Siber Savaş – Siber Terörizm

Dr. A. Koltuksuz

Bilgisayar Mühendisliği Bölümü

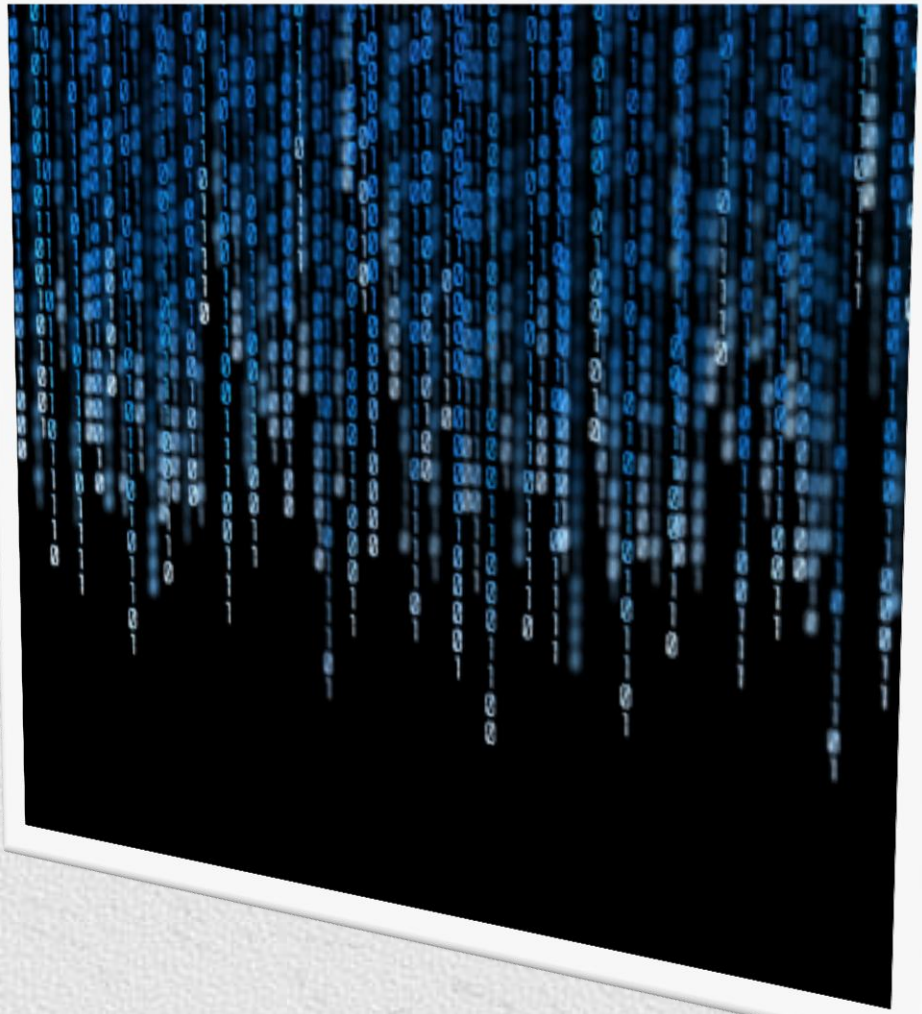
Yaşar Üniversitesi

Gündem

- Bölüm 1 Temel Tanımlar ve Kavramlar
- Bölüm 2 Siber Güvenlik Eğitimi
- Bölüm 3 İşbirliği Önerisi
- Sonuçlar

Bölüm 1 Temel Tanımlar ve Kavramlar

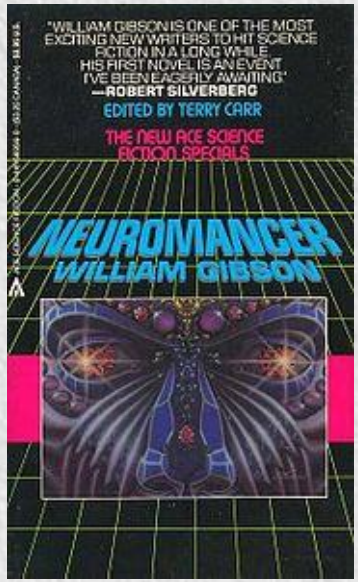
- **Siber Uzay tanımı.**
- **Siber Terörizm ve ilişkin görüşler.**
- **Siber Savaş**
- **Siber Tehditler**
- **NATO 2020**



