<table>
<thead>
<tr>
<th>Category</th>
<th>Role of training programmes</th>
<th>Target group</th>
<th>Learning outcomes</th>
<th>Status</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Manager</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Define the policy area called the area of freedom, security and justice (AFSJ) including the roles of the different kinds of illicit trade on the clear web, in particular in social media. 2. Discuss most common modi operandi, specifically the illicit use of firearms for criminal purposes. 3. Demonstrate the advantages of using Europol’s operational services in dealing with EU-level and international crime. 4. Explain the set of rules and legislation which regulates the abolishment of border controls at the internal borders.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
<tr>
<td>- Cyber &amp; Organised Crime</td>
<td>Expert</td>
<td>Police, Law Enforcement, and Security Officers</td>
<td>1. Achieve B1 independent user level in accordance with the CEFR on generic English language within the LE field. 2. Discuss international and national legal aspects of firearms control and firearms trafficking; 3. Describe main criminal patterns linked to firearms; 4. Enhance the use of general OSINT techniques suitable for the collection of intelligence; 5. Recognise challenges and future trends in the area of cybercrime.</td>
<td>Available as of 1st of January 2020</td>
<td>6/2020</td>
</tr>
</tbody>
</table>
Upon completion of the activity the participants will be able to:

- Analyse financial intelligence and draw conclusions, build workable hypothesis for the ongoing investigation.
- Discuss good practices with regard to the investigation of cross-border alcohol, tobacco and mineral oil and fraud.
- Understand the added value of Europol and international cooperation instruments.
- Design and apply an intelligence collection plan, for investigative or intelligence purposes according to the needs/circumstances of criminal/administrative methods.
- Recognise security features for identity cards/documents, their method of verification by the person.
- Demonstrate good inter-agency cooperation examples through concrete cases especially between law enforcements practitioners, prosecutors, legal experts, financial investigators, and other enforcement and judicial authorities.
- Share best practices how to obtain operational information from the local communities, private sector, NGOs and prosecutors working in cyber-law enforcement.
- Recognise specific methods and techniques of managing, analysing and evaluating financial data.
- Identify crime patterns on various forms of money laundering (cash based, electronic, underground banking, etc.)
- Understand the importance of money laundering investigations independently or alongside investigations related to serious crime.
- Understand the impact of underground banking, the use of virtual currencies and other emerging technologies on criminality.
- Pay special attention to the follow up of money laundering studies, regular updates on Europol’s Money Laundering and the Financing of Terrorism (MLFT) Report.
- Discuss the importance ofologies (financial environment, key players, phase of money laundering).
- Understand the added value of information on the rules and investigation techniques. To develop guidelines for the application of tools and techniques in order to support serious organised crime and laundering.
- Understand the added value of operational information from the local communities, private sector, NGOs and prosecutors working in cyber-law enforcement.
- Recognise the role of the competent authorities – FIUs, police, tax and customs agencies, financial sector in supporting serious organised crime and tax fraud investigations; to improve asset tracing, determine the value of identified assets, seize related assets, and give evidence of the assets.
- Understand the added value of Europol and international cooperation instruments.
- Design and apply an intelligence collection plan, for investigative or intelligence purposes according to the needs/circumstances of criminal/administrative methods.
- Recognise security features for identity cards/documents, their method of verification by the person.
- Demonstrate good inter-agency cooperation examples through concrete cases especially between law enforcements practitioners, prosecutors, legal experts, financial investigators, and other enforcement and judicial authorities.
