Our Digital Future
Addressing Digital Transformation and Cybersecurity
Capacity development workshop series focused on developing countries
Linked to the UN Sustainable Development Goals 9 and 16

Summary of Workshop I
8 September 2021 | 12:30-14:00 UTC

Driven by the call in the UN Decade of Action to cooperate for the Sustainable Development Goals (SDG), this workshop engaged over 150 stakeholders of different backgrounds and regions in a dialogue focused on safe digital transformation in connection with the SDG 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation; and SDG 16: Promote just peaceful and inclusive societies.

In four virtual table discussions, participants exchanged views on several policy aspects, including the progress status of digital transformation of government services, multistakeholder cooperation for a safer digital ecosystem, impact of cyber conflicts and efforts aimed at standardisation.

The fruitful and vibrant exchanges underlined the need for all stakeholders to adapt to the rapid development of digital technologies. All stakeholders, including governments, businesses, civil society and technical communities, need to cooperate in an adaptable manner, given the rapid change digitalisation brings.

Below is the summary of the exchanges at each policy discussion table.

Discussion table I

Facilitated by Mr. Mike Yeh, Associate General Counsel and Director Corporate External and Legal Affairs for Asia region at Microsoft

*How do developing countries advance progress on the implementation of the SDG 9 which calls for all stakeholders to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation. Specifically, what is the status of progress on the digital transformation of government services? How can we realize more and better citizen services? Where else can we do more?*
This table discussion emphasised the importance of the sustainable development goals and their direct connection with the Internet, digital technologies and enabling policies for digital transformation. To illustrate the benefits of the digitalization process in the public sector services, a success story from the government of Mexico was presented. Namely, Mexico pioneered a process where citizens tax filing system has been revamped with a digitalisation effort, which further resulted in a significant extra income in tax revenue for the government. In this dedicated breakout room, participants continued to discuss how communities are progressing on realizing SDGs goals 9 and 16, specifically by focusing on the digital transformation of governments to advance citizen services. Participants underlined that the primary condition for the Internet access relates to stable infrastructure. However, some stressed that it is critical to understand that this does not relate only to cables and routers, but to essential public utilities such as electricity which many developing countries, especially the least developed countries, do not have in regular supply. Further, participants noted that even when online services are accessible, they are not necessarily safe and secure. Some note that this may be due to a lack of awareness, lack of standards, enabling policies and laws. The exchanges reflected on the need for the digitalisation of public services requires everyone to be involved in its implementation. Therefore, multistakeholder input and best practices needs to be recognized and integrated in the digital transformation of all public authorities. Digitalization of public services is a nuanced process. Not everyone shares the same level of awareness or opportunities to become aware, engaged and finally benefit end-users of these processes. This especially is the case with people living in remote and rural areas, or people with disabilities. Engagement of youth from early stages, as well as the effective transition of strategy and implementation across successive governments, guarantees long-term sustainability of these digital transformation efforts and processes.

Discussion table II

Facilitated by Ms. Hariniombonana Andriamampionona, IGF 2021 Best Practice Forum (BPF) on Cybersecurity co-facilitator and member of the IGF Multistakeholder Advisory Group from Madagascar, supported by the BPF editor, Mr. Wim Degezelle.

How can multi-stakeholder cooperation contribute to more effective cybersecurity?

Speaking as a representative of the IGF’s Best Practice Forum on Cybersecurity, the need for active and equal inclusion of state and non-state actors in developing and implementing cyber norms. It was noted that cybersecurity agreements are put in place to solve complex issues where it is impossible to come up with a clear,
immediate way to fix them. Therefore, this purpose and the overall complexity of the Internet, raises the importance of the inclusion of stakeholders from different disciplines to cooperate and rethink best solutions. Only a relatively small number of agreements that were looked at by the IGF Best Practice Forum (BPF) on Cybersecurity have a clear multi-stakeholder input. A number of very positive initiatives involved stakeholders, however, the multi-stakeholder involvement happened afterwards, when the basic part of the agreement’s text was already there or when the concept and ideas were already formed. Participants underlined the need for stakeholders to begin cooperating at the early stages of drafting an agreement, and not after it is done. Regulations and adoption of best practices agreements should not start with governments alone, but should also include the private sector at early stages to position such regulations and agreements to achieve subsequent private sector compliance or participation. Some issues need to be concretely addressed by the authorities, and not only by goodwill, because cyber security is a critical issue that affects essential infrastructure.

Discussion table III

Facilitated by Mr. John Hering, Senior Government Affairs Manager, Digital Diplomacy team at Microsoft

*How does escalating conflict in cyberspace, and increasingly sophisticated cyberattacks, jeopardize peace, justice and strong institutions around the world? And what can be done to advance security and stability in cyberspace to support SDG 16?*

The immense transformative power digital technologies have for the well-being of people can be slowed down or completely stopped by malicious online activities. These cyberattacks can have a massive impact, when targeting various societal systems, such as health care, energy, food and water chain supplies. The UN’s efforts to advance cybersecurity across the world were recognized, especially through its Open-Ended Working Group (OEWG) and the UN Governmental Group of Experts (GGE).

However, concerns were shared that despite these good efforts, cyber harms continue to pose threat and cause harm. Participants jointly discussed how escalating conflicts in cyberspace jeopardise peace and justice and brainstormed what could be done to ensure the SDG 16 is realized for achieving peace, justice and strong institutions worldwide. Many recognized the need for multistakeholder cooperation at local and global levels to ensure safety and security frameworks online, as well as the role of law enforcement in executing those. Building on this, the discussion also reflected on the debate about whether the interference of public institutions in online activities is legitimate or illegitimate. In this view, the inconsistent application of the
existing international standards and laws on cyber behaviour was remarked on. The discussion also reflected on the role of non-binding norms for cyber principles that could help long-term to build a culture which supports trust and safety between public authorities and citizens. While the majority spoke about internationally agreed cyber norms and policies, several participants emphasised that these can only be effective if strong institutions are in place at the national level.

Discussion table IV

Facilitated by Mr. Wout De Natris, co-facilitator of IGF DC-ISSS and supported by the DC co-coordinator, Mr. Mark Carvel

Addressing procurement and purchasing departments that they need to order secure Internet products, devices and services and speed up the deployment of Internet standards and ICT best practices.

The discussion opened with recognition of an existing gap between the theory of the ideal standards/best practices and the daily practices related to the security of digital devices. Amongst other factors, the cause is related to the lack of international standardisation of what constitutes a safe and secure ICT product. This is closely connected with the government and private sector-led procurement processes. The discussion further developed around making procurement outlets more responsive in respect to the adoption of Internet security standards. Some participants suggested that toolkits of best practices could be developed to help build the capacity of procurement entities. Some recognized the need to focus on developing country procurement administrators, working in different departments, like education. Furthermore, many gathered around the view that the deployment of security rules and practices is moving slowly, given the fast-developing and changing digital landscape. To remedy this, all stakeholders must be part of shaping a solution, including the industry, as well as the Internet service providers as the router is a gateway for all e-devices and has its security/defensive functions. The sustainability of these processes is also dependent on the active inclusion of young people as early adopters of digital technologies.