|  |  |
| --- | --- |
|  | **Document IEG-WTPF-26-2/9** |
| **13 January 2025** |
| **English only** |
|  |  |
| Contribution by Germany and the United Kingdom of Great Britain and Northern Ireland  |
| DRAFT OPINION ON THE RESILIENCE OF TELECOMMUNICATIONS/ICTS |
| **Purpose**Draft Opinion on resilience of telecommunications/ICTs.**Action required**The Informal Expert Group on WTPF-26 is invited to **consider** this document. |

DRAFT OPINION

Resilience of telecommunication/ICTs

The seventh World Telecommunication/ICT Policy Forum (Geneva, 2026),

recalling

*a)* Resolution 70/1 of the United Nations General Assembly, on Transforming our World: the 2030 Agenda for Sustainable Development, in particular, Sustainable Development Goals 12 (Responsible Consumption and Production) and 13 (Climate Action);

*b)* UNGA Resolution 70/125, on the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society (WSIS);

*c)* Resolution 136 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on the use of telecommunications/ICTs for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief;

*d)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on strengthening the role of the ITU in building confidence and security in the use ICTs;

*e)* Resolution 182 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on the role of telecommunications/ICTs in regard to climate change and the protection of the environment;

*f)* Resolution 45 (Rev. Kigali, 2022) of the World Telecommunication Development Conference, on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam,

noting

Resilient telecommunications/information and communication technologies (ICTs) are capable of predicting, responding to, and withstanding a variety of shocks, including, but not limited to, climate-related ones, the safety of users, and of the security of critical telecommunications/ICTs infrastructure from cyber incidents, natural hazards or disasters,

taking into account

*a)* that building resilient telecommunications/ICTs capable of withstanding natural disasters or hazards, cyberthreats and non-malicious technical outages is vital at a time when accessing and delivering essential services and information depends on the Internet;

*b)* that resilience initiatives are increasingly important because climate change is contributing to a greater number of disasters which affect telecommunications/ICTs;

*c)* that the deployment of resilient telecommunications/ICTs must be accessible to historically unserved and underserved groups, as crises can exacerbate pre-existing inequalities and digital divides;

*d)* the multiple and interacting challenges of geographical digital divides when designing and deploying resilient telecommunications/ICTs in least developed countries, landlocked developing countries, and small island developing states, where limited capacity to build resilience and vulnerable locations make the impact of shocks more severe on their economies and infrastructures;

*e)* the importance of developing resilient telecommunications/ICTs that can withstand different threats, while also meeting the diverse user experiences, particularly the requirements of persons with disabilities and persons with specific needs, to ensure resilient telecommunications/ICTs are deployed equitably;

*f)* that the United Nations Committee on the Elimination of Discrimination against Women, noted in its General Recommendation No. 37 that a lack of active participation by women in programmes related to disaster risk reduction and climate resilience can impede their development and effectiveness,

considering

*a)* that resilient and secure telecommunications/ICT systems are critical in supporting business continuity, public service delivery, and access to essential services in times of crisis;

*b)* that the use of telecommunications/ICTs for sharing of information in the event of a crisis is a powerful decision-making tool for rescue and response services and operating entities, and for communication with and between individuals;

*c)* that ICTs are essential for climate resilience activities, such as monitoring climate, monitoring and protecting natural ecosystems, data gathering, rapid information transfer and managing the risks of climate change, and that resilient telecommunication networks and information technologies are essential in ensuring that communications reach people and the appropriate relief organizations;

*d)* that telecommunications/ICTs must remain secure and dependable against a spectrum of external disruptions, such as natural disasters or hazards, power cuts, and cyber incidents;

*e)* resilience should be incorporated into all stages of the design and deployment of telecommunications/ICTs to uphold durability throughout their lifecycle, to withstand changing environments, and to avoid exacerbating or threats and vulnerabilities;

