2. An unrealistic expectation that the end-user is able, willing or aware enough to be responsible for the security of his/her own PC/Mac computer or mobile device, and therefore also of the network (e.g. botnets).

3. Divergent legal systems and laws relating to cyber-crime and cyber-security; some countries have no laws relating to cyber-crime or cyber-security legislation while others have relatively advanced cyber-security frameworks. There will always be the challenge of dual criminality issues between legal systems but without, at a minimum, an international framework to “track and trace”, there is little hope of catching the criminals.

4. Virtually no consequences / sanctions impunity for cyber-criminals due to the difficulties inherent in implementing legal procedures within national borders for a crime committed in a borderless world (the internet). This is made particularly difficult when many countries do not have legislation in place that even recognizes cyber-crime as a crime.

5. The inability of some governments to cooperate fully due to national security priorities.

6. The lack of reporting and monitoring of cyber-crimes, malware and fraud on-line.

7. The challenge of balancing increased security with the principles of the Internet, which have made it such a success: freedom, chaos, a hotbed of new ideas….

8. The challenge for developing countries to finance necessary cyber-security measures; without which the global system remains highly insecure.

It was therefore noted that that there is an urgent need for a common global cyber-security platform integrating all stakeholders including national governments, industry, CERTs, ISPs, Domain Name Registrars, ICANN, law enforcement, justice ministries, Interpol, Financial Action Task Force (FATF), Telcos, etc.