



SECURITATEA CIBERNETICĂ - PROVOCĂRI ȘI PERSPECTIVE ÎN EDUCAȚIE

EDITORI

Ioan-Cosmin MIHAI, Costel CIUCHI, Gabriel PETRICĂ

**ROMÂNIA
2020**

CUPRINS

Prefață	5
Dan CÎMPEAN	
Cuvânt-înainte	7
Ioan C. BACIVAROV	
CEPOL - The European Union Agency for Law Enforcement Training Activities in the Field of Cybercrime.....	9
Detlef SCHRÖDER, Ioan-Cosmin MIHAI	
CSDP Cyber Education, Training, Exercise and Evaluation (ETEE) Platform under the ESDC	21
Dirk DUBOIS, Marios THOMA, Gregor SCHAFFRATH	
Cybersecurity from a University Perspective	29
Udo HELMBRECHT	
Cyber Higher Education in Israel - From Cybersecurity to Cyberspace.....	39
Tal PAVEL	
Cyber Law. How to Upgrade Knowledge at the University Level: Building the New Generation of Cyber Professionals	49
Nathalie RÉBÉ	
Model de cooperare la nivel internațional: CyberEDU 202X.....	57
Daria CATALUI	
Aspecte privind aplicarea principiilor eticii și integrității în spațiul cibernetic	63
Lisa-Maria ACHIMESCU, Angela IONIȚĂ	
Impactul schimbărilor digitale asupra nevoilor educaționale ale tinerilor din România	105
Eliza VAȘ, Bogdan MUREȘAN	
De la paradoxul confidențialității la acțiunea colectivă. Provocările unui curs privind protecția vieții private	121
Răzvan RUGHINIȘ	
Cybersecurity for Online Learning	131
Răzvan BOLOGA, Tiberiu-Marian GEORGESCU	

Provocările revoluției digitale în domeniul politicii. Educația pentru o societate digitală.....	137
Mihai SEBE	
Provocări în dezvoltarea unui ecosistem rezilient pentru educație în securitatea cibernetică	143
Costel CIUCHI	
Cinci decenii de învățământ tehnic superior în domeniul siguranței în funcționare în România	155
Ioan C. BACIVAROV	
Growing the Cybersecurity Ecosystem: a Higher Education Perspective	175
Cătălin MIRONEANU, Simona CARAIMAN	
Propunere pentru abordări practice în educația privind securitatea informației.....	183
Larisa GĂBUDEANU	
Dezvoltarea unui program de masterat în cybersecurity personalizat pentru domeniul Electronică, Telecomunicații și Tehnologii Informaționale	191
Eduard-Cristian POPOVICI, Octavian FRATU, Simona-Viorica HALUNGA, Laurențiu BOICESCU	
Educația în fața provocărilor ciberneticе	201
Mircea-Constantin ȘCHEAU	
Online Child Sexual Abuse During COVID-19 Pandemic. The Importance of Law Enforcement Training in this Area.....	215
Iulian-Marius COMAN	
Educația pentru o lume digitală. Studiu de caz: educația școlară pentru combaterea dezinformării online.....	221
Handy-Francine JAOMIASA	
In Search of Lost Cyber Talents	229
Liviu MORON	
Ecosistemul CDI universitate-industrie - un pilon esențial pentru creșterea competenței și rezilienței ciberneticе	233
Olivia COMȘA, Sorin MIRIȚESCU, Marius PÂRVU, Florin POPESCU	
Cyber4Kids.ro - contribuția industriei de securitate cibernetică la educația copiilor.....	247
Ionuț FLOREA	
Despre autori / About authors.....	255

CEPOL - The European Union Agency for Law Enforcement Training Activities in the Field of Cybercrime

Dr.h.c. Detlef SCHRÖDER, Dr. Ioan-Cosmin MIHAI
European Union Agency for Law Enforcement Training (CEPOL)
info@cepol.europa.eu

1. About CEPOL

The European Union Agency for Law Enforcement Training (CEPOL) is dedicated to developing, implementing, and coordinating training for law enforcement officials. CEPOL brings together a network of training institutes for law enforcement officials in EU Member States and supports them in providing frontline training on security priorities, law enforcement cooperation and information exchange. It contributes to a safer Europe by facilitating cooperation and knowledge sharing among law enforcement officials from the EU Member States and, to some extent, from other countries, on issues stemming from EU priorities in the field of security; in particular, from the EU Policy Cycle on serious and organised crime.

