GUÍA DOCENTE
2025 - 2026

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Cyberspace and Cybersecurity
Código	E000013485
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	Daniel Pérez Fernández
Departamento / Área	Departamento de Relaciones Internacionales
Correo electrónico	dpfernandez@ext.comillas.edu
Profesor	
Nombre	João Luís Gonçalves dos Reis Nunes
Departamento / Área	Departamento de Relaciones Internacionales
Correo electrónico	jnunes@comillas.edu
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

SC3 Ability to identify and work with multiple actors and institutions to address uncertainty in the global security landscape in an adaptive manner.

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.

SC7 Ability to carry out research work with academic and scientific rigour on international security topics.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

1, *AI, algorithms and the digital realm: Societal and individual security implications*

Assess the implications, for societal and individual security, of the growing use of AI.

Topics to be discussed include the use of AI for surveillance; the weaponisation of AI by extremist movements and in disinformation campaigns; and the implications of AI biases.

This topic will also discuss the implications of increasingly digital security apparatuses, including the societal and individual impact of datafication and algorithms.

2, *Introduction to cyber-risk management*

The primary objective of this topic is to provide students with an initial understanding of cyber-risk management.

The aim is for students to become familiar with the various categories of risks and threats inherent to cyberspace (distinguishing between internal and external threats, as well as between malicious and non-malicious ones), and to comprehend the diverse strategies applicable for their prevention, treatment, and mitigation or (if possible) resolution.

3, *The regulation of AI*

The purpose of this topic is to provide students with a foundational understanding of the principles underlying artificial intelligence regulation, both generally and in specific sectors.

It aims for students to grasp the inherent limitations of this process, given that AI is a rapidly evolving tool with emergent properties. Through this block of content, students are expected to comprehend these and other factors impacting any regulatory endeavor concerning AI, as well as to understand the specific and distinctive approaches taken to regulate (albeit partially) artificial intelligence in the European Union, the United States, the United Kingdom, and China.

4, *Responding to Cyber Crises*

- Define what constitutes a “cyber crisis” and distinguish between its main types (nation-state attack, hacktivism, infrastructure failure, etc.).
- Analyse landmark case studies (Estonia 2007, “Melilla cyberattack,” and the Spanish national power-grid outage) to understand attack vectors and impact.
- Identify root causes of cyber crises and trace escalation pathways from intrusion to full-blown crisis.
- Map key stakeholders (CIO, CSIRT, legal, PR, law enforcement, regulators) and clarify each one’s role in crisis response.
- Appreciate the strategic communications (STRATCOM) dimension: why coordinated messaging is vital during and after an event.

5, *Cyber Weapons use and regulation*

- Define "cyber weapons," classify their main types (malware-based, logic-bombs, zero-days, botnets, etc.) and capabilities.
- Describe the full weapons life-cycle (research, development, testing, deployment, and retirement) and frame proliferation as a strategic risk.
- Analyze existing and emerging regulatory frameworks (international law, arms-control treaties, export controls, norms building) and discuss options for stronger governance.
- Understand how to integrate cyber-weapons into broader military planning and doctrine, including target selection, collateral-damage estimation, and rules of engagement.
- Apply decision-making frameworks in a simulated military offensive cyber-operation.

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 in cybersecurity, fostering critical thinking.

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

Simulation Exercises: Hands-on simulations for incident response planning, policy drafting, and AI integration in threat detection.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Evaluation	(%)
Final project	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).

Committing a serious academic offense—such as plagiarism of previously published materials, cheating during an exam or other assessed activity, or failing to respect basic rules of conduct—may lead to disciplinary proceedings and the loss of two exam sessions.

The use of AI to generate entire assignments or substantial parts thereof, without citing the source or tool used, or when not explicitly allowed in the assignment instructions, will be considered plagiarism and regulated in accordance with the University's General Regulations.

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

- Arunesh, S., Nguyen, T. H., Kar, D. 2015. "From physical security to cybersecurity", *Journal of Cybersecurity*, *1*(1), 19–35.
- Beskow, D. A., Carley, K. M. 2019. *Social cybersecurity: an emerging national security requirement, military review*, March–April 2019 (https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/).
- Graham, M., Dutton, W. H. (eds). 2014. *Society and the Internet: How Networks of Information and Communication are Changing Our Lives*, Oxford University Press, Oxford.
- Goolsby, R. 2020. "Developing a new approach to cyber diplomacy". *Future Force*, *6*(2), 8–15.
- Henriksen, A. 2019. "The end of the road for the UN GGE process: The future regulation of cyberspace", *Journal of Cybersecurity*, *5*(1), 1-9.
- Howard, P.N., Kollanyi, B. 2016. "Bots, #strongerin, and #brexit: computational propaganda during the UK-EU referendum". Available at *SSRN 2798311*.
- Howard, P. N., Woolley, S., Calo, R. 2018. "Algorithms, bots, and political communication in the US 2016 election: the challenge of automated political communication for election law and administration". *J Inform Tech Polit 15*(2), 81–93.
- Karpf, D. 2012. "Social science research methods in internet time", *Information, Communication & Society*, *15*(5), 639–661.
- Lucas, E., Nimmo, B. 2015. "Information warfare: what is it and how to win it". CEPA Infowar Paper 1.
- Romanosky, S. 2016. "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, *2*(2), 121–135.

Bibliografía Complementaria

This will be shared before each session.