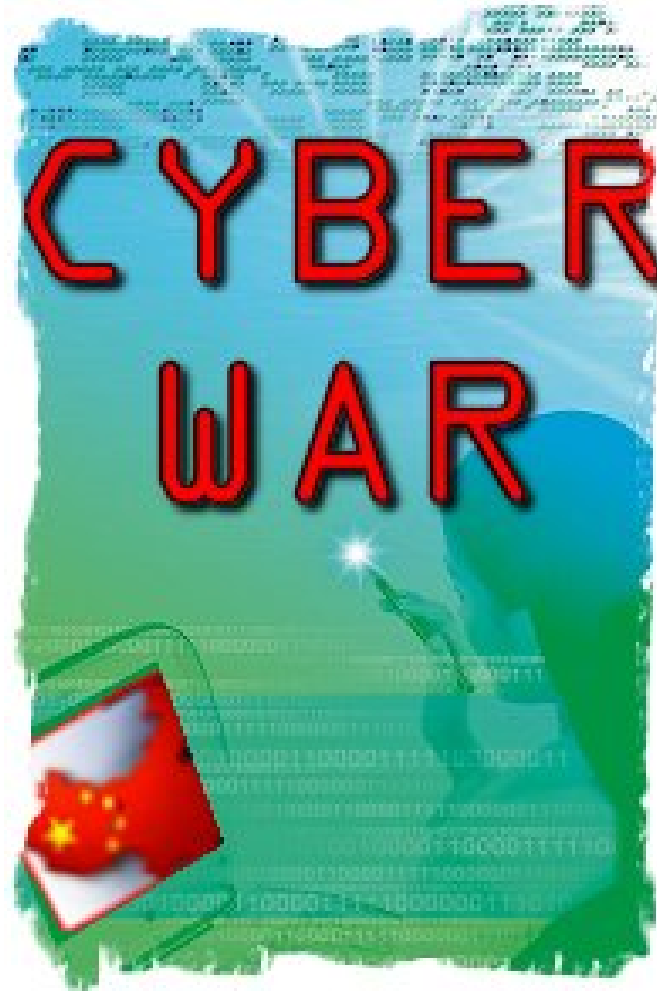


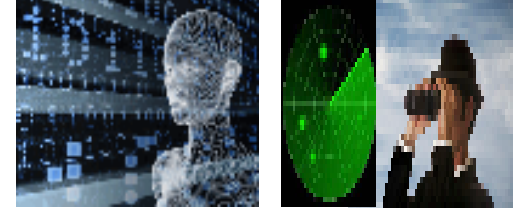


aselsan

# Siber Güvenlik ve SAHAB

Ali YAZICI

# Siber Savaş



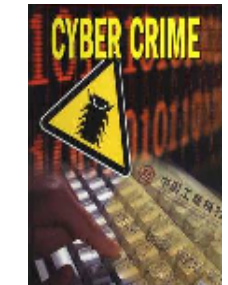
- **Siber Savaş,**
  - **ülkede yerleşik sivil, askeri ve hükümete ait bilgi ve iletişim sistemlerinin siber saldırılara karşı savunulması,**
  - **ekonomik, politik veya askeri nedenlerle hedef seçilen ülkeye bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılardır.**

***Çoğrafi sınırlardan bağımsız olarak gerçekleşir***



# Siber Savaş

- **Siber Savaşta yapılabilecek saldırılar;**
  - Hizmet dışı bırakma, (DoS/DDoS)
  - Web sayfalarının ele geçirilmesi,
  - Gizlilik dereceli bilgilerin ele geçirilmesi, değiştirilmesi, silinmesi,
  - Kritik sistemlere yönelik saldırılar (enerji, iletişim, finans, güvenlik altyapısı vb.)



# Siber Savaşlara Örnek

- Pentagon Bilgisayar Ağı (Çin Haker/Haziran 2007)
- Estonya (Rusya Federasyonu/Mayıs 2007)
- Gürcistan (Rusya Federasyonu/Temmuz 2008)
- İran nükleer programına STUXNET saldırısı (2010)
- Fransa Hükümetinin G20 Dosyaları (2010)



***Siber savas küresel bir tehdit haline dönüşmüştür.***

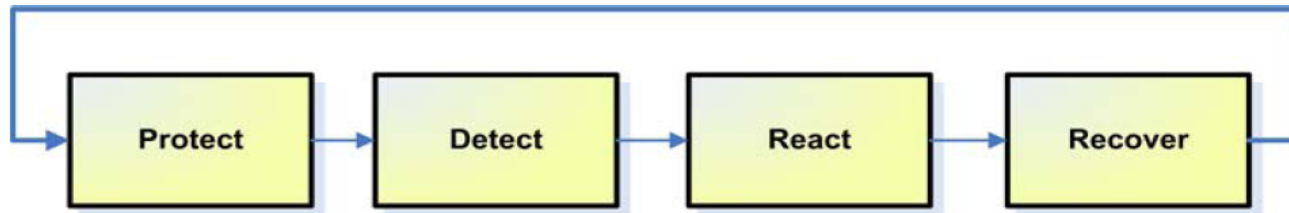
# Siber Tehdit Araçları

- **Hizmetin engellenmesi (DoS /DDoS) saldırıları**
- **Kötücül yazılımlar (Malicious Software)**
  - **Bilgisayar virüsleri**
  - **Kurtçuk (“worm”)**
  - **Truva atı (“trojan”)**
  - **Klavye izleme (“key logger”) yazılımları**
  - **İstem dışı olarak gönderilen tanıtım (“adware”) yazılımları**
  - **Bilgi toplayan casus (“spyware”) yazılımlar**
- **Yemleme (“phishing”)**
- **İstemdışı elektronik posta (“spam”)**
- **Şebeke trafiğinin dinlenmesi (“sniffing” ve “monitoring”)**
- **Botnet saldırıları**