CEPOL employs a multi-layered approach to learning, including:

- *Onsite activities*, which are typically comprised of courses, conferences, workshops, and seminars. With some exceptions, they normally last a week and are held in a training institute in one of the Member States or at the CEPOL HQ. Residential activities provide an opportunity to gain a deeper understanding of a subject.
- *Online learning* is a way of computer-based distance learning. Online learning takes place in form of webinars, online modules, online courses, cyberbites, e-Workshops, and e-Lessons.
- *The CEPOL Exchange Programme* allows law enforcement officers to spend one week with a counterpart in their own country, exchanging knowledge and

good practices, initiating cooperation projects, and fostering long-lasting learning and networking opportunities.

In particular, the onsite training activities and the Exchange Programme provide excellent opportunities for building up professional networks and trust among the officers engaged.

All activities are supported by CEPOL's Law Enforcement Education platform (LEEd). Through LEEd, users have access to tools and resources that support and deepen the learning experience. The LEEd platform also provides access to a large collection of e-Books and e-Journals, which provides registered users with access to international scientific publications related to police science and police practices.

2. CEPOL Cybercrime Academy

The different forms of cybercrime are a major threat for the internal security of Europe. In consequence, CEPOL has identified cybercrime as one of its key priorities for the upcoming years. In order to respond to the growing training demand in the cyber area, CEPOL has strengthened its cyber-training portfolio and has established the European Cybercrime Training Academy, which is properly equipped and configured to train one hundred participants simultaneously.



The CEPOL Cybercrime Academy Laboratory

The CEPOL Cybercrime Academy was officially inaugurated on the 13th of June 2019 in Budapest, by the European Union Agency for Law Enforcement Training (CEPOL), in the presence of a number of high-level guests and speakers, including the Deputy Prime Minister of Hungary, Dr Sandor Pinter, as well as the Director for Security at the European Commission, Mr Laurent Muschel.

The Academy is equipped with state-of-the-art hardware and software, fully configured to train up to one hundred participants at the same time. Cybercrime is one of the fastest growing forms of crime. The European Union is fully aware of the increasing consequences of cybercrime, and the need to protect cyberspace from incidents and malicious activities has become crucial for the functioning of our societies and economies. Developing the necessary knowledge and expertise in law enforcement authorities across Europe is key in addressing the evolving challenge of cybercrime.

Speaking at the opening event, CEPOL's Executive Director, Dr. h.c. Detlef Schröder, underlined that: *"All electronic learning cannot replace the learning experience in a group of officers from different countries from the same profession in a classic training setting. This Academy will enable that we can offer to our Member States the required training on a by far higher scale"*.

