Regional Dialogue for the Asia-Pacific (ASP)

Securing Critical National Infrastructure

16 September 2020, 14:00 – 16:00 (Bangkok)

Atsuko Okuda

Regional Director, ITU Regional Office for Asia-Pacific

Thank you for joining us today at this "Regional Dialogue for the Asia-Pacific (ASP) Securing Critical National Infrastructure". I believe that we could not have chosen a more relevant topic for the region, which is coping with the enormous challenges of the unprecedented health emergency, while at the same time undergoing rapid digitization of economies.

Before I begin, let me take a moment to thank Mr. Alexandru CACIULOIU from UNODC for the continued support, in particular sharing with us insights on the role of law enforcement in protecting critical infrastructure as well as legislation and international cooperation. I also take this opportunity to thank Mr. Paul Wilson, Director General, Asia-Pacific Network Information Center (APNIC), which is an essential ITU partner in designing and implementing CIRTs in the Asia-Pacific region.

Likewise, I also wish to welcome Mr. Carsten Rudolph, Associate Professor and Research Director of the Oceania Cyber Security Centre (OCSC) who partnered with ITU in conducting the review for the Cybersecurity Capacity Maturity Model for Nations (CMM) along with the CIRT assessment in Pacific Island countries, among others. I am delighted to welcome Jeneral Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed, from Malaysia who is representing as Chair for Asia-Pacific CERT and brings with him invaluable insights and experience to help create a safe cyber space in Asia and the Pacific through global collaboration.

Let me now turn to the topic of the Regional Dialogue. The ITU's most populous region, Asia and the Pacific is growing digitally, with increased reliance on digital payment, healthcare, commerce, trade, work, and educational solutions just to name a few. As a result, cybersecurity is more important than ever. As the coronavirus pandemic continues to disrupt essential social and economic functions, the risk of cyber threats has increased due to our increased reliance on digital tools and platforms.

Critical infrastructure is the foundation on which daily, and vital, societal and economic functions depend. The disruption or loss to any elements of the critical infrastructure has the potential to severely impact our lives, especially during pandemic times when most of the personal as well as professional work is carried out online. Working together and sharing good practices, approaches, and experiences will help promote and enhance national – and global – critical infrastructure security today, and in the future. Policies related to digital security risk to essential services tend to be anchored in both digital security strategies and national risk management frameworks. This is partly the consequence of widespread adoption of a whole-of-government approach in setting

policies for the protection of essential services against digital security risk across countries.

Effective mechanisms and institutional structures at the national level are necessary to deal with cyber threats and incidents. In this context, the National Computer Incident Response Teams (CIRT) plays an important role in the solution. ITU is working with Member States to build the necessary capacity at national and regional levels, deploy capabilities, and assist in establishing and enhancing CIRTs. To date, ITU has completed CIRT assessments in 76 countries and established or enhanced CIRT in 14 countries. After the CIRT assessment, ITU assists with planning, implementation, and operation of the CIRT. ITU's continued collaboration with the newly established CIRT ensures that support remains available, and institutions can be further enhanced.

ITU also carries out CyberDrills, in-person and online training for cooperation, information sharing, and discussions on current cybersecurity issues, and provides hands-on exercise for national CIRTs.

As part of the Cyber Drill 2020, this Regional Dialogue provides a unique platform for leaders from the Asia-Pacific cybersecurity ecosystem to share their experience in addressing cybersecurity issues such as incident response capabilities, latest tools and strategies to mitigate online threats in protecting critical national infrastructure. This Regional Dialogue will also discuss the implications of COVID-19 on cybersecurity at the regional and national levels.

Through a good information-sharing platform, such as this, and concerted efforts among all of us, I believe that cyber incidents can be minimised, prevented, and mitigated faster. Cybersecurity and the protection of CNI are the foundation to build back better from the COVID-19 pandemics and ensure inclusive and sustainable digital transformation in a safe and secure digital environment.

I look forward to a lively and illuminating Dialogue today. Thank you.