Siberuzayda Savunma ve Güvenlik

Dr. A. Koltuksuz

Bilgisayar Mühendisliği Bölümü

Yaşar Üniversitesi

Gündem

- 1 Temel Tanımlar ve Kavramlar
- 2 Siberuzayda Tehditler
- 3 Siberuzayda Suçlular
- Sonuçlar

Bölüm 1 Temel Tanımlar ve Kavramlar

- **Siber Terörizm.**
- **Siber Savaş.**
- **Bilgi Savaşları**
- **Tanımlama Sorunları.**

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, 2011

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.

Kevin Coleman,
"*Directions*"

Siber Terörizmin Yapısal Amaçları

1. Doğruluk ve Bütünlüğü yok etmek yoluyla, bilginin uygun olmayan biçimde değişimini yapılabilir hale getirmek.
2. Yetkili kullanıcıların kullanacağı kritik bilgi sistemlerini kullanılamaz hale getirmek.
3. Gizliliği yok ederek kritik gizli bilgilerin yetkisiz kişilerce kullanılmasına yol açmak.
4. Fiziksel olarak bozulmaya yol açacak komutlar verdirmek yoluyla sistemleri çalışamaz hale getirmek.

Siber Terörizmin İşlevsel Amaçları

1. Fon oluşturma
2. Eğitim
3. Adam devşirme
4. Gizli haberleşme
5. Veri madenciliği
6. Propaganda ve Dezenformasyon
7. Radikalizasyon

Bazı Siber Terörizm Saldırı Tipleri

- Sızma: Bilgi Sistemlerine sızma.
- Bilgi Sistemlerinin fiziksel ve/veya mantıksal tahribi.
- Dezenformasyon: Belirgin bir hedefin tahribi için yıkıcı etkide bir dedikodu/söylence yaratmak.
- TCP/IP paketlerinin sürekli gönderimiyle bilgi sistemlerinde hizmetin reddini sağlamak, sistemi çalışamaz hale getirmek.
- Propaganda veya reklam amaçlı söylemleri eklemek suretiyle web sitelerini değiştirmek, bozmak.

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
"Principles of Cyber warfare", 2001

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, siberuzayda hakimiyeti ele geçirmek imkansız olabilir.",**
- **"Siber savaş, istihbarat ve kaynaklara ciddi gereksinim duymaktadır. Siberuzaydaki 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: Bilgi Savaşları

- Düşmana karşı üstünlük kazanmak amacıyla; bilgi sistemleri ve ilişkin bilgi teknolojilerinin kullanımı ve yönetimidir. Siber Savaş tekniklerini de içerir.
- Bilgi Savaşlarında aşağıdaki etkinlikler gerçekleştirilir:
  - Taktik ve operasyonel bilgi toplama.
  - Geçerli ve güncel bilgiye erişildiğinin güvencesinin sağlanması.
  - Propaganda veya dezenformasyon çalışmaları.
  - Düşmana yönelik bilgi kalitesini sabote etmek.
  - Düşmanın bilgi toplama imkan ve kabiliyetlerini yok etmek.

Tanımlama Sorunları

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

terimleri arasındaki sınırlar, (henüz) **net değildir!!**

Bölüm 2 Siberuzayda Tehditler

- **Siberuzay Tehdit Kaynak Sınıflaması.**
- **Siber Saldırıda *modis operandi* .**
- **Siber Saldırı ve Savunma.**
- **Bazı Güncel İstatistikler.**

Siberuzay Tehditlerinin Kaynak Sınıflaması

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

US CERT
Control Systems Security Program (CSSP)

Siberuzay Tehditlerinin 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

Siberuzay Tehditlerinin 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.

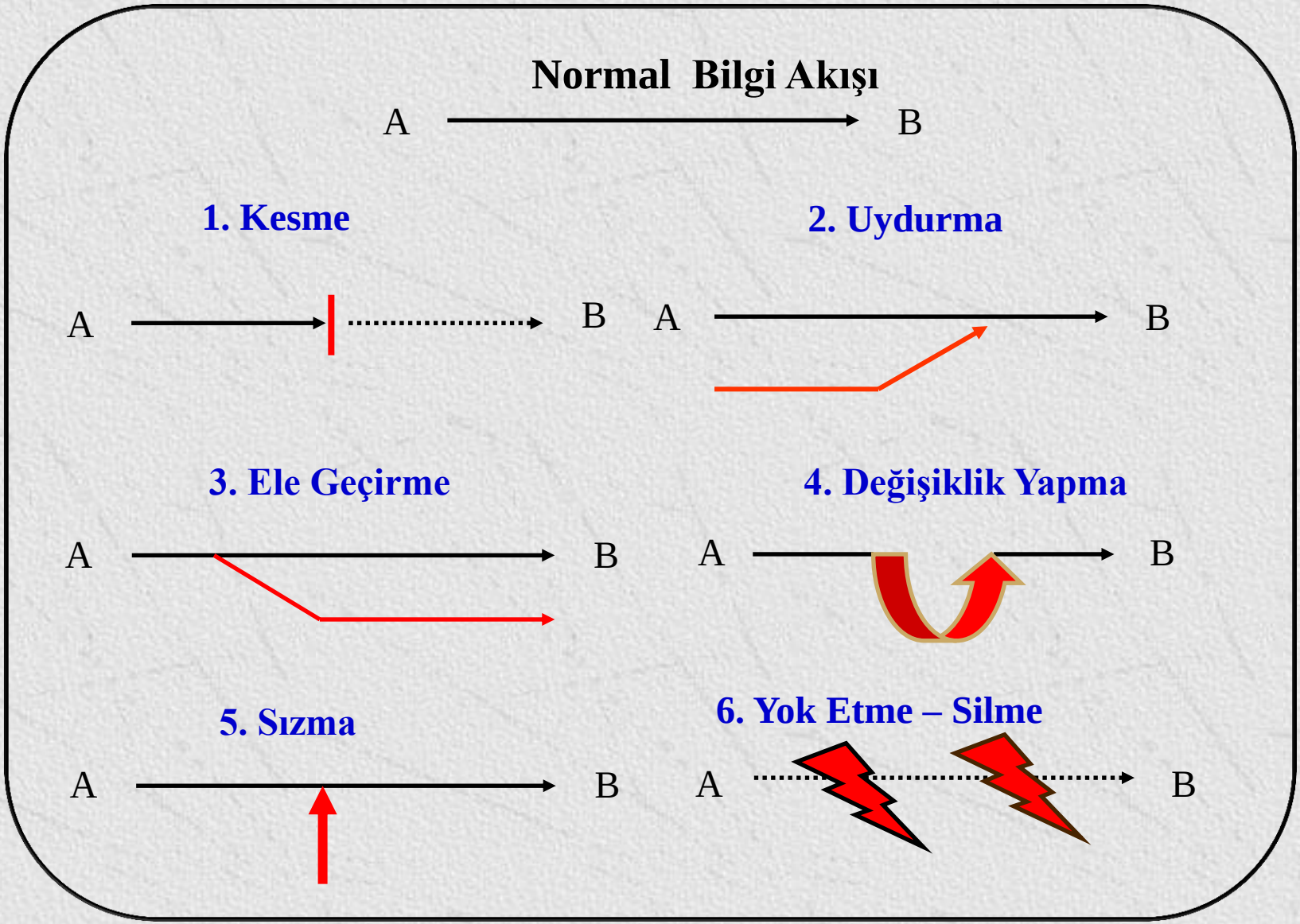
Siberuzay Tehditlerinin Kaynak Sınıflaması

