Module name: Cybersecurity and contemporary conflicts

Academic year: 2019/2020  Code: ICBZ-1-514-s  ECTS credits: 4

Faculty of: Computer Science, Electronics and Telecommunications

Field of study: Cyberbezpieczeństwo  Specialty: —

Study level: First-cycle studies  Form and type of study: Full-time studies

Lecture language: English  Profile of education: Academic (A)  Semester: 5

Course homepage: —

Responsible teacher: dr Świątkowska Joanna (joanna.swiatkowska@cc.agh.edu.pl)

Module summary
The emergence of new technologies has brought significant ramifications on all the aspects of our reality. It has also changed the paradigms of national and international security systems and the nature of modern conflicts. Currently, cybersecurity issues are clearly seen as strategic challenges both to nation states and international organizations. The main goal of the course is to identify and analyse the main consequences of this process.

Description of learning outcomes for module

<table>
<thead>
<tr>
<th>MLO code</th>
<th>Student after module completion has the knowledge/ knows how to/is able to</th>
<th>Connections with FLO</th>
<th>Method of learning outcomes verification (form of completion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>M_K001</td>
<td>The course helps to understand the societal, security and economic implications of the cybersecurity. It shows how important is to constantly analyze how cyberspace influence our reality. Students will understand that this must be done in the interdisciplinary ecosystem, and that the team work is the key.</td>
<td>CBZ1A_K04, CBZ1A_K01, CBZ1A_K06, CBZ1A_K02, CBZ1A_K05</td>
<td>Project, Presentation, Participation in a discussion, Oral answer, Involvement in teamwork, Case study, Activity during classes</td>
</tr>
</tbody>
</table>

Skills: he can
| M_U001 | Students gain skills related to cybersecurity from the strategic perspective. They understand impact of modern technologies on the functioning of private and public actors. Thanks to that they know how to implement required solutions, mechanisms, build cooperation. | CBZ1A_U04, CBZ1A_U10 | Project, Presentation, Participation in a discussion, Involvement in teamwork, Execution of laboratory classes, Execution of exercises, Execution of a project, Completion of laboratory classes, Case study, Activity during classes |
| Knowledge: he knows and understands |
| M_W001 | Students know theoretical aspects of the international security system functioning. They understand what challenges and threats (but also opportunities) cyberspace brings to the international community. Thanks to that the participants understand nature of modern conflicts. They also have knowledge how main actors function in this new environment. | CBZ1A_W08, CBZ1A_W09 | Project, Presentation, Participation in a discussion, Involvement in teamwork, Execution of laboratory classes, Execution of a project, Completion of laboratory classes, Case study, Activity during classes |
| M_W002 | Students understand and have knowledge about modern threats and challenges. | CBZ1A_W09 | Activity during classes |

### Number of hours for each form of classes

<table>
<thead>
<tr>
<th>Form of classes</th>
<th>Suma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lectures</td>
<td>60</td>
</tr>
<tr>
<td>Auditorium classes</td>
<td>15</td>
</tr>
<tr>
<td>Laboratory classes</td>
<td>15</td>
</tr>
<tr>
<td>Project classes</td>
<td>0</td>
</tr>
<tr>
<td>Conversation seminar</td>
<td>30</td>
</tr>
<tr>
<td>Seminar classes</td>
<td>0</td>
</tr>
<tr>
<td>Practical classes</td>
<td>0</td>
</tr>
<tr>
<td>Fieldwork classes</td>
<td>0</td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
</tr>
<tr>
<td>Prace kontrolne i prężyściowe</td>
<td>0</td>
</tr>
<tr>
<td>Lektorat</td>
<td>0</td>
</tr>
</tbody>
</table>

### FLO matrix in relation to forms of classes

<table>
<thead>
<tr>
<th>MLO code</th>
<th>Student after module completion has the knowledge/ knows how to/is able to</th>
<th>Form of classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Lectures</td>
</tr>
</tbody>
</table>

Social competence: is able to
The course helps to understand the societal, security and economic implications of the cybersecurity. It shows how important it is to constantly analyze how cyberspace influence our reality. Students will understand that this must be done in the interdisciplinary ecosystem, and that the team work is the key.

Students gain skills related to cybersecurity from the strategic perspective. They understand impact of modern technologies on the functioning of private and public actors. Thanks to that they know how to implement required solutions, mechanisms, build cooperation.

Students know theoretical aspects of the international security system functioning. They understand what challenges and threats (but also opportunities) cyberspace brings to the international community. Thanks to that the participants understand nature of modern conflicts. They also have knowledge how main actors function in this new environment.

Students understand and have knowledge about modern threats and challenges.

