The “cyber-crime law” is part of the ITU Toolkit provided to countries, in line with the ITU’s mandate and responsibility to implement Action line C5 of the Geneva Action Plan of the World Summit on the Information Society. Continued multilateral discussions are needed to create global stability.

Mr de Sa stressed that the weakest link of cyber-security is the ISP; most services are “buggy” and extremely easy to hack. The Sans Institute recently issued a report stating that “most products that are developed to secure are vulnerable”. The technological component of security requires urgent attention; how to figure out the right incentives to create safer software and applications?

Mr Patel recommended the creation of a global international police agency, modeled along the IAEA, to minimize threat and risk level.

There was a general consensus on the need to make security measurable and to create an international structure through which it would be possible to actually catch the “bad guys”. At the moment the criminals are winning. Special agencies are needed at the national level in addition to CERTs, which only address the internet; “national security centers for IP based public networks”.

The ISO certificates for cyber-security were deemed useless for the private sector as anyone can hack into an SSL.

In terms of actually locating the criminal, there was a debate as to whether we can’t find him/her or whether due to the lack of national and international legislation/cooperation, arrests are virtually unheard of. “Estonia couldn’t pinpoint Russia in the attack because Russia didn’t pick up the phone”.

Tracking and tracing cooperation is essential to increase the moral pressure to act. Without an international framework there is no requirement to track and trace.