- Bir diğer siber tehdit sınıflaması… (devam)

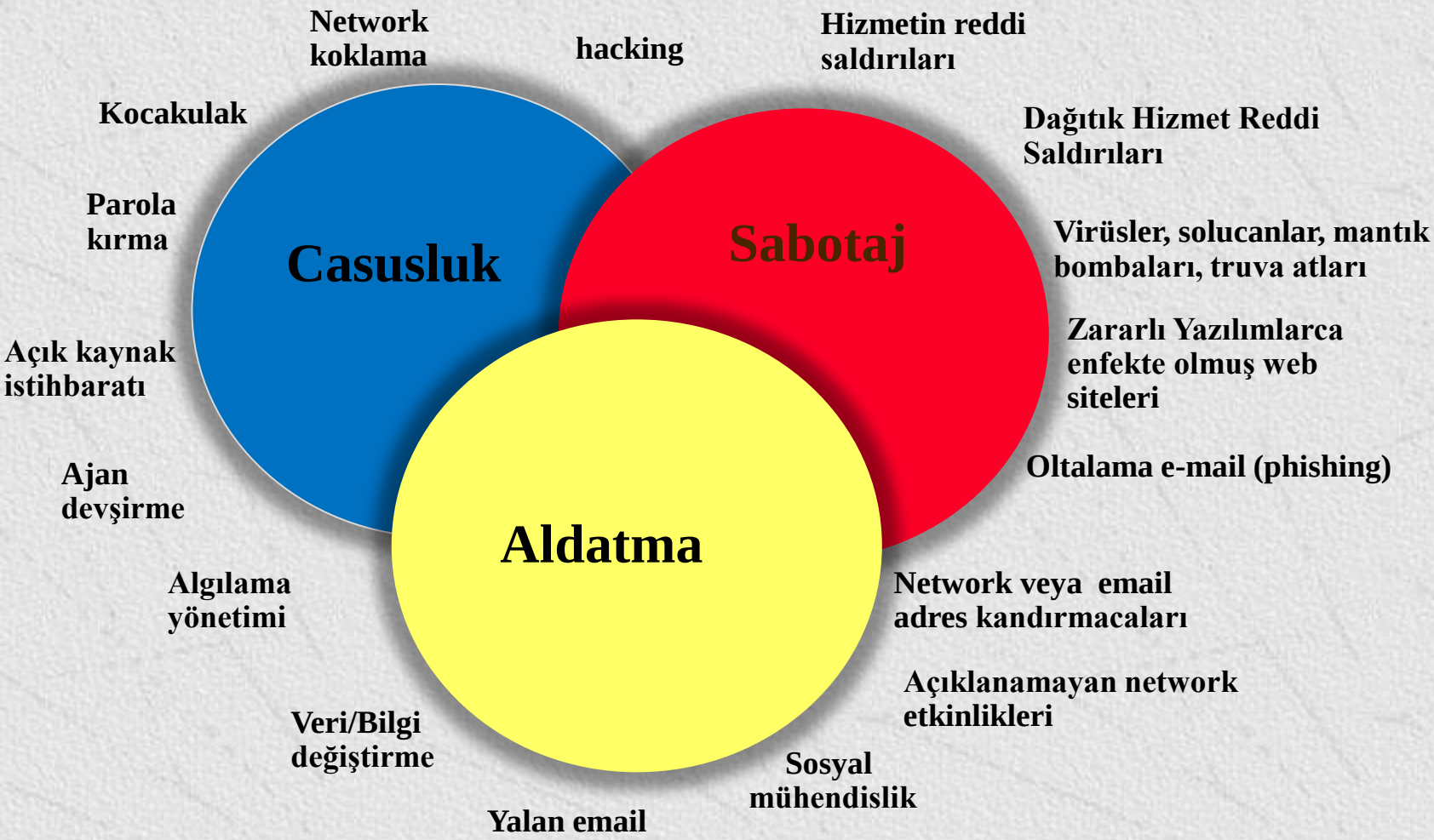
Threat-Source	Motivation	Threat Actions
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	. Economic exploitation . Information theft . Intrusion on personal privacy . Social engineering . System penetration . Unauthorized system 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.