Student workload (ECTS credits balance)

<table>
<thead>
<tr>
<th>Student activity form</th>
<th>Student workload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Udział w zajęciach dydaktycznych/praktyka</td>
<td>60 h</td>
</tr>
<tr>
<td>Preparation for classes</td>
<td>5 h</td>
</tr>
<tr>
<td>przygotowanie projektu, prezentacji, pracy pisemnej, sprawozdania</td>
<td>15 h</td>
</tr>
<tr>
<td>Realization of independently performed tasks</td>
<td>35 h</td>
</tr>
<tr>
<td>Contact hours</td>
<td>5 h</td>
</tr>
<tr>
<td>Summary student workload</td>
<td>120 h</td>
</tr>
<tr>
<td>Module ECTS credits</td>
<td>4 ECTS</td>
</tr>
</tbody>
</table>

Additional information
Module content

Lectures
2. Deterrence in cyberspace – strategies, obstacles, challenges and chances.
3. Conflict escalation and de-escalation in cyberspace (cyberdiplomacy, CBMs etc).
4. Warfare in the digital era – how cyberspace influence modern military conflicts (the lecture includes cyberspace usage in context of hybrid conflicts).
5. Espionage in cyberspace.
7. Information warfare in cyberspace.

Auditorium classes
During the first classes students will be divided into a few working groups. Each of them will receive materials related to the topics discussed during lectures, and will be asked to prepare presentations which will deepen the analyzed problems.

Project classes
Designated groups of students will be asked to work on series of tasks which would help them to analyze various aspects related with the potential situation of conflicts. Each group will play the role of different actor and will be asked to conduct various exercises (risk analysis, strategy preparation etc.). All of that will lead to the creation of final projects, which would be presented at the end of the course.

Teaching methods and techniques:
Lectures: The content presented at the lecture is provided in the form of a multimedia presentation.
Auditorium classes: During the auditorium classes, the students solve the problems they have previously asked. The lecturer systematically applies the explanations and moderates the discussion with the group over the given problem.
Project classes: Students carry out the project on their own without major intervention. This is to create a sense of responsibility for group work and responsibility for making decisions.

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:
Participation in the lecture is not mandatory.
Participation in the auditorium classes - participation mandatory - students will be asked to prepare a presentation.
Project classes - first classes will serve for the introductionary purposes. Next, students will independly work on the project having possibility to consult milestones (eventuall concerns, questions) with the teacher.

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:
Lectures:
- Attendance is mandatory: No
- Participation rules in classes: Students participate in the classes gaining knowledge related to its content (according to the syllabus). Students should constantly ask questions and discuss doubts. Audiovisual recording of the lecture requires the teacher's consent.
Auditorium classes:
- Attendance is mandatory: Yes
- Participation rules in classes: Students joining the exercises are required to prepare themselves in the
scope indicated each time by the teacher (eg in the form of task sets). The student’s work assessment can be based on oral or written statements in the form of a colloquium, which according to the AGH study regulations translates into a final grade.

Project classes:
- Attendance is mandatory: Yes
- Participation rules in classes: Students carry out practical work aimed at obtaining competences assumed by the syllabus. The project implementation method as well as the final result are evaluated.

**Method of calculating the final grade**
The final grade will be given based on the quality of performed tasks and presence at the classes.

**Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:**
Nie określono

**Prerequisites and additional requirements**
Language skills
Ability of analytical thinking
Ability to work in a group
Ability to read regulatory documents
Preferably knowledge acquired during the course: Organizacje międzynarodowe a cyberbezpieczeństwo

**Recommended literature and teaching resources**
Main readings – during the lectures students will know which elements from the literature are crucial:

Julia Barlińska, Agata Malecka, Joanna Świątkowska, Cyberbezpieczeństwo: charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali, Warszawa: Tektur, 2018
Martin Libicki, Crisis and escalation in cyberspace. RAND 2012. [Available online].
Materials prepared and suggested during the course by the teacher (especially when it comes to the preparation of the presentations and projects).

Additional:
Joanna Świątkowska (eds.), NATO Road to Cybersecurity, Kosciuszko Institute 2016. [Available online].
NATO Stratcom, Daesh information campaign and its influence, 2016. [Available online].

NATO Stratcom, The Kremlin and Daesh information Activities, 2016. [Available online].


NATO Stratcom, The Next Phase of Russian Information Warfare (by Keir Giles), 2016. [Available online].


James A. Green (eds.), Cyber Warfare a Multidisciplinary analysis, Routledge 2015.

Sean Kanuck, Protecting The Electoral Process And Its Institutions, GCSC Thought Piece, January 2018.

Scientific publications of module course instructors related to the topic of the module


Additional information

None