# Siber Tehditlerin Amaçları

- **Sisteme yetkisiz erişim,**
- **Bilginin değiştirilmesi, yok edilmesi ve açığa çıkması,**
- **Hizmetin/Servisin engellenmesi,**



# Siber Güvenlik

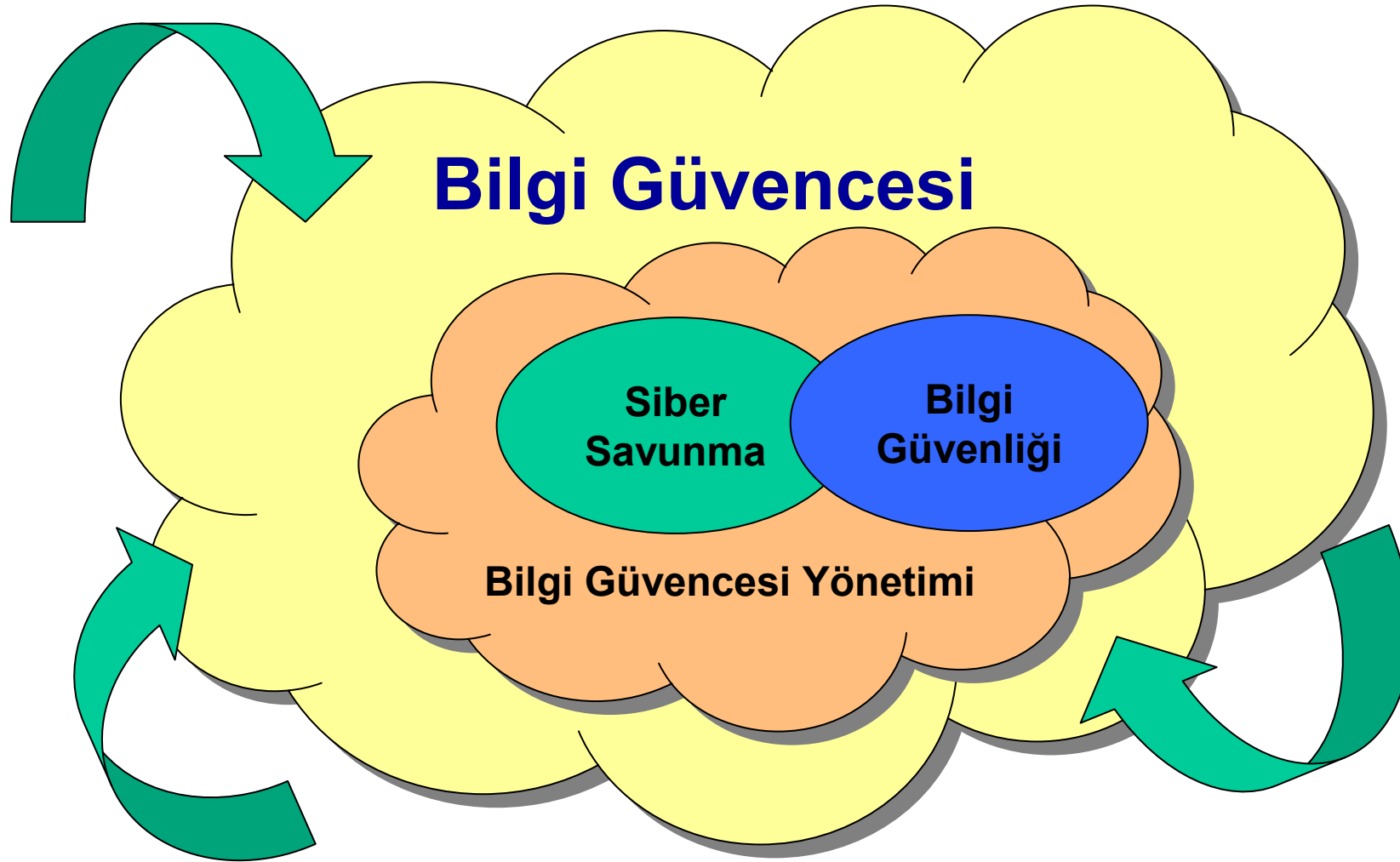
- Siber ortamda, kurumların varlıklarını korumak amacıyla kullandıkları uygulamalar ile teknolojilerin bir bütünüdür.

(yöntem, araç, politika, yönerge, risk yönetimi, eğitim vb.)

- Kullanılan kriptografik yöntem ve/veya mekanizmalar;
  - Veri Gizliliği
  - Veri Bütünlüğü
  - Erişim Denetimi
  - İnkâr Edilemezlik
  - Kimlik Doğrulama
  - İletişim Güvenliği



# Bilgi Güvencesi



# Siber Tehditlerin Gelişimi

| Basit Sistemler                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                               | Kompleks Sistemler                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><u>Hedefler:</u></b><br><b>İşletim Sistemleri</b> <ul style="list-style-type: none"><li>•Microsoft</li><li>•Linux</li><li>•Solaris</li></ul>                                                                                                       | <b><u>Hedefler:</u></b><br><b>Uygulamalar</b> <ul style="list-style-type: none"><li>•Veritabanları</li><li>•Yazılım paketleri</li><li>•WEB tabanlı uygulamalar</li></ul>                                                                                      | <b><u>Hedefler:</u></b><br><b>Yeni Nesil Teknolojiler</b> <ul style="list-style-type: none"><li>•Sanal Sistemler</li><li>•Ağlar</li><li>•Yazılım Hizmetleri<br/>(SaaS/ ITsaas)</li></ul>                                                                                        |
| DÜN                                                                                                                                                                                                                                                   | BUGÜN                                                                                                                                                                                                                                                         | YARIN                                                                                                                                                                                                                                                                           |
| <b><u>Saldırgan Profili:</u></b> <ul style="list-style-type: none"><li>•Az eğitilmiş</li><li>•Şöhret amaçlı</li></ul><br><b><u>Saldırı Çeşitleri</u></b> <ul style="list-style-type: none"><li>•E-mail sistemleri aracılığıyla virüs yaymak</li></ul> | <b><u>Saldırgan Profili:</u></b> <ul style="list-style-type: none"><li>•İyi eğitilmiş</li><li>•Maddi kazanç elde etmek</li></ul><br><b><u>Saldırı Çeşitleri</u></b> <ul style="list-style-type: none"><li>•Web siteleri aracılığıyla malware yaymak</li></ul> | <b><u>Saldırgan Profili:</u></b> <ul style="list-style-type: none"><li>•Deneyimli</li><li>•Servis sağlayıcılara yönelik saldırılar</li><li>•Bot saldırıları</li></ul><br><b><u>Saldırı Çeşitleri</u></b> <ul style="list-style-type: none"><li>•Polimorfik saldırılar</li></ul> |
| Az eğitilmiş                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                               | Profesyonel                                                                                                                                                                                                                                                                     |

