Course Title:	Cyber Intelligence and Open Source Intelligence (OSINT) Based Operations
Training Area:	481 - Informática
Training Type:	B-learning
Organizational Method:	
Minimum Number of Trainees	8
Maximum Number of Trainees	16
Total Course Hours:	70
Theoretical Course Hours:	40
Practical Course Hours:	30
Pedagogical Team:	
Pedagogical Coordinator:	
Trainers	
Start Date	
End Date	
Course Schedule	
Course Location	

PROGRAM OBJECTIVES

General Goals:	In the end of the course, the students should be able to: • Develop a comprehensive understanding of intelligence operations and their role in contemporary security challenges • Acquire knowledge and skills in utilizing OSINT tools, techniques, and methodologies for intelligence gathering • Comprehend the ethical and legal considerations associated with OSINT and intelligence operations • Analyze and evaluate geopolitical factors and deterrence strategies relevant to intelligence operations
Specific Goals:	In the end of the course the students should be able to: • Gain insights into the cyber threat landscape and the integration of OSINT in cyber warfare • Apply advanced OSINT techniques for social media intelligence, web scraping, dark web investigations, and analytical methods • Learn intelligence fusion approaches, collaboration, and effective reporting of intelligence findings

PREREQUISITES AND SELECTION METHOD:

Access Requirements	Knowledge of Computer systems, cybersecurity and computer security.
Triage process	Individual Interview

EVALUATION

The evaluation of the trainees will be carried out continuously, based on **quantitative** parameters:

- Evaluation form at the end of each Unit (Formative)
- Final Evaluation (Summative)
- Attendance (minimum attendance of 90% of the total course load, missing a complete unit not allowed)

And based on **qualitative** parameters, through observation:

- Punctuality, Participation, Motivation, Interest, Maturity, Relationship with peers, and Relationship with trainers.

Final Grade = Grade from the final evaluation form (weighted in relation to qualitative parameters)

All trainees with a Final Grade equal to or higher than 50% will be approved, according to the following grading scale:"

0% - 49%	Insufficient	Unfit
50% - 69%	Sufficient	Fit
70% to 89%	Good	
90% to 100%	Very Good	

All trainees who achieve satisfactory performance will be awarded a Professional Training Certificate issued by the training entity.

Non-compliance with attendance rules, lack of progress, or failure to make the required payments will result in the non-issuance of the Professional Training Certificate.