Dr. Ahmet Koltuksuz

Tanım: Siber Uzay

- "…her ulustan milyonlarca yasal kullanıcının, matematiksel kavramları öğrenen çocukların, her gün yaşadığı anlaşmalı yanılsama. İnsan sistemindeki her bir bilgisayarın kayıtlarından yansıtılan verilerin grafiksel sunumu. Kavranamayacak bir karmaşıklık. Zihnin uzaysızlığında; ışık çizgileri, öbekler ve takımyıldızlar şeklinde düzenlenen veriler…"



William GİBSON
Neuromancer, 1984

Tanım: Siber Uzay

- Sayısallaştırılmış bilginin bilgisayar ağları üzerinden iletişime sokulduğu kavramsal ortam.
- Internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü prosesler ve kontrol birimlerini de içeren, birbirine karşılıklı olarak bağımlı olan, bilgi teknolojisi altyapıları ağı tarafından oluşturulan küresel ortam.

A.B.D. Savunma Bakanlığı

Siber Uzayın Omurgası

Dr. Ahmet Koltuksuz

Siber Uzay ve Bilgi

- **Siber Uzayın en önemli ve değerli değer varlığı BİLGİDİR.**

- **Bilginin her koşulda ve her zaman korunması gereken BAZI temel nitelikleri:**

Bilginin Korunması Gereken Bazı Nitelikleri

- Gizlilik (secrecy)
- Özgünlük (authenticity)
- Doğruluk-Bütünlük (integrity)
- Zamanlılık (timeliness)
- Konuyla İlgili Olma (relevancy)
- Tutarlılık (consistency)
- Tam Olma (completeness)
- Güvenilirlik (reliability)
- Süreklilik (continuity)
- Reddememe (non-repudiation)
- Doğruluk (accuracy)
- Var Olma (availability)
- Tarafsızlık (objectivity)
- Kesinlik (precision)
- Fazlalık (redundancy)
- Okunabilirlik (readability)
- Erişilebilirlik (accessibility)
- Ölçülebilirlik (measurable)

Dr. Ahmet Koltuksuz

Tanım: Siber Terörizm

- Siber terörizm; belirgin bir politik, sosyal veya ideolojik gündeme uygun olarak, bir hükümet veya halkı etkilemek amacıyla; var olan bir kitle üzerinde karmaşa ve belirsizlik oluşturarak, korku ve dehşet yaratmak için; şiddet, yıkım ve/veya hizmetlerde aksama ile sonuçlanacak biçimde, bilgisayarların ve telekomünikasyon imkan ve kaabiliyetlerinin kullanılmasıyla işlenen bir suçtur.

FBI

Tanım: Siber Terörizm

- **Taammüden**; bilgisayarlara ve/veya ağlara karşı zarar vermek maksadıyla veya sosyal, ideolojik, dini, politik veya benzeri amaçlarla, yıkıcı etkinliklerin yapılması, tehdit oluşturulması. Ya da bu amaçlar doğrultusunda olmak üzere herhangi bir insanı korkutmak.

Tanım: Siber Terörizm - İki Ayrı Görüş

- Bu terim uygun değildir; çünkü:
  - Yaygın bir siber saldırı basitçe kişileri sinirlendirir. Bir bomba, kimyasal-biyolojik-radyolojik veya nükleer bir silah gibi teröre yol açmaz.
- Bir başka görüş:
  - Yaygın bir bilgisayar ağı saldırısının etkileri tahmin edilemezdir ve bu nedenle ekonomik durgunluğa, korku ve sivil ölümlerine yol açabilir; dolayısıyla, siber terörizm terimi doğru ve geçerlidir.