# İhtiyaç Duyulan Yetenekler

- **Siber tehditlere karşı koyabilmek için sahip olunacak yetenekler;**
  - **Siber Analiz,**
  - **Açıklık Taraması,**
  - **Sızma Tespiti,**
  - **Ortak Bilgi Güvencesi Resmi,**
  - **Bilgisayar Olaylarına Müdahale Yeteneği,**
  - **Kötücül Yazılım Tespiti ve Engellenmesi.**





# Yapılması Gerekenler

- Bilgi Güvenliđi yasal düzenlemelerinin yapılması,
- Ülke yeteneklerinin geliştirilmesi,
- Farkındalık yaratmak için eğitim ve konferanslar,
- Kritik altyapıların güvenliđi,

*(finans, enerji, ulaşım, iletişim, güvenlik vb. )*

- Bilgisayar Olaylarına Müdahale Organizasyonunun ulusal seviyede kurulması,
- Uluslararası eşgüdümün sağlanması,
- Siber ordu oluşturulması,



# Uygulamalar

- Almanya Hükümeti tarafından Şubat 2011'de onaylanan “Siber Güvenlik Stratejisi” belgesinde;

“Siber ortamda yer alan bilgilerin doğruluğu, güvenilirliği ve gizliliği 21'inci yüzyılın en önemli sorunlarından biri haline gelmiş durumdadır.”

- Federal Enformasyon Teknolojileri Güvenliği Dairesi çatısı altında Ulusal Siber Savunma Merkezi kurulmuştur. Bu birimde çalışanların görevi;

“internet üzerinden yapılan saldırıları tespit etmek ve bu saldırılara, karşı-atak yöntemleri geliştirmek.”

# Uygulamalar

- ABD’de Mayıs 2010 tarihinde “Siber Komutanlık” resmi olarak kurulmuş ve göreve başlamıştır.

*“Siber Komutanlık, siber uzaydaki savunma faaliyetlerini tek çatı altında toplamakta ve gerektiğinde saldırı gerçekleştirebilme yeteneğinede sahip bulunmaktadır.”*

- ABD siber komutanı General Keith Alexander;

*“Siber saldırıların Estonya üzerindeki etkisi ciddi fakat geçici olmuştur. Gelecekte bu saldırılar kalıcı hasarlar verecek hale gelebilir. Amerika’nın altyapısı bu tip tehlikelere karşı güvenli değildir. Teknoloji kanun ve politikalardan daha hızlı ilerlemektedir, bunu düzeltmek gerekmektedir. Komutanlığın bir görevi de Anayurt Güvenliği Bölümünü desteklemektir, fakat komutanlığın sivil altyapı üzerinde bir yetkisi yoktur. Kongre’nin gerekli kanun değişikliklerini yapması gerekmektedir”*

# Siber Saldırlara Milli Çözümler

- **Bilgi teknolojileri ve güvenliği konularında etkin olarak çalışmalarını sürdüren Aselsan tarafından özgün olarak geliştirilen milli çözümler;**
  - **Yeni Nesil IP Ağ Kripto Cihazı-2064**
  - **Sanal Hava Boşluğu-SAHAB,**
  - **Milli Güvenlik Duvarı-MİLGÜD,**
  - **Emniyetli Sabit Disk-2195**



# 2064Mini IP Kripto Cihazı

- Yüksek Güvenlik Özellikleri
- Mobil IP (Dinamik Keşif Protokolleri) Desteği
- IPSec Standartlarına Uyumlu
  - IPSec Security Architecture, RFC 4301
  - Authentication Header, RFC 4302
  - Encapsulating Security Payload, RFC 4303
- İki Algoritma Desteği (GİZLİ /ÖZEL)
- 10/100/1000 Mb/s Ethernet Arayüzü
- SDIP-27 TEMPEST Uyumlu
- Manual ve Elektronik Anahtar Yükleme
- Web Tabanlı Yerel ve Uzak Yönetim Arayüzü (SNMP)



## Desteklenen İletişim Protokolleri

- IP
- ARP
- ICMP
- OSPF
- BGP



# 2064 IP Ağ Kripto Cihazı

## Mobil IP Desteęi

- Güvenli Ağların Dinamik Keşif Protokollerine İzin Verir
  - OSPF, BGP

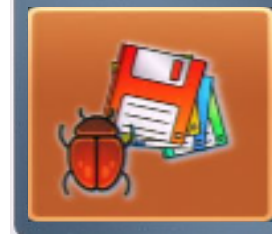


- IPKC Cihazları Birbirlerini Dinamik Alarak Bulabilirler
  - TED, Tunnel Endpoint Discovery Protokol