Content and Pedagogical Strategy

Unit/Module 1	Intended learning outcomes Knowledge, skills and competences to be developed by the students-:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Introduction to Intelligence Operations and OSINT	• Understand the fundamentals of intelligence operations and OSINT. • Comprehend the significance of OSINT in contemporary intelligence gathering. • Develop an awareness of the legal and ethical considerations associated with OSINT. • Acquire basic knowledge of OSINT tools, techniques, and methodologies.	• Introduction to Intelligence Operations: Concepts, principles, and objectives • Understanding the Role of OSINT in Intelligence Gathering • Overview of Modern Threat Landscape and the Importance of OSINT • Ethical Considerations and Legal Frameworks in OSINT • Introduction to OSINT Tools, Techniques, and Methodologies	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 2	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Covert Operations and Intelligence	• Understand the concept and purpose of covert operations. • Gain insights into the planning and execution of covert operations • Recognize the role of intelligence collection in covert operations. • Analyze the relationship between covert operations and OSINT. • Evaluate case studies to understand the practical application of covert operations and intelligence gathering.	• Covert Operations: Definition, objectives, and historical context • Covert Operations Planning and Execution • Intelligence Collection in Covert Operations • Covert Operations and OSINT: Synergies and Challenges • Case Studies: Real-world examples of successful covert operations and their intelligence aspects	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 3	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Geopolitics, Deterrence, and Cybersecurity	• Assess geopolitical factors impacting intelligence operations. • Comprehend the theory and application of deterrence strategies. • Identify key cybersecurity threats, actors, and motivations. • Analyze the role of OSINT in assessing geopolitical risks and deterrence strategies. • Utilize OSINT techniques to gather and analyze cyber threat intelligence.	• Geopolitical Considerations in Intelligence Operations • Understanding Deterrence: Theory and Application • Cybersecurity Landscape: Threats, Actors, and Motivations • The Role of OSINT in Assessing Geopolitical Risks and Deterrence Strategies • Analyzing Cyber Threat Intelligence through OSINT	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 4	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Military Doctrine and Cyber Warfare	• Understand military doctrine in the cyber domain. • Explore offensive and defensive cyber operations strategies and tactics. • Identify the role of OSINT in military cyber operations. • Analyze case studies to observe the integration of OSINT into military cyber operations.	• Military Doctrine in the Cyber Domain: Principles and Components • Offensive Cyber Operations: Strategies and Tactics • Defensive Cyber Operations: Techniques and Best Practices • Integrating OSINT into Military Cyber Operations • Case Studies: Military Cyber Operations and OSINT Integration	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 5	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Advanced OSINT Techniques	• Explore advanced techniques for social media intelligence (SOCMINT) • Understand web scraping and data mining for OSINT purposes. • Familiarize with dark web investigations techniques and considerations! • Learn advanced analytical methods for OSINT analysis.	• Social Media Intelligence (SOCMINT): Strategies and Tools • Web Scraping and Data Mining for OSINT • Dark Web Investigations: Techniques and Considerations • Advanced Analytical Methods in OSINT	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 6	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Intelligence Fusion and Reporting	• Understand the concept and importance of intelligence fusion • Explore fusion centers and collaboration in intelligence operations • Learn effective reporting and dissemination techniques for intelligence findings • Discover how to leverage OSINT for intelligence fusion and reporting purposes	• Intelligence Fusion: Concepts and Approaches • Fusion Centers and Collaboration in Intelligence Operations • Reporting and Dissemination of Intelligence Findings • Leveraging OSINT for Intelligence Fusion and Reporting	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 7	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Darknet Intelligence Gathering	• Understand the concept and significance of the Darknet in the cybersecurity landscape. • Gain insights into the key concepts, technologies, and tools associated with Darknet intelligence gathering. • Identify and analyze different types of Darknet activities and threat actors. • Acquire knowledge about legal and ethical considerations when conducting Darknet investigations. • Apply practical skills through hands-on case studies and exercises to gather Darknet intelligence effectively.	• Introduction to Darknet and Cybersecurity • Key Concepts in Darknet Intelligence • Darknet Tools and Techniques • Darknet Threat Actors and Activities • Case Studies and Practical Exercises	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Content and Pedagogical Strategy

Unit/Module 8	Intended learning outcomes Knowledge, skills and competences to be developed by the students:	Syllabus	Teaching methodologies	Teaching Resources and Activities
Gamified Real-Life Based Training Exercise	• Apply the intelligence cycle and methodologies for effective cyber intelligence operations. • Acquire hands-on experience in incident response, threat hunting, and APT analysis based on real-life scenarios. • Develop skills in conducting OSINT investigations and gathering intelligence from open sources. • Enhance decision-making abilities and countermeasures formulation against cyber threats. • Apply OSINT tools and techniques to gather information in real-world scenarios. • Develop skills in incident response, threat actor profiling, and social engineering investigations. • Enhance critical thinking and analytical abilities for cyber intelligence operations.	• Real-Life Scenario 1: Incident Response and Threat Hunting • Real-Life Scenario 2: Advanced Persistent Threat (APT) Analysis • Real-Life Scenario 3: Social Engineering and Insider Threats • Attribution and Reporting for Mitigation • Conducting Cyber and OSINT gathering to Identify Threat Actors and Malware • Improving Cyber Intelligence and OSINT Skills • Reviewing the Findings and Insights from the Exercises	Expository Theoretical and Practical Sessions in the Laboratory	Computer Networks Laboratory, Computers, Servers, and Operating System Software

Total Curricular Hours	**60 h**