DEVCO.B5
Mr Olivier LUYCKX
Opening remarks

GLACY+
15 June 2017, 9.00-10.00h
Sofitel Hotel, Pl. Jourdan, Brussels
Cybercrime Training Strategies & ECTEG

Dear partners and colleagues –

On behalf of the European Commission and the Directorate General for International Cooperation and Development, I am delighted to have the opportunity to welcome you to Brussels, at this International Workshop in the context of the joint EU-Council of Europe Global Action on Cybercrime extended project.

It is a particular pleasure to have such a large number of representatives from all over the world - from the GLACY+ priority countries from Africa, Asia and the Pacific but also from our close neighbours from the Western Balkans, Turkey and Eastern Partnership, through the link with the iPROCEEDS and Cybercrime@EAP projects.

Cybercrime has evolved into one of the greatest challenges for the rule of law across criminal jurisdictions while the penetration of electronic evidence into of any type of crime further complicates the puzzle for criminal justice authorities. The cross-over of the use of new technologies by terrorist and organised crime groups is no longer an alarming trend but a reality.

Criminals quickly deploy and adapt new technologies into their modi operandi or build brand-new business models around them with great skill and to great effect.

Having you all here is indicative that we are all facing the same challenges and that international cooperation is a key factor in addressing cybercrime.

The EU's approach the fight against cybercrime consists of a comprehensive toolkit that involves:

- the adoption and update of appropriate legislation on the basis of standards that capture international best practice, namely the Budapest Convention on Cybercrime,
- the support to cooperation frameworks amongst criminal justice actors and across sectors particularly with industry which controls a large part of information infrastructures and services,
- financial resources to allow for research and development that provide access to the right technology to address market failures,
- as well as increased focus on training programmes to enhance the capacities and expertise of law enforcement and judiciary in this area.

Our efforts in external capacity building through our programmes is to mirror this experience and also capitalise on synergies as we are doing through our joint programmes with the Council of Europe, and the structured cooperation we

have with the European Cybercrime Centre at Europol, the European Cybercrime Training and Education Group and Interpol.

The threat landscape shows that the Crime-as-a-Service model is getting even more mature in its capacity to provide tools and services across the entire spectrum of cybercrime and cyber-enabled crime. And most recently we witnessed globally with WannaCry how ransomware, the fastest growing malware threat, can affect not only simple users but also critical infrastructure operators and service providers – like the UK's National Health Service.

At the same time, legitimate anonymity and encryption services are misused for illegal purposes not allowing law enforcement access to essential intelligence and evidence across all crime areas; while extremist and terrorist groups make extensive use of the internet, particularly through social media, for recruitment, propaganda and incitement.

In this environment, you are confronted with immense difficulties in doing your job effectively. To combat these threats we need to devise new ways of monitoring and reporting cybercriminal activity, and to work together across borders and across society while striking the balance between national security and fundamental freedoms in upholding the rule of law in cyberspace.

To achieve this we need to have a strategic and agile planning on how to increase the response capacities. Rather than multiple partners investing in and developing the same highly specialised training material, we see an added value in a more effective model where we can capitalise on existing initiatives and leveraging on existing knowledge and expertise networks.

In recognising this need, from our side in DG DEVCO since 2013 that we stepped up our efforts to address cybercrime and cyber threats globally, we work closely with other EU services and particularly DG Migration and Home Affairs and the European Cybercrime Centre at Europol to tailor programmes that maximise these synergies with our partners outside the EU.

Our strategic partner in this endeavour has been the Council of Europe with which we have for some years already joint programmes in the Western Balkans and Eastern Partnership countries, while with GLACY since 2013 we have managed to scale up to the global level.

To help us in this joint work we are also working with Interpol, and we are also very happy to facilitate your contacts with the European Cybercrime Training and Education Group that has been at the forefront of creating harmonised EU-wide cybercrime training courses for several years.

In this spirit, I am confident that you will have very constructive exchanges during this workshop on cybercrime training strategies and material that can foster a streamlined approach within your institutions and governments.