- *Which specific challenges need to be tackled by EU action in the coming five years regarding international crime, radicalisation and terrorism, cybercrime and cyber-attacks, natural and man-made disasters? What role should the border security have in addressing those challenges*

As the use of telecommunications technologies in everyday life has become more and more ubiquitous, the opportunities for individuals to leverage technology for criminal purposes are become more frequent. Moreover, the increasing connectedness of the technology makes it easier for large scale, organised, criminal activity across international borders to take place. Domestic homes, motor vehicles and government supplied services are all deploying integrated telecommunications technologies that will transform the way in which ordinary citizens manage their lives. As an example, Apple HomeKit will transform an ordinary home into a 'smart' home that has highly advanced automatic systems for lighting, temperature control, multi-media, security, window and door operations, and many other functions; while BMW ConnectedDrive will effectively turn a motor vehicle into a mobile computer, allowing the driver to control the car from their phone, and set the car for automatic steering, braking and acceleration. The advantages for the user are that they can manage their energy usage; control costs; secure their homes and drive more safely. The real risks are that criminal gangs could access and control the technology, using it for a range of nefarious purposes. The objective of the crime could be terrorism; extortion; radicalism; or something else. What is common across the criminal range is that internet technology is being used to commit the act. Terrorism becomes a cybercrime; radicalism becomes a cybercrime, and so on. Therefore the expectation should be that telecommunications technology will play a larger and larger role in future criminal activity, with old crimes being perpetrated using new technology.

- *Taking into account the developments in the next five years, which are the actions to be launched at the EU level?*

Develop actions that support capacity building of law enforcement agencies to tackle not only cybercrime, but also cyber-enabled crime. Also explore methods through which industry could be encouraged to build security into new telecommunications products and services. Security-by-design will become an essential weapon in fight against technology enabled crime.

- *Which specific research, technology and innovation initiatives are needed to strengthen the EU´s capabilities to address security challenges?*

Extend the digital forensics research areas beyond the traditional modes of cybercrime activity, into other domains. For example, vehicle forensics – where data can be captured and analysed from computerized components found in motor vehicles. For example, extracted data can show how and where a vehicle was used. This information can be triangulated against mobile phone data to match an individual to a vehicle. Tools for the extraction and analysis of motor vehicle data would assist law enforcement in building strong prosecution cases against any crime where a motor vehicle has been involved.

What is needed to safeguard rights of European citizens when developing future EU security actions?

The key area is to ensure that personal data is safeguarded. Currently most European citizens are woefully unaware of when and why personal information about them is gathered and collated. Industry in particular use a range of questionable practices to obtain information that may support profitability. Any EU actions should be proactive in ensuring and respecting the rights of the citizen to maintain control over their personal information.