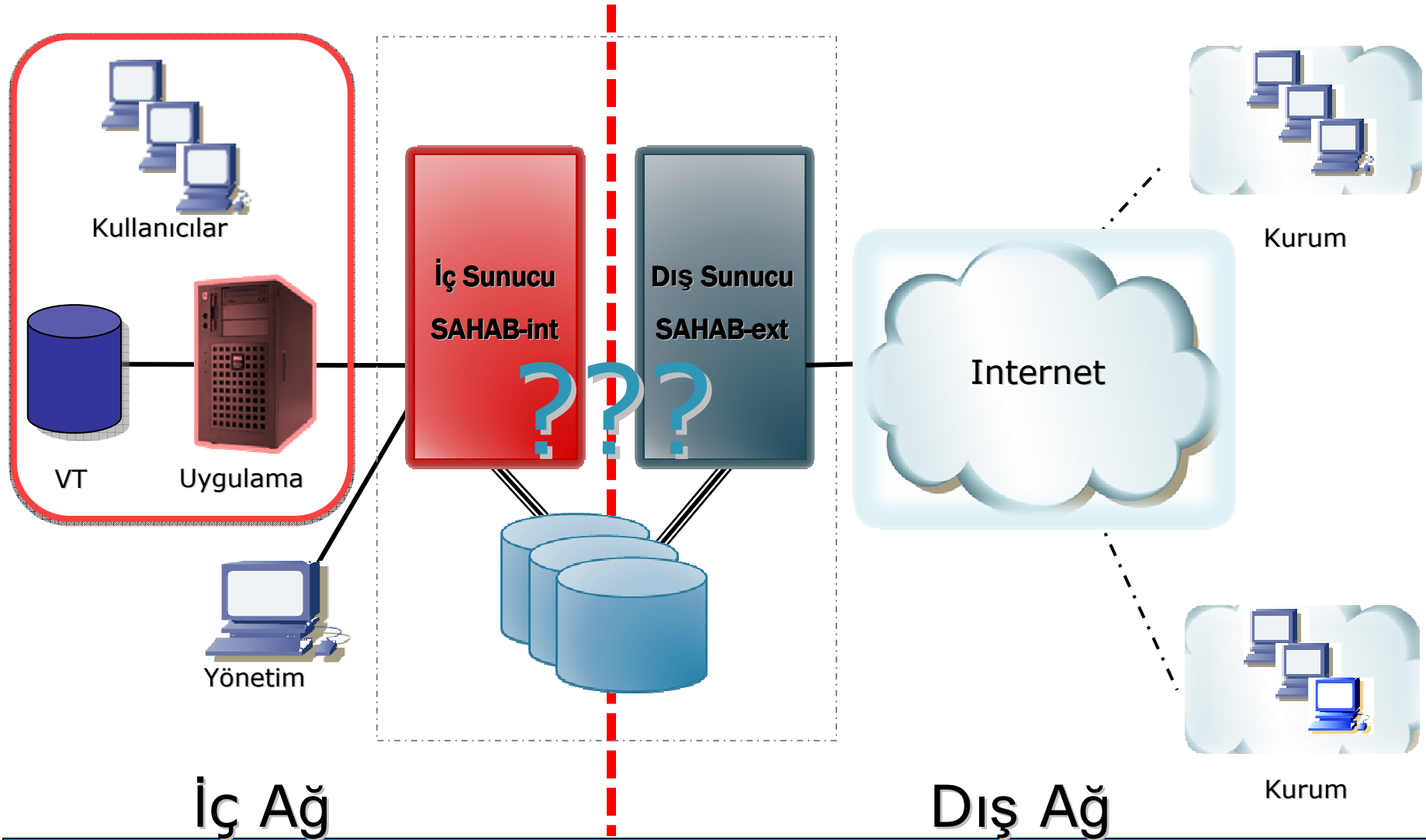
# Sanal Hava Boşluğu - SAHAB



- Gizlilik seviyesi daha düşük bir ağdan gizlilik seviyesi daha yüksek bir ağa gerçek zamanlı güvenli iletişim sağlamak,
- Denetimsiz, doğrudan veya dolaylı yoldan erişime izin vermemek,
- Gizlilik Derecesi Yüksek olan ağın güvenliğini korumak.