- Share best practices how to obtain operational information from the local communities, private sector, NGOs and prosecutors working in cyber-law enforcement.
- Recognise specific methods and techniques of managing, analysing and evaluating financial data.
- Identify crime patterns on various forms of money laundering (cash based, electronic, underground banking, etc.)
- Understand the importance of money laundering investigations independently or alongside investigations related to serious crime.
- Understand the impact of underground banking, the use of virtual currencies and other emerging technologies on criminality.
- Pay special attention to the follow up of money laundering studies, regular updates on Europol’s Money Laundering and the Financing of Terrorism (MLFT) Report.
- Discuss the importance ofologies (financial environment, key players, phase of money laundering).
- Understand the added value of information on the rules and investigation techniques. To develop guidelines for the application of tools and techniques in order to support serious organised crime and laundering.
- Understand the impact of underground banking, the use of virtual currencies and other emerging technologies on criminality.
- Pay special attention to the follow up of money laundering studies, regular updates on Europol’s Money Laundering and the Financing of Terrorism (MLFT) Report.
- Discuss the importance ofologies (financial environment, key players, phase of money laundering).
- Understand the added value of information on the rules and investigation techniques. To develop guidelines for the application of tools and techniques in order to support serious organised crime and laundering.
- Understand the impact of underground banking, the use of virtual currencies and other emerging technologies on criminality.
- Pay special attention to the follow up of money laundering studies, regular updates on Europol’s Money Laundering and the Financing of Terrorism (MLFT) Report.
- Discuss the importance ofologies (financial environment, key players, phase of money laundering).
- Understand the added value of information on the rules and investigation techniques. To develop guidelines for the application of tools and techniques in order to support serious organised crime and laundering.
- Understand the impact of underground banking, the use of virtual currencies and other emerging technologies on criminality.
- Pay special attention to the follow up of money laundering studies, regular updates on Europol’s Money Laundering and the Financing of Terrorism (MLFT) Report.
- Discuss the importance ofologies (financial environment, key players, phase of money laundering).
- Understand the added value of information on the rules and investigation techniques. To develop guidelines for the application of tools and techniques in order to support serious organised crime and laundering.
1. Explain the importance of a personal integrity in policing
2. Recognise the legal and ethical considerations in taking statements from persons suspected of involvement in cybercrime.
3. Define the key role of the police in managing diversity.
4. Share good practices to trace, seize and confiscate VCs.
5. Recognise the Ulterior Motives as a Ground for Investigation.
6. Define direct and indirect evidence in criminal investigations involving cybercrime.
7. Describe the Post-Mortem and Live Data Acquisition.
8. Demonstrate the importance of law enforcement cooperation and information sharing.
9. Conduct Memory Acquisition and perform basic Memory Analysis.
10. Explain the Ulterior Motives as a Ground for Investigation.
11. Understand how data protection in related to the information exchange concerning police cooperation.
13. Search, collect and preserve electronic evidence on the crime scene.
15. Determine the botnet architecture of a malware sample from network analysis.
16. Outline a risk-analysis tacking in account the cyber threats picture.
17. Explain good intervention practice towards persons from different cultures in the situations of: a) Physical violence, b) Psychological violence, and c) Cyber violence.
18. Discover hidden file streams in NTFS file system.
19. Rebuild deleted files history in NTFS file system.
20. Follow modern leadership and communication principles.
22. Rebuild deleted files history in Windows file system.
23. Follow modern leadership and communication principles.
24. Define the key role of the police in managing diversity.
25. Conduct E-mail Investigations.