Tanım: Siber Savaş

- Siber Savaş; siber uzayda bilgisayarlar ve internetin kullanılmasıyla yapılan savaştır.
- Siber savaş; bilgi savaşlarının bir alt bileşeni olup; siber uzayda gerçekleşen eylemlerden oluşur". "Siber savaş, bilgisayar ağından gelen saldırı, bilgisayar ağı yoluyla yapılan savunma ve, bir olasılıkla, özel bilgi operasyonlarının birleşimidir.

Parks & Duggan

SECURING CYBERSPACE FOR THE 44TH PRESIDENCY

CSIS, 2008

Dr. Ahmet Koltuksuz

Major Findings

- The Commission's three major findings are:

1. Cyber security is now a major national security problem for United States.
2. Decisions and actions must respect privacy and civil liberties.
3. Only a comprehensive national security strategy that embraces both the domestic and international aspects of cyber security will make U.S. more secure.

Steps

- In order to achieve success against cyber terrorism, We recommend the following steps:

1. Creating a comprehensive national security strategy for cyberspace.
2. *New organizations for cyber security.*
3. *Redesigning the public-private partnership.*
4. ***Regulating the cyber space.***
5. ***Modernize laws.***
6. *Modernize digital identities and security.*

Tanım: Siber Savaş Kavramı Üzerine

- Amerikan Hava Kuvvetleri'nden siber uzay ve siber savaşa ilişkin yaklaşımlar:

- **"Ağlar başlı başına bir silah sistemi olarak ele alınmalıdır."**
- **"Ağ karmaşıktır ve bütünüyle güvenli hale getirilemez."**

Brig. Gen. Charles Shugg,

vice commander of the **Air Force Cyber Command (AFCYBER)**,

25 Ocak 2011, Arlington, Va., ABD

Tanım: Siber Savaş Kavramı Üzerine

- Amerikan Deniz Kuvvetleri'nden siber uzay ve siber savaşa ilişkin yaklaşımlar:

- **"Fiziksel ortamların tersine, siber uzayda hakimiyeti ele geçirmek imkansız olabilir.",**
- **"Siber savaş, istihbarat ve kaynaklara ciddi gereksinim duymaktadır. (Siber uzaydaki) Hedeflerimizi ve zayıflıklarımızı bilmek ve aralarındaki ilişkileri anlamak zorundayız".**

Rear Adm. William Leigher, deputy commander of **Navy Fleet Cyber Command.**

26 Ocak 2011, San Diego, ABD.

Tanım Sorunları

- Kavramlar halen biraz bulutsu bir yapı arz etmekte olup;
  - Bilgi Savaşları
  - Siber Savaş
  - Siber Terörizm
  - Bilişim Suçları
  - Online Sosyal Aktivizm

terimleri arasındaki sınırlar, **net değildir!!**

Tanım: Siber Savaş Kavramı Üzerine

Technology & the Warfighter

	Civil War	WWI	WWII	Gulf War	Kosovo	Iraq/Afghan
						
Data Transfer Rate	20 BPS	32 BPS	71 BPS	256 KBPS	1.544 MBPS	? GPS/TPS
Soldiers to Cover 10^2 Km	38,830	4,040	300	24	3	?
Time Line	1865	1914	1945	1991	1999	2007 2010
Technology	 Telegraph	 Telephone	 Computer	 VTC	 Web Tools	 Cognitive Tools

Dr. Ahmet Koltuksuz

Siber Tehditler

- Doğruluk/Bütünlük (integrity) niteliğini yok etmek
- Var oluşu (availability) yok etmek.
- Gizliliği (confidentiality) yok etmek.
- Fiziksel yıkıma yol açmak.