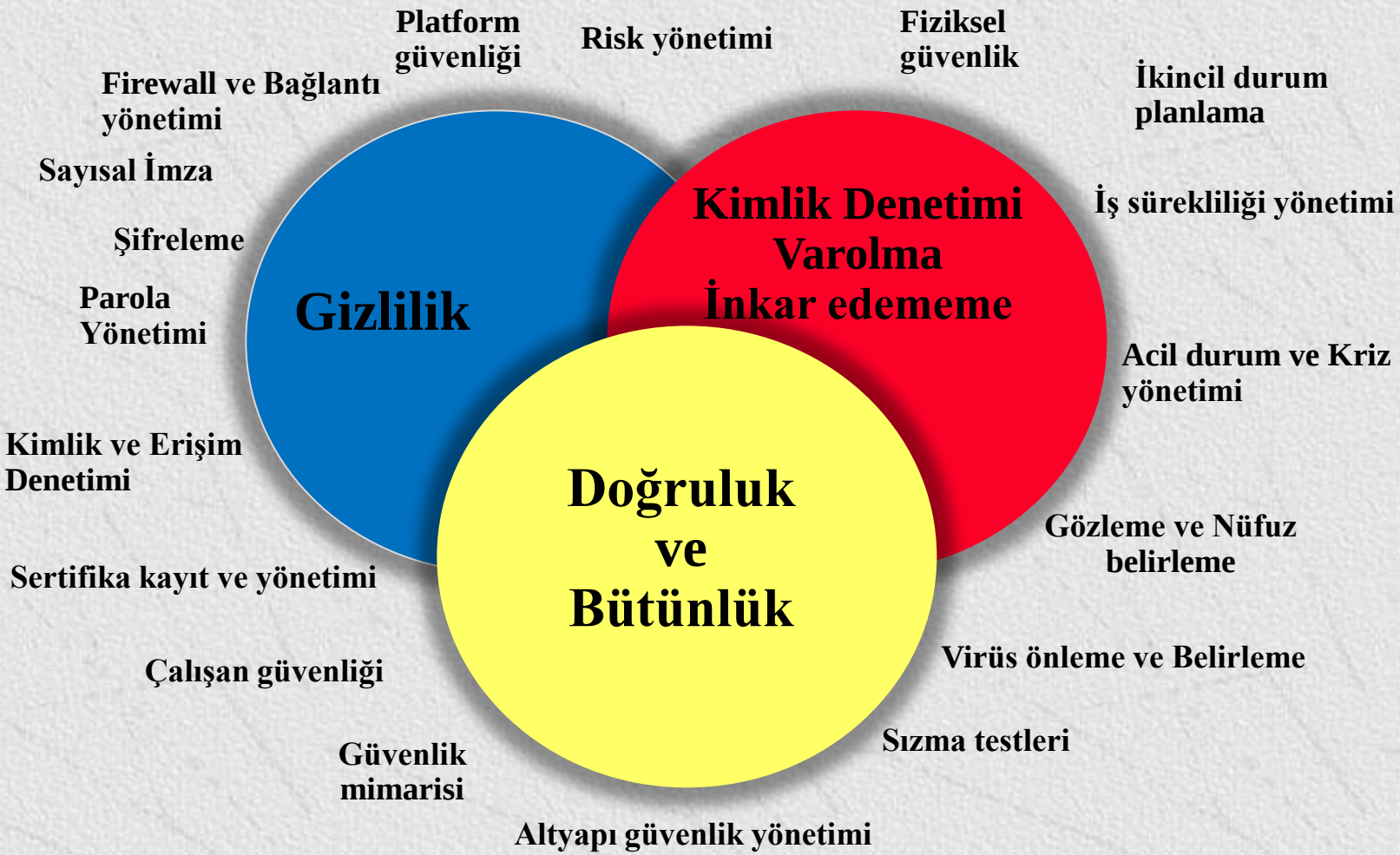
Bir Siber Saldırının İmzası (modis operandi)