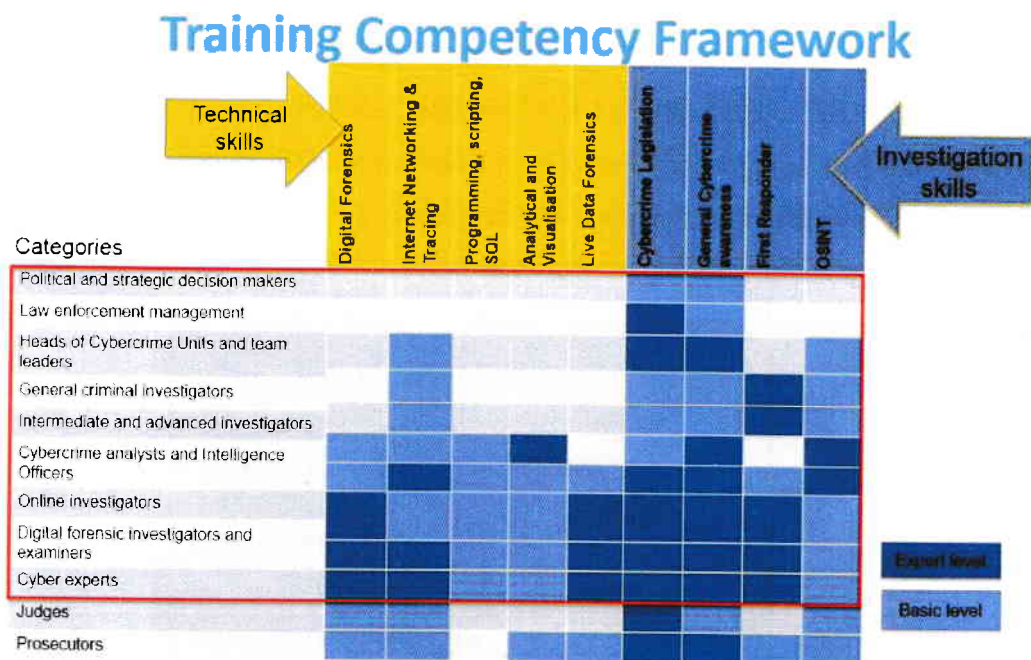


Opening Ceremony of CEPOL Cybercrime Academy

3. Training needs analysis on cybercrime

Training needs are analysed based on the Training Competency Framework (TCF) developed periodically by CEPOL in cooperation with The European Union Agency for Law Enforcement Cooperation (Europol), The European Union Agency for Criminal Justice Cooperation (Eurojust), The European Cybercrime Training and Education Group (ECTEG), The European Union Cybercrime Task Force (EUCTF), The European Judicial Training Network (EJTN). The TCF on Cybercrime identifies the required competencies and skills in combating cybercrime at the EU level for key actors ranging from law enforcement to the judiciary.

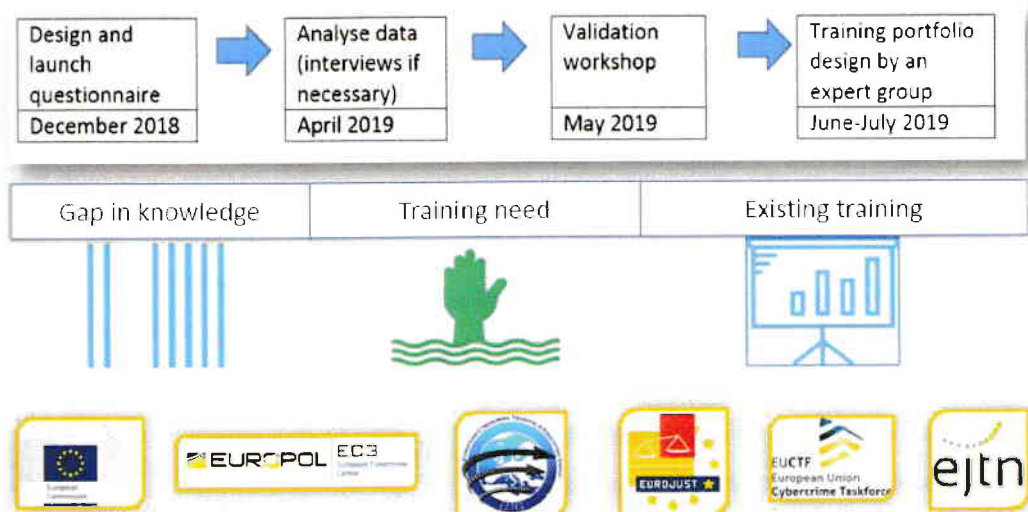
The TCF defines the level of knowledge LE officials taking part in cyber investigations should have in all roles and competencies. It distinguishes between basic and expert level of knowledge necessary to fulfil their daily tasks.



The Training Competency Framework

The analysis, its consequent prioritisation of training needs, and the design of the training portfolio is the outcome of a joint effort coordinated by CEPOL, Europol's EC3, ECTEG, EUCTF, Eurojust, European Commission, and EJTN – all

organisational members of the so-called Training Governance Model (TGM). The target groups for the Cyber Training Needs Analysis (TNA) are Heads of Cybercrime Units and Cyber-experts nominated by the Member States and Europol.



