Siber Güvenliğe Genel Bakış
ve
Güncel Trend

Tahsin TÜRKÖZ
tahsin.turkoz@tubitak.gov.tr

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

11 Ekim 2013

Sunum İçeriği

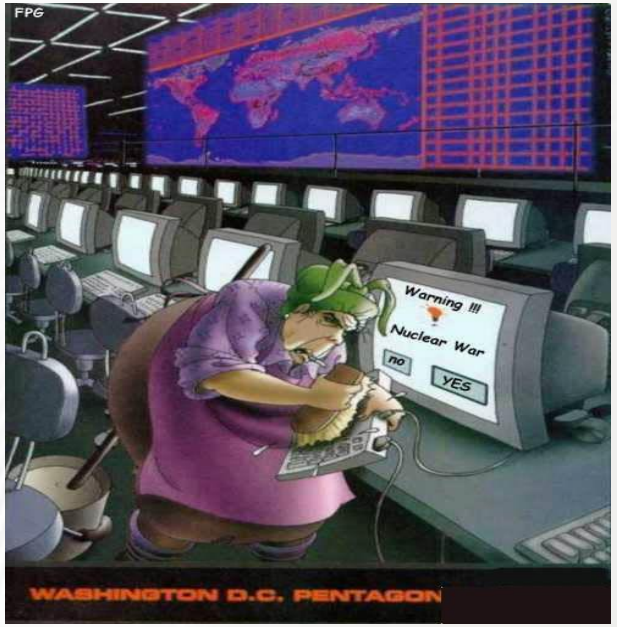
- Siber Güvenliği Bakış
- Siber Uzayda Tehdit
- Dünyada Ne Değişti?
- Siber Güvenlik Yönetimi

Fiziksel ve Sanal Dünyada Davranış Modelimiz

* Maslow's hierarchy of human needs

Siber Savunma İle İlgili Yanlış Düşünceler

- Antivirüs yazılımımız var, dolayısıyla güvendeyiz!
- Bilgimin kopyasını alıyorum, güvenlikten bana ne!
- Güvenlikten bilgi işlem sorumludur.



"Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim."

(Albert Einstein)

Siber Savunma İle İlgili Yanlış Düşünceler (2)

- Kurumumuz güvenlik duvarı (firewall) kullanıyor, dolayısıyla güvendeyiz!

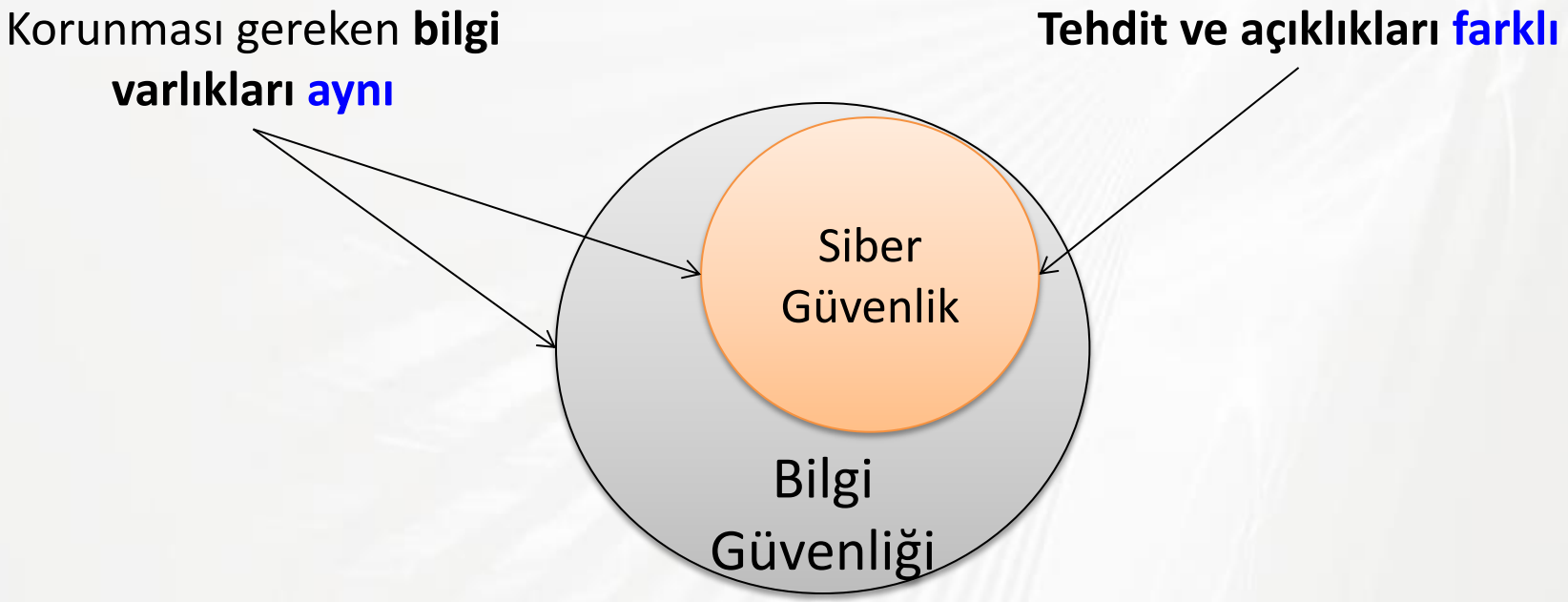
- Bir çok güvenlik saldırısı kurum dışından geliyor!