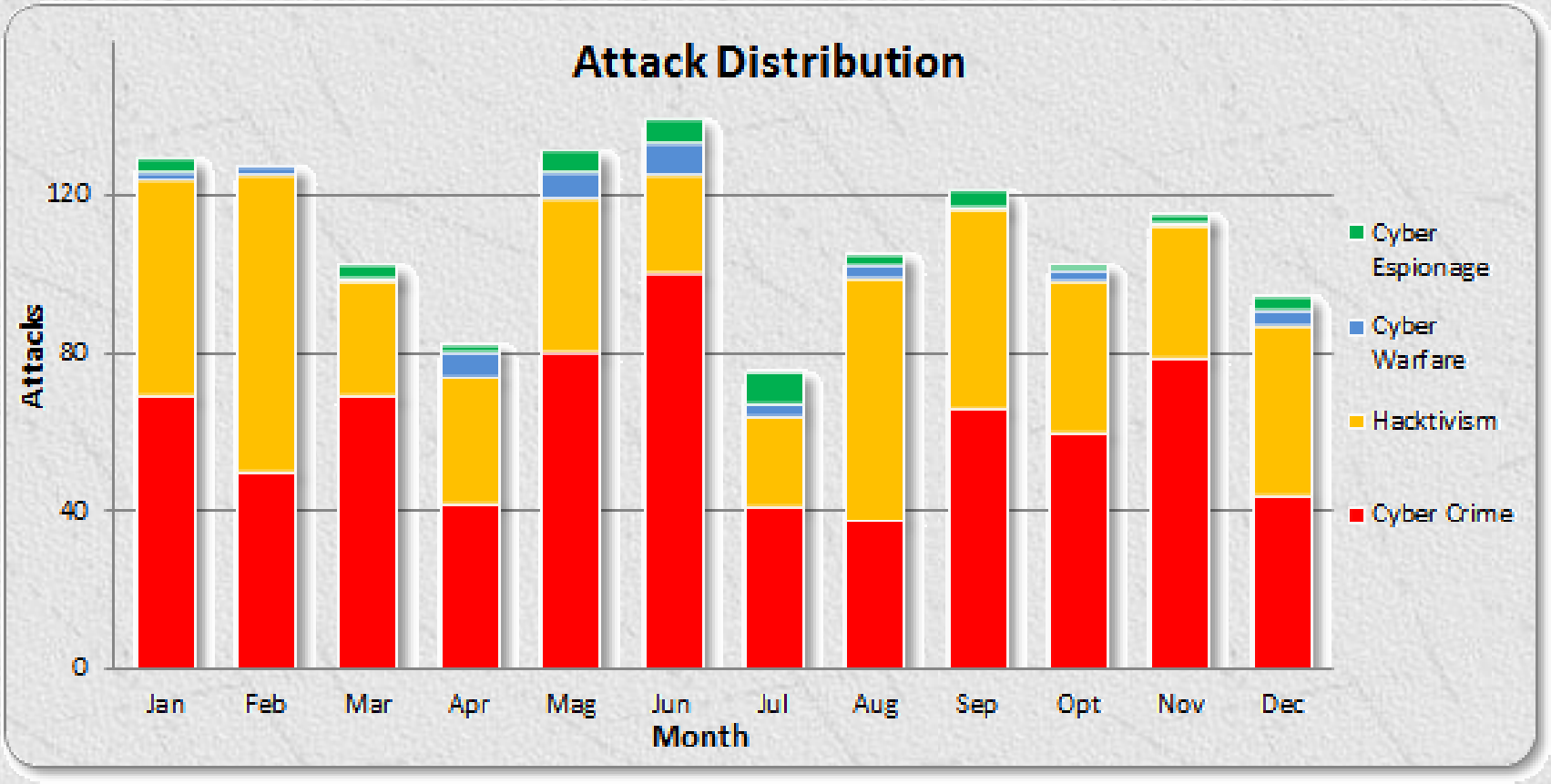
Siber Saldırı Tipleri



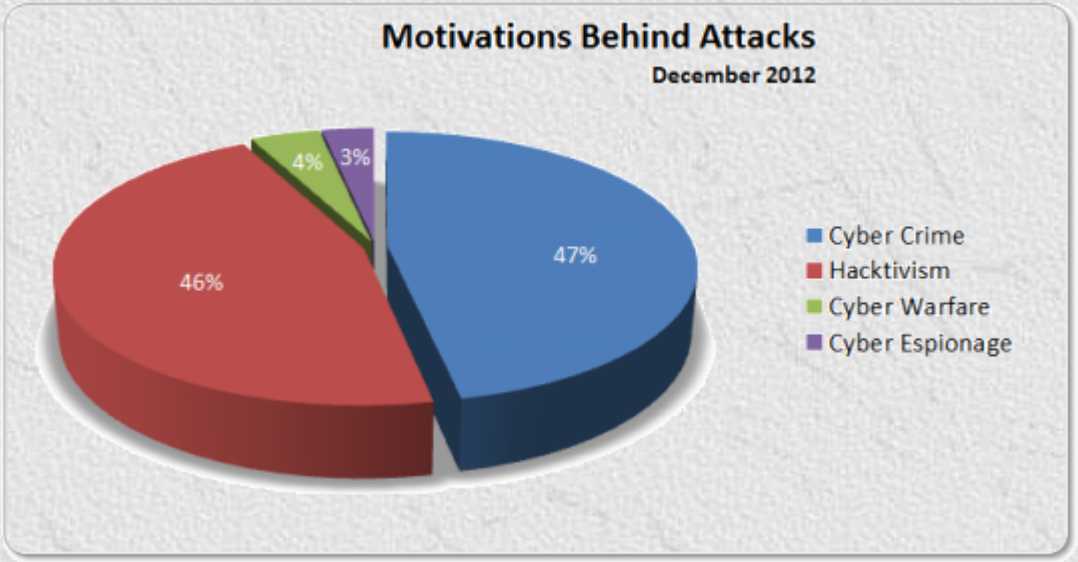
Siber Savunma Araçları

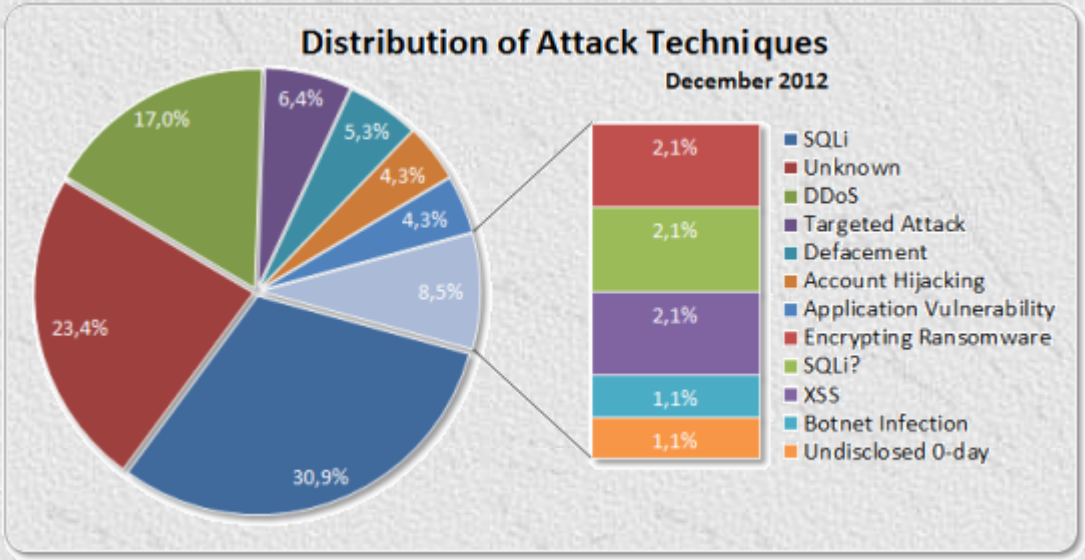


Aralık 2012 itibariyle rakamlar



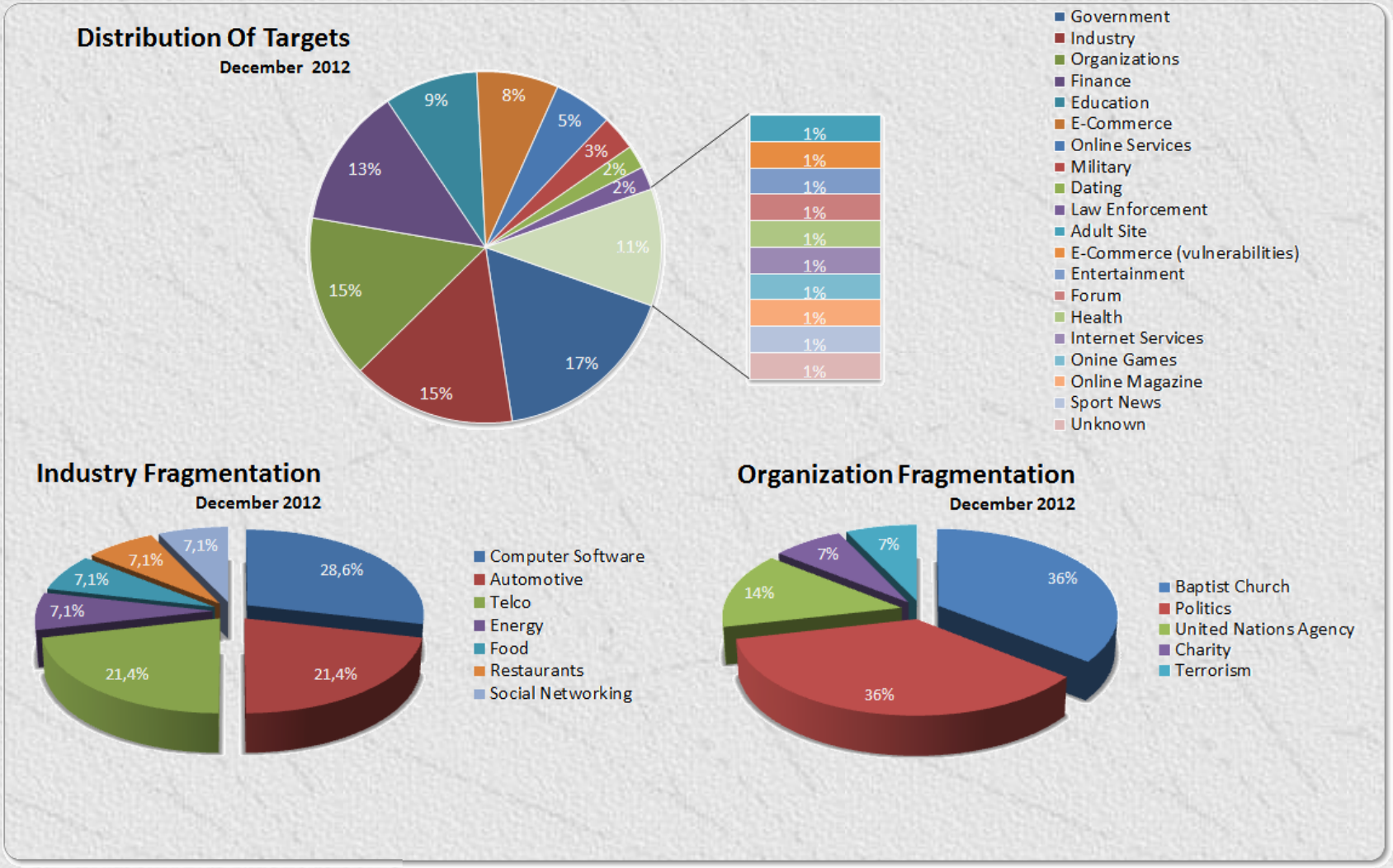
Aralık 2012 itibariyle rakamlar





Dr. Ahmet Koltuksuz

Aralık 2012 itibariyle rakamlar



Dr. Ahmet Koltuksuz

Bölüm 3 Siberuzayda Suçlular

- **Kim Bunlar?**
- **Niye Siberuzaydalar?**
- **Olası Hedefleri Nelerdir?**
- **Ne Yapıyorlar?**
- **Hangi Araçları Kullanıyorlar?**
- **Siber Suçlunun Anatomisi**

