Key questions:
– How vulnerable is the system that is at the base of every service, transaction, communication and exchange required for the steady functioning of the global economy and individual well-being?
– Is there a real risk? From who? What? What are the most vulnerable targets?
– Did we learn from Estonia?
– How are international multilateral cooperative mechanisms evolving?
– What gaps still need to be filled?

Summary of debate

The Cyber-security portion of the ITU Telecom Forum, World 2009 was launched with a high-level plenary session looking at the urgent need for effective global partnerships to fight cyber-threats.

One of the key challenges identified is that while cyber-criminals make a lot of money from their illegal activities they face minimal risk of legal consequences. Unfortunately, the internet network on which the global community depends daily is highly insecure. Mr Kaspersky, CEO and Founder, Kaspersky Lab, Russia, stated that there needs to be serious regulation of internet safety not only cooperative mechanisms. This new "Internet country" in which we all live requires a new criminal, regulatory and legal system. Mr Solari, Alcatel-Lucent agreed that the financial losses, numbering in the 100s of billions USD, are staggering. Software companies continue to bring technology to market replete with vulnerabilities and consumers, at all levels, continue to buy security technology software after the fact; making us reactive instead of pro-active. There is an urgent need to create the right incentives and responsibility starts with the industry. The responsibility and accountability lie with the engineers who develop the technology and software. Mr Solari's new book, "Security by Design", advocates integrating security into the original design of a given product to avoid the continuously reactive approach to cyber-threats.