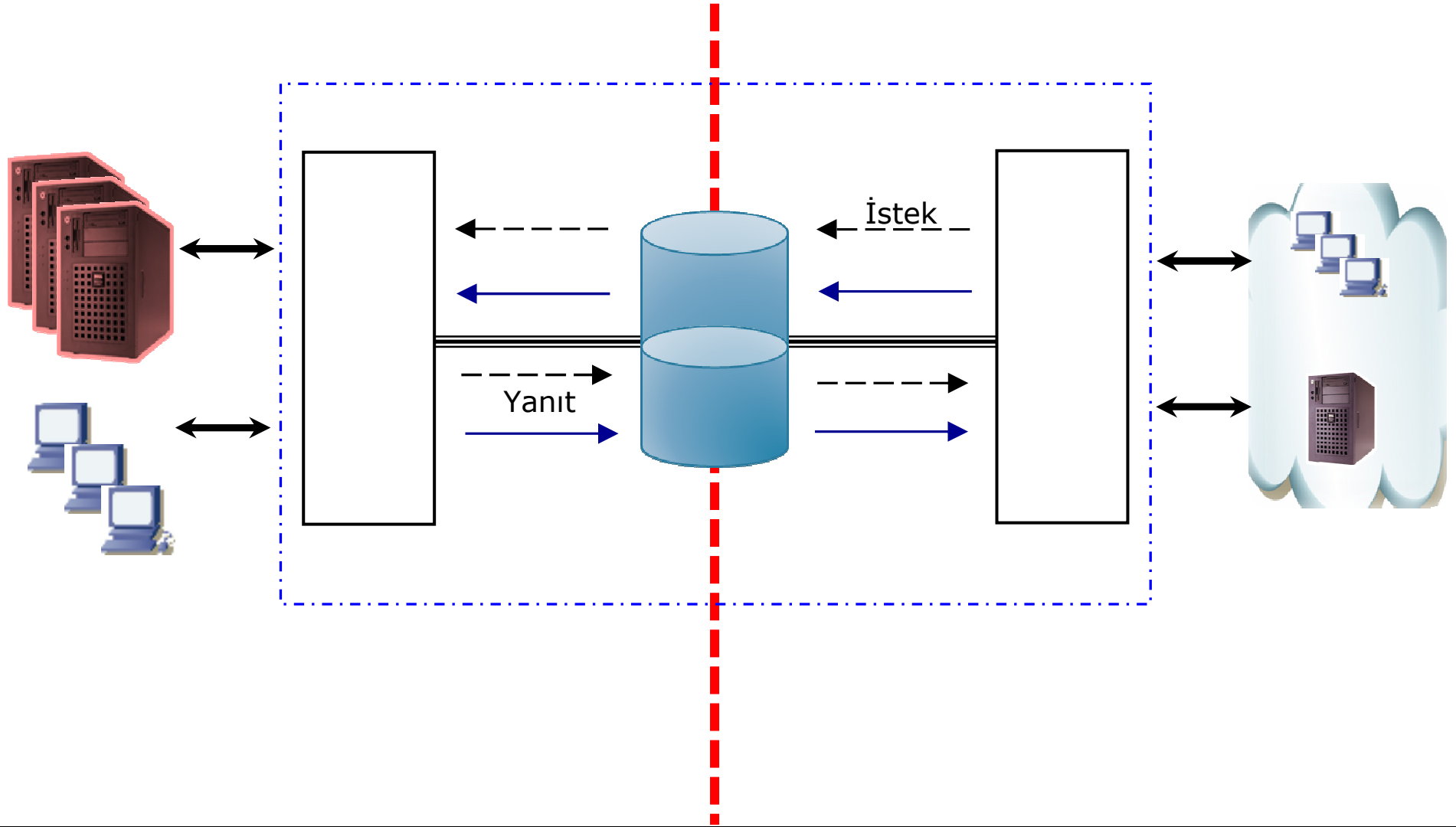


# Sanal Hava Boşluğu - SAHAB





# SAHAB İletişim Modeli

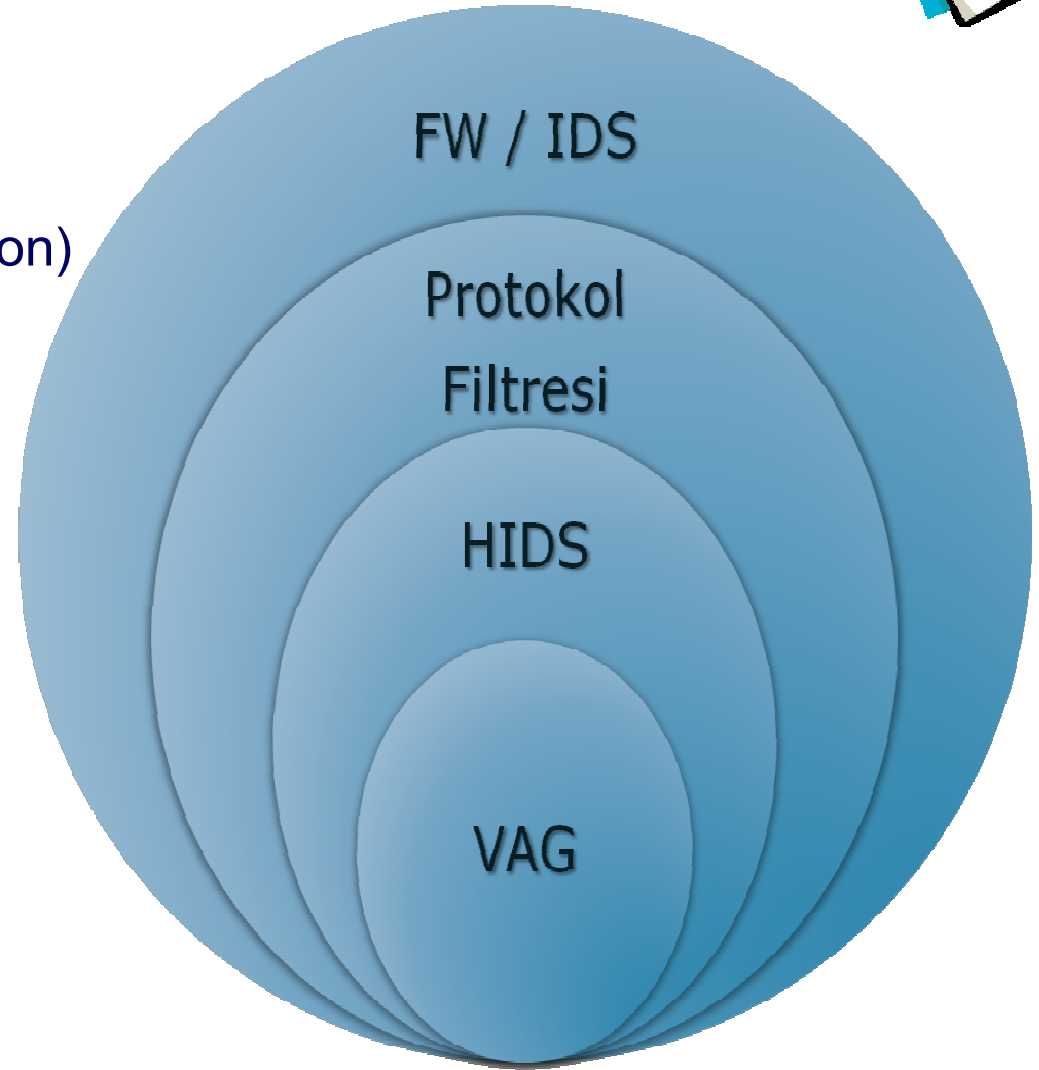


# SAHAB Bileşenleri



- **Koruyucu Bileşenler**

- Firewall
- Intrusion Detection
- İmzalı kodlar (Trusted Execution)
- Obfuscation (şaşırtma)
- Bütünlük denetimi (HIDS)



