

Subject	Technology and Terrorism			
	Type	Semester	ECTS	Code
	Obligatory (O)	V	5	
Lecturer of Subject	Prof. Ass. Dr.			
Assistant	n.a			
Tutor	n.a			
Aim and Objective	<p>Specific Objectives:</p> <p>This course will explore the rapidly changing face of cyber warfare and cyber terrorism. Intensive study in specific areas of homeland security with regards to nation-state cyber warfare. This course addresses the definition of, and challenges involved in “cyber warfare” as a subset of information warfare within the context of trans-national state-sponsored actors. To understand these concepts, this seminar will provide an overview of cyber-attack history, the difficulty with cyber-attribution, the myth of cyberterrorism, the very real but poorly understood areas of cyber-espionage and cyber-sabotage. This course also will make clear the digitalization of international terrorism and the new terrorist threats through the internet platform.</p>			
	<p>Course Objectives:</p> <ul style="list-style-type: none"> - Compare several cyber attacks sponsored by rogue nations using open source intelligence and analyze the attack vectors that were implemented in each. - Identify and analyze the historical and conceptual frameworks that precipitate terrorism in the modern world. 			
	<ul style="list-style-type: none"> - Employ the methods of research to find information, analyze its content, & incorporate information into written work about international terrorism - Explain and define the concept "International Terrorism." - Identify and analyze the roots/history of international terrorism - Similarities and differences between Terrorism and Cyber Terrosim. - Compare the motivations behind cyber warfare and cyber terrorist attacks against corporate and government systems. 			

Learning outcomes	<p>After successful completion of this course, students will be able to:</p> <p>Upon successful completion of this module, students will:</p> <ul style="list-style-type: none"> - Define terrorism in their own words, and identify examples of cases of violence that do and do not fit within their definition. - Differentiate between terrorism and insurgency. - Explain why suicide terrorism can be logical in certain situations. - Identify several ways in which terrorists recruit support from non-combatants and international actors. - Identify, analyze, synthesize, and disseminate information about threats and critical incidents. - Demonstrate ability to appropriately use existing and develop new technology and scientific research to contribute to National Security on a global basis. - Articulate strategies for Homeland Security principles for the benefit our global partners. - Identify important civil and human rights concerns generated by security needs and explain the appropriate balance of security with personal privacy, cybersecurity, and commerce. 	
	Content	Course plan
<ul style="list-style-type: none"> - Introduction - Syllabus Overview: Content of the course, concepts, methods, organization, and course requirements. - International Terrorism. - Radical Terrorism and Ideological Terrorism . - Cyber Terrorism and Hackers. - National Security and Political Solutions against Terrorism and Cyber Terrorism. - Terrorism and Social Media platforms. - First test. - Tor, Onion router and Dark Web. - Cyber Crime (Documentary). 		<p style="text-align: right;">1</p> <p style="text-align: right;">2</p> <p style="text-align: right;">3</p> <p style="text-align: right;">4</p> <p style="text-align: right;">5</p> <p style="text-align: right;">6</p> <p style="text-align: right;">7</p> <p style="text-align: right;">8</p> <p style="text-align: right;">9</p>

	- Consequences of Terrorism: Psychological and Political			10
	- Counterterrorism Options and Strategies.			11
	- Case Studies and Simulations:			12
	- International actors and the cooperation against Cyber Terrorism.			13
	- Review, student presentations, and preparation for the final exam.			14
	- Final Exam.			15
Activity / ECTS workload	Aktiviteti			Weight (%)
	34. Interactive lectures			50%
	35. Seminars+exercises (research paper)			30%
	36. Case studies			10%
	37. Simulation (role play)			5%
	38. Study visit			5%
Assessment Methods	Assessment activity	Number	Week	Weight (%)
	10. Participation	1	2-15	50%
	23. Presentations of scientific/professional articles	1	2-15	10%
	24. Participation in lectures	15	1-15	40%
Sources and tools of concretization	Means			Number
	35. Classes			1
	36. Laborator			n/a
	37. Moodle			1
	38. Softuer MATLAB/SPSS/SIMULINK			n/a
	39. Projector			1
ECTS workload	Activity type		Week	Total load
	48. Lectures		2	30
	49. Seminars		1	15
	50. Consultations		0.5	7
	51. Research paper		n.a	21
	52. Independent learning		2-3	50
	53. Exams		1	2
	54. Total			

Literature/References	<p>Basic literature:</p> <ul style="list-style-type: none">- Tilly, Charles (2004), "Terror, Terrorism, Terrorists"- Shapiro (2013), Terrorist's Dilemma- Meronova (2019), From Freedom Fighters to Jihadists.- Spam Nation by Brian Krebs- Cybercrime & The Darknet: Revealing The Hidden Underworld of the Internet by Cath Senker
Contact	
Note:	<ul style="list-style-type: none">- Assessment in this course, as explained above, consists of 3 components: individual research work, presentation of articles and other assignments distributed during the week, and physical and active participation in lectures.- Students who have 3 absences during the semester, the maximum grade they can receive in this course is 7 (seven). Meanwhile, those who have 4 or more absences during the semester, the maximum grade they can receive in this course is 6 (six).- The course instructor reserves the right to make changes and adaptations during the semester in order to achieve the course objectives more effectively. Of course, students will be notified in advance of these changes.