

# International Workshop on Cybercrime Training Strategies for Law Enforcement Agencies and access to ECTEG materials

**Brussels**  
**15-16 June 2017**

Mr. Olivier LUYCKX, Head of Unit Security and Nuclear Safety, European Commission

Mr. Takayuki OKU, Assistant Director, INTERPOL

Mrs. Malgorzata SOBUSIAK-FISCHNALLER, representative of the European Cybercrime Center of Europol

Mr. Yves VANDERMEER, Chairman of the European Cybercrime Training and Education Group

Delegates all from Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Dominican Republic, Georgia, Ghana, Kosovo\*, Mauritius, Morocco, Moldova, Philippines, Senegal, Serbia, Sri Lanka, The Former Yugoslav Republic Of Macedonia, Tonga, Turkey, Ukraine

Dear partners and colleagues,  
Ladies and gentlemen,

On behalf of the Council of Europe, and of the Cybercrime Programme Office (C-PROC), it is my pleasure to welcome you all at the International Workshop on Cybercrime Training Strategies for Law Enforcement Agencies and access to ECTEG materials.

The C-PROC Office, as all of you know has been created by the Council of Europe with the specific goal to **Support countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence.**

I want to here acknowledge the contribution of the European Union in supporting the initiatives of the Council of Europe to prevent and fight organized crime, in particular cybercrime, in line with international legal instruments and human rights norms, standards and good practices.

We regard at cybercrime as a **criminal justice matter**, and as such we focus on building capacities of criminal justice authorities along the whole process that we can see from this angle: from reporting to investigation, prosecution and – of course – adjudication of cases.

And we don't only focus on cybercrimes as criminal offences committed through the use of technology, but we include also all those crimes where investigations, prosecutions and adjudications can request the **use of electronic evidence.**

The continuous evolution of the information society requires today as never before that criminal justice authorities, and especially those who are in charge of enforcing the law, are equipped with competencies and technical skills that could allow them to effectively handle increasingly sophisticated cases.

We can certainly think of the recent WannaCry attack that has been already cited.

- Spread to more than 100 countries
- Involved the use of darknets and exchange of information on its design
- Made use of virtual currencies as a means of payment

Its impact was huge in terms of disruption of critical systems that were reached, although the financial gain of the criminals was quite limited.

And its global reach represented at the same time a strength, but also a weakness, as it called the immediate attention of the international community, which could find a way to contain and "switch it off" rather quickly. But many more similar threats are in the wild, which get less attention and are more difficult to stop.

We are aware of the **increasing challenges** that investigators must face, when confronted with such a continuously evolving landscape, where technical competencies are amongst the most needed resources that must be treasured, especially within the Law Enforcement environment.

And in order for a capacity building programme to be effective in reaching its goal, we don't aim at just providing a training in one single shot. What we want to do is to stimulate **a whole process** that could be sustainable by the local authorities that receive it.

Sustainability is actually one of the keywords of a good capacity building programme and this is why we focus on training strategies for law enforcement.

Together with ECTEG, which is well acknowledged as the European cybercrime training platform for Law Enforcement we want to promoting **standardization of methods and procedures for training programmes** on cybercrime and electronic evidence.

Of course this implies the provisioning of **training and education on cybercrime** and electronic evidence on the basis of the needs identified in the countries' initial assessment of Law Enforcement capacities and capabilities and on additional feedback received from the interested counterparts;

Facilitating the **access to the ECTEG materials** for trusted entities vetted by the Council of Europe, in full respect of the ECTEG materials distribution policies;

Admitting the supported countries to enroll selected resources in a **pilot certification programme** to be held in the European Union.

We wish that these two days could

- foster a fruitful exchange of ideas, good practices and experiences in the field,
- represent an opportunity to network with international experts, colleagues and peers, and
- put the basis for a thread of specific activities that we will develop under the our Projects,

with the ultimate goal to strengthen capacities of criminal justice authorities worldwide in the fight against cybercrime.

Thank you very much!

Matteo LUCCHETTI  
Project manager  
Council of Europe