*f)* the importance of iterative long-term strategies and risk management plans that coordinate the resilience of a range of telecommunications/ICTs, which make it easier to anticipate and respond to issues across contexts and address constantly evolving threats and vulnerabilities;

*g)* the need to foster public awareness of basic security measures for resilience, including cyber hygiene, and to ensure that messaging is accessible to a diverse range of users, such as Neurodivergent persons, persons with disabilities, women, and children, to protect themselves,

recognising

*a)* that resilient telecommunications/ICTs are an essential foundation for sustainable development and bridging digital divides;

*b)* the role of the private sector, civil society, the technical community, academia, and regional and international organisations in providing telecommunication/ICT equipment and services, expertise and capacity-building assistance to support resilience initiatives;

*c)* the work of the ITU in key resilience activities, such as the Early Warnings for All Initiative, Global Initiative on Resilience to Natural Hazards through AI Solutions, the Climate Risk and Early Warning Systems initiative, the ITU regional cyberDrills, and the International Advisory Body for Submarine Cable Resilience;

*d)* the work of the study groups of the ITU’s Radiocommunication Sector (ITU-R) in particular, Study Group 1 and Study Group 3, in adopting recommendations that provide technical information on satellite and terrestrial radiocommunication systems and wired networks and their role in disaster management, including important recommendations pertaining to the use of satellite networks in times of disasters;

*e)* the work of the ITU’s Telecommunication Standardisation Sector (ITU-T) study groups in developing and adopting relevant recommendations on issues such as climate change and the resilience of service provision (Study Group 2), the resilience of ICTs (Study Group 5), and the resilience of networks to attacks (Study Group 17);

*f)* the activities carried out in the ITU’s Telecommunication Development Sector (ITUD), including Study Group 1 under study Question 3/1, on the use of telecommunications/ICTs for disaster risk reduction and management, and Study Group 2 with respect to sustainable development of ICTs,

is of the view

1 that resilience initiatives should be multi-facetted encompassing cybersecurity, early warnings systems and early action, climate monitoring, disaster risk reduction initiatives;

2 that enhancing resilience across society necessitates that different stakeholders work together, including local and national governments, the private sector, civil society, the technical community, and academia;

3 that it is essential to build resilience into all stages of telecommunications/ICTs design, development and deployment;

4 that bridging the digital divide and ensuring affordable access to telecommunications/ICTs is integral to building resilience;

5 that a multi-channel approach to public-awareness raising should be adopted to ensure relevant resilience messaging, such as emergency communications and cyber hygiene-related advice, reaches a wide audience and enables individuals to act earlier and protect themselves;

6 that climate change represents one of the greatest challenges of our time, and resilience to its impact can be strengthened through the establishment of early-warning systems for emergency situations and national emergency telecommunication plans;

7 that building cyber resilience across society is essential to tackling the growing cyber threat;

8 the ITU should continue to conduct training programmes, workshops, and capacity building to promote resilience,

invites Member States

1 to develop and implement policies that promote resilient, secure, and inclusive telecommunications/ICT infrastructures, ensuring alignment with international standards and best practices;

2 to mainstream a gender perspective into national strategies dealing with resilience and ensure that decision-making is inclusive;

3 to work with the private sector, civil society, the technical community, and academia to promote resilient telecommunications/ICTs by providing programmes of technical support and advice to people, organisations, and businesses;

4 to adopt relevant ITU recommendations that could contribute to the building of resilience and effective response to crises;

5 to continue to deploy all necessary efforts to integrate cyber incident response, disaster risk reduction, disaster mitigation, disaster relief and resilience into telecommunication/ICT development plans, considering the specific needs of persons with disabilities, children, older persons, women and girls, displaced persons and the illiterate, and the importance of collaborating with all stakeholders in all disaster phases;

6 to support international activities to promote capacity building for resilience, especially for Least Developed Countries, Landlocked Developing Countries, and Small Island Developing,

invites the Secretary-General

to continue to facilitate and enhance international efforts to strengthen frameworks and promote the resilience of telecommunications/ICT systems.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_