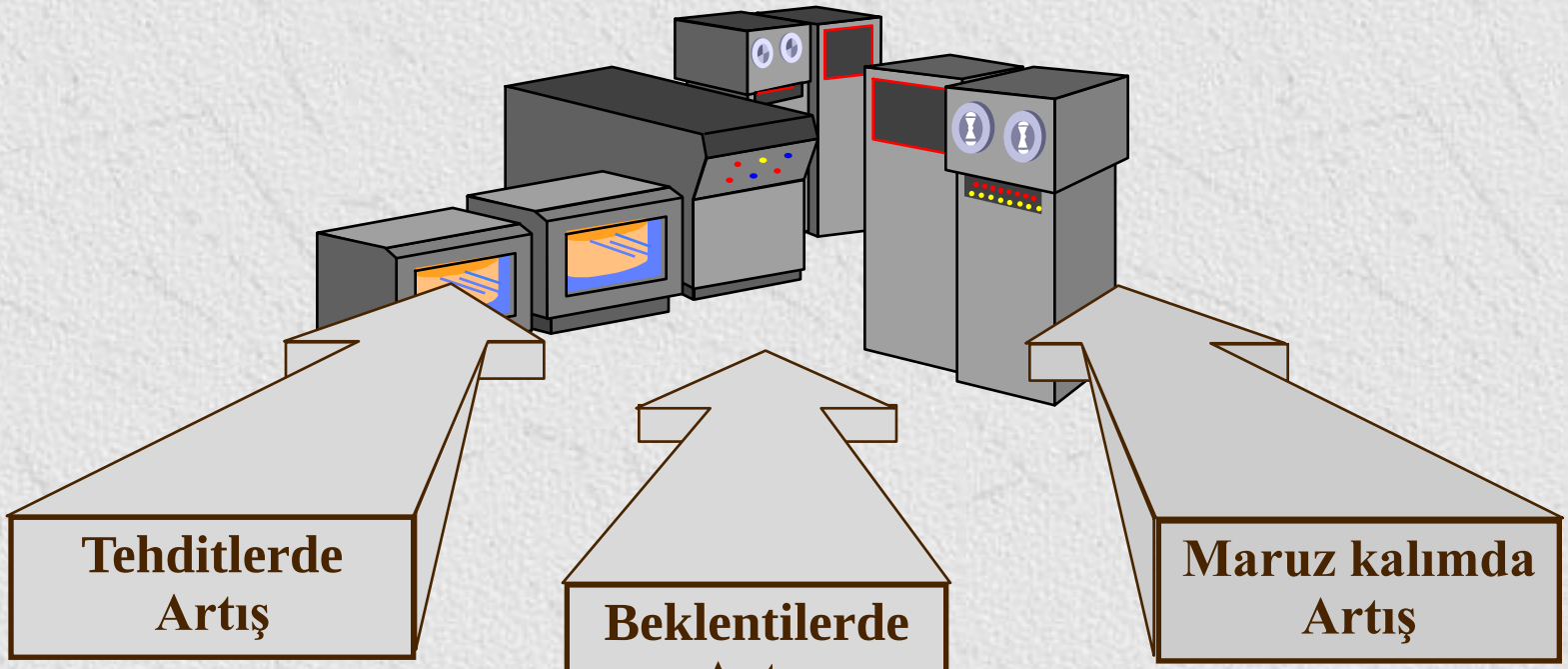
Kim Bunlar?

- Uluslararası terörist gruplar.
- Sınır aşan siber suç teşekkülleri.
- Bireysel aşırı uçlar.
- Bireysel ulusal yada uluslararası teröristler.

Niye Siberuzaydalar?

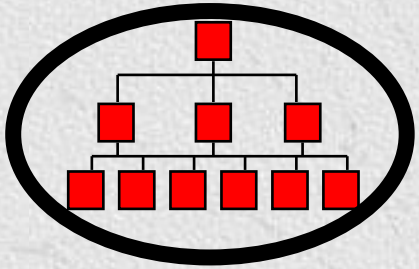
- Anonimlik – Kimliğin belirsiz olması
- Farklı hedeflerin bolluğu
- Belirlenme, farkedilme riskinin düşüklüğü
- Kişisel yaralanma-fiziksel zarar görme olasılığının düşüklüğü
- Düşük yatırım maliyeti
- Hemen her yerden eylem yapabilme olasılığı
- Operasyonlar için kaynak gereksiniminin azlığı

