Opening of the Regional Cybercrime-Cybersecurity Assessment Conference
Manila, November 11 - 12, 2015

On behalf of the Delegation of the European Union to the Philippines, I am delighted to be here with you today for the Opening of the Regional Cybercrime-Cybersecurity Assessment Conference. Let me first **thank** the **Office of Cybercrime of the Department of Justice, the Information and Communication Technology Office of the Department of Science and Technology of the Philippines** as well as the **Council of Europe** for **organising** this important event and for inviting the European Union to deliver opening remarks.

Allow me to start by making an obvious statement: **technology helps us achieve a better future**. It provides access to education, promotes freedom of speech; it connects people worldwide and enables essential services. There is increasing evidence of the **strong link between internet connectivity and social and economic progress**. Technology also acts as a great global equaliser. **Internet empowers people in all corners of the world,** young and old, rich and poor.

According to the Internet and Organised Crime Threat Assessment (iOCTA) 2014 of EUROPOL, we have an estimated 2.8 billion people on our planet accessing the internet using over 10 billion internet-enabled devices. However, the report also states: "The advent of the **Internet of Everything (IoE)** combined with the ever **increasing number of Internet** users globally creates **a broader attack surface**, new attack vectors and **more points of entry**, including social engineering methods, **for criminals to exploit, making endpoint security even more important**."[1] We will not be able to reap all the potential benefits of the online economy if **countries around the world** cannot **protect their citizens** and **provide them with a safe and secure Internet environment**. In this context, we are talking about **cybersecurity**. At the same time, our growing dependence on Information and Communication Technologies (ICTs) is also coupled with the **potential vulnerability to threats such as cybercrime**.

As far as the 28 members states of the European Union (EU) are concerned, **cyberattacks predominantly originate from jurisdictions outside of the EU**, particularly from countries where the proceeds of online crime notably outweigh income from legitimate activities. **The trans-national nature** of cybercrime creates **challenges for law enforcement** to secure and analyse **electronic evidence** in countries from where the attacks originate.

The trans-national nature is one of the reasons why the **EU is cooperating** with many countries in the fight against cybercrime and in the area of cybersecurity. Under the so-called **Instrument contributing to Stability and Peace (IcSP)**, the EU is funding the Global Action on Cybercrime Project (GLACY) which is implemented by **the Council of**

[1] [bold not included in the original text]

Europe (CoE). In the Philippines, GLACY collaborates with the Department of Justice and the Philippine National Police **to support and train judges, prosecutors, and law enforcement officers in how to handle cybercrime cases, and electronic evidence**. While GLACY will end in 2016, the preparation of the project **GLACY+** which has a **€ 9 million EU support**, that is three times the budget of GLACY, is underway and should start next year.

The aspect of capacity building is particularly pertinent since not all the countries in the world have an equal technical capability, preparedness and legal frameworks to address cybercrime and other cyber threats. Many policy-makers are looking for efficient frameworks how to structure capacity building efforts, what methods to use and how to measure their efficiency.

A key lesson from the EU's experience to date is that an **essential part** of any national cyber effort is the existence of a **proper legal framework**, which is updated in order to address cybercrime. This includes measures to **criminalise offences related to** computer crime, and to harmonise minimum penalties with general international practice, while of course **ensuring that core values are respected**.

To this end, the **Budapest Convention on Cybercrime provides an excellent model that includes all necessary safeguards and conditions for successful cybercrime investigation**. As you are aware, the EU has been actively contributing to the promotion of the Budapest Convention which is in fact **considered by the EU as "the legal framework of reference for fighting cybercrime at global level"**.[2]

Within the EU, much experience has been gained during the past decade in particular with respect to the development of standardised and scalable training, cooperation and information sharing between specialised cybercrime units and other fields. The **European Cybercrime Centre** (EC3) which opened in 2013 and is based in the Netherlands[3] **has been instrumental in enhancing the EU's capacity in addressing cybercrime and will also continue to allow the EU to share this experience with third countries.**

Analyses indicate that **cybercrime is among the most underreported offences**. While **cybercrime is increasing in scale and impact,** there is a **lack of reliable figures,** trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage. Therefore, it is very encouraging to see that this conference of today and tomorrow also addresses the issue of statistics and reporting mechanisms within cybercrime and cybersecurity frameworks and strategies.

