering as possible.

- The production and dissemination of illegal and harmful content are two different things that both require a high level of vigilance. On top of that, one needs to avoid that algorithmic amplification automates the dissemination of the bad.

Messages related to Overarching Policy Question 3

How to create an environment that fosters a stakeholder dialogue, where mistrust, fear and misunderstanding makes place for mutual trust and recognition of each other's role, and players collaborate on holistic answers to the safety and security challenges of our online world?

- Through collaboration and cooperation, business, government, the technical community, and multilateral organizations can develop adequate answers to challenges at national, international and global level, arising from crises such as COVID-19.

- The pandemic has shown how technology and social media can be a lifeline to stay connected with friends and family, to continue economic activity and to gather information. The IGF should facilitate the dialogue on the shared responsibility and actions of stakeholders, including regulation where needed, to make sure that users are able to interact and communicate in a secure online environment at all times.

- Initiatives to include multistakeholder views and perspectives in the UN cybersecurity dialogues are well received, but more effort is needed to make the dialogues and opportunities to provide input more visible, including support and capacity building to involve nations and communities across the digital divide.

- All stakeholders share responsibility for the protection of children online, including in online games. They should strengthen their coordination, and work on a systematic approach towards an evidence-based governance of online gaming, with a combination of public, private, legal and voluntary measures at national and international levels.

- Concerns about the protection of children in the online world are shared by many. Parents, educators, the industry, and policy makers should, as standard practice, consult with children on matters that have an impact on their lives, and this includes their online lives.

- Trust, legitimacy and the involvement of all relevant stakeholders are the pillars for any beneficial capacity building project. Trust among stakeholders within and between regions will foster the exchange of good practice.

- Differences between regions (geography, economics, politics, culture) may be significant and make that best practices are not directly applicable to every region. The involvement of multiple partners is beneficial to a sustainable cyber capacity building. Cooperation and good practice sharing between more and less advanced regions and countries is as important as the cross-regional sharing amongst equally advanced partner regions.

- Capacity building initiatives for governments in developing countries should prepare them to participate in international and global cyber norms discussions and initiatives.

- Governance in child online gaming is an emerging and rapidly developing policy area, and an indispensable part of global internet governance. The protection of children in online gaming requires a careful balance between managing the risks and maximizing the opportunities. All stakeholders shouldering responsibility for protecting children online should strengthen cooperation and coordinate an

adequate combination of public, private, legal and voluntary measures at national and international levels.

- Trust mechanisms in cyberspace should be established, based on principles of responsibility, transparency, respect, mutual consultation and mutual understanding. Initiatives should establish an open cooperation among parties including governments, international organizations, enterprises, technical communities, scientific research institutions and individuals as the main actors, and explore a wide range of tools such as laws and regulations, IT capabilities, social responsibility, ethics, supervision and self-discipline, as well as norms and standards.

- Ensuring the security and privacy is essential for the IoT ecosystem to thrive while the guidelines and related decision-making process have to involve diverse stakeholders including civil society and policy makers. There's a lack of knowledge about the IoT associated risks and the need of capacity building actions to present best practices and prevent threats. The IGF is well placed to intermediate such a process.