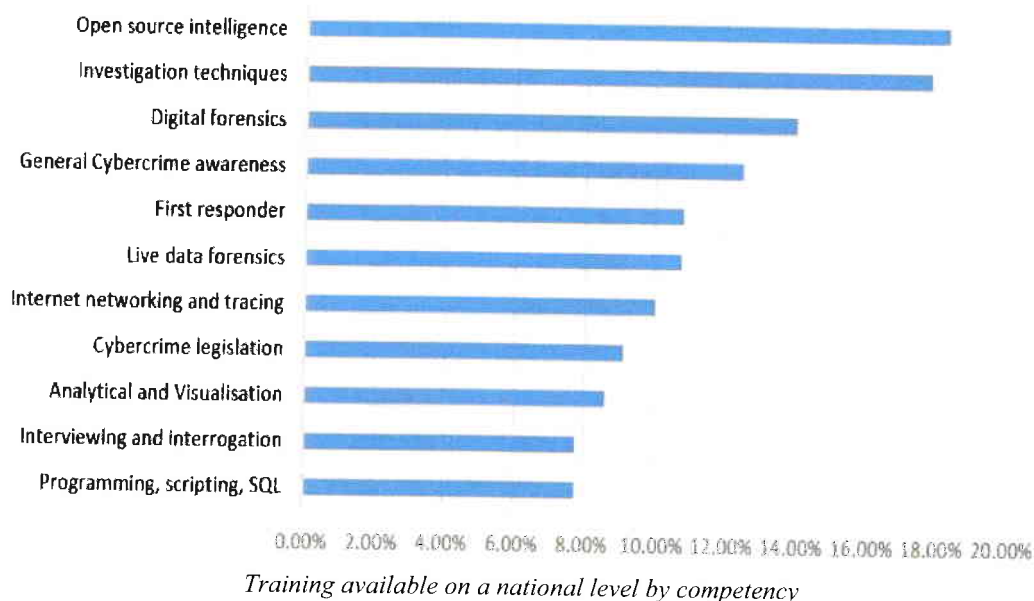
The Cyber Training Needs Analysis Methodology

The training is a matter of urgency, as it should be provided between six months and one year. The need is most pressing for cybercrime analysts, intelligence officers, digital forensic investigators, and examiners, whereas it can be delivered within a year to intermediate and advanced intelligence officers and to law enforcement management.



Training available on a national level by role

Existing training is scarce for all roles and competencies, meaning that only 10% of respondents indicated that national level training activities on this topic area are provided on a sufficient level. The profiles where most training is available is the one of digital forensic investigators and examiners.



The competency most targeted by training on a national level is the use of Open Source Intelligence. Less than 10% of respondents indicated that national level training is available to enhance competencies in programming, scripting, SQL, analytical and visualisation, interviewing and interrogation, and cybercrime legislation.

In the profiles of intermediate and advanced intelligence officers, online investigators, cyber experts and first respondents, there are hardly any training opportunities available.

Based on the latest training needs assessment conducted by CEPOL, in close cooperation with the EU Member States, the demand towards qualifications offered by CEPOL on Cybercrime would require an annual training volume of approx. 3,800 officers to be trained.

4. Cybercrime training activities

CEPOL, in the last years, has invested in an enhanced portfolio of cybercrime related training opportunities. In 2019, CEPOL has trained 7,477 officials from EU Member States on such topics. For 2020, despite the massive challenges stemming from the COVID-19 pandemic, CEPOL estimates to reach out to 7,100 individuals from law enforcement services in EU Member States.

CEPOL covers all three EMPACT (European Union Policy Cycle) priorities on cybercrime: attacks against information systems, child sexual abuse and sexual exploitation, and non-cash payment fraud. CEPOL will implement in 2021 the following courses:

- *Child Sexual Exploitation on the Internet - Undercover Operations*

The aim of this course is to enhance the fight against child sexual exploitation by creating and/or improving skills to operate undercover online and to bolster cooperation involving the identification of such crimes, and the production and dissemination of child abuse material on the internet by the organised crime groups.

- *Child Sexual Exploitation – Victim Identification*

This course is designed to strengthen collaboration between law enforcement institutions from the EU MS, the Associate countries and the Candidate countries, in the identification of child victims of sexual exploitation, and to instil or develop skills of specialised law enforcement officers in the task of victim identification at the national and international levels.

- *Strategies in Managing Child Sex Offenders*

The goal of this course is to facilitate the knowledge transfer between Member States on the application and coordination regarding the implementation of Directive 2011/93/EU of the European Parliament and of the Council, of 13 December 2011, on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework-Decision 2004/68/JHA.

- *Combating card fraud*

The course provides a framework of cooperation and shared experiences on investigative methods involving crimes in the field of skimming devices and non-cash payment fraud, and aids in the development of skills dedicated to the collection of forensic evidence in matters of payment card fraud, such as skimming, as well as perspectives on the card-not-present fraud cases. Additionally, it helps to improve national and cross-border operational capacity on countering ATM attacks.

