EU opening remarks

- Undersecretary Erickson Balmes, Department of Justice (DoJ), Philippines,
- Court Administrator Jose Midas Marquez, Supreme Court (SC), Philippines,
- Honourable Secretary of State of Cambodia, Mr. Sieng Lapresse,
- Ms. Kaori Ambo, International Safety and Security Cooperation Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan,
- Dear Alexander Seger, Executive Secretary of the Cybercrime Convention Committee and Head of the Cybercrime Division at the Council of Europe,
- Distinguished partners and participants from South-East Asia,

Good morning,

On behalf of the Delegation of the European Union to the Philippines, I am delighted to have the opportunity to welcome you at this Regional Conference on Cybercrime with a particular focus on criminal justice access to evidence in the cloud.

I wish to extend our gratitude to the Philippine Department of Justice for their leading role in this effort, and of course to the Council of Europe as our long-standing partner in various joint programmes with the European Union in the fight against cybercrime, including the Global Action on Cybercrime extended (GLACY+) project that since 2013 has been the leading global programme in supporting partner countries in Asia, Africa and most recently also Latin America, enhancing their capacities in addressing cybercrime and cooperating at international level.

We are all gathered here today at the backdrop of a digital revolution. While it offers so many empowering opportunities and development venues to achieve a better future, it also comes hand-in-hand with serious potential vulnerabilities as

cyber space has created a new dimension for criminal actors to operate. In the past decades, cybercrime has evolved as one of the greatest challenges for criminal justice across different jurisdictions.

The current scale, nature and impact of cybercrime are such that they do not only undermine confidence and trust in ICT, but also represent a serious threat to the fundamental rights of individuals, to the rule of law in cyberspace and to democratic societies.

Even traditional crime is not the same anymore in the age of technology. Europol's recent Serious and Organised Crime Threat Assessment (March 2017) highlights how criminals quickly adopt and integrate new technologies into their modi operandi or build brand-new business models around them with great skill and to great effect.

Governments all over the world are not only struggling with increasing levels of cybercrime, but also trying to address the complexities of securing electronic evidence for any type of crime. The puzzle for criminal justice authorities is further complicated for electronic evidence that is stored in servers in foreign, multiple or unknown jurisdictions – the formidable "cloud".

Clearly, the rule of law is jeopardised if only a small portion of cybercrime and other offences entailing electronic evidence is investigated and adjudicated, while states risk failing systematically in their positive obligation to protect the rights of individuals and society against crime. From an economic perspective, the cost entailed undermines gravely human development opportunities.

In this context, we see that the traditional law enforcement mechanisms are often rendered ineffective, and we all recognise the need to find ways to secure

and obtain electronic evidence more quickly and effectively by intensifying cooperation amongst countries globally and with service providers.

In the EU, the development of a common EU approach on improving criminal justice in cyberspace is treated as a matter of priority and is currently pursued in a way which is consistent with the work under way by the Cybercrime Convention Committee of the Council of Europe, which is the global framework of reference both for the development of comprehensive national legislation as well as for international cooperation.

To address these challenges, we can identify three main strands of work:

- Enhance cooperation with service providers.
- Streamline mutual legal assistance (MLA) proceedings.
- Review rules on enforcement jurisdiction in cyberspace.

It goes without saying that these should be guided by the principles of necessity and proportionality, while a balance must be struck vis-à-vis fundamental rights and data protection that have to be fully respected in the framework of any practical solution towards improving the enforcement of the rule of law in cyberspace and obtaining e-evidence in criminal proceedings.

Enhanced and effective modalities of cooperation with the private sector and service providers in particular is a sine qua non in this field.

Considering the ongoing efforts of many actors in this area, including the Parties to the Budapest Convention and the European Union, it is very topical to use this opportunity to share updates and expertise with partners here in South-East Asia, with international organisations active in this field and, of course, with the private sector, also taking into account the specificities of the cybercrime threat in this region.

I would like to conclude by pointing out that the EU strongly believes that we need to work together across borders and across society. It is for this reason also that we invest in international cyber cooperation. That is why in parallel to EU's efforts in addressing cybercrime and cybersecurity internally, we engage with partner countries in capacity building programmes, with increased funds since the adoption of the EU Cybersecurity Strategy in 2013, through a holistic and programmatic model. The Council of Europe, and Alexander Seger in particular, is a strategic partner in our endeavour to support third countries enhancing their capacities in the fight against cybercrime through a number of joint programmes, including GLACY+.

Following its GLACY, GLACY+ is designed as a global facility:

- to provide support for the development of cybercrime legislation compliant with international standards and principles, as prescribed in the Budapest Convention,
- as well as to enhance the capacities of law enforcement and the judiciary in investigating, adjudicating and prosecuting cybercrime.
- But, at its core, GLACY+ is also a facility for promoting effective triangular and international cooperation.

For this reason we consider that initiatives such as this of the Philippine Department of Justice are essential for sharing knowledge and promoting a harmonised approach in our response. In this spirit, let me wish you, on behalf of the Delegation of the European Union to the Philippines, a very fruitful and constructive discussion during this regional conference with concrete ideas for enhanced cooperation in our way forward. Thank you.

Contact: Nayia BARMPALIOU, European Commission - OC, Drugs, Cyber
Slightly adjusted by Robert FRANK, Delegation of the European Union to the Philippines