Küreselleşen Siber Suç



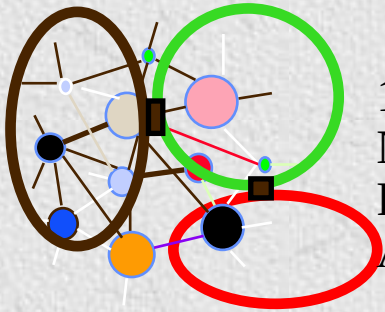
Küreselleşen Siber Suç

Güvenli Binalar



1980ler
Sırça köşk: Bilgiişlem Merkezleri

Ağ Yönetimi

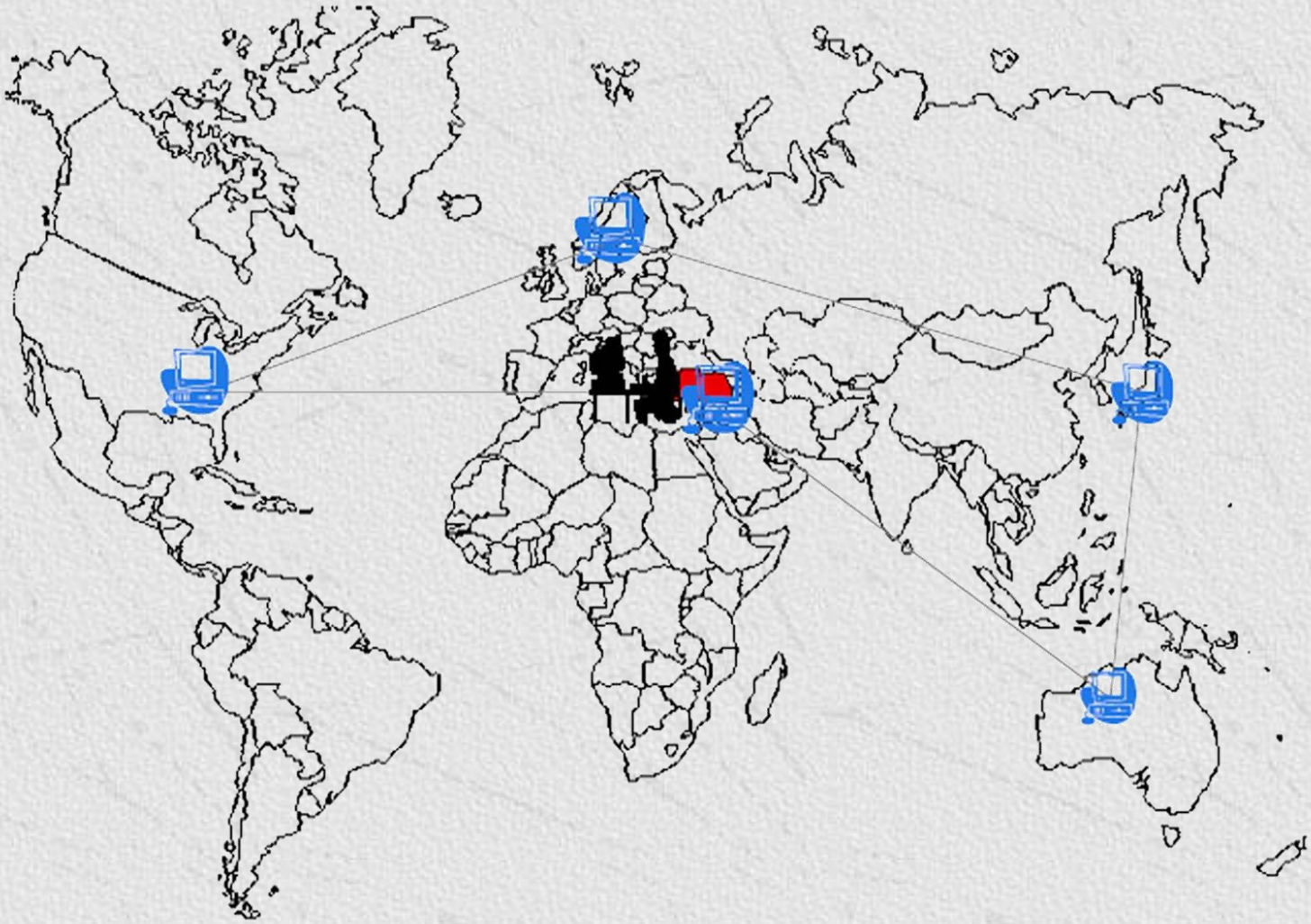


1990lar
Network
Firewall'ları,
Ağ üzerinden saldırılar

Sokak kullanıcıları

2000 ve ötesi
Siber savaşçılar

Küreselleşen Siber Suç



Olası Hedefleri Neler?

1. Bilgi teknolojilerini kullanarak; donanım ve/veya yazılımı yok etmek, çalışamaz duruma getirmek, personele fiziksel zarar vermek.
2. Ulusal hava trafik kontrol sistemini bozarak kaos ve yıkım oluşturmak.
3. Demiryolları sinyalizasyon sistemini bozarak tren ve metroları çalışamaz duruma düşürmek.
4. Su ve elektrik denetim sistemlerini bozmak.
5. Ticari komünikasyon sistemlerini bozmak veya hatalı çalışmalarını sağlayarak ekonomik yıkıma yol açmak.

Ne Yapıyorlar?

- Interneti kullanım amaçları

1. Radikalizasyon ve propaganda dağıtım makinası
2. Adam devşirme ve organizasyon
3. Eğitim ortamı
4. Siber suç yoluyla fon oluşturma
5. İletişim

Kullandıkları Temel Araçlar

- Aşırı uçlar yoğun olarak aşağıdaki unsurları kullanmaktadır:
  - Chat'leşme odaları, internet kafeler
  - Özel amaçlı server'lar
  - Web siteleri
  - Sosyal Ağlar
  - Youtube kanalları
  - Facebook-Twitter

Kullandıkları Temel Araçlar

- Gerçek bir siber teröristin temel silahı ağlardır.
- Ağlar aracılığıyla emirler ve mesajlarını iletir, zararlı yazılımları yerleştirir, siber suçları işler, amaçları doğrultusunda bilgiye erişir.
- Web sitelerini bozar, hedef ağların segmentlerini işlemez duruma getirir, hasmına ilişkin bilgi toplar, diğer grupların ağlara erişimini engeller, finansal sistemleri manipüle eder böylece kaos ve akabinde de paniğe neden olur.

Kullandıkları Temel Araçlar

- Veri/bilgi veya web sitesi gibi fiziksel olmayan ortamların ya da bilgi yoluyla algıların ve davranış tavırlarının manipülasyonu, bozulması ve/veya değişikliğe uğratılması diğer saldırı biçimlerindendir.
- Finansal işlemlerin elektronik kayıtlarına yapılacak yok etme saldırısı veya geniş ölçekli/yayılımlı bir elektronik hırsızlık yoluyla ülkeye ciddi bir ekonomik darbe vurulması da yine saldırı araçlarıdır.
- Bir hedefin resmi web sitesinde bilgi veya görünüş değişikliğine yol açmak; fiziksel bir girişim yapmaksızın bir teröristin negatif algılar veya yanlış bilgi yayabilmesini sağlamaktadır. Bu yolla da siber saldırı olabilir.