26. Know how to find Pictures and Metadata.
27. Identify and secure electronic evidence.
28. Conduct Offline Analysis.
29. Document the malware analysis process for evidential purposes.
31. Conduct Online Analysis.
32. Provide an overview of the tools and techniques available to Law Enforcement.
33. Provide an overview of the tools and techniques available to Law Enforcement.
34. Share good practices to trace, seize and confiscate VCs.
35. Share good practices to trace, seize and confiscate VCs.
36. Share good practices to trace, seize and confiscate VCs.
37. Share good practices to trace, seize and confiscate VCs.
38. Share good practices to trace, seize and confiscate VCs.
39. Share good practices to trace, seize and confiscate VCs.
40. Share good practices to trace, seize and confiscate VCs.
41. Share good practices to trace, seize and confiscate VCs.
42. Share good practices to trace, seize and confiscate VCs.
43. Share good practices to trace, seize and confiscate VCs.
44. Share good practices to trace, seize and confiscate VCs.
45. Share good practices to trace, seize and confiscate VCs.
46. Share good practices to trace, seize and confiscate VCs.
47. Share good practices to trace, seize and confiscate VCs.
48. Share good practices to trace, seize and confiscate VCs.
49. Share good practices to trace, seize and confiscate VCs.
50. Share good practices to trace, seize and confiscate VCs.
51. Share good practices to trace, seize and confiscate VCs.
52. Share good practices to trace, seize and confiscate VCs.
53. Share good practices to trace, seize and confiscate VCs.
54. Share good practices to trace, seize and confiscate VCs.
55. Share good practices to trace, seize and confiscate VCs.
56. Share good practices to trace, seize and confiscate VCs.
57. Share good practices to trace, seize and confiscate VCs.
58. Share good practices to trace, seize and confiscate VCs.
59. Share good practices to trace, seize and confiscate VCs.
60. Share good practices to trace, seize and confiscate VCs.
61. Share good practices to trace, seize and confiscate VCs.
62. Share good practices to trace, seize and confiscate VCs.
63. Share good practices to trace, seize and confiscate VCs.
64. Share good practices to trace, seize and confiscate VCs.
65. Share good practices to trace, seize and confiscate VCs.
66. Share good practices to trace, seize and confiscate VCs.
67. Share good practices to trace, seize and confiscate VCs.
68. Share good practices to trace, seize and confiscate VCs.
69. Share good practices to trace, seize and confiscate VCs.
70. Share good practices to trace, seize and confiscate VCs.
71. Share good practices to trace, seize and confiscate VCs.
72. Share good practices to trace, seize and confiscate VCs.
73. Share good practices to trace, seize and confiscate VCs.
74. Share good practices to trace, seize and confiscate VCs.
75. Share good practices to trace, seize and confiscate VCs.
76. Share good practices to trace, seize and confiscate VCs.
77. Share good practices to trace, seize and confiscate VCs.
78. Share good practices to trace, seize and confiscate VCs.
79. Share good practices to trace, seize and confiscate VCs.
80. Share good practices to trace, seize and confiscate VCs.
81. Share good practices to trace, seize and confiscate VCs.
82. Share good practices to trace, seize and confiscate VCs.
83. Share good practices to trace, seize and confiscate VCs.
84. Share good practices to trace, seize and confiscate VCs.
85. Share good practices to trace, seize and confiscate VCs.
86. Share good practices to trace, seize and confiscate VCs.
87. Share good practices to trace, seize and confiscate VCs.
88. Share good practices to trace, seize and confiscate VCs.
89. Share good practices to trace, seize and confiscate VCs.
90. Share good practices to trace, seize and confiscate VCs.
91. Share good practices to trace, seize and confiscate VCs.
92. Share good practices to trace, seize and confiscate VCs.
93. Share good practices to trace, seize and confiscate VCs.
94. Share good practices to trace, seize and confiscate VCs.
95. Share good practices to trace, seize and confiscate VCs.
96. Share good practices to trace, seize and confiscate VCs.
97. Share good practices to trace, seize and confiscate VCs.
98. Share good practices to trace, seize and confiscate VCs.
99. Share good practices to trace, seize and confiscate VCs.
100. Share good practices to trace, seize and confiscate VCs.
Upon completion of the activity the participants will be able to:

1. Communicate in English more efficiently in professional environment
2. Organise effective learning environments for adult learners
3. Review capabilities of existing unmanned aerial vehicle technology
4. Utilise Covert Human Intelligence Sources in a cost-effective way
5. Analyse task, assemble information and recommend solutions
6. Analyse task, assemble information and recommend solutions
7. Correctly use the professional vocabulary
8. Evaluate challenges for efficient anti-corruption strategies and policies
9. Identify links between suspects and their involvement in organised crime or terrorism
10. Diagnose the potential public response to police action influenced by social inequality
11. Prioritise in a way enabling to foster the "value for money" approach
12. Identify needs of a police leader with European perspective (training gaps)
13. Deliver analytical findings through a standardised oral reporting format

Instruments and Methods:

4. Discuss the various steps of strategic advising:
   - Identifying the problem
   - Setting the objectives
   - Identifying appropriate solutions
   - Implementing the recommendations
   - Evaluating the outcomes

5. Use appropriate tools in managing and leading the components of missions, including aspects of
   - Decision-making
   - Crisis management
   - Resource allocation
   - Risk management

6. Use functional language in various policing contexts and environments

7. Analyse the potential impact of further technological developments for law enforcement

8. Review opportunities for continuous quality improvement during residential/online courses by applying
   - Kirkpatrick’s evaluation methodology
   - Continuous quality improvement models

9. Disseminate and harmonise European training styles

10. Diagnose the potential public response to police action influenced by social inequality

11. Prioritise in a way enabling to foster the "value for money" approach

12. Identify needs of a police leader with European perspective (training gaps)

13. Deliver analytical findings through a standardised oral reporting format

14. Analyse task, assemble information and recommend solutions

Gender balance and other EU fundamental principles.
Research and Science Conference
Cybercrime: Fraud & counterfeiting of non-CEPOL online

Webinar
Hungary
Q3
To share good intelligence and investigative
Excise fraud I
Webinar
CEPOL online
29/2020
10/2020
Webinar
CEPOL online
30/2020
To present the criminal phenomena around
Police Cooperation I
09/2020
CEPOL online
June
Q4
02/2020
To enhance the enforcement of environmental
08/2020
CEPOL online
CEPOL online
9 - LE Technologies, Forensics and other
1 - Serious and organised crime - Envi
2 - Cyber related crime
7 - Higher Education and Research
4 - Criminal finances and money laundering I: Anti-
5 - Illicit firearms trafficking I: EU regulations in
6 - Drug trafficking: Heroin/Cocaine/Cannabis

Upon completion of the activity the participants will be able to share knowledge and good practice regarding
1. Understand how police stops and searches as well as profiling are done in a correct manner whilst
especially using TOR-networks and Darkweb
2. Be able to identify the profile of the illegal ammunitions dealers;
3. Be familiar with the most common ways for supply the illegal ammunitions market.
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Describe INCB operational approaches to prevent and interdict NPS, synthetic opioids and precursors;
2. Demonstrate and exchange good practices of asset recovery by using CARIN.
3. Exchange share knowledge and practices on
Exchange share knowledge and practices on
tackling document fraud; experienced
front line police officers, customs enforcers; criminal police forces; forensic
forces; criminal police forces; forensic
experts and document
4. Recognise existing INCB global communication tools;
5. Identify opportunitis for setting-up JITs and recent developments;
6. Be able to identify the existence of a VC wallet, especially using TOR-networks and Darkweb

Upon completion of the activity the participants will be able to:
1. Improve the use of electronic evidence in investigation and prosecution of cybercrime and relevancy and
practicability of such evidence.
2. Identify genuine and forged documents offered via Telegram;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Describe the AMON network in general, the added value of Europol services;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Discuss CARIN features and its added value ;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Identify opportunitis for setting-up JITs and recent developments;
2. Be able to identify the existence of a VC wallet, especially using TOR-networks and Darkweb

Upon completion of the activity the participants will be able to:
1. Discuss CARIN features and its added value ;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Improve the use of electronic evidence in investigation and prosecution of cybercrime and relevancy and
practicability of such evidence.
2. Identify genuine and forged documents offered via Telegram;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Discuss CARIN features and its added value ;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Discuss CARIN features and its added value ;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.

