Course Outline

Code: SEC702  
Title: Cyber Intelligence

School: Science & Engineering  
Teaching Session: Semester 1  
Year: 2019  
Course Coordinator: Dennis Desmond  
Course Moderator: Professor David Lacey

Please go to the USC website for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1 Description
In this online course, you will learn about the conduct of open source intelligence collection, and the measures used by criminals to conceal and obfuscate their online identities and activities. You will learn about useful software applications and tools, identity exploitation and techniques, online cyber tradecraft, markets and currencies. You will learn about useful software applications and tools, identity exploitation and techniques, and online cyber tradecraft that will enable you to develop the professional skills of a cyber investigator.

1.2 Field trips, WIL placements or activities required by professional accreditation

<table>
<thead>
<tr>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

2. What level is this course?
700 level Specialised - Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?
12 units
4. **How does this course contribute to my learning?**

<table>
<thead>
<tr>
<th>Specific Learning Outcomes</th>
<th>Assessment tasks</th>
<th>Graduate Qualities or Professional Standards mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>On successful completion of this course, you should be able to:</td>
<td>You will be assessed on the learning outcomes in task/s:</td>
<td>Completing these tasks successfully will contribute to:</td>
</tr>
<tr>
<td>Plan a strategy to collect OSINT while maintaining operational security</td>
<td>3</td>
<td>Empowered</td>
</tr>
<tr>
<td>Apply open source collection techniques used by cyber investigators</td>
<td>1, 2, 3</td>
<td>Empowered</td>
</tr>
<tr>
<td>Develop online tradecraft skills to conceal intent and obfuscate your identity to facilitate online collection of investigatory information.</td>
<td>1, 2</td>
<td>Empowered</td>
</tr>
<tr>
<td>Recognise and mitigate vulnerabilities in Identity data and Personal Electronic Devices (PEDs).</td>
<td>1</td>
<td>Empowered</td>
</tr>
<tr>
<td>Perform identify resolution to authenticate and differentiate online identities and analyse findings.</td>
<td>3</td>
<td>Creative and Critical Thinker</td>
</tr>
<tr>
<td>Detect illicit online behaviour</td>
<td>2</td>
<td>Knowledgeable</td>
</tr>
<tr>
<td>Communicate online investigatory findings and competencies</td>
<td>1, 3</td>
<td>Engaged</td>
</tr>
</tbody>
</table>

5. **Am I eligible to enrol in this course?**

Refer to the [USC Glossary of terms](#) for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1 **Enrolment restrictions**

Enrolled in program Sc510 or SC704

5.2 **Pre-requisites**

Nil

5.3 **Co-requisites**

SEC701

5.4 **Anti-requisites**

Nil

5.5 **Specific assumed prior knowledge and skills (where applicable)**

Students will be assumed to understand how the Internet operates and its role in society. They will be expected to have a working knowledge of computer systems and networks.

6. **How am I going to be assessed?**

6.1 **Grading scale**

Limited – Pass (PU), Fail (UF). All assessment tasks are required to be passed for successful completion of the course.
6.2 Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment during tutorials.

6.3 Assessment tasks

<table>
<thead>
<tr>
<th>Task No.</th>
<th>Assessment Product</th>
<th>Individual or Group</th>
<th>Weighting</th>
<th>What is the duration/length?</th>
<th>When should I submit?</th>
<th>Where should I submit it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Digital Portfolio</td>
<td>Individual</td>
<td>PU/UF</td>
<td>3000 words equivalent</td>
<td>Week 15</td>
<td>Online Assignment Submission</td>
</tr>
<tr>
<td>2</td>
<td>Identity Intelligence</td>
<td>Individual</td>
<td>PU/UF</td>
<td>2,000 words equivalent</td>
<td>Week 7</td>
<td>Online Assignment Submission</td>
</tr>
<tr>
<td>3</td>
<td>Open Source Collection Management</td>
<td>Individual</td>
<td>PU/UF</td>
<td>2,000 words equivalent</td>
<td>Week 11</td>
<td>Online Assignment Submission</td>
</tr>
</tbody>
</table>

Assessment 1: Digital Identity Portfolio

**Goal:** The goal of this task is to demonstrate the skills necessary to operate securely and effectively online.

**Product:** Portfolio

**Format:** This task will involve developing and mastering a number of online tradecraft competencies. You will present evidence that you can configure devices to harden them against intrusion and exploitation from criminal or nation state attacks.

**Criteria:** Demonstration of:
- Application of open source collection techniques.
- Development of tradecraft skills
- Recognition and mitigation of vulnerabilities
- Communication of competencies

Assessment Task 2: Identity Intelligence

**Goal:** The goal of this task is to demonstrate your understanding in the development of an online persona and acquisition of social media accounts to collect open source intelligence.