Bilişim Suçlusunun Anatomisi-PROFILING

Üç Dönem Halinde incelenecektir.

1. Internet Öncesi, Romantik Dönem: 1950-1980
2. Internet Dönemi: 1980-2000
3. Sayısal Toplum: 2000 ve ötesi

Dr. Ahmet Koltuksuz

DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE

1. Internet Öncesi, Romantik Dönem: 1950-1980

• 20-33 yaşları arasında, genç, dinamik, üst düzey eğitimli ve bilgili, parlak ve başarılı.

• Zeki, kendisine güvenilen, terbiyeli, saygılı.

• Sağlıklı, beyaz ırka mensup, ***çoğunlukla*** erkek.

• ÇOĞUNLUKLA SABIKA KAYDI OLMAYAN.

• İnsanlarla ilişki kurmakta zorlanan.

• Kendini kanıtlama gereksinimi duyan.

• Değerinin anlaşılmadığını düşünen.

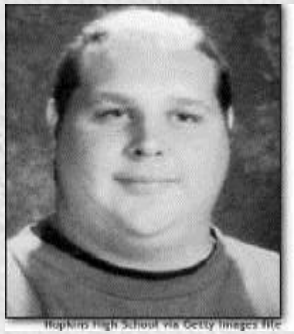
• Tüzel kişilere karşı eylem yaptıklarından, bireylere karşı sorumluluk ve suçluluk duyguları taşımayan.

• Uyanık, sabırsız, çabuk motive olan, teknolojik anlamda iddiacı. Aşırı hırslı, sonsuz sabırlı.

• Ancak bir bilgisayarla varlığını hisseden kişilik.

1. Internet Öncesi, Romantik Dönem: 1950-1980






Ticari bir hedef YOK!!!


Kevin Mitnick in his younger days.


Kevin Mitnick

Dr. Ahmet Koltuksuz

1. Internet Öncesi, Romantik Dönem: 1950-1980

Name: Peiter Mudge Zatko
Handle(s): Mudge, PeiterZ
Marital status: Single
Current residence: New England, USA
Job: Chief Scientist, Intrusic
First computer: Tektronix 4051
Best known for: Creating L0phtCrack
Area(s) of expertise: "Thinking outside of the box"

Pieter Mudge Zatko

1. Internet Öncesi, Romantik Dönem: 1950-1980

Name: Raven Alder
Handle(s): Raven
Age: 28
Place of birth: Mississippi, USA
Marital status: Single
Current residence: Maryland, USA
Job: Security consultant, True North Solutions
First computer: Home-built 8088 machine in 1988
Best known for: Tracing spoofed distributed denial of service attacks
Area(s) of expertise: ISP backbone networking, protocol decoding and design, Linux/BSD security, and cryptography


Raven Alder

2 Internet Dönemi: 1980-2000

Hedefsiz ve Bilinçsiz Saldırgan

Amacı yoktur, rastgele hedef seçer.
Teknik düzeyi zayıftır, Kulaktan dolma bilgisi vardır.
Kolay takip edilir ve yakalanır.
Tehlikelidir, Saldırgan kitlesinin büyük çoğunluğunu oluşturur.

Hedefli ama Bilinçsiz Saldırgan

Amacı vardır, plansız ve programsızdır.
Bilgi seviyesi az düzeyde genelde kulaktan dolmadır.
Otomatik araçlar kullanır. Kendini ispatlama çabası vardır.
Çok fazla iz bırakır.

Hedefsiz ama Bilinçli Saldırgan

Amacı yoktur, rastgele hedef seçer.
Tehlikelidir, Teknik Bilgi ve Becerisi Mevcuttur.
Kendine Özel veya Rastgele Araçlar Kullanır.
Yakalanma kaygısı vardır. Gizlenir.

Hedefli ve Bilinçli Saldırgan

Amaçlıdır, planlı ve programlıdır.
Çok tehlikelidir. Teknik Bilgi ve Becerisi Yüksektir.
Kendini Saklamaya Özen Gösterir.
Kendine Özel Araçlar Kullanır.

2 Internet Dönemi: 1980-2000

Hacker: En iyileri, Siyah Şapkalı (Black Hat) – Beyaz Şapkalı (White Hat). Kimliklerini ve faaliyetlerini gizlerler.

Cracker: Şifre Kırıcılar. Genellikle yazılım şifreleri. Kimliklerini ve faaliyetlerini gizlerler. Hacker olma yolundadırlar.

Lamer: Hazır araçları ve virusleri kullanırlar. Şan ve Şöhret Peşindedirler. Hacker olduklarını iddia ederler.

Script-Kid/Cyber-Punk: Bilgisayar konusunda uzman, genç yaşta ve hazır araçları kullanırlar. Egolu ve kendini ispat peşindedirler.

Meraklılar, Kullanıcılar: Bilgisayara meraklı, çoğunlukla farketmeden zarar veren, veya çalıştığı yerden intikam alma amacında olan kişilerdir.

3 Sayısal Toplum: 2000 ve Ötesi

Temel motivasyon: **PARA**

Uzman Niteliğinde Bilişim Suçluları

Alt Uzmanlık Alanlarına Sahip Bilişim Suçluları

Linux, Windows, Mac
Virüs, Solucan, Trojan, Botnet,
PinPad, Skimmer, Tahsilatçı, Komisyoncu

