FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura

Nombre completo	Open Source Intelligence
Código	E000013487
Impartido en	Master in International Security Management [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	5,0 ECTS
Carácter	Optativa
Departamento / Área	Departamento de Relaciones Internacionales
Responsable	Ileana Daniela Serban
Descriptor	Cyber-challenges and narrative information management track

Datos del profesorado

Profesor

Nombre	Pau Muñoz Pairet
Departamento / Área	Departamento de Relaciones Internacionales
Correo electrónico	pmpairet@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

Cyber-challenges and narrative information management track

Competencias - Objetivos

Competencias

SC2 Ability to identify and use the information necessary for the drafting and presentation of memoranda, reports and recommendations on international security issues.

SC4 A systemic understanding and identification of interconnected security challenges.

SC5 Ability to conduct risk assessments at all levels of security management and governance.

SC6 Applied theoretical knowledge needed by any international security professional working in different security areas.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

1. **Understand the Foundations of Open Source Intelligence (OSINT):**
   - Define the concept of open sources and their relevance in contemporary intelligence gathering.
   - Identify the types, characteristics, and primary uses of open sources in intelligence work.
2. **Apply OSINT Principles to Practical Scenarios:**
   - Develop skills in the collection, synthesis, and filtration of information from open sources.
   - Analyse open-source data to produce reliable and actionable intelligence for decision-making at the state and corporate levels.
3. **Enhance Analytical and Decision-Making Skills:**
   - Evaluate the credibility, accuracy, and relevance of open-source information.
4. **Engage with Real-Time OSINT Applications:**
   - Conduct live case studies to explore the practical applications of OSINT in various contexts.
   - Use state-of-the-art tools and methodologies for open-source information gathering and analysis.
5. **Develop Expertise in OSINT Tools and Techniques:**
   - Gain hands-on experience with OSINT platforms, tools, and technologies.
   - Understand the ethical and legal considerations involved in open-source intelligence operations.
6. **Contribute to Strategic Decision-Making Processes:**
   - Utilise OSINT to inform strategies and decisions in security and policy contexts.
   - Communicate findings effectively to diverse stakeholders, ensuring clarity and actionable insights.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Lectures and Readings: Core concepts and frameworks will be introduced during the lectures, while preparatory readings and materials will be shared in advance.

Case Study Analysis: Students apply theoretical knowledge to real-world case studies, fostering critical thinking.

Group Discussions: In-class debates on emerging threats, international policies, and ethical concerns.

Simulation Exercises: Hands-on simulations.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Evaluation	(%)
Final evaluation	50%
Participation	20%
In-class exercises	30%

Calificaciones

To be eligible to sit the ordinary exam session, students must not have unjustifiably missed more than one third of the classes. Failure to meet this requirement may result in the loss of both the ordinary and extraordinary exam sessions (Art. 93.1 of the General Regulations).

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica
TBC for each activity.