In this spirit, let me wish you, on behalf of the Delegation of the European Union, to the Philippines **successful conference** and **thank you** for your attention.

[2] Stockholm Programme (2010-2014)

[3] including the European Cybercrime Training and Education Group (ECTEG) and the EU Cybercrime Task Force

SCENE SETTER

• Considering the extremely various levels of technical capabilities, preparedness and legal frameworks found in different countries to address cyber threats, the EU policy-makers are looking how to structure efficient capacity building efforts, what methods to use and how to measure their impact.

• Cyber capacity building (CB) means constructing safer and more reliable communication networks worldwide to improve access to technology, as well as increasing technical and organisational preparedness to fight cyber threats and address cybercrime.

• Demand for support to third countries is so high that a coordinated, if not collective effort, in capacity building is necessary to ensure that limited resources are well coordinated in both preventing the emergence of safe havens and ensuring that developing countries can fully harness the benefits of ICTs/internet.

• Need to draw lessons learnt from other areas of capacity building experiences/communities (for ex. security sector reform; good governance) and try to overcome the disconnect between the cyber and the development communities.

• Work towards mainstreaming cyber issues in development cooperation is necessary. The EU Member States and the US are facing similar challenges to make cyber more mainstreamed into the development assistance work.[4]

• Cyber capacity building is one of the thematic areas of focus for the Instrument contributing to Stability and Peace (IcSP) which has a dedicated allocation both for cybersecurity and cybercrime.

• EU capacity building in addressing cybercrime is well advanced given that it is an area where much experience has been gained (esp. regarding the development of standardised and scalable training, cooperation and information sharing between specialised cybercrime units and other fields). The establishment of the European Cybercrime Centre at Europol (EC3) has been instrumental in enhancing the EU's capacity in addressing cybercrime and shall allow the EU to share this experience with third countries.

• The EU has worked with the Council of Europe (CoE) in neighbouring countries and launched last in November 2013 the Global Action on Cybercrime (GLACY) (3MEUR) under IcSP also implemented by the CoE in partnership with EC3 and some EUMS (France, Romania) while another action (GLACY+) (9MEUR) is planned to start in 2016 by the CoE and Interpol.

• EU capacity building in cybersecurity is less advanced as ICT projects did not traditionally foresee cybersecurity components. The EU commenced in 2014 a pilot project involving 3 countries (Kosovo, FYROM Macedonia, Moldova). Lessons-learnt and

good practices of this pilot action will feed into new actions that are in the pipeline (IcSP AAP 2016, estimated start in 2017).

• A global "Conference on Cyber Needs and Development" was organised by DEVCO and the EU Institute for Security Studies (EUISS) in consultation with EEAS on 23-24 February 2015.

BACKGROUND: CYBER CAPACITY BUILDING THROUGH IcSP

A. <u>Cybercrime</u>

Most forms of illicit trafficking, money laundering and other financial crimes as well as terrorism and violent radicalisation, have an increasingly important 'cyber' dimension — to an extent that today it is no longer possible for law enforcement to effectively combat these threats without addressing their related criminal activities in the cyberspace. Cybercrime is therefore not just a new form of crime, but also a new environment where organised crime has expanded. **The main challenge throughout developing countries clearly is lack of capacity to apply legislation on cybercrime and electronic evidence in practice.**

• Global Action against Cybercrime (GLACY)

In this context, cyber crime has become a new priority area for IcSP. In November 2013 a new project has started in collaboration with the Council of Europe: **"The Global Action against Cybercrime (GLACY)"** with an EU contribution of EUR 3 million (total amount: EUR 3.35 million) aims at promoting accession to the Budapest Convention on Cybercrime and enabling criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of this treaty.

