İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Bilişim Uzayındaki Savaşlar	Cyber Warefare, Cybersecurity and Defense

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 606	Güz/Bahar (Fall/Spring)	3	7,5	Dr. (Ph.D.)

Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	Türkçe/İngilice (Turkish/English)

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Bilgi güvenliği alanındaki savaşlar, Güvenlik birimleri ve süreçleri, Bilişim uzayının temel özellikleri, Kritik alt yapı ve sistemleri, Stratejik ve işlevsel savaşlar, Saldırı kaynakları, Saldırı türleri, Savunma sistemleri, Gelişmiş siber silahların saptanması ve önlenmesi, Savunma mimarisi, Şifreleme uygulamaları, Elektronik Güvenlik, Bilgi güvenliği standartları, Casusluk ve istihbarat yöntemleri, ulus-devlet düzeyinde siber savaşın işlevsel gereksinimleri, Savaş sistemleri, kavramları, yönetimi, Savaş varlıklarının entegrasyonu, kontrolü ve etkin kullanımı, Savunma yaklaşımları
	Cyberwars, Security units and processes, Basic properties of the cyber world. Critical infrastructures and systems. Strategic and functional cyberwars. Attack sources. Attack types. Defense systems. Detecting advanced cyber weapons and preventing them. Defense architecture. Cryptography applications. Electronic security. Information security standards. Espionage and intelligence methods. Requirements of a cyberwar as a nation / state. Cyberwar management. Integration of cyberwar treasury, its control and efficient use.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	• Siber savaş kavramının tanıtılması • Siber savaşın boyutları üzerine tartışılması • Siber savaş stratejileri üzerine tartışılması • Siber savaş konusunda bilinen açıkların ve önlemlerin öğrenilmesi
	• Introducing cyberwar concept • Discussions on the range of cyberwars • Strategies on cyberwars • Teaching known vulnerabilities and defense methods of cyberwar
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Öğrenciler siber savaş konusunda bilgi sahibi olacaklardır. 2. Öğrenciler siber savaş konusunda akıl yürütecek, yeni ve denenmemiş saldırılar ve savunmalar üzerine tartışacak yetenekte olacaklardır. 3. Siber savaş konusunda bugüne dek karşılaşılan örnekler incelenecek ve bu konuda bir kültür oluşturulacaktır. 4. Politikanın siber savaşa ve bilgi güvenliği mekanizmalarının politikaya etkileri tartışılacaktır
	1. Student will learn cyberwar concept 2. Students will deduce on cyberwar, be able to discuss on novel attacks 3. Students will gain culture by means of discussing previous cyberwar stories 4. Effects of politics to cyberwar and effects of information security mechanisms to politics will be discussed

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1. Cybersecurity and Cyberwar: What Everyone Needs to Know, P.W. Singer, Allan Friedman, 2014, Oxford University Press. 2. Cyber Security Policy Guidebook, Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus Sachs, Jeffrey Schmidt, Joseph Weiss, 2012, Wiley. 3. Cyber War: The Next Threat to National Security and What to Do About It, Richard A. Clarke, Robert Knake, 2012, Ecco. 4. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2nd Ed., Jason Andress, Steve Winterfeld, 2013, Syngress. 5. Cyberpower and National Security, Franklin D. Kramer, Stuart H. Starr, Larry Wentz, 2009, Potomac Books Inc.
Ödevler ve Projeler **(Homework & Projects)**	1 Dönem Ödevi 1 Term Paper
Laboratuar Uygulamaları **(Laboratory Work)**	-- --
Bilgisayar Kullanımı **(Computer Use)**	-- --
Diğer Uygulamalar **(Other Activities)**	-- --

Başarı Değerlendirme Sistemi

(Assessment Criteria)

Faaliyetler (Activities)	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
Yıl İçi Sınavları (Midterm Exams)	1	% 30 (30 %)
Kısa Sınavlar (Quizzes)	-	-
Ödevler (Homework)	-	-
Projeler (Projects)	-	-
Dönem Ödevi/Projesi (Term Paper/Project)	1	% 30 (30%)
Laboratuar Uygulaması (Laboratory Work)	-	-
Diğer Uygulamalar (Other Activities)	-	-
Final Sınavı (Final Exam)	1	% 40 (40%)

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Siber savaş kavramının tartışılması	
2	Saldırılar: siber savaşın yıkıcı ya da ölümcül silahları	
3	Kritik altyapıları denetleyen bilişim sistemleri	
4	Saldırı kaynakları, yöntemleri ve türleri	
5	Kritik sistemlerin denetlenmesi ve analizi	
6	Saldırı önleme yöntemleri	
7	Saldırı geçiştirme yöntemleri	
8	Saldırı sonrası toparlanma yöntemleri	
9	Casusluk ve istihbarat yöntemleri	
10	Ulusal güvenlik ve ulusal bilişim savunma sistemleri	
11	Politik ve işlevsel perspektiflerden siber savaştan kaçınma	
12	Politik ve işlevsel perspektiflerden siber savaş gereksinimleri	
13	Siber savaş savunma ve saldırı stratejileri, ulusal bilişim kaynaklarının entegrasyonu	
14	Siber savaş hukuku	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Discussion on cyberwar concept	
2	Attacks: destructive and lethal weapons of cyberwar	
3	Information systems that control critical infrastructures	
4	Attack sources, methods and types	
5	Control and analysis of critical systems	
6	Attack prevention methods	
7	Defense methods	
8	Post attack recovery	
9	Espionage and intelligence	
10	National security and national informatics defense systems	
11	Preventing cyberwar: from political and functional perspectives	
12	Requirements of cyberwar: from political and functional perspectives	
13	Cyberwar defense and attack strategies, integration of national information systems	
14	Cyberwar laws	

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Doktora Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).		X	
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).			X
iii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).	X		
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).		X	
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).	X		
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	X		
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	X		
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	X		
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).			X
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			X
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).			X
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).		X	

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (PhD) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).		X	
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).			X
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).	X		
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).		X	
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).	X		
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).	X		
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).	X		
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility)	X		
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).			X
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			X
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).			X
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).		X	

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Prof. Dr. Eşref ADALI	31.03.2014	