Next-Gen Cybercrime Investigation & Response	
GANNDALF NextGen Collaborative Cybercrime Investigation Framework	**Course title: Understanding AI-based cyberthreats**
Overall aim	Creating a modern approach to investigating and preventing AI-driven cybercrime by enhancing the skills of investigators and law enforcement through targeted training on emerging AI-based threats and contemporary cybercriminal tactics.
Proficiency level	Advanced
Duration	1 day (4 hours total, divided into 2 sessions)
Target audience	LEAs, prosecutors, and judicial actors
Number of participants	20
Learning outcomes	Getting knowledge of AI threats, how to recognize, investigate, and prepare responses to AI-driven attacks: • Understand the shift from traditional to AI threats • Understand how artificial intelligence is being weaponized • Learn how AI enables phishing, impersonation, and deception at scale • Identify investigation and evidence handling techniques for AI driven attacks • Understand how AI applications can be used against citizen • Recognize how AI is used to create malicious digital content (e.g. fake news, deepfake, fake documents) • Detecting AI manipulated content (using tools and red flags) • Learn methods to detect AI powered bots and textual content
Main thematic areas (topics, subtopics)	**Session 1: Overview of AI-Driven Attacks & Deepfakes (2 hours):** 1. Cybercrime evolution: from malware to AI-powered automation 2. Quick intro to modern AI 3. Why AI threats are harder to detect and trace 4. AI-enhanced spear phishing and social engineering 5. Deepfake videos and audio in cybercrime and fraud 6. Chatbots and generative AI used by threat actors 7. Discussion: • Real-world examples of AI attacks against humans and institutions. 8. Demo and exercise: • Examples of generative AI based attacks **Session 2: Detecting AI-Driven attacks (2 hours):** 1. What is an AI powered system in the era of Generative AI? 2. How AI bots mimic human behaviour on platforms like X (Twitter), Reddit, etc.

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951

	3. Detecting AI-powered disinformation campaigns 4. Detecting AI-generated fake documents (e.g., forged receipts, invoices, IDs) 5. Detecting harmful AI chatbots 6. Challenges in identifying visible indicators of an AI-Driven attack 7. Tools & Examples: • Case examples: e.g. Disinformation spread through US election campaign through AI chatbots in X. • GPTZero, OpenAI Text Classifier - checking if content is AI-generated • **GANNDALF tools - Practical demonstration** 8. Scenario Exercise: a targeted AI powered system that used by thousands of users - team must identify: • Attackers' possible entry methods • Targeted AI subcomponents • Follow-on exploitation 9. Group Discussion: how to integrate AI threat awareness into policing **10. Wrap-Up: Resources and recommendations for further learning**
Cross-cutting and/or horizontal aspects	Raising awareness, increasing in the capabilities of officers for crime detection and investigation, enhancing re- and up-skilling of investigators and law enforcement officers, gaining a comprehensive knowledge of the numerous elements contributing to AI based cyber-attacks
Methods and learning strategy	Trainings in person or online training, real world scenarios, case study simulations, exercises
Learning environment	Conference room with a large screen for displaying/ online platform
Number of trainers	1
Participants' assessment/testing	yes
Course evaluation	yes
Course certification	yes

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951