# REGIONAL CONFERENCE ON CYBERCRIME 2017

Enhancing regional and international cooperation
to improve the rule of law in cyberspace

27 – 29 June 2017
Cebu City, Philippines

organised by the Philippine Department of Justice
in cooperation with the Council of Europe under the GLACY+ project

## Opening remarks
Alexander Seger, Head of Cybercrime Division, Council of Europe

Excellencies, ladies and gentlemen, dear friends,

Welcome on behalf of the Council of Europe. I would like to thank the Office on Cybercrime of the Department of Justice for taking the initiative to hold this conference here in Cebu; and in this connection to congratulate the Government of the Philippines to the presidency of ASEAN this year.

We are supporting this conference under the GLACY+ joint project with the European Union on Global Action on Cybercrime Extended.

Ten years ago, in 2007, I visited the Philippines for the first time when we started to discuss legislation on cybercrime which then became the Cybercrime Prevention Act 2012.

This is a good moment to reflect on developments over the last ten years.

In 2007, some 10% of people of the Asia and Pacific region used the Internet. Now it is more than 40%. This has brought tremendous opportunities for social and economic development. It also brought risks in terms of cybercrime.

In 2007, Sri Lanka and Thailand had just adopted their cybercrime laws. It will be interesting to hear about their experience since then.

In 2007, Estonia was the target of a major cyberattack. That was a wake-up call for governments around the world to beef up their cyber security. Many of them have since adopted cyber security strategies and other measures. There are now millions of attacks every single day but in the vast majority of situations defences hold and attacks are not successful.

The attack on Estonia also stressed the need for international cooperation on cybercrime, and more countries began to join the Budapest Convention on Cybercrime. In the beginning of 2007, 18 countries were Parties to the Budapest Convention. The USA became a party on 1 January 2007. Now in 2017, three times more, that is, 55 States are Parties. From the Asia/Pacific region, Australia, Japan, Sri Lanka and a few weeks ago also Tonga joined this treaty.

Ten years ago already, information technologies and cybercrime were linked to many aspects of our lives and our societies. Now, in 2017, we realise that information technologies affect, if not determine, many –

and soon most – aspects of our lives. The recent Wannacry ransomware that paralysed hospitals and other services around the world is just another illustration.

Looking at the grand picture, we realise that cybercrime affects not just some aspects but core values of societies:

- Cybercrime affects human rights.
  - Hacking into computers and the theft of hundreds of millions of user data are attacks against the right to private life. Denial of service and other attacks against civil society organisations and media are attacks against the freedom of expression.
  - On the other hand, the bulk collection of data and mass surveillance by governments or blocking access to websites also affects fundamental rights.

- Cybercrime affects democracy.
  - Countries increasingly experience the hacking of computers of parliamentarians and other politicians or of electoral systems. Information obtained illegally may then be used for targeted misinformation, for discrediting candidates in elections or for producing and disseminating fake news. This undermines trust in the functioning of democracy and in the outcome of elections. The Secretary General of the Council of Europe has pointed this out in his recent "report on the state of democracy, human rights and the rule of law in Europe". His report focuses on populism as a threat to democracy.
  - On the other hand, we also see governments using crime as pretext to close down critical media and civil society organisations or prosecute journalists or members of the opposition with adverse consequences for democracy.

- Cybercrime affects the rule of law.
  - Governments do have a positive obligation to protect society and individuals against crime. If only a very small fraction of cybercriminals is identified and brought to justice, this will undermine trust in the rule of law. In most countries, less than 1%, or rather 0.1%, of cybercrime cases reported to police, end up in criminal convictions. More effective criminal justice action on cybercrime is needed, therefore.
  - However, coercive measures – such as the search and seizure of computers, or the interception of communications and data – interfere with the rights of individuals. Such measures are only allowed if clearly and precisely prescribed by law and if such law enforcement powers are subject to safeguards. We need to discuss this in more detail in the course of this conference.
  - Unfortunately, we see in some countries, not only in Asia but also in Europe, that data collected by intelligence services outside criminal procedure law and without judicial supervision, are then used as evidence in courts. This is not compatible with rule of law requirements.
  - To underline once more: criminal justice authorities need the power to secure evidence on computers. Such powers are foreseen in the Budapest Convention in Articles 16 to 21. These Articles should be transposed into domestic criminal procedure law and be subject to conditions and safeguards as prescribed in Article 15 Budapest Convention.

What does all of this mean for this conference?

1. Cybercrime and electronic evidence are highly relevant challenges. They are no isolated, peripheral matters. They affect all aspects of our lives and core values of societies. This is also true for the solutions, for the responses to these issues. If we go wrong, we will make matters worse and further erode human rights, democracy and the rule of law.

2. We need intelligent, smart solutions to complex problems. Simple, populist solutions will not work. There is no silver bullet to do away with cybercrime – as one cannot get rid of crime through bullets anyway.

   For example, we will discuss in detail in this conference on how to secure evidence in the cloud for criminal justice purposes. Electronic evidence that may be stored on servers in foreign, multiple or unknown locations. How can law enforcement access and secure such data without violating the laws or sovereignty of other states, without violating the privacy and other rights of individuals and without violating rule of law standards? Again, we need smart solutions.

3. We need cooperation at all levels. This includes not only interagency and public/private cooperation within countries or cooperation between countries. It will also need to include public/private cooperation across countries. Again, we are facing complex questions in this respect.

   Earlier this month, the Parties to the Budapest Convention decided to go ahead with the negotiation of an Additional Protocol to the Budapest Convention. Direct cooperation with service providers in other jurisdictions is one of the questions on the agenda.

   Cooperation requires trust. Over the last ten years, I have been discussing with hundreds of cybercrime experts from governments and industry across the world. They all confirm that cooperation is the key to effective action on cybercrime. And the main reason they give for cooperating or for refusing cooperation with counterparts in other countries is whether rule of law or human rights conditions allow for cooperation.

   For example, if the other country does not have the laws in place to obtain data, they will not provide the data. The same applies if there is a risk that the data may be misused for political prosecutions.

   Being a party to the Budapest Convention is an important criteria as it means that there is a legal basis for cooperation, because it requires that a Party has the necessary domestic legislation in line with the provisions of this treaty and because it means that law enforcement powers are subject to rule of law safeguards.

Dear friends,

I look very much forward to debates during this conference. Together we should be able to find smart solutions and develop the trust necessary for cooperation on such relevant and complex matters.