Siber Uzay (2)

1. Kara
2. Deniz
3. Hava
4. Uzay
5. Siber Uzay

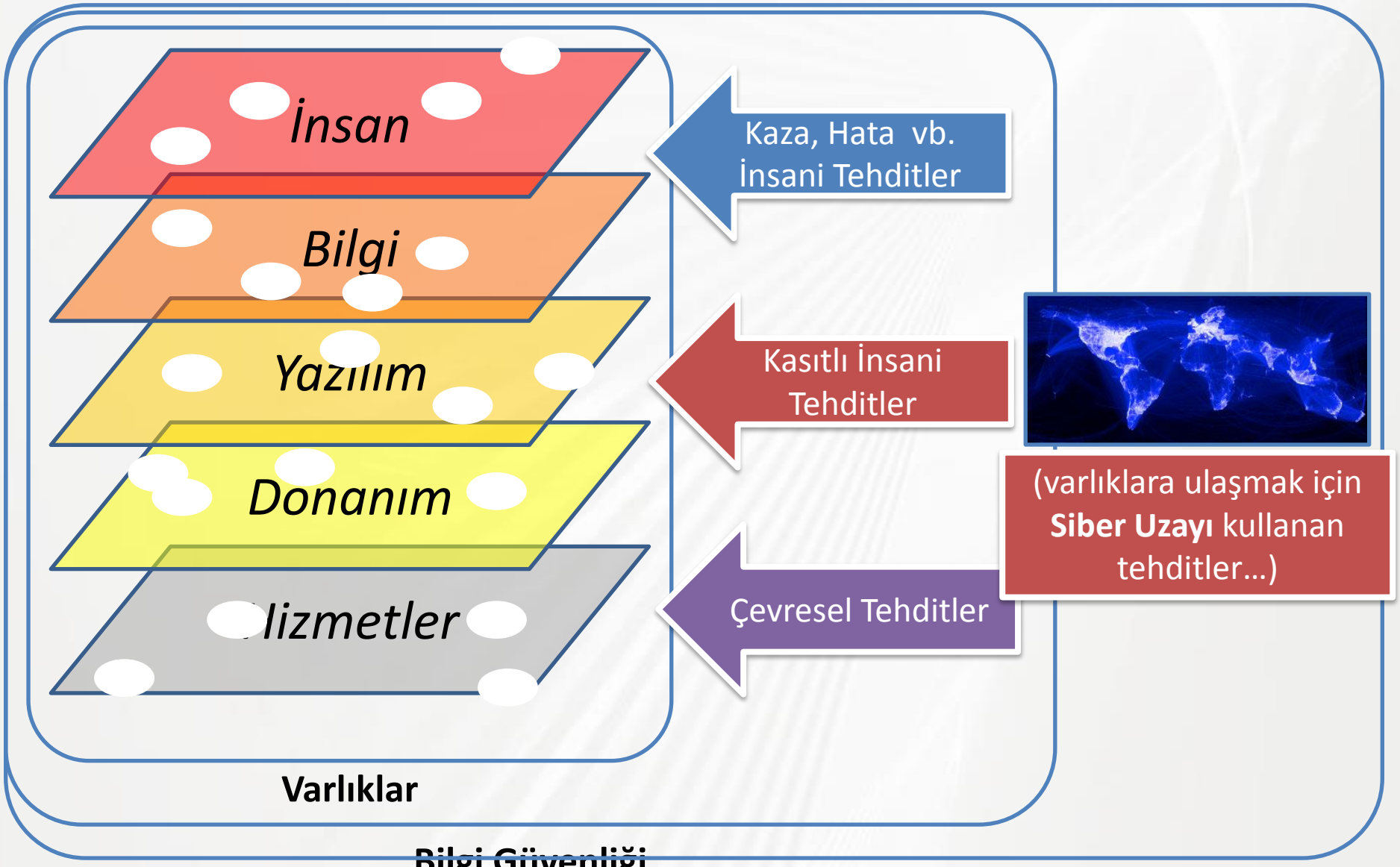
İletişim halindeki bilgisayar ağlarından oluşan elektronik ortama Siber Uzay denir.