Siber Tehdit Kaynak Sınıflaması

- Siber tehditlerin gelebileceği başlıca alanlar aşağıdaki gibidir.
  - Ulusal Hükümetler
  - Terröristler
  - Endüstriyel Casuslar
  - Organize Suç Grupları-Örgütleri
  - Hacktivistler
  - Hacker'lar

US CERT
Control Systems Security Program (CSSP)

Siber Tehdit Kaynak Sınıflaması

- Bir başka siber tehdit kaynak sınıflaması ise şöyledir:
  - Botnet operatörleri
  - Kriminal gruplar
  - Yabancı istihbarat servisleri
  - Hacker'lar
  - İçeriden saldırılar
  - Phising-oltalama saldırıları
  - Spam'ciler
  - Casus yazılımlar– Zararlı yazılımlar (spyware-malware)
  - Teröristler

NIST 800-82,
"Guide to Supervisory Control and Data Acquisition (SCADA)
and Industrial Control System Security

Siber Tehdit Kaynak Sınıflaması

- Bir diğer siber tehdit sınıflaması:

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	. Hacking . Social engineering . System intrusion, break-ins . Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	. Computer crime (e.g., cyber stalking) . Fraudulent act (e.g., replay, impersonation, interception) . Information bribery . Spoofing . System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	. Bomb/Terrorism . Information warfare . System attack (e.g., distributed denial of service) . System penetration . System tampering

"Cyber Operations and Cyber Terrorism, Handbook Number 1.02", 15 August 2005.

