Training for Investigators at local level

Concept and objectives : This training would be delivered over a period of 2 times 1 week.

Duration of the Course	**2 TIMES 1 WEEK**
Objectives of the Course	**Develop the capacities of local investigation units in the field of fight against cybercrime by educating in each of them one investigator that would become the local referent, capable to make the best advantage of his competences in local criminal cases, and to communicate adequately with local prosecution office about cases related to cybercrime or cyber enabled crime.**
Educational outcomes	**After completion of the course, the Attendees will be able to :** - identify criminal offense realted to cybercrime / cyber enabled crime - legally gather the evidence of accessible cyber related criminal cases - localize and identify the items that could be exploitable for digital forensic operations - collect open source intelligence (OSINT) and use geolocation tools - utilize the channels of cooperation with ISPs and social networks. - understand the concept and functionning of crypto assets, transaction process, tracking methods and further proceedings
Expected final impact	Generalize the understanding of cybercrime in local criminal investigations units (typology, proceedings, procedures, forensic operations, cooperation, crypto assets) Develop a ressource of investigator capable to deal with accessible cyber enabled crime or cyber crime cases
Profile of the Attendees	**Investigator from local investigation units WILLING :** • **to indulge in the field of fight against cyber crime** • **to attend in this Course**

Schedule of the training

WEEK 1 : Local Police Investigators (only)

Day 1	ToC 1	ToC 1	ToC 2		ToC 3	ToC 3	ToC 4
Day 2	ToC 5	ToC 5	ToC 5		DEC 1	DEC 1	DEC 2
Day 3	DEC 2	DEC 3	DEC 3		DEC 4	DEC 4	DEC 4
Day 4	OSINT 1	OSINT 2	OSINT 3		OSINT 4	OSINT 4	OSINT 4
Day 5	OSINT 5	OSINT 5	OSINT 5		ICA 1	ICA 2	ICA 3

Block 1 : Typology of Crime
Block 2 : Digital Evidence Collection and Cooperation
Block 3 : Open Source Intelligence
Block 4 : Introduction to Crypto Assets

Block 1 : Typology of Crime

Module	ToC 1 Expertise = WB3C
Title	Introduction to Cybercrime and its environment
Duration	2 hours (in two slots with 10 minutes break in the middle)
Outcomes	Introduce Cybersecurity and distinguish Cybercrime *per se* and Cyber enabled crime Distinguish Internet / Web / DeepWeb / Darknet / Darkweb Introduce the following : Protocols / Domains / IP / Hash Introduce the general functioning and architecture of Information system

Module	ToC 2 Expertise = WB3C + Beneficiaries
Title	Typology of Cyber enabled Crime - 1
Duration	1 hour 15
Outcomes	Describe the following cyber enabled crimes, and their modus operandi : • Child exploitation materials : distribution of pedopornographic materials / child abuse / live-streaming of child sexual abuse **Domestic legislation** Describe the elements constituting the offence Describe the digital evidence collection process

Module	ToC 3 Expertise = WB3C + Beneficiaries
Title	Typology of Cyber enabled Crime - 2
Duration	2 hour (in two slots with 15 minutes break)
Outcomes	Define the following cyber enabled crimes • Online Trafficking (weapons, drugs, counterfeit credit cards, false documents, …) • Trading of criminal services (all sorts, …) • Online Frauds (CEO, online payment system, carding …) • Digital identity theft on social networks **Domestic legislation** Describe the elements constituting the offence Describe the digital evidence collection process

Module	ToC 4 Expertise = Beneficiaries
Title	Typology of Cyber enabled Crime - 3
Duration	1 hour 30
Outcomes	Define the following cyber enabled crimes • Cyberstalking – Cyberbullying • Hate on line • Radicalisation on line **Domestic legislation** Describe the elements constituting the offence Describe the digital evidence collection process

Module	ToC 5 Expertise = WB3C + Beneficiaries
Title	Typology of attacks on automated data processing systems - Cybercrime
Duration	3 hours 30 (in three slots with 15 minutes breaks)
Outcomes	Distinguish the following types of attacks and their respective implementation process • Hacking - Malware (all types) • Ransomware • DdoS attacks / DoS attacks • Botnets • Phishing (all types) • Compromised email • Drive-by downloads / USB Drop attacks • Social engineering • Man-in-the-middle / Rogue cell tower / Backdoor • Administrative data breaches / GDPR – LED Directive – Human rights **Domestic legislation** Describe the elements constituting the offence Describe the digital evidence collection process