<u>Key areas of action:</u>

- **Awareness raising** and engagement of decision-makers on cybercrime threats and rule of law/human rights implications and identification of strategic priorities regarding cybercrime

- **Harmonisation of legislation** in line with the Convention on Cybercrime (Budapest Convention); and improvement of legislation and regulations on data protection and child online protection

- **Judicial training**: Enhanced skills for judges and prosecutors regarding cases on cybercrime and electronic evidence

- **Law enforcement capacities**: Enhanced specialised skills and institutions for investigations of cybercrime and electronic evidence

- **International cooperation**: Enhanced international law enforcement and judicial cooperation against cybercrime - Information sharing: Increased public/private and interagency information sharing in line with data protection standards

Geographical scope:

In the context of GLACY, the undertaking of the relevant activities is subject to certain prioritisation on the basis of the following:

- **For activities relating to Result areas 1 (decision-makers) and 2 (legislation):**

Any non-EU/non-OECD State interested in implementing the Budapest Convention or using it as a guideline for legislation.

- **For activities relating to Result areas 3 (judicial training) and 4 (law enforcement):**

States in Africa and Asia/Pacific (non-OECD) that are Parties, signatories or that have requested accession to the Budapest Convention and that are not benefiting from similar support through other EU and Council of Europe projects. **At present, these include: Mauritius, Morocco, Philippines, Senegal, Sri Lanka, South Africa, Tonga**. These countries may serve as regional hubs. Additional participants from neighbouring States may be invited to join activities. It is expected that additional States will seek accession in the near future and will be included in this list. Up to 10 States will receive more detailed support for activities under Result areas 3 and 4.

- **For activities under Result 5 (international cooperation):**

Any non-EU/non-OECD State which is either Party or Signatory or which has requested accession to the Budapest Convention. At present these include:

Europe: Albania, Bosnia and Herzegovina, Montenegro, Serbia, FYROM Macedonia, and Turkey; as well as Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.[5] Activities will also involve Kosovo[6]

Africa: Mauritius, Morocco, Senegal, South Africa Americas: Argentina, Colombia, Costa Rica, Dominican Republic, Mexico, Panama[7]

Asia/Pacific: Philippines.

---

[5] Note: These countries as well as Croatia and Kovoso* have benefitted extensively from the CyberCrime@IPA joint project (2010-2013) or the CyberCrime@EAP project under the Eastern Partnership Facility. They are likely to receive additional support under future IPA and ENPI projects, including a follow up to the CyberCrime@EAP project. They are therefore not priority countries for support through GLACY. Their involvement in GLACY will allow them to share their experience with other regions of the world. Synergies between GLACY and future projects in the ENPI or IPA regions are to be ensured.

[6] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

[7] States of the Americas are not priority countries under the present GLACY project. It is nevertheless important that they maintain cooperation with European and other Parties, signatories and invitees to the Budapest Convention to form a community of trust.

- **For activities under Results 6 (information sharing) and 7 (assessment of progress):**

Any State may benefit since GLACY will serve as a resource to this end. Specific and more comprehensive support may be provided to the 10 States that participate in Results 3 and 4 or other States upon decision by the Steering Committee.

- **Capacity Building for Cybercrime**

In order to respond to the increasing need for capacity building in this area, particularly in Africa and Asia, and also creating a bridge between cyber crime and cyber security, **a new action named GLACY+ is in the pipeline (AAP 2014) to start in 2016** with an indicative commitment of **9 million**, bringing the total amount of EU commitment in this area to approximately EUR 12 million. It will be implemented by the Council of Europe in partnership with INTERPOL.