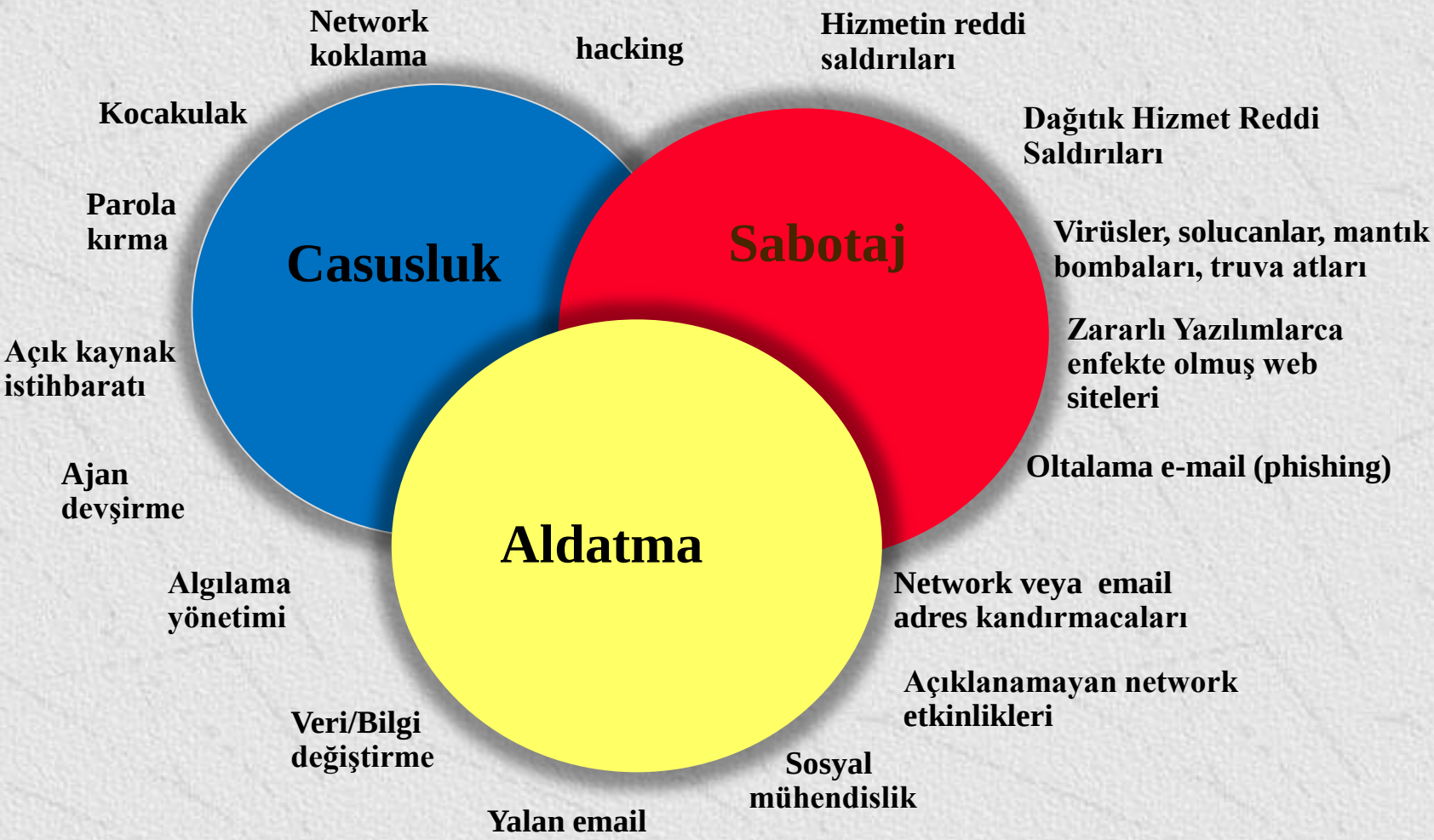
Siber Tehdit Kaynak Sınıflaması

- Bir diğer siber tehdit sınıflaması… (devam)

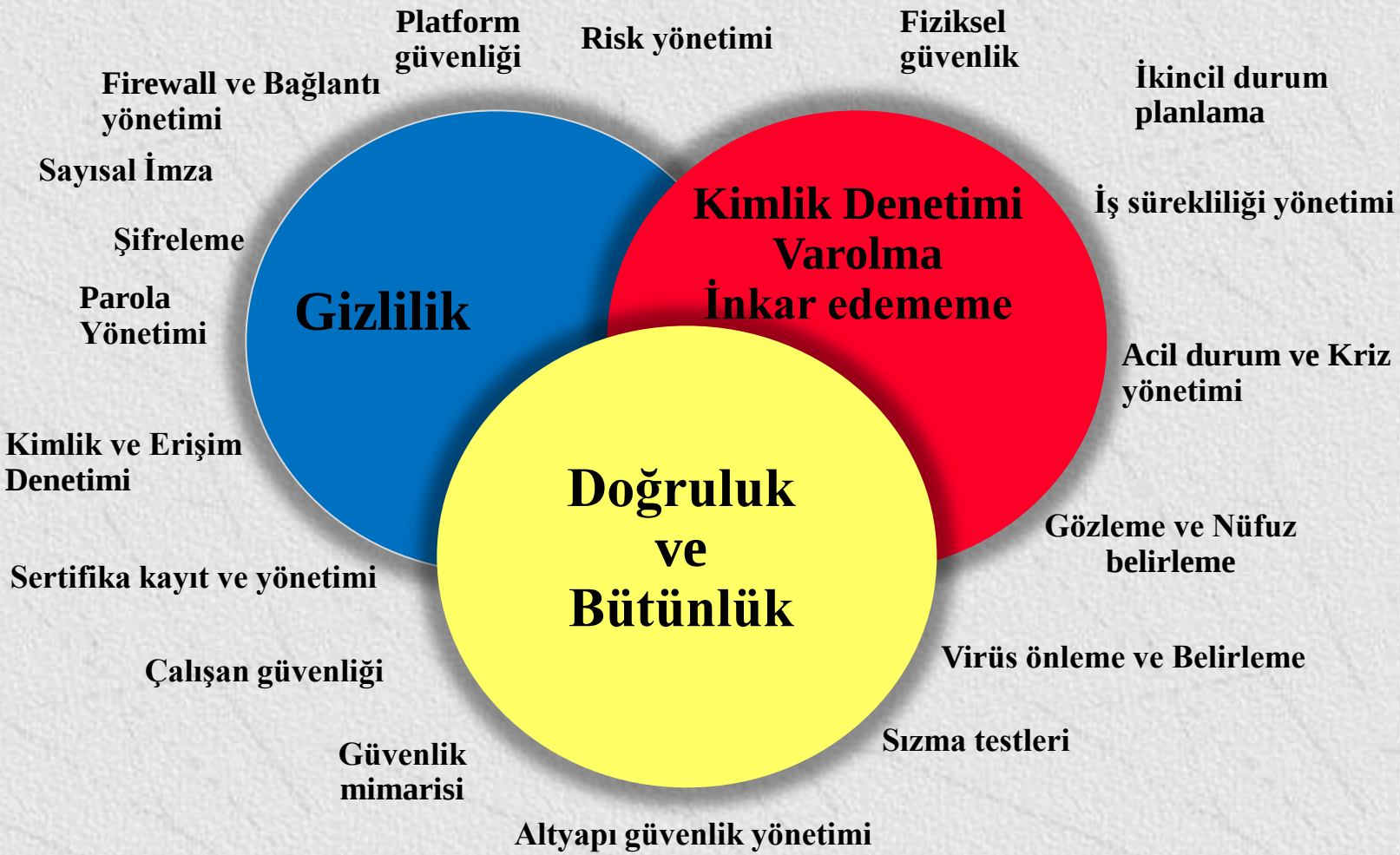
Threat-Source	Motivation	Threat Actions
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	. Economic exploitation . Information theft . Intrusion on personal privacy . Social engineering . System penetration . Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	. Assault on an employee . Blackmail . Browsing of proprietary information . Computer abuse . Fraud and theft . Information bribery . Input of falsified, corrupted data . Interception . Malicious code (e.g., virus, logic bomb, Trojan horse) . Sale of personal information . System bugs . System intrusion . System sabotage . Unauthorized system access

