Good morning Ladies and Gentlemen,

I am Heung Youl Youm, Chairman of Study Group 17.

I thank Dr. Reinhard Scholl, Deputy Director, TSB, for his kind remark for this ITU workshop on Artificial Intelligence, Machine Learning and security.

It is a pleasure to add my welcome to you to this ITU workshop. This is the fifth workshop organized by SG17 in this 2017-2020 study period and follows the successful workshop in August 2018 on Advanced Cybersecurity Attacks and Ransomware.

SG17 is the ITU-T's core competency center on security, attracting security experts across the world. SG17's work is responsible for building confidence and security in the use of information and communication technologies (ICTs).

Intelligent and targeted cyber-attacks are occurring across borders, and are aimed at our real lives and important cyber assets, including critical information infrastructures. ITU-T SG17 will lead comprehensive efforts to provide various technical controls to address such intelligent and targeted cyber-attacks.

ITU-T SG17 has been very active in developing high quality technical Recommendations which are implementable by industries. SG17 is also active in adopting important specifications prepared by other organizations such as two FIDO Alliance's Specifications that are now Recommendations ITU-T X.1277 (FIDO Universal Authentication Framework (UAF)) and X.1278 (Client to Authenticator Protocol/Universal 2-factor framework). I think they will be widely used in many industry sectors, including the financial sector.

I strongly believe that this adoption provides clear evidence of our wiliness to cooperate with other groups to develop the high quality technical standards, and to increase our role of a global competence center in security.

Artificial Intelligence (AI) and Machine Learning (ML) technologies are advancing at a remarkable speed and lead to many widely beneficial applications, ranging from machine translation to medical image analysis. In addition, AI and ML technologies can contribute to improving the cyber defense capability to protect the evolving cyber threats. But the ubiquitous use of AI and ML empowered applications also increase cybersecurity challenges.

Thus, this workshop will focus on two aspects: identifying how AI and ML technologies can be used to prevent the cyber-attacks, and what are security and privacy risks of AI and ML applications.

The workshop responds in particular to the increasing demands from industries for utilizing AI and ML technologies in such a way that security analysts will become more effective and accurate in their detection of security threats and related decision-making.

The findings of the workshop will feed into ITU's standardization expert group responsible for 'building confidence and security in the use of ICTs', ITU-T Study Group 17, which meets immediately following this workshop from 22 to 30 January 2019. ITU-T SG 17 will continue to address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs, taking into account new emerging ICT technologies such as AI and ML, by developing global standards.

To close my remarks, I express my sincere gratitude to the steering committee members of this ITU

workshop on Artificial Intelligence, Machine Learning and security.

I also express special thanks to the TSB for their outstanding efforts in supporting and implementing this timely workshop.

I'd also thank our all the distinguish speakers, panelists and session moderators for your support and outstanding work.

I wish all of us an insightful and productive discussion, with ideas that will lead to new implementable security standards for cybersecurity.

Thank you.

21 January, 2019, Geneva