- *Open-Source Intelligence (OSINT) and IT Solutions – 2 courses*

The aim of these courses is to enhance cyber-crime investigation by improving the collection, evaluation, collation, analysis and distribution of information for the purpose of tackling all forms of crime, in particular terrorism and organised crime, and by improving the quality and quantity of collected intelligence.

- *Darkweb and Cryptocurrencies – 2 courses*

These courses focus on magnifying the cooperation on cross-border cases by employing the TOR-network and the Darkweb, and augmenting capabilities of finding virtual currencies (VC) in the course of criminal investigations, as well as identifying the existence of a VC wallet, notably in the context of searches.

- *Conducting Forensic Searches in Various IT Devices*

The course seeks to enhance cyber forensics work by improving the skills of forensic experts in the matter of recovering digital evidence or data from electronic devices, particularly mobile and Internet of Things (IoT) devices, and by sharing experiences on computer data analysis, technical aspects of Internet investigations and examination of IT devices.

- *Cybercrime - advanced Windows file system forensics*

This course is designed to provide cyber forensics experts with detailed knowledge on the recovery of evidence from file systems, and to allow them to explain forensic tools reports and conduct searches beyond commonly

reported traces in order to establish a trace history and potential use of anti-forensics.

- *Cross border exchange of e-evidence*

The goal of this course is to improve prosecutors' and law enforcement officials' use and exchange of electronic evidence in investigation and prosecution of cybercrime, as well as the relevancy and admissibility of such evidence, ultimately enhancing cyber-investigations.

- *Digital forensic investigators training*

The objective of this course is to ameliorate high-tech crime investigations by augmenting the officers' knowledge on Open-Source forensic software, file systems, data carving, evidential digital artefacts, networking and network security, cloud computing, email investigations, computer forensic strategies and live data forensics, based on the latest investigation techniques and methods.

- *First responders and cyber forensics*

This course focuses on enriching cyber-forensics work by providing law enforcement officials with practical abilities in computer forensics, such as revealing and investigating traces of cybercrimes, by enhancing cooperation and harmonising investigative methods between law enforcement departments with regard to assessing a crime scene in case of a cyber-incident and to handling electronic evidence.

- *Cyber-Intelligence*

The Cyber-Intelligence course provides necessary knowledge and skills to enable law enforcement officials to perform role tracking and analyses, and to counter digital security threats in order to produce actionable intelligence.

- *Malware Investigation*

The scope of this course encompasses retrieval of information from the malware analysis process which will aid in locating criminals and their infrastructure during the course of the cyber-investigation.

- *Live Data Forensics*

The purpose is to strengthen cyber-forensic work of law enforcement investigators by introducing them to powerful Live Forensics investigative techniques with an overview of Live Data Forensics and its uses.

- *Mac Forensics*

The course offers general and practical knowledge of Mac OS X forensics at a basic level.

- *Linux Forensics*

The course offers general and practical knowledge of Linux forensics at a basic level.

Due to the COVID-19 Pandemic situation, some of the aforementioned courses will be available online, on LEEd – CEPOL’s online learning platform.

Additionally, different activities such as online modules, webinars, and cyberbites (micro-learning products delivered in the area of cybercrime – videos with interactive elements), alongside new CEPOL products like e-Workshops and e-Lessons, are already implemented or will be made available in due time.

The CEPOL e-Workshops are e-learning products that focus on interactive learning in small groups, which will be organised as a series of two to three online workshops over a period of 3-4 hours involving a maximum of ten participants and one or two trainers. The e-Workshops that will be implemented by CEPOL are:

- *CEO Fraud/Business Email Compromise.*

The purpose is to improve performance of LE officers by sharing best practices, methods, and tools for fighting online fraud against companies.

- *Analysing Email-based Attacks.*

The aim of this e-Workshop is to enhance the officers’ investigation capacity in order to lower the number of email-based attacks.

The CEPOL e-Lessons are comprised of an estimated study time of up to sixty minutes, divided over a specific number of chapters or sub-topics. Overall, the e-Lessons are an interactive and explorative learning environment. The first e-Lesson to be implemented by CEPOL Cybercrime Academy is “*Cyber investigations in social*