Gelecek Öngürüleri ve Projeksiyonları Olan Suç Grupları

3 Sayısal Toplum: 2000 ve Ötesi

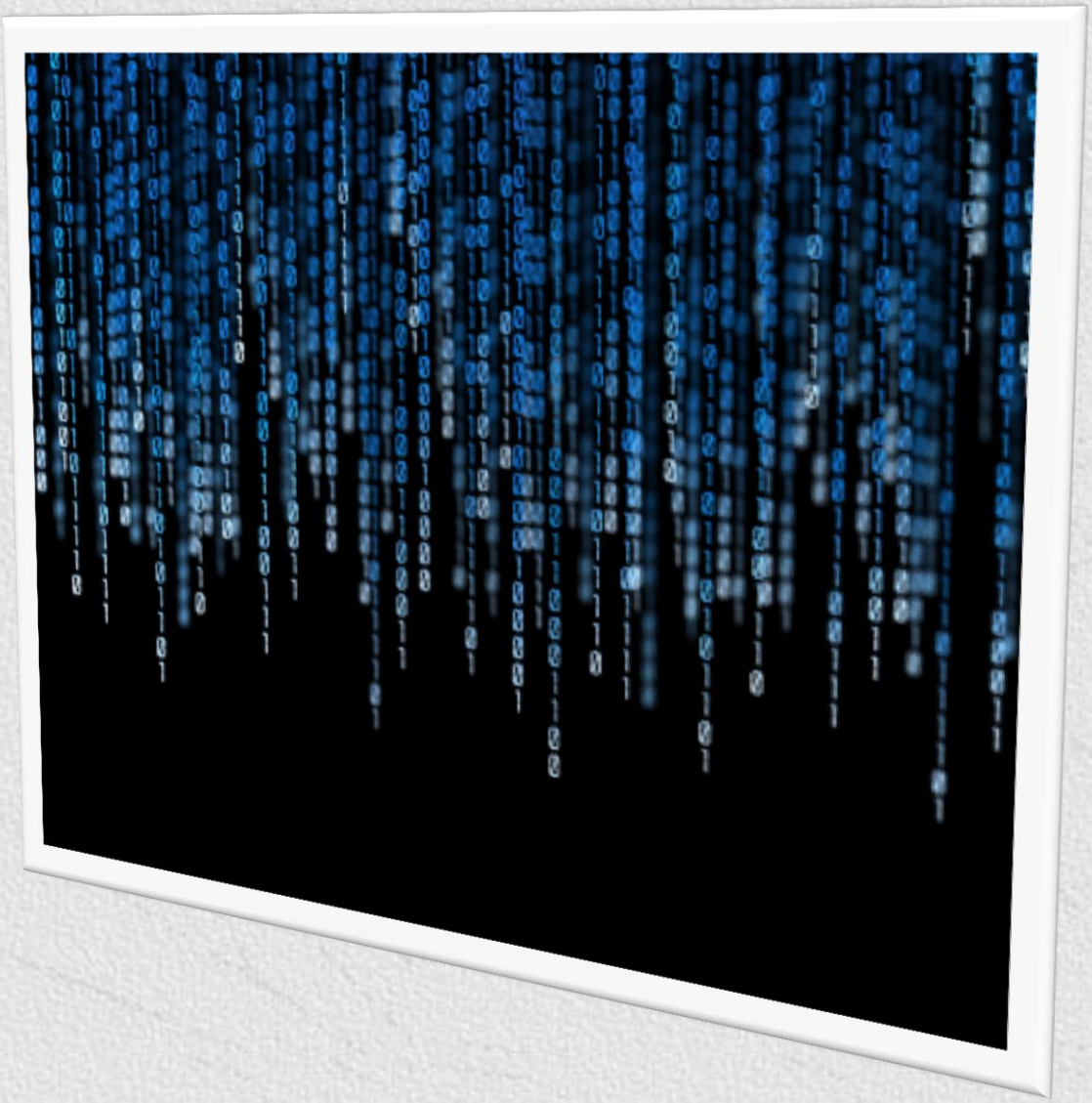
Yeraltı Pazarına Hoşgeldiniz!!!

Talep	Önceki	Mallar ve Hizmetler	Getiri	Önceki	Fiyat
1	2	Banka hesapları	22%	21%	$10-1000
2	1	Kredi kartı	13%	22%	$0.40-$20
3	7	Tam kimlik	9%	6%	$1-15
4	N/R	Online açık arttırma site hesapları	7%	N/A	$1-8
5	8	Scams	7%	6%	$2.50/wk - $50/wk (hosting); $25 design
6	4	Mailers	6%	8%	$1-10
7	5	Email Adresi	5%	6%	$0.83-$10/MB
8	3	Email Passwords	5%	8%	$4-30
9	N/R	Drop (request or offer)	5%	N/A	10-50% of drop amount
10	6	Proxies	5%	6%	$1.50-$30

Dr. Ahmet Koltuksuz

Sonuçlar

- **Siber Savaş ve Siber Terörizm.**
- **Siber Suçlular – Bilişim Suçluları.**



Sonuçlar: Siber Savaş ve Siber Terörizm

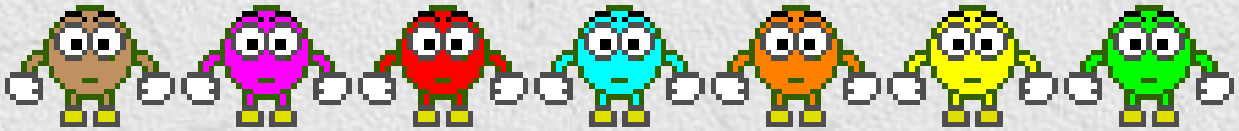
1. Siber savaş etkinliklerinde ve siber terörizme karşı savaşta **ULUSAL ve ULUSLARARASI İŞBİRLİĞİ ŞARTTIR**.
2. Ancak, ulusal ve özellikle uluslararası arenada tam ve karşılıklı bir anlayış, işbirliği ve dayanışmadan daha zor elde edilebilen bir şey de yoktur.
3. O halde, bir yerlerden ve hemen başlamak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

Sonuçlar: Siber Suçlar – Bilişim Suçları

1. Her gün gelişen, büyüyen yeraltı pazarı-ekonomisi söz konusudur.
2. Satılık hazır alet çantası, kiralık bilgisayar korsanı mevcuttur. Örneğin; 100'lük BotNet =10$ veya 2000'lik BotNet = 100$ civarında fiyata alıcı bulmaktadır.
3. Çeşitlenen finansal aktörler ve birbirine dönüştürülebilen yeni para birimleri (E-Gold, Paypal, E-Bullion, WebMoney gibi) süreci hızlandırmaktadır.
4. Bilişim suçluları; bireysel, fırsatçı amatörler olmaktan çıkıp, profesyonel ve organize suç örgütleri haline gelmişlerdir.

Sonuçlar: Siber Suçlar – Bilişim Suçları

5. Teknoloji tabanlı bu yeni suç spektrumu, artan ivmesi ile artık tam bir illegal **ENDÜSTRİ'**dir.
6. Hiçbir sınırı ve engelleyici unsuru olmayan bu suçlular ile Kolluk Kuvvetleri ve Cumhuriyet Savcıları kanunlar ve imkanlar ile sınırlı bir şekilde mücadele etmektedirler.
7. Ancak; sadece Kolluk ve Adalet Mekanizmasının çözebileceği bir sorun olmaktan çıkmıştır. İlk ve Orta Eğitim, Üniversiteler, Araştırma Merkezleri ve Özel Sektör ile yakın işbirliği şarttır.
8. **Özetle; toplumsal bir eğitim - bilinç ve karşı duruş gerekmektedir.**



Zaman, ilgi ve sabrınız için çok teşekkür ederim.

Dr. Ahmet Koltuksuz