# SAHAB Bileşenleri



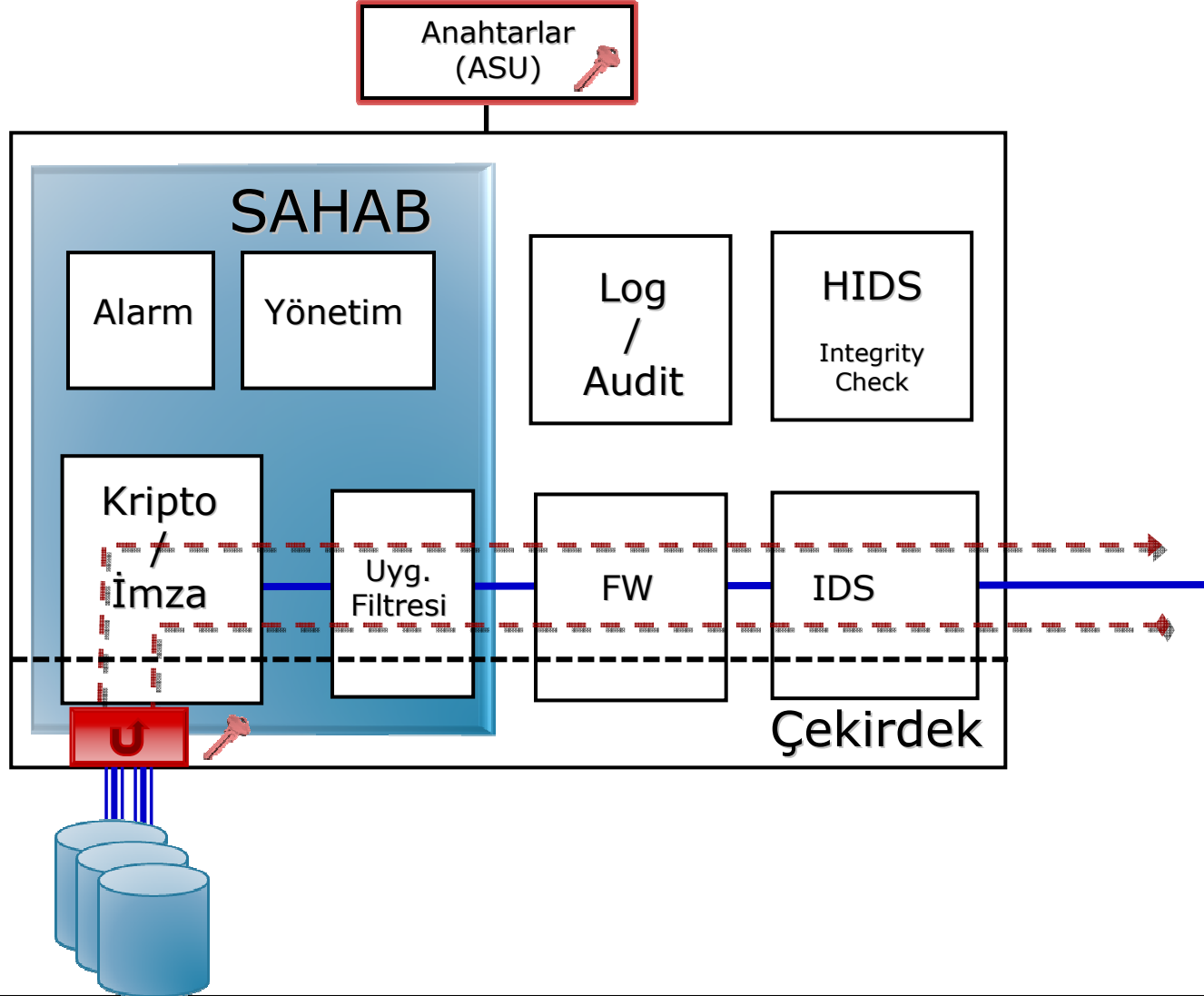
- **3 Katmanlı Yapı**

- Uygulama katmanında çoklu protokol desteği
  - HTTP, **FTP**, E-posta, vb.
- Protokol'den bağımsız mesaj katmanı
- Güvenli Disk Erişimi ("Air Gap") (Çekirdek)



**EAL4+**

# SAHAB Sunucu Mimarisi



# SAHAB Temel Özellikleri



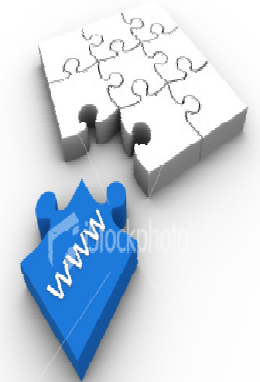
- **Ölçeklenebilirlik**
  - Multi-threaded Yazılım Yapısı
    - Multi-Core İşlemci Desteği
  - Birden fazla disk kanalı ve kanal teknolojisi
    - SAS, FC, SATA, vb.
  - Çok sayıda fiziksel disk



