Module Layout
SEC101 Principles of Cyber Warfare

<table>
<tr><td><b><i>Faculty</i></b></td><td>STHEE</td><td colspan="5">Faculty of Pure and Applied Sciences</td></tr>
<tr><td><b><i>Programme of Study</i></b></td><td>SEC</td><td colspan="5">Security and Defense</td></tr>
<tr><td><b><i>Module</i></b></td><td>SEC101</td><td colspan="5">Principles of Cyber Warfare</td></tr>
<tr><td rowspan="3"><b><i>Level of Study</i></b></td><td colspan="2"><b>Undergraduate</b></td><td colspan="4"><b>Graduate</b></td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2"><b>Master</b></td><td colspan="2"><b>Doctoral</b></td></tr>
<tr><td colspan="2">✓</td><td colspan="2"></td></tr>
<tr><td><b><i>Language of Instruction</i></b></td><td colspan="6">English</td></tr>
<tr><td><b><i>Mode of Delivery</i></b></td><td colspan="6">Distance Learning</td></tr>
<tr><td rowspan="2"><b><i>Module Type</i></b></td><td colspan="3"><b>Required</b></td><td colspan="3"><b>Electives</b></td></tr>
<tr><td colspan="3">✓</td><td colspan="3"></td></tr>
<tr><td rowspan="2"><b><i>Number of Group Consulting Meetings</i></b></td><td colspan="2"><b><i>Total</i></b></td><td colspan="2"><b><i>Physical Presence</i></b></td><td colspan="2"><b><i>Online</i></b></td></tr>
<tr><td colspan="2">14</td><td colspan="2">0</td><td colspan="2">14</td></tr>
<tr><td><b><i>Number of Assignments</i></b></td><td colspan="6"><i>2 Assignments, 12 Interactive Exercises</i></td></tr>
<tr><td rowspan="2"><b><i>Final Grade Calculation</i></b></td><td colspan="2"><b><i>Assignments</i></b></td><td colspan="2"><b><i>Interactive activities</i></b></td><td colspan="2"><b><i>Final exam</i></b></td></tr>
<tr><td colspan="2">30%</td><td colspan="2">20%</td><td colspan="2">50%</td></tr>
<tr><td><b><i>Number of European Credit Transfer System (ECTS)</i></b></td><td colspan="6">10</td></tr>
</table>

Module Description
The purpose of this module is to introduce students with the basic principles of cyber warfare, the key actors involved in cyber operations, the common threats in the cyber space but also with the latest threats in physical installations and the respective counter measures. Through historical incidents, the course delves into the cyber capabilities of the most active countries and how these have been used either to defend the domestic infrastructures or attack an adversary and gain competitive advantage in a conflict. The course also presents the tools, tactics and techniques that are used in such conflicts and their impact to the adversaries. Subsequently, it is discussed how cyber warfare can be combined with psychological or hybrid warfare in order to magnify its impact. Then, particular cyber space operations are discussed such as cyber terrorism and cybercrimes which blossom and constitute an incessant threat against nations and individuals. The use of social media and how can someone be easily exposed is finally discussed and protection techniques are explained. The course concludes by providing a glimpse of future technologies that will drive cyber warfare and its foreseen implications in cyber war.

Pre-requisite Modules	
None	

Co-requisite Modules	
None	

Grading Scheme				
Assessment Method	***Percentage on Final Grade***	***Workload***		
		Hours	***ECTS***	
Weekly study- Assignments -Group Meetings *(14 weeks *~14 hours)*	**0%**	175-210	7	
Assignment 1	**15%**	25-30	1	
Assignment 2	**15%**	25-30	1	
Interactive activities	20%	25-30	1	
Final exam	**50%**	3		
Total	**100%**	**250-300**	**10**	

Grading Rules and Assessment methods

- Students are evaluated with 9, if they earn 90% of the possible grade, I.e. 90%*10=9, etc.
- Passing rate
  - 50% of the Assignments
  - 50% of the Interactive Activities
  - Students are allowed to participate in the final exam of a Module if they have overall earned the minimum grade (≥ 50 %) in both their Assignments and Interactive Activities
  - 50% of the Final exam

If a student earns a grade with decimal points, then it is rounded to the nearest half unit.