"The biggest challenge that we face today with respect to the use of ICTs is one that we heard this morning and throughout the day – the need to ensure greater access and getting the unconnected online, primarily through mobile devices. By 2020, the mobile industry will have invested over $1.4 trillion US dollars to ensure that there is 4.6 billion unique mobile subscriptions also by the year 2020.

But in order to ensure that those who are currently connected can remain connected and those that are unconnected get online, it is up to all stakeholders to build confidence, trust and security in the use of ICTs and, in particular, in the use of mobile Internet access – the way most people will access the Internet today. It is because of this mobile industry plays and unique role in the first line of defence for issues that may hamper or impede access.

The mobile industry believes in the four following points on Internet governance and cybersecurity:
1. Maintaining an open Internet that is safe, secure, stable, trustworthy and interoperable;
2. Continuing the decentralised development of the Internet which is not controlled by any particular business model or regulatory approach;
3. Encouraging collaborative, diverse and inclusive models for Internet governance decision-making that enable participation by the appropriate stakeholders; and
4. Promoting the globalisation of key Internet governance functions in a transparent way that preserves the resiliency, security and stability of the Internet.

In the context of the WSIS+10 review and the Zero draft paper, it is rightly noted that governments, businesses, civil society and all other stakeholders play an integral role in building confidence and security. The capacity building that the mobile industry undertakes currently is done in conjunction with governments, international organisations and civil society in order to ensure consumer awareness, develop technical skills and infrastructure management and collaborate with law enforcement nationally and internationally in order to fight criminal use of ICTs and the Internet. The GSMA's recent launch of 'We Care in Bolivia' for consumer safety or the Mobile Alliance against Child Sexual Abuse content are just some examples among many which governments and all organisations in this room identify and participate. Capacity building is, perhaps, the most important aspect of ensuring trust and confidence through the empowerment of the user as well as collaborative work to address the technical and criminal issues online.

It is important to respect the sovereignty of nation states when it comes to national security and national issues, but cybersecurity in ICTs knows no national boundaries. Fortunately there are international frameworks for addressing cybersecurity issues including the Budapest Convention, the UN Charter in building confidence and security in the use of ICT and, most recently, the UN Report of Experts. These frameworks set out norms, rules and principles for responsible behaviour by individuals and states, collaboration among those states and but also ensure human rights, privacy, and freedom of expression. The annual Global Conference on Cyberspace, through the London process, as well as the annual Internet conference in China, among others, offer a place to discuss cybersecurity issues in an ongoing way. New calls for international cybersecurity legal frameworks must acknowledge the current frameworks and legal instruments in place and not be purely political in its agenda.

In closing building trust and confidence in ICTs – and in particularly through mobile access as how most of the world will gain access – is the role of all stakeholders from governments to the private sector to civil society. We are all responsible, in our technical, societal, and national security roles, for ensuring trust and confidence in ICTs.

Thank you and I look forward to our discussion."