**Product:** Artefact - Creative

**Format:** You will develop an online persona with multiple accounts with the purpose of collecting social media Intelligence (SOCMINT). You will produce a profile with persona data and evidence of accounts created.

**Criteria:**
- Application of open source collection techniques
- Development of tradecraft skills
- Detection of illicit online behaviour Recognition and mitigation of vulnerabilities
Assessment Task 3: Open Source Collection Management

<table>
<thead>
<tr>
<th>Goal:</th>
<th>The goal of this task is to develop an effective collection management strategy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product:</td>
<td>Artefact - Creative, and Written Piece</td>
</tr>
<tr>
<td>Format:</td>
<td>You will produce evidence of your ability to identify sources of information, the tools and techniques needed to collect and harvest the information, analyse the results and report the findings</td>
</tr>
</tbody>
</table>
| Criteria: | • Application of open source collection technique  
• Analysis of collection results  
• Preparation of data collection strategy  
• Communication of findings |

7. What are the course activities?

7.1 Directed study hours

The directed study hours listed here are a portion of the workload for this course. A 12 unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

<table>
<thead>
<tr>
<th>Location:</th>
<th>Directed study hours for location:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>This online course will take between 10-12 hours per week and may have a combination of: webinar, peer to peer collaboration, asynchronous online materials and work, and synchronous lecturer and peer to peer zoom meetings.</td>
</tr>
</tbody>
</table>

7.2 Course content (Draft)

<table>
<thead>
<tr>
<th>Week # / Module #</th>
<th>What key concepts/content will I learn?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Introduction to Cyber Intelligence and Open Source Intelligence</td>
<td>Cyber Intelligence and Open Source Intelligence as collection disciplines, Structure of the Internet, Basic Operating Systems, HTML and XML, Browser Basics, Major Search Engines, Bots and Indexing, Keyword and Boolean Search techniques, Specialty Search Engines and Google Dorking, Automated, Manual, Commercial and Custom Search tools, Image matching and Web Scraping Techniques</td>
</tr>
<tr>
<td>2 Identity Management</td>
<td>Identity Defence and Privacy Protection in Online Environments Online Identity Anonymity through VPNs, Proxies and TOR Management and Obfuscation Techniques, Privacy and Minimisation Rules, Finding People, Social Media Exploitation, and Resolving identities in OSINT</td>
</tr>
<tr>
<td>4 Device Security</td>
<td>Technical (Device) Exploitation, OPSEC While Using Personal Devices, Privacy and Information Management, Location Services, Wi-Fi and Bluetooth, Ad Servers and Application Data Leakage, Device Security, Phauna – Hostile Software, NETSEC, PERSEC, COMSEC, INFOSEC</td>
</tr>
</tbody>
</table>

8. What resources do I need to undertake this course?

Please note that course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Blackboard site. Please log in as soon as possible.
8.1 Prescribed text(s) or course reader
Please note that you need to have regular access to the resource(s) listed below as they are required:

<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Title</th>
<th>Publisher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bazzell, Michael</td>
<td>2017</td>
<td>Personal Digital Security</td>
<td>Nil</td>
</tr>
</tbody>
</table>

8.2 Specific requirements
This is an online course and will require access to a personal computer, laptop or tablet and access to the Internet for at least 10 hours per week.

9. How are risks managed in this course?
Health and safety risks for this course have been assessed as low.
It is your responsibility as a student to review course material, search online, discuss with lecturers and peers, and understand the health and safety risks associated with your specific course of study. It is also your responsibility to familiarise yourself with the University’s general health and safety principles by reviewing the [online Health Safety and Wellbeing training module for students](https://example.com), and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1 Assessment: Academic Integrity
Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

10.2 Assessment: Additional requirements
Limited Graded Course:
This course will be graded as Pass in a Limited Grade Course (PU) or Fail in a Limited Grade Course (UF) as per clause 4.1.3 and 4.1.4 of the Grades and Grade Point Average (GPA) - Institutional Operating Policy of the USC. In a course eligible to use Limited Grades, all assessment items in that course are marked on a Pass/Fail basis and all assessment tasks are required to be passed for a student to successfully complete the course. Supplementary assessment is not available in courses using Limited Grades.

10.3 Assessment: Submission penalties
You must contact your Course Coordinator and provide the required documentation if you require an extension or alternate assessment.
10.4 Study help
In the first instance, you should contact your tutor, then the Course Coordinator. Additional assistance is provided to all students through Academic Skills Advisers. To book an appointment or find a drop-in session go to Student Hub.
Contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au

10.5 Links to relevant University policy and procedures
For more information on Academic Learning & Teaching categories including:
- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website:
http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.6 General Enquiries
In person:
- USC Sunshine Coast - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- USC SouthBank - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- USC Gympie - Student Central, 71 Cartwright Road, Gympie
- USC Fraser Coast - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay

Tel: +61 7 5430 2890
Email: studentcentral@usc.edu.au