"Cyber Operations and Cyber Terrorism, Handbook Number 1.02", 15 August 2005.

Siber Saldırı Tipleri



Siber Savunma Araçları

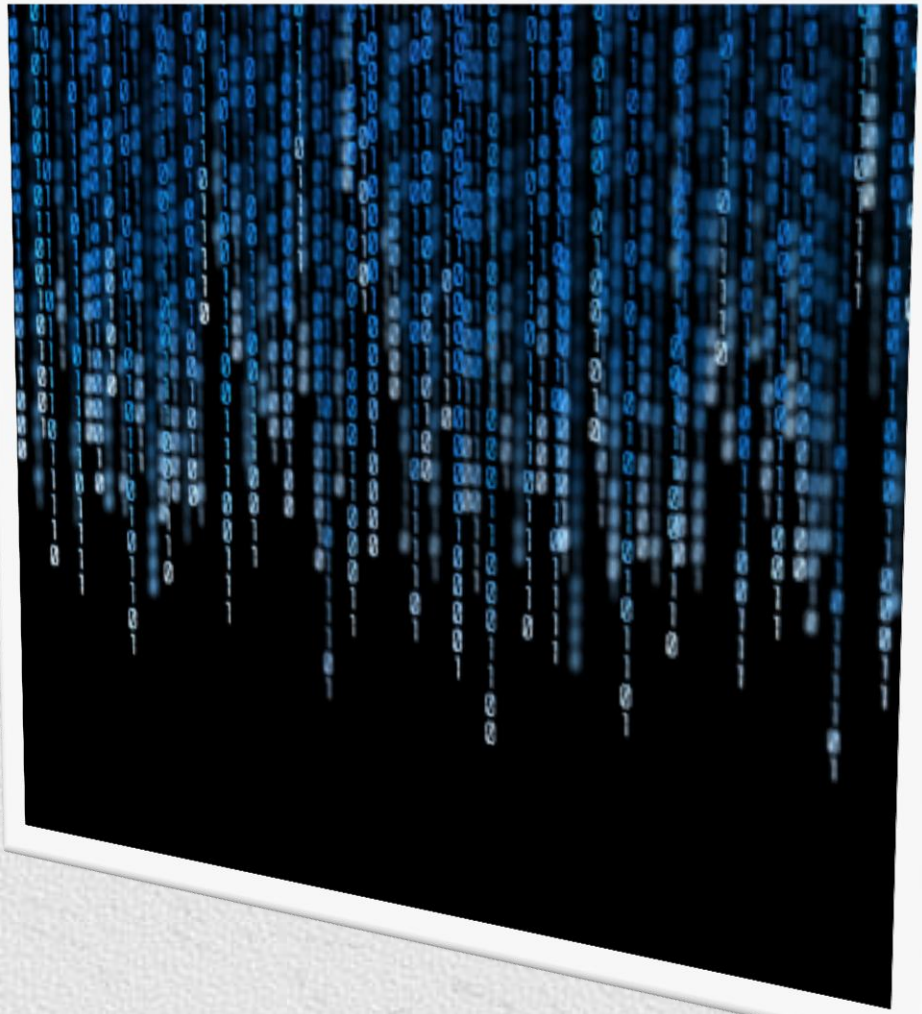


NATO'dan Yeni Stratejik Konsept

- 1960-2010: İki kutuplu, simetrik, kinetik, konvansiyonel ve/veya nükleer savaş tehdit algılaması.
- 2011-2020: Çok kutuplu, asimetrik, konvansiyonel ve/veya nükleer tehditlerin yanısıra, ilk defa **SİBER SAVAŞ** algılaması.
- Türkiye bu yeni stratejik algılamaya imza koymuş durumdadır.

Bölüm 2 Siber Güvenlik Eğitimi

- **Siber Güvenlik Bilim Dalı**
- **Müfredat**



Dr. Ahmet Koltuksuz

Siber Güvenlik Bilim Dalı

- Yaşar Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı

- 24 Mayıs 2012 Tarih ve 8/1 nolu kararı uyarınca:

  Bilgisayar Mühendisliği Anabilim Dalı altında,

  2012-2013 Güz döneminden itibaren,

  Siber Güvenlik Bilim Dalı açılmasına…

Siber Güvenlik Bilim Dalı Müfredatı

- 2 yıllık, tezli, toplam 120 AKTS (ECTS) Yüksek Lisans eğitimi

First Year

Semester & courses		Codes	COURSES	ECTS
1st	1	CENG 551	Probability and Stochastic Processes for Engineers	8
	2	CENG 504	Advanced Information Security	8
	3	CENG 506	Information Theory	8
	4	CENG 535	Computational Number Theory	8
Semester ECTS Credits				32
2nd	1	CENG 502	Algorithm Analysis and Complexity Theory	8
	2	CENG 550	Information Warfare	8
	3	CENG 531	Cryptography	8
	4	CENG 598	Seminar	4
Semester ECTS Credits				28