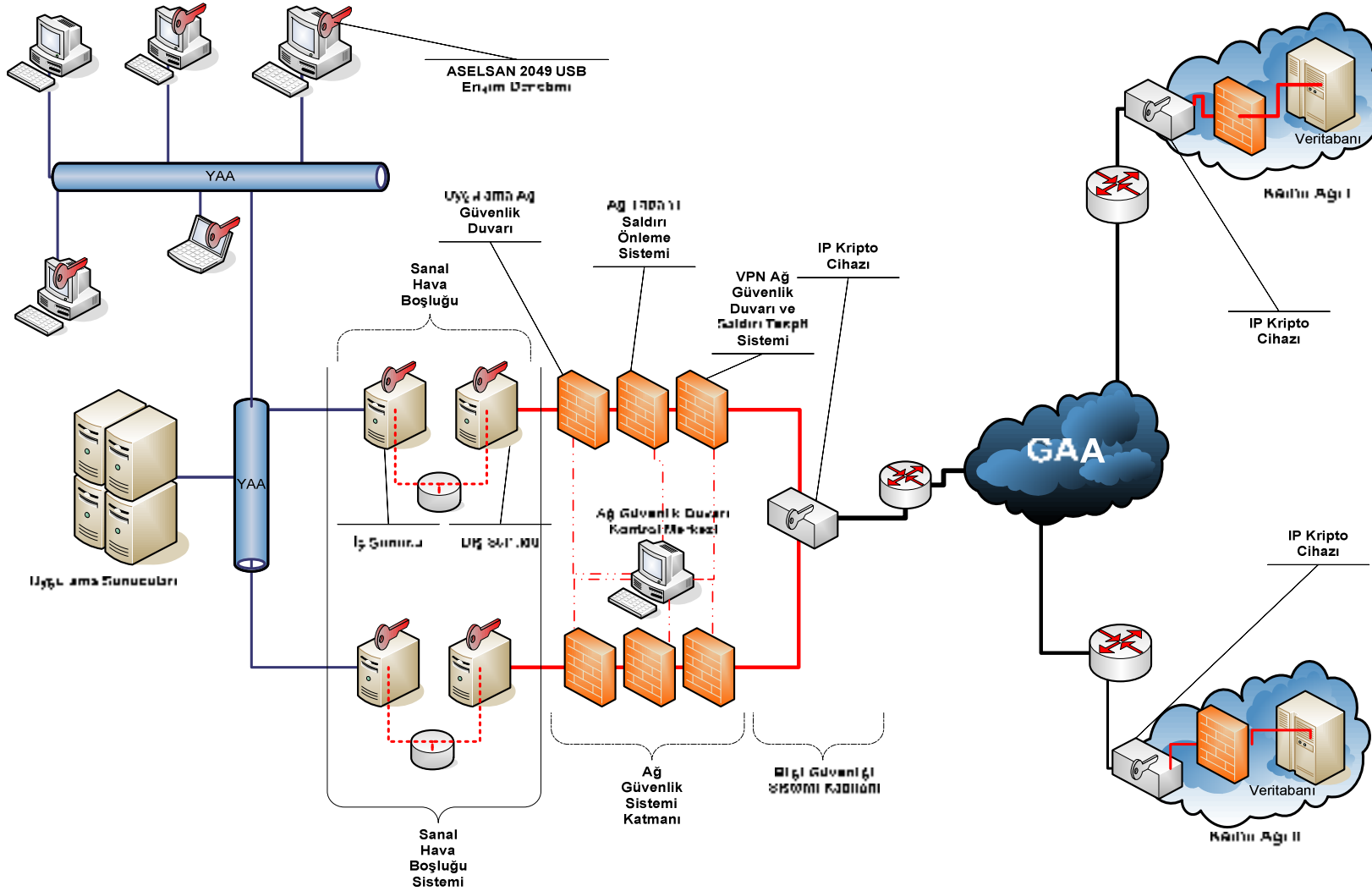
# SAHAB Güvenlik Özellikleri



- Disk (Pasif Bileşen)
  - Mesajlar iç ve dış sistemlerin iradesi ile okunur ve işlenir
  - Sadece SAHAB protokolü kalıbına uyan mesajlar yazılır ve okunur
    - IP vb. diğer protokoller disk sınırını aşamaz
- Disk Erişimi
  - Dosya Sistemi (NTFS, FAT, EXT3, vb.) yok!
  - Sektör, track bazında “özel” erişim yöntemi
- Şifreleme / İmzalama
  - İstekler ve yanıtlar şifrelenmiş ve imzalanmış mesajlar olarak yazılır ve okunur
  - Anahtarlar açılış sırasında ASU’dan alınarak çekirdek içinde gizlenir



# 2180 SAHAB GENEL MİMARİ





# MİLGÜD- Milli Güvenlik Duvarı

**Merkezi Tehdit Yönetim yapısına uyumlu tasarıma sahip MİLGÜD aşağıdaki özelliklere sahiptir;**

- Güvenlik Duvarı
- Sızma Önleme Sistemi
  - sınırsız sayıda saldırı paterni tanımlayabilme
- Hizmet Dışı Bırakma Saldırılarına Karşı Koruma
  - SYN/Dos/DDoS
- Kullanımı Kolay Grafik Arayüz Yazılım Modülü
- Milli Algoritma Desteği
- Ağ Erişim Denetleme
- Sanal IP Desteği ile Ağ Gizliliği



# MİLGÜD - Milli Güvenlik Duvarı

- **Desteklenen servis ve sunucu özellikleri**

- DHCP sunucusu / yönlendirme,
- VPN sunucusu / yönlendirme,
- HTTP proxy, posta yönlendiricisi (mail ağ geçidi), spam filtresi, FTP yönlendiricisi (ağ geçidi), SSH proxy,
- SNMP, OSPF/RIP,

- **Kriptografik özellikler**

- Milli algoritma desteği
- Standart algoritma desteği
  - (AES-128/256,3DES,DES,4096 bit RSA Private CA)



- **Yönetim Özellikleri**

- Zaman ayarlı dinamik kural yönetimi,
- Çok yönlü (multipath) yük dengelemesi (load balancing)
- Entegre geniş alan ağı (WAN) optimizasyon,
- Nesneye yönelik (object-oriented) kural kümesi tanımlayabilme
- USB bağlantısı üzerinden güncel veya ilk konfigürasyona geri alma (roll back) ve felaket kurtarma (disaster recovery)

# 2195 Emniyetli Sabit Disk

**“GİZLİ”** gizlilik dereceli Emniyetli Sabit Disk kullanımı ile;



- Diske yazılan tüm verilerin fiziksel seviyede kriptolanması,
- Veri Diski ve/veya İşletim Sistemi Diski olarak kullanılabilme özelliği,
- Donanım yapıli kriptolama
- IDE, SATA ve USB arayüz desteği
- 2.5 inch ve 3.5 inch boyutlarına uygunluk
- Harici ve Dahili Kullanım özelliği

