Decision of the Management Board 01/2020/MB

ADOPTING OF THE UPDATED CONTENT DESCRIPTION OF THE ONLINE MODULE CYBERCRIME AND REPEALING DECISION 24/2013/GB

Adopted by the Management Board

On 26 February 2020

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ó utca 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu

THE MANAGEMENT BOARD,

Having regard to Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA[1], and in particular Article 9(1)(s) thereof,

Having regard to the Governing Board Decision 24/2013/GB adopting the Content Description of the Online Learning Module Cybercrime and amending Decision 19/2011/GB,

Having regard to the Management Board Decision 15/2019/MB amending Decision 32/2018/MB on the CEPOL Single Programming Document: 2019-2021

Having regard to Executive Director Decision 41/2019/DIR on non-substantial amendment of the Annual Work Programme 2019;

Whereas:

(1) The steps to be taken and matching responsibilities in the development of the online learning modules are based on Governing Board Decisions 2/2009/GB and 18/2010/GB.

(2) The content of the module was developed by experts appointed with the Executive Director's Decision 15/2019/DIR.

(3) CEPOL National Units, National and Organisational Contact Points and the Commission DG HOME have been involved in the final validation of the content of the online learning module.

(4) The update of the online module content on cybercrime as set by the Governing Board Decision 24/2013/GB, was planned to take place in the course of 2019. By decision 41/2019 of the Executive Director on non-substantial amendments of the annual work plan of 2019, the completion of the update was postponed to 2020.

[1] OJ L319, 4.12.2015, p.1.

(4) It is for the Management Board on the basis of Article 9(1)(s) of Regulation (EU) 2015/2219 of the European Parliament and of the Council to adopt the content descriptions of the online learning modules.

(5) There is a need to repeal Decision 24/2013/GB adopting the existing content description of the Online Learning Module on Cybercrime;

HAS ADOPTED THIS DECISION:

Article 1

1) The Content Description of the Online Learning Module Cybercrime as detailed in the Annex to this Decision is hereby adopted.
2) Decision 24/2013/GB is hereby repealed.

Article 2

The present Decision shall take effect on the day following that of its adoption.

Done at Tampere, on 27 February 2020

For the Management Board
<< Signature on file>>
……..
Dr Kimmo Himberg
Chair of the Management Board

Annex

Table of Contents

A. Product Breakdown Structure

The Product Breakdown Structure (PBS) represents the content of the *Cybercrime* module as it is set up in the online learning environment. Key sections of the PBS are displayed below, covering the online learning module's topics of the Knowledge Landscape and the keywords.

Cybercrime Knowledge Landscape:

1. Module introduction
2. Types of cybercrime and cyber-enabled crime
3. First response
4. Investiging cybercrime
5. Digital forensics and e-evidency
6. Legislation
7. International cooperation 1: Law enforcement cooperation
8. International cooperation 2: Judicial and public sector cooperation
9. Prevention and capacity building
10. Challenges and future trends
11. Glossary

B. Elaboration of the Content – Knowledge Landscape

The module was developed with the aim to introduce the area of cybercrime and cyber-enabled crime. This includes: identifying and preventing cybercrime and cyber-enabled crime; conducting first response; protecting assets and persons; the legal framework; investigating cybercrime and cyber-enabled crime; and challenges and good practices. The module is intended for people all law enforcement officers, prosecutors and judges who deal with or in the future may deal with cybercrime and cyber-enabled crime. The online module is relevant for all the actors involved in cybercrime investigations, as identified by the Training Competency Framework on Cybercrime, Europol (February 2019), adopted by CEPOL, Eurojust and the European Cybercrime Training and Education Group (ECTEG).

Following introduction of the module in chapter 1, chapter 2 provides an overview of the different types of cybercrimes that law enforcement may face in their investigations. Chapter 3 focuses on those situations that do not require the immediate onsite imaging of electronic devices. It covers the procedures that should be followed by first responders, including how they should preserve and investigate the crime scene, collect devices and transport them to an established evidence-storage location where proper forensic imaging may be completed. The subject of chapter 4 is the collecting

of information (intelligence and evidence) during an investigation. It does not include digital forensics or e-evidence, which are both covered in Chapter 5. The next chapter, 5, covers digital forensics as the analysis of electronic devices and the investigation of digital evidence (e-evidence). This chapter discusses what e-evidence is, and the objectives and processes involved in digital forensics. Chapter 6 presents the national, regional and international legislation related to cybercrime, and includes the trends of the law-making process and the challenges faced by the judicial authorities. Chapter 7 is the first of two chapters on international cooperation, this chapter is concerned with the cooperation facilitated by EU and international law enforcement organisations and networks. Chapter 8 is is the second of two chapters on international cooperation, and covers the organisations and networks involved in judicial cooperation and cooperation with the private sector. Chapter 9 covers prevention, making people more aware of cybercrime phenomena and of how to avoid becoming victims of cybercrime. It also discusses capacity building, including the education and training of law enforcement personnel, and the resources available to them, to help them tackle cybercrime. Chapter 10 looks at the cybercrime-related challenges to law enforcement that have arisen in recent years, and also takes a look at the current and likely future trends in the area.

C. Diagnostic Self Evaluation: My progress

Users can test their own knowledge on *Cybercrime* at any time while using the online module through the My Progress section of the module. Test items, in the form of True/False questions, are pooled according to the recurring topics of the knowledge landscape. A random selection of the items will be offered to users every time they decide to take the self-test for each of the individual topics. Based on the outcomes of the self-test, users will receive feedback and reflection possibilities, which enable them to increase their further professionalisation in the domain of the module.

D. Glossary

The keywords and acronyms from individual chapters are listed together (in alphabetical order) in the online module and are provided to the user to aid navigation through the material.

Annex I

Cybercrime
Online Module Content

(The content of the module will be made **available only** in a restricted area in CEPOL's e-Net),