Second Year

Third Semester

Code	Course Name	Credits	ECTS
CENG 599	Master's Thesis	0	30

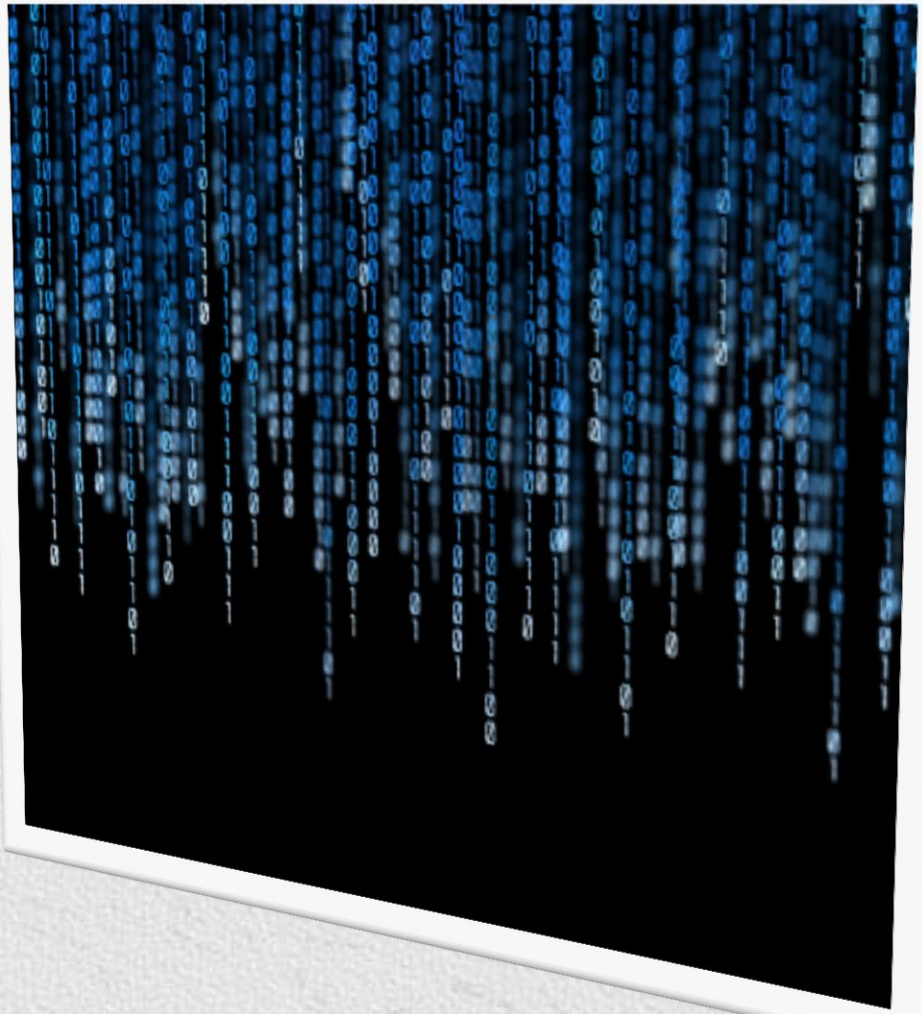
Fourth Semester

Code	Course Name	Credits	ECTS
CENG 599	Master's Thesis	0	30

Dr. Ahmet Koltuksuz

Bölüm 3 İş Birliği Önerisi

- Yüksek Lisans ve Doktora
- Öğrenci etkinliği



İşbirliği İmkan ve Önerileri - 1

- Siber Güvenlik Yüksek Lisans ve doktora programlarını ulusal düzeyde ortak yürütelim.
- Bu amaç doğrultusunda, her üniversite ile, her düzeyde işbirliğine hazırız. Bu işbirliğinin imkan ve kabiliyetleri vardır.
- İzmir Üniversiteleri Platformu buna örnektir.

İşbirliği İmkan ve Önerileri - 2

- 2005 yılında ABD, San Antonio, Texas'da başlamış olan, Üniversiteler Ulusal Siber Savunma yarışması (**National Collegiate Cyber Defense Competition NCCDC - http://www.nationalccdc.org/**) gibi oluşumlar ortaya konmalıdır.

İşbirliği İmkan ve Önerileri

- Üniversiteler Ulusal Siber Savunma yarışması için:
- Planlama-Organizasyon-Koordinasyon-Finansman açısından gerekli imkan ve kabiliyetlerimiz var.

İşbirliği İmkan ve Önerileri

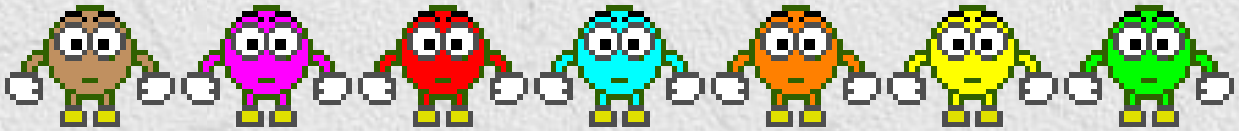
Varız!!!! diyorsanız,

ahmet.koltuksuz@yasar.edu.tr

(532) 316 52 63

Sonuçlar

1. Siber savaş etkinliklerinde ve siber terörizme karşı savaşta **ULUSAL ve ULUSLARARASI İŞBİRLİĞİ ŞARTTIR**.
2. Ancak, ulusal ve özellikle uluslararası arenada tam ve karşılıklı bir anlayış, işbirliği ve dayanışmadan daha zor elde edilebilen bir şey de yoktur.
3. O halde, bir yerlerden ve hemen başlamak gerekir!!!



Zaman, ilgi ve sabrınız için çok teşekkür ederim.

Dr. Ahmet Koltuksuz