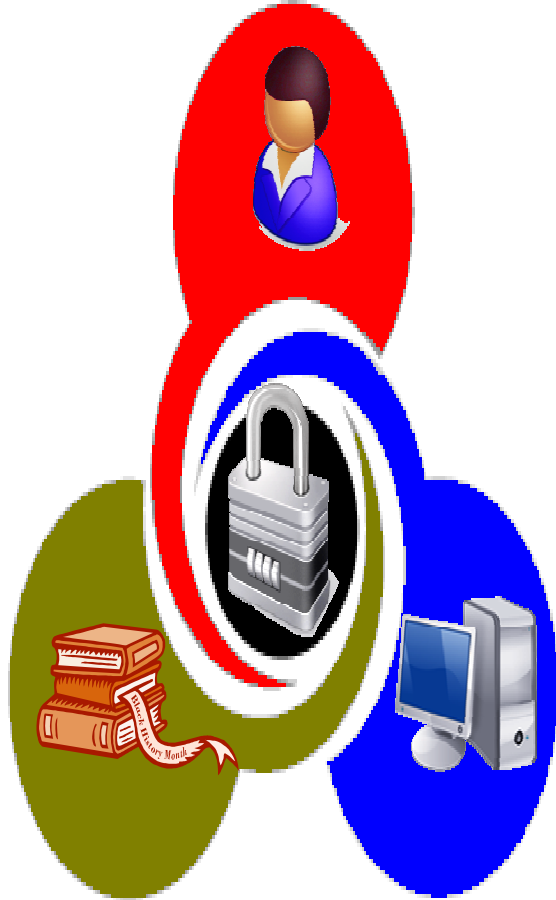
# SONUÇ

**Siber ortamda savaş amacıyla kazanılmasına ihtiyaç duyulan yeteneklerin milli çözümler ile karşılanması önem arz etmektedir,**

**aselsan** 35 yıllık deneyimi, bilgi güvenliği ve kriptoloji alanında ulaşmış olduğu olgunluk seviyesiyle;

- **Bilgi Teknolojileri,**
- **Bilgi Güvencesi,**

**hizmet sağlama ve ürün geliştirme yeteneğine sahiptir.**



***Arz Ederim...***



**aselsan**

**Siber Güvenlik İçin  
Milli Çözümler**

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

# Kapsam

- **Kripto ve Bilgi Güvenliđi Yetenekleri**
- **Siber Güvenlik Ürünleri**
- **IP Kripto Ürün Ailesi**
- **Sonuç**

**aselsan**

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

# Kripto ve Bilgi Güvenliği Yetenekleri

## •Kriptografik Ürün Tasarımı

- On-line Uçtan-uca krypto
- On-line Link krypto
- Off-line krypto

## •Kriptografik Algoritma Tasarımı

- Simetrik Algoritma Tasarımı (COMSEC/TRANSEC)
- Asimetrik Algoritma Tasarımı/Açık Anahtar Altyapısı (PKI)
- Özet Algoritma Tasarımı (HASH)
- Analiz ve Simülasyonu

## •Anahtar Yönetim Sistemi/Güvenlik Yönetim Sistemi

- Kripto Anahtarı /RSA Anahtarı Üretimi, Arşivlenmesi ve Testi
- Manuel / Elektronik Anahtar Dağıtımı
- Havadan Anahtar Dağıtımı
- EKİM Yönetimi
- Erişim Denetim ve Yönetimi
- Konfigürasyon ve Alarm Yönetimi

## •Kriptografik Protokol ve Mekanizma Tasarımı

- Kimlik Doğrulama Yöntemleri
- Veri Bütünlüğü Yöntemleri
- Sayısal İmzalar
- Anahtar Değişim Protokolleri
- Erişim Denetimi Yöntemleri

**Kripto ve Bilgi Güvenliği alanında yüksek düzeyde bilgi birikimi, ürün geliştirme ve tasarım yeteneği bulunmaktadır.**



**Gizlilik**  
**Kriptolama**

**Doğrulama**  
**Sayısal İmza**



**Erişim Denetimi**  
**Sayısal İmza/İşlem**  
**Kayıtları**

**Veri Bütünlüğü**  
**Özet Algoritması/ Sayısal İmza**

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011



# Siber Güvenlik Ürünleri



aselsan

**Siber Güvenlik  
Ürünleri**



aselsan

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

# 2049 PCMCIA / USB Kripto Cihazı



**aselsan**

**2049**

**PCMCIA/USB  
Kripto Cihazı**



**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

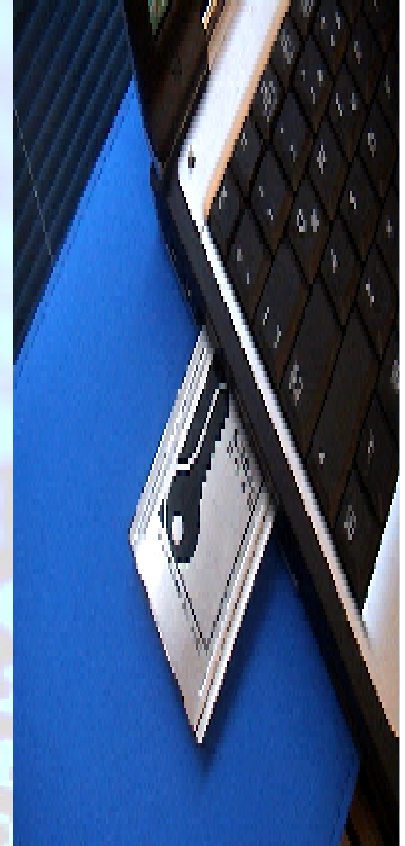
# 2049 PCMCIA / USB Kripto Cihazı



Yetkisiz erişimin engellenmesinin yanı sıra,  
Kişisel bilgisayarlar üzerindeki gizlilik dereceli  
dosyaların;

- Şifrelenmesi
- Güvenli olarak saklanması
- Güvenli olarak dağıtılması
- Güvenli e-posta hizmeti

amacıyla kullanılan donanım yapıli kripto  
ürünüdür.