Siber Güvenlik ve Bilgi Güvenliği



Siber Güvenlik, bilgi güvenliğinde söz konusu olan tehdit ve açıklıkların bir altkümesi ile ilgilenir.

Bilgi Güvenliği ve Siber Güvenlik



Siber Tehditlerin Özellikleri

- Farklı coğrafi konumlardan saldırı şansı (Saldırganın konumu?)

- Düşük maliyet (Bilgisayar + Internet)

- Taşeron kullanma şansı

Kiralık Botnet:
40 USD / 1000 Bilgisayar

Siber Uzay'daki Tehditlerden Örnekler

- Kötücül yazılım (bilgisayar virüsleri, solucanlar, vs.)
- Servis dışı bırakma saldırıları ("DDoS")
- Yığın E-postalar
  - Yığın e-postaların toplam e-posta trafiğine oranı:

2010: **%88.5** **(50 milyar / gün)**

2011: **%75.1** **(42 milyar / gün)**

- Parola balıkçılığı ("Phishing") siteleri
- İçerik değiştirme / bilgiye yetkisiz erişim…

Siber Uzay'da Ticaret ve Hırsızlık

- **8 trilyon USD** yılık **e-ticaret** hacmi
- Günde **bir milyon madur**.
- Yılda **388 milyar USD** kayıp (e-ticaret hacminin **%5**'i…).

- Yıllık küresel marihuana, kokain ve eroin ticaretinin toplamından **(288 milyar USD)** fazla!!!

Norton Cybercrime Report 2011, Symantec, 7 September 2011

- Siber suç giderek yayılan karlı ve düşük riskli bir suç türüdür...

Dünyada Ne Değişti?

Saldırgan Profili

- Kişisel tatmin amaçlı saldırganlar
- Fin. veya politik fayda sağlayan gruplar
- **Ülkeler (ABD, İran, K. Kore)**

Korunma Mekanizmaları

- Firewall, antivirüs, SSL, IDS
- IPS, SIEM, Content Filtering, IDM,
- **DLP, APT Detection, DPI**

Korunma Profili

- Kişisel bilgiler
- Kurumsal bilgiler
- **Kritik altyapılar**

Konuyu Ele Alışımız

- Ağ güvenliği
- Bilişim Sistemleri Güvenliği
- **Siber Güvenlik**

Savunma Teknolojilerinin Maliyeti

Ortalama bir siber silah	**$1 M**
Tomahawk (Tactical) füzesi	$1.45 M
Patriot füzesi	$4.54 M
Stuxnet	**$5M - $10 M**
15 MH-60S helikopter	$19.7 M
Siber ordunun yıllık maliyeti *	**$49 M**
F35(A) uçağı	$107 M
DDG-51 Guided Missile Destroyers	$1.100 M

* Charlie Miller, How to build a cyber army to attack the U.S

Ülkelerin Yatırımı

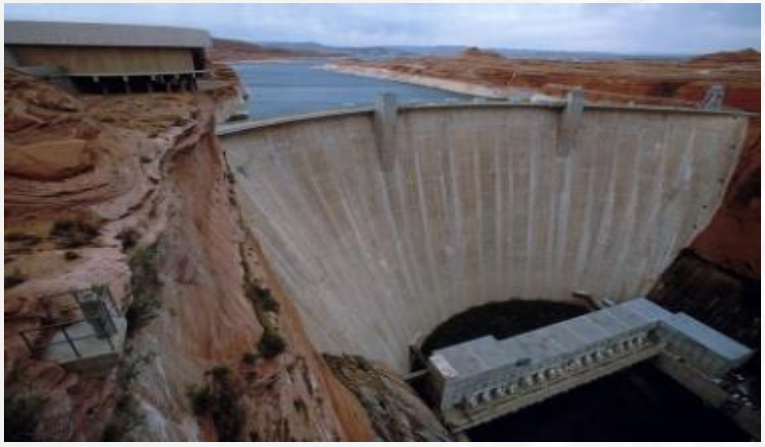
Ülkelerden Örnekler

- ABD'nin yıllık savunma bütçesi: 708 Milyar $
  - CyberCom bütçesi: **105 Milyon $**
- Kuzey Kore savunma bütçesi: 5 Milyar $
  - Siber savaş bütçesi: **56 Milyon $**
- İran'ın siber savaş bütçesi: **76 Milyon $**

Siber Tehditlerin Hedefleri

Siber tehditler neleri hedef alıyor?

