Training for Prosecutors

Concept and objectives : This training would be delivered over a period of 2 separate weeks (2 TIMES 1 WEEK)

Duration of the Course	**2 WEEKS (1 + 1)**
Objectives of the Course	**Develop the capacities of prosecution offices in the field of fight against cybercrime by educating one prosecutor in each of them, who would become the referent, capable to make the best advantage of his competences in criminal cases, to orientate adequately investigations about cases related to cybercrime or cyber enabled crime, and to have the proper understanding in order to present adequately the case in court.**
Educational outcomes	**After completion of the course, the Attendees will be able to :** - identify criminal offense related to cybercrime / cyber enabled crime - understand the collect process of digital evidence on cyber related criminal cases (Forensic / Osint / Requests to ESPs and social medias / …) - comprehend international cooperation instruments and possibilities they offer (Cross-border access to digital evidence - MLA - European investigative order) - identify the exploitable items in digital forensic operations - understand the concept and functionning of crypto assets, transaction process, tracking methods and further proceedings
Expected final impact	Generalize the understanding of cybercrime in prosecution offices (typology, proceedings, procedures, digital evidence collection, cooperation, crypto assets) Develop a ressource of prosecutor capable to deal with accessible cases
Profile of the Attendees	**Prosecutors from Prosecution offices WILLING :** • **to indulge in the field of fight against cyber crime** • **to attend in this Course** **1+ per Prosecution office (30 total)**

Schedule of the training

WEEK 1 : Prosecutors ONLY

Day 1	INTRO	ToC 1	ToC 1		ToC 2	ToC 3	ToC 3
Day 2	ToC 4	ToC 5	ToC 5		DEC 1	DEC 1	DEC 2
Day 3	DEC 2	DEC 3	DEC 3		DEC 3	DEC 4	DEC 4
Day 4	ICA 1	ICA 2	ICA 3		EXPL. IN COURT		SUMMARY

Block 1 : Typology of Crime
Block 2 : Digital Evidence Collection and Cooperation
Block 3 : Introduction to Crypto Assets
Block 4 : Exploitation in Court

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
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 on incriminations** Identify their respective elements constituting the crime Describe the digital evidence collection process

Module	ToC 3 Expertise = WB3C + Beneficiaries
Title	Typology of Cyber enabled Crime - 2
Duration	2 hours (in two slots with 10 minutes break in the middle)
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 their respective elements constituting the crime Describe their respective 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** Identify their respective elements constituting the crime Describe the digital evidence collection process

Module	ToC 5 Expertise = WB3C + Beneficiaries
Title	Typology of attacks on automated data processing systems - Cybercrime
Duration	2 hours (in two slots with 20 minutes break in the middle)
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 • Other forms of data breaches / GDPR – LED Directive – Human rights **Domestic Legislation** Describe their respective elements constituting the crime Describe their respective digital evidence collection process

Block 2 : Digital Evidence Collection and Cooperation

Module	DEC 1 Expertise = WB3C
Title	Legal framework - Budapest Convention - Cloud Act - Challenges
Duration	2 hours (in two slots with 20 minutes break between)
Outcomes	Introduce the principle of territoriality related to localisation of data Present International instruments (Cybercrime / Digital evidence Collection) • Procedural rules of Budapest Convention + 2nd protocole • Digital Markets Act (DMA) / Digital Services Act (DSA) • Cloud Act and cooperation with USA : Alert to the problems of probable cause when gathering evidence from USA jurisdiction - Underline the discordance between the different sources of law

Module	DEC 2 Expertise = Beneficiaries
Title	Legal Framework on Cooperation with internet service providers Legal Framework on Cooperation with social medias
Duration	3 hours (in two slots)
Outcomes	Discriminate the different sorts of datas : • contents data / trafic data / subscribers data Describe 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 / ISPs Define the respective limits and possibilities of these procedures Describe 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	3 hours (in two slots with 20 minutes break)
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	2 hours (in two slots with 20 minutes break)
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 : Introduction to Crypto Assets

Module	ICA 1 Expertise = WB3C
Title	Introduction to Crypto Assests (Cryptocurrencies / Tokens / NFT)
Duration	1 hour 30 (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 this form of criminality

Module	ICA 2 Expertise = WB3C
Title	Introduction to Criminal uses of Crypto Assets Introduction to Criminal Crypto Assets identification / seizure / confiscation / transformation
Duration	1 hour 30
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 Expertise = Beneficiaries
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

Block 4 : Exploitation in Court

Module	Exploitation in Court
Title	
Duration	2 hours

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

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