• IcSP Commitments / Planning (in million EUR)

CYBER CRIME	ONGOING	3
	TO BE CONTRACTED	9
	MIP (indicative AAP 2017)	1.5
	TOTAL	14

B. <u>Cybersecuritv</u>

Societies all over the world increasingly rely on the use of Information and Communication Technologies (ICT) and networks that underpin all critical services and support the smooth functioning of global economy, as well as providing essential public services. Yet cyber intrusions and attacks have increased dramatically over the last decade, both in number and in sophistication, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. Many third countries, particularly developing countries, have rather limited capacity to monitor and manage such incidents in cyberspace.

• IcSP Actions

Cyber security is a new area of priority for IcSP. IcSP aims at providing support to transition and developing countries that need to **introduce both technological and organisational measures** that will enable them to build their resilience to cyber incidents.

A pilot project of EUR 1.5 million started in January 2014 with an objective to **increase the security and resilience of Information Communication Technologies networks** in the beneficiary countries by building and training local capacities **to adequately prevent, respond to and prosecute cyber attacks and/or accidental failures**. The

target countries are: Azerbaijan, FYROM, Kosovo, Moldova and this project is implemented by an EUMS Consortium (ADETEF and CIVIPOL).

Key areas of action:

- Creation and/or development of the capacities of national **Computer Incident Response Teams (CERTs) and 24/7 Contact Points.**

- Support the adoption of **national Cyber Security Strategies / Legislation.**

- **Increase awareness** of decision-makers and private sector about cyber security and the protection of critical IT infrastructures.

- Foster the creation of **Public Private Partnerships (PPPs) and partnerships with academia**

- **Enhance international cooperation** at inter-governmental level as well as amongst law enforcement institutions with private entities and CERTs.

Lessons-learnt and best practices of this pilot phase will feed into new actions that are in the pipeline to start in 2017 (AAP 2016) with an indicative commitment of EUR 11 million, bringing the total amount of EU commitment in this area (from AAP 2012 to AAP 2016) to approximately EUR 12,5 million.

• Commitments / Planning

CYBER SECURITY	ONGOING	1.5
	TO BE CONTRACTED	0
	MIP (indicative AAP 2016)	11
	TOTAL	12.5

C. Background

"Conference on Cyber Needs and Development"; 23-24 February 2015. During the conference of the EU Institute for Security Studies "Cyber capacity building as a development issue: What role for regional organisations?" held in March 2014, it was made clear that the donor community needs to be more effective in identifying the needs of the beneficiaries in order to make the cyber capacity building efforts more efficient and sustainable.

The necessity to hold a broader consultation with developing countries about their needs in terms of capacity building in the area of cyber security is particularly pertinent in relation to the **programming exercise of the Instrument contributing to Stability and Peace (IcSP).** An indicative amount of 11 MEUR has been allocated under its Annual Action Plan of 2016, as detailed in the IcSP Multi-annual Indicative Programme 2014-2017.

In order to mark the start of the identification exercise for this new action of the IcSP, DEVCO has teamed up with EIUSS and is **now commencing preparations for a joint conference that would scrutinise more thoroughly the needs of developing countries** which will help the EU define its capacity building priorities.

The conference will focus on needs of actors requiring assistance in building up their cyber capacities that would further stimulate their economic and social development. This includes different constellations of actors (governments, private sector and civil society) at the national, regional and international level. The event will aim at addressing the questions about a structure and resources needed for creation of networks enhancing economy, development and security and in particular the two main issues:

• What are the needs of developing countries with regard to cyber capacity building? What are their priorities?

• What are the expectations of beneficiaries towards the donor community? How could the relationship between donors and beneficiaries be further improved?

Participants in the conference will be government officials and representatives of international, regional and civil society organisations with stakes in cybersecurity and capacity building. The total number of expected participants is approximately 150 people.

D. <u>Octopus Project:</u>

See attached fact sheet, EU MS funding it with public funds: Estonia, Romania, UK

E. <u>Contacts:</u>

DEVCO: Nayia BARMPALIOU, DEVCO.B5 (57268),

EEAS: Heli TIIRMAA-KLAAR, EEAS K3

Delegation to the Philippines: Robert FRANK