Block 2 : Digital Evidence Collection and Cooperation : 11 hours

Module	DEC 1 Expertise = WB3C
Title	Legal framework (national or enthity) - Budapest Convention - Cloud Act
Duration	1 hour 30
Outcomes	Introduce the challenges to the principle of territoriality related to localisation of data International instruments on cybercrime / Digital evidence Collection Introduce procedural rules of Budapest Convention + 2nd protocole Digital Markets Act (DMA) / Digital Services Act (DSA) / UN Future Conv. Underline discordance with Cloud Act and problems of for cooperation with US jurisdiction

Module	DEC 2 Expertise = Beneficiaries
Title	Legal Framework on Cooperation with internet service providers Legal Framework on Cooperation with social medias
Duration	2 hours + 1 hour
Outcomes	Discriminate the different sorts of datas : • contents data / trafic data / subscribers data Introduce the different forms of data requests to internet service providers : • data retention order • data emergency reponse request to providers • direct request for providers Describe voluntary cooperation of MSPs Define the respective limits and possibilities of these procedures Introduce the different forms of data requests to social medias : **Domestic Practice / Specificities**

Module	DEC 3 Expertise = Beneficiaries
Title	International cooperation – Cross-border access to digital evidence
Duration	2 hours 30
Outcomes	Describe the following processes : • European investigation order • Mutual legal assistance (MLA) – Competent authorities Introduce European production and preservation orders Discriminate Exchange of intelligence and MLA Define their process, context and methodology **Domestic Practice**

Module	DEC 4 Expertise = WB3C + Beneficiaries
Title	Digital Forensics examinations
Duration	3 hours 30 (three slots)
Outcomes	Describe the different data acquisition forensic methods and respective technical specifications, refinement and processing Itemize the types of equipments that can be examined Search, seizure and preservation of computer and mobile data Interception of content data and trafic data **Domestic Practice / Specificities** Introduce « Council of Europe Guide on Digital Evidence »

Block 3 : Open Source Intelligence

Module	OSINT 1
Title	What is OSINT ? Exploitation in Investigation – Domestic legislation
Duration	45 min.

Module	OSINT 2
Title	Securing my working station
Duration	45 min.

Module	OSINT 3
Title	Operational watch
Duration	1 hour 45

Module	OSINT 4
Title	Active OSINT - Investigations
Duration	3 hours 30

Module	OSINT 5
Title	Practical exercises
Duration	3 hours 30

Block 4 : Introduction to Crypto Assets

Module	ICA 1
Title	Introduction to Crypto Assests (Cryptocurrencies / Tokens / NFT)
Duration	1 hour 15 (in two slots – one break)
Outcomes	Describe the concept and phenomenon of Crypto Assets (Cryptocurrencies / Tokens / NFT) and its processes (creation, utilisation, storage, transactions) EU legislation (MiCA/travel rule) stable coins and basic introduction on the challenges of DeFi.

Module	ICA 2
Title	Introduction to Criminal uses of Crypto Assets Introduction to Criminal Crypto Assets identification / seizure / confiscation / transformation
Duration	1 hour 15
Outcomes	Enumerate the crimes related to / criminal uses of Crypto Assets Describe the process of identification (Seed / Wallets / Masterkey / Blockchain / Hash…) Identify how to search for information in open sources on crypto-assets

Module	ICA 3
Title	Domestic Legislation
Duration	1 hour
Outcomes	Analyse the domestic legal framework per country related to : Criminal uses of Crypto Assets Crypto Assets in WB (seizure / confiscation / transformation) Financial investigations assets management and recovery

WEEK 2 : Prosecutors + Police Investigators (TOGETHER)

Day 1	CASE STUDY 1 – STX 1		CASE STUDY 1 – STX 2
Day 2	CASE STUDY 2 - STX 1		CASE STUDY 2 – STX 2
Day 3	CASE STUDY 2 - STX 3		CASE STUDY 3 – STX 1
Day 4	CASE STUDY 3 – STX 2		CASE STUDY 3 – STX 3

Block 1 : Case Study 1
Block 2 : Case Study 2
Block 3 : Case Study 3

Block 1 : Case Study 1

Module	CS 1 – Situational Training Exercise 1 - STX 1
Title	
Duration	3 hours 30

Module	CS 1 – Situational Training Exercise 2 - STX 2
Title	
Duration	3 hours 30

Block 2 : Case Study 2

Module	CS 2 - Situational Training Exercise 1 - STX 1
Title	
Duration	3 hours 30

Module	CS 2 - Situational Training Exercise 2 - STX 2
Title	
Duration	3 hours 30

Module	CS 2 - Situational Training Exercise 3 - STX 3
Title	
Duration	3 hours 30

Block 3 : Case Study 3

Module	CS 3 - Situational Training Exercise 3 - STX 1
Title	
Duration	3 hours 30

Module	CS 3 - Situational Training Exercise 2 - STX 2
Title	
Duration	3 hours 30

Module	CS 3 - Situational Training Exercise 3 - STX 3
Title	
Duration	3 hours 30