	MS in CYBER SECURITY (NON THESIS) PROGRAM OUTCOMES	NATIONAL QUALIFICATIONS OF RELATED FIELD*																																										
		ENGINNERING																														COMPUTER												
		A1	A2	A3	A4	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	E1	E2	E3	E4	E5	E6	E7	E8	F1	F2	F3	F4	A1	A2	B1	B2	B3	C1	D1	C3	D1	E1	E2	E3	F1
1	Develop the ability to use critical, analytical, and reflective thinking and reasoning	x			x		x	x	x		x					x		x	x				x			x	x					x	x	x										
2	Reflect on social and ethical responsibilities in his/her professional life.																					x						x															x	x
3	Gain experience and confidence in the dissemination of project/research outputs																			x											x											x		
4	Work responsibly and creatively as an individual or as a member or leader of a team and in multidisciplinary environments.	x								x	x												x							x							x							
5	Communicate effectively by oral, written, graphical and technological means and have competency in English.																			x											x										x			
6	Independently reach and acquire information, and develop appreciation of the need for continuously learning and updating.		x		x		x	x										x							x	x														x				
7	Design and model engineering systems and processes and solve engineering problems with an innovative approach.	x	x	x		x	x	x			x	x	x	x			x	x	x				x	x	x				x					x	x									
8	Establish experimental setups, conduct experiments and/or simulations.		x	x		x	x		x			x	x		x		x	x						x	x		x		x						x									
9	Analytically acquire and interpret data.		x	x		x			x			x			x		x							x			x		x						x									
10	To have acquired basic theoretical knowledge and technical infrastructure in the field of cyber security,	x									x												x									x	x											
11	To have developed a deep experience and understanding on the basic methods and human-induced and techinal weaknesses followed by the existing and future cyber attacks, threats and counterfeiting,				x											x																		x	x									
12	To be able to analyze an IT infrastructure comprehensively and to determine risk by monitoring the existing weaknesses and to determine a cyber security strategy,		x																							x								x	x									
13	To take the necessary measures to prevent possible costs and destruction during the occurrence of cyber attacks,	x									x												x											x	x									
14	To be able to use current cyber security software tools and related software for professional purposes,		x																							x												x						
15	To follow the cyber security intelligence news and to combine and analyze data from different sources to take measures for preventing or reducing the prospective cyber attacks,				x																					x												x						
16	To be able to take preventive measures to hinder possible drawbacks by creating a deep understanding and awareness in legal, ethical and social aspects of protecting the security and privacy of personal and corporate data.																											x							x									x

* Please check **http://tyyc.yok.gov.tr/** for the list of national qualifications.

A: KNOWLEDGE, Theoretical & Factual
B: SKILL, Cognitive & Applied
C: COMPETENCY, Working Independently & Taking Responsibility
D: COMPETENCY, Ability to Learn
E: COMPETENCY, Communication & Social Competencies
F: COMPETENCY, Field Specific