Upon completion of the activity the participants will be able to:
1. Discuss CARIN features and its added value ;
2. Recognise existing INCB global communication tools;
3. Be able to identify the profile of the illegal ammunitions dealers;
4. Demonstrate investigative methods on how to investigate Darkweb networks
5. Exchange information via the available international channels, in particular Europol and Frontex.
9 - LE Technologies, Forensics and other Specific Areas

Social network analysis

Webinar 46/2020 CEPOL online

To provide a comprehensive overview on the main work processes and general techniques that are necessary for the accomplishment of Law Enforcement OSINT.

Upon completion of the activity the participants will be able to:
1. Summarise the LE OSINT approach;
2. Use of general OSINT techniques suitable for the collection of intelligence;
3. Provide input to the analysis and distribution of information for the purpose of tackling all forms of crime in clearweb, socialmedia.

Law enforcements analysts who have some experience of High-Tech crime investigations in clearweb.

TBC

9 - LE Technologies, Forensics and other Specific Areas

Intelligence-led policing

Webinar 47/2020 CEPOL online

To increase the capability of law enforcement officers to collect, evaluate, collate and analyse strategic information and intelligence related to serious and organised crime and submit their results to decision-makers for further exploitation. Enhance the capacities for producing strategic analysis and share effective techniques in order to improve the intelligence-led policing.

Upon completion of the activity the participants will be able to:
1. Understand the concept of intelligence-led policing and evaluate the way this is applied
2. Apply the intelligence-led policing model for effective prevention or suppression of crime
3. Promote the cooperation between intelligence and law enforcement agencies of the EU
4. Clarify certain law restrictions in the implementation of intelligence-led policing model
5. Use technical and analysis tools (e.g. crime mapping) for the intelligence management and analysis
6. Apply and develop new investigation and analytical methods and techniques

Law enforcement officials with tasks related to intelligence cycle and Intelligence-led Policing implementation processes.

TBC

9 - LE Technologies, Forensics and other Specific Areas

Strategic Intelligence Analysis

Webinar 48/2020 CEPOL online

To increase the capability of law enforcement officers to collect, evaluate, collate and analyse strategic information and intelligence related to serious and organised crime and submit their results to decision-makers for further exploitation. Enhance the capacities for producing strategic analysis and share effective techniques in order to improve the intelligence-led policing.

Upon completion of the activity the participants will be able to:
1. Establish the direction of a strategic intelligence analysis project and plan in accordance with expectations of the decision maker;
2. Collect and evaluate information, determine collation methods suitable for different types of data;
3. Utilise risk and/or threat assessment techniques;
4. Analyse quantifiable and non-quantifiable data using various analytical techniques;
5. Understand and apply critical thinking: in deductive and inductive logic, hypotheses development, when constructing conclusions and intelligence requirements

Law enforcement officials possessing knowledge or officers to be prepared to conduct strategic analysis and work experience in the field of strategic criminal analysis particularly with regard to organised crime and terrorism.

TBC

9 - LE Technologies, Forensics and other Specific Areas

Social Media Implications in Law Enforcement

Webinar 49/2020 CEPOL online

To raise awareness of social media implications in Law Enforcement.

Upon completion of the activity the participants will be able to:
1. Demonstrate sufficient theoretical and empirical knowledge about most relevant social media channels
2. Comprehend the effects of various social media on law enforcement procedures and operations
3. Reflect on new investigative opportunities as well as legal, ethical and professional limits
4. Understand the impact of social media for cross-border and transnational police cooperation
5. Discuss how to intervene in practical situations (e.g. with regard to bullying via social media, online sexual abuse, use of social media in public riots, combat radicalisation through social media, etc.)
6. Use various forms of social media (e.g. Twitter, Facebook, YouTube etc.) for law enforcement purposes and to share good professional practice

Law enforcement officials interested in sharing concepts and best practice in how social media can be applied for gathering of relevant information to prevent crime and to conduct investigations and other law enforcement actions.

TBC