09 Cyber Security: A Fundamental Right
Breakout Session

Freddy Dezeure (Head of CERT-EU)
Isao Echizen (National Institute of Informatics, Tokyo)
Lokke Moerel (Tilburg University, The Netherlands)
Günther Müller (University of Freiburg, Germany)
Reinhard Posch (Graz University of Technology; CIO of the Austrian Federal Government)
Bart Preneel (University of Leuven, Belgium)
A Min Tjoa (TU Wien, Austria)
Edgar Weippl (TU Wien & SBA Research, Austria)

The fact that cyber security has become important is evident. In this breakout session the panelists explored whether cyber security is an essential fundamental right for the society we now live in. Fitting to Alpbach's general topic of the age of (new) enlightenment, privacy and security may be the very foundations of a democratic society in the 21st century.

The panelists addressed:

(1) *European values*: Many technology companies are based in the US or Asia and tend to enforce their societies' privacy principles. Having more global European IT companies would make it easier for Europe's privacy rules to become a global standard.
There was a vivid discussion on whether European countries really embrace Europe's "privacy principles"? There was a common understanding that the US expectation of privacy is more aligned with company needs. Bart Preneel summed up the problem "Even if European companies build security technology, American companies buy it and destroy or modify it" (e.g. Skype).

(2) *Political changes*: Today, free expression creates many digital traces when data is being transmitted and stored. With powerful tools such as sentiment analysis and network analysis, governments or groups of malicious people have a much greater opportunity to quickly identify potential opponents and people with dissenting opinions.

(3) Reinhard Posch highlighted a dilemma: The government needs laws to act, whereas companies are allowed to do everything unless forbidden. The challenge is to close that gap.

There was a heated discussion whether and to what extent it is the governments' responsibility to protect privacy or whether it is each individual's discretion to decide the level of protection. Bart Preneel advocated a move from cloud-based big data storage to small local data so that data can stay with users, to build decentral and open Internet solutions to give back users the control of their data.

The threats we are facing in the IoT (Internet of Things) when it comes to privacy and security questions were pointed out by several panelists. "Technology is available, but the awareness is lacking", Reinhard Posch said. "We are rolling out the IoT without having ensured cyber security and are creating a problem for the future generationany protection", summarized Lokke Moerel.

In the concluding remarks all panelists summed up the key points that we need to address:
- We have to be optimistic and believe that we can do better in protecting our core values such as fundamental privacy rights.
- Education is key. Keeping knowledge and IPRs in Europe is essential. Security sensitive hardware and software production facilities should remain in Europe.
- It may prove a competitive advantage if companies comply with European privacy and security requirements. These companies benefit from a stable political and predictable legal environment.
- Education should encompass computational thinking starting at a very early age in primary school. It should include ethics and responsibility contributing to our societies' enlightenment.