Course Title	Cyber Threat Intelligence				
Course Code	CYS660				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year/1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	3 Hours / 14 weeks	Laboratories / week	None
Course Purpose and Objectives	The course will help students: • become familiar with the CTI lifecycle, • understand common intelligence formats, • explain the different types of threat actors and what impact they can have on an organisation. • understand the adversary. • gather intelligence requirements. • formulate a collection plan and align relevant sources and agencies • analyse information in order to produce actionable intelligence. • identify, collect, and integrate intelligence feeds. • understand the intelligence requirements of an organisation.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Find, evaluate, and integrate CTI sources • Identify sources of information about threats to an organization • Produce CTI from public and private data sources • Disseminate threat intelligence and threat findings for decision-makers • Apply CTI models including the Diamond Model, Cyber Kill Chain, F3EAD, the Intelligence Cycle, OODA, MITRE ATT&CK et.al • Identify how threat actors conduct activities in cyberspace to achieve their objectives. • Discover previously unknown threats • Logically assess and criticize threat intelligence from any source and improve your own • Explain how CTI is used within an organisational context • Explain what the intelligence cycle is and how it is used by CTI analysts to produce actionable intelligence • Safely probe, infiltrate and monitor adversary campaigns • Use Structured Analytics Techniques to attribute cyber attacks • Produce threat intelligence products such as reports, briefings and IOCs • Explain how vulnerabilities in information systems are discovered.				

<table>
<tr><td></td><td colspan="3">

- Applying cyber intelligence to make recommendations for changes to information system security design, implementation, policies, and practices

</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>CYS600</td></tr>
<tr><td>Course Content</td><td colspan="3">

- What is CTI, Defining CTI Analysis,
- Advantages of CTI
- Understanding CTI
- Objectives of CTI
- Tactical intelligence
- Operational intelligence
- Strategic intelligence
- The Six Phases of the CTI Lifecycle and Frameworks
- Analytical Frameworks for CTI
- Attack Lifecycle, Kill Chain, Diamond
- CTI Environment
- Applying Intelligence
- Collecting Intelligence
- Generating Intelligence
- CTI for Security Operations
- CTI for Incident Response
- CTI for Vulnerability Management
- CTI for Vulnerability Management
- CTI for Risk Analysis
- CTI for for Digital Risk Protection
- Clarify your CTI needs and goals
- Developing the CTI team
- How organizations use CTI
- Case studies

</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">E-Learning
As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.</td></tr>
<tr><td>Bibliography</td><td colspan="3">Cyber Threat Intelligence_ The No-Nonsense Guide for CISOs and Security Managers, Aaron Roberts

Incident Response with Threat Intelligence, Roberto Martinez

Practical Threat Intelligence and Data-Driven Threat Hunting, Valentina Palacín

The Threat Intelligence Handbook Christopher Ahlberg</td></tr>
<tr><td>Assessment</td><td colspan="3">

Examinations	50%
Assignments/On-going evaluation	50%
	100%

</td></tr>
<tr><td>Language</td><td colspan="3">English</td></tr>
</table>