- Bilgi sistemleri ve kritik ulusal altyapılar
  - Finans
  - Ulaştırma
  - Enerji v.b
- Sık sık güncellenemeyen sistemler
- Değer ifade eden sektörler



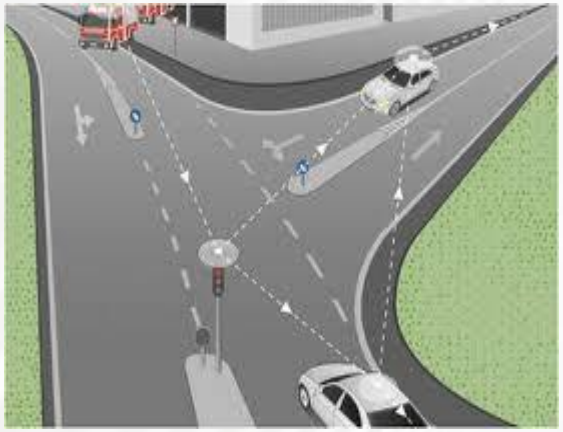
Siber Tehditlerin Hedefleri (2)

- Know-how en değerli devlet sırrı
- Ülkenin kritik sektörlerine ait know-how
  - Savunma sanayi en önemli hedef

- Ulusal güvenliğe ait kritik bilgiler
  - Sağlık verileri
  - Kritik ekonomik veriler

Siber Tehditlerin Hedefleri (3)

- Fiziksel siber güvenlik tehditleri
- BT sistemlerinin ve fiziksel mekanizmaların iç içe olduğu sistemleri hedefleyen sistemler
- Mobil uygulamalar ve gömülü sistemler
- Örnek uygulamalar
  - Uzaktan hasta takip sistemleri
  - Araç içi ağ sistemleri ve araçtan araca iletişim sistemleri



Siber Savaşa Giden Yol

- Estonya örneği
  - Estonya'daki e-devlet uygulamalarının yaygınlığı
  - Estonya bilgi sistemlerine bilgisayar korsanlarının saldırması
  - Ülkenin ekonomik ve toplumsal olarak zarar görmesi
- Gürcistan'ı hedef alan saldırılar
- İran nükleer santrallerini hedefleyen Stuxnet
- Flame, Duqu

A new aPproach to the Threads

Advanced

- Sıfırıncı gün açıklıkları
- Özel hazırlanmış saldırı teknikleri
- Gerektiği kadar karmaşık

Persistent

- Hedefli
- Bütün zayıf noktalar arama
- Uzun süre sistemde kalma
- İz bırakmama

Mandiant APT1

Genel Özet

- 2006 yılından bu yana
  - 20 sektörü kapsayan çalışma
  - 141 kurumda APT tespiti
- Yüzlerce terabyte veri
- Ortalama kurumlarda kalma süresi: 356 gün
- En uzun süre: 1,764 gün
- Bir kurumdan 10 ayda çalınan veri: 6.5 terabyte
- Hedefler: Çin'in 12. kalkınma planında yer alan öncelikli 7 sektörden 4'ü

Defans ve Bağımlılık Bakışı

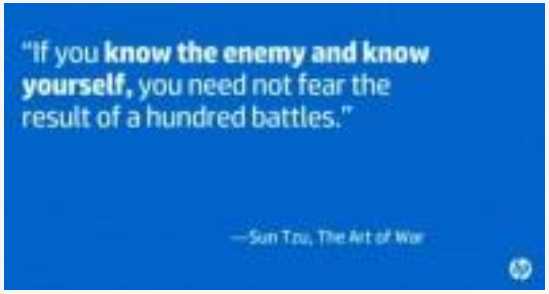
Formül *

Siber Güç= f (Saldırı, Defans, Bağımlılık)

Countries	Siber Saldırı Kabiliyetleri	Siber Savunma Kabiliyetleri	Siber Ortama Bağımlılık (Ters orantı)	Genel Değerlendirme
Kuzey Kore	2	7	9	18
Rusya	7	4	5	16
Çin	5	6	4	15
İran	4	3	5	12
ABD	8	1	2	11

* Richard Clarke, Cyber War

Siber Numaralar



94 - 416 - 71 – 84*

* Art Gilliland, RSA Conference 2013

TÜBİTAK

Teşekkürler