**Summary of Session 5: Security, privacy and trust​**

Session 5: Security, privacy and trust of the SGLA was held at 14:00-16:00, 10 Sept 2019 to discuss and distinguish the interrelated concepts of ‘security’, ‘privacy’ and ‘trust’, review ongoing activities in ITU-T SGs and discuss future strategic directions of ITU-T standardization on these important areas, especially focused on how to ‘architect’ ITU-T security standardization and cooperate/collaborate internally/externally.

**Mr. Arnaud Taddei,** WP3/17 Chairman**,** pointed out that the fundamental difficulty in cybersecurity standardization is that different stakeholders have different understanding, interests and talking confusing languages with cultural misalignment.

5G will bring in billions of virtual machines, containers, players and complex implementation of complicated systems, lead to increased attack surface. Latest protocols to enhance endpoint privacy (e.g, TLS 1.3, QUIC, DNS over HTTPS) brought new challenges to network defence. All such fragmented advances lead to ever-growing security issues that we lack of resource and skills to fight. Cybersecurity becomes a ‘Frankenstein’ – a giant issue we created by ourselves.

He drew cybersecurity as analogue to public health issue. SG17 just started to define Cyber Defence Centers (Security Operation Center, Computer Emergence Response Team, etc.) at ITU (X.framcdc), aka ‘Centers for Disease Control and Prevention’ (CDC) in health sector, which have been established since 1940s.

Finally on ITU-T security standardization, he proposed a fundamental revisit on how we ‘architect’ the interactions between ITU-T SGs and FGs regarding security, and change the current “Security by Design” doctrine into a real integrated end-to-end approach.

Responding to how to move from framework/requirements/architecture to implementable technical solutions, Mr Taddei’s experience is to remind editors that security principles should also apply to ‘adds-on’ security control system and always take into consideration of composition need of this additional security component into the subject’s architecture.

Regarding how ITU-T should organize standardization work of overlapping area like ‘security of subject X’, SG17 beliefs it should be done in a place that could bring together knowledge of both ‘subject X’ and security. SG17 as a center of excellence in ITU-T with security expertise is working in collaboration with many other groups in various subjects and benefits ‘subject X’ experts with security principles and disciplines.

**Mr Heung Youl Youm,** ITU-T SG17 Chairman, introduced SG17 mandate, current structure and a 5G security overview of threats to unified access, RAN and core network. SG17 organized a workshop on 5G security in March 2018, which called for SG17 to collaborate and coordinate with relevant groups (esp. 3GPP SA3) and participate in JCA on IMT2020. Ever since then SG17 started five 5G security work items in Q6/17.

Regarding ITU-T strategic directions on 5G security, Mr Youm suggested to:

* utilize ITU-T SG17 as a security competence centre.
* establish a JCA-5G security inviting 3GPP and ETSI,
* collocate meeting with other groups.
* develop a 5G security standardization roadmap and identify roles and responsibility of each group.

**Ms Xiaojie Zhu,** ITU-T SG11 Vice-chairman, talked about security issues in SS7. SG11 has revised SS7 related standards Q.731.3, Q.731.4, Q.731.5 and Q.731.6 in April 2019 and continues to work on:

* ITU-T Q.SR-Trust: Signaling requirements and architecture for interconnection between trustable network entities
* Technical Report ITU-T TR-SS7-DFS: SS7 vulnerabilities and mitigation measures for digital financial services transactions

SG11 is organizing an ITU Workshop on Brainstorming session on SS7 vulnerabilities and the impact on different industries including digital financial services” in Geneva on 22 October 2019 to promote the implementation of revised ITU-T Q.731.3, Q.731.4, Q.731.5 and Q.731.6. Ms Zhu called for more input to promote implementation of revised SS7 protocal standards.

**Mr Gyu Myoung Lee,** WP3/13 co-chair, talked about ITU-T SG13 work on trust in data and AI, clarified that trust is about relationship and more people-centric than security.

SG13 Q16/13 (Knowledge-centric trustworthy networking and services) has developed ITU-T Recommendations on basic principles, overview of trust provisioning in trusted environment in ICT infrastructure, and framework of trust-based media services, and is developing more standards on trust of service provisioning and personal data management.

He also mentioned that IEEE and ISO/IEC are working on trustworthiness of AI, and recognized that SG17 work on security and SG20 work on ‘Security, privacy, trust and identification for IoT and SC&C’ are relevant. Mr. Lee called for more understanding and consideration from all ITU groups on trust, both its technical and non-technical aspects and proposed ITU-T to focus and create a new group for Trust in Data and AI.

**Bret Jordan,** Chairman of both OASIS CTI TC subcommittees STIX and TAXII, pointed out that network security has been traditionally inward focused, based on a fallacy that we can know and/or fix all vulnerabilities. However, inward focus (hygiene) is necessary but inadequate, since security operations, procedures and policies are slow, manual, reactive, understaffed and underfunded.

He introduced OASIS work on STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Intelligence Information), CACAO (Collaborative Automated Course of Action Operations for Cyber Security) toward automated playbook for cyber defence, and concluded that herd immunity is only possible when we share cybersecurity threat intelligence in an automated machine-to-machine structured format.

Regarding ITU-T work on security standardization, Mr Jordan reiterated the CTO meeting’s call for global coordination across SDOS, and suggested ITU to take a more active role to standardize solutions that enable cyber defense and threat intelligence and playbook sharing.