

12	Cybercrime training strategies and curriculum building for law enforcement and criminal justice authorities
Room 3	Thursday, 18 October 2018, 9h30-13h00
<u>Background</u>: With the pervasive use of information technology in everyday life of general public, the day-to-day tasks of any law enforcement or judiciary officers may include components of electronic evidence and Internet investigations. The knowledge and skills on IT investigation is required not only for the members of cybercrime units, but also for any other officers in other branches of the law enforcement agencies. However, such courses are seldom taught in training institutions of the LEA. <u>Purpose</u>: What are the knowledge and skills that LE needs? Does patrol officers need to know what IP address is, or how to deal with mobile phones? Can we train the existing officers, or do we need to recruit technical officers? Through this workshop, we aim to (1) identify the need and challenges in training, (2) present models of training development, and (3) discuss how to develop and deliver sustainable training for the law enforcement officers. <u>Chair</u>: Takayuki OKU, Director of Cybercrime Directorate, INTERPOL <u>Rapporteur</u>: Dong Uk KIM, Project Manager – Cybercrime Directorate, INTERPOL <u>Panel</u>: ► Cybercrime Training Needs and Challenges [40 mins] - Country Situation Reports [Botswana, Nigeria] - Challenges in Developing Training [INTERPOL] - Discussions ► Cybercrime Training Strategy: a Survey [40 mins] - Current Situations and Challenges - Strategies for Cybercrime Training for LE - Questionnaires to be prepared, collected by INTERPOL ► Building the Future Opportunities [40 mins] - CERT's role in cybercrime training [Nigeria] - Progress Report on Judicial Training [Council of Europe] - Developing Standard Cybercrime Curriculum [INTERPOL] ► Discussions : How to enhance international cooperation in Africa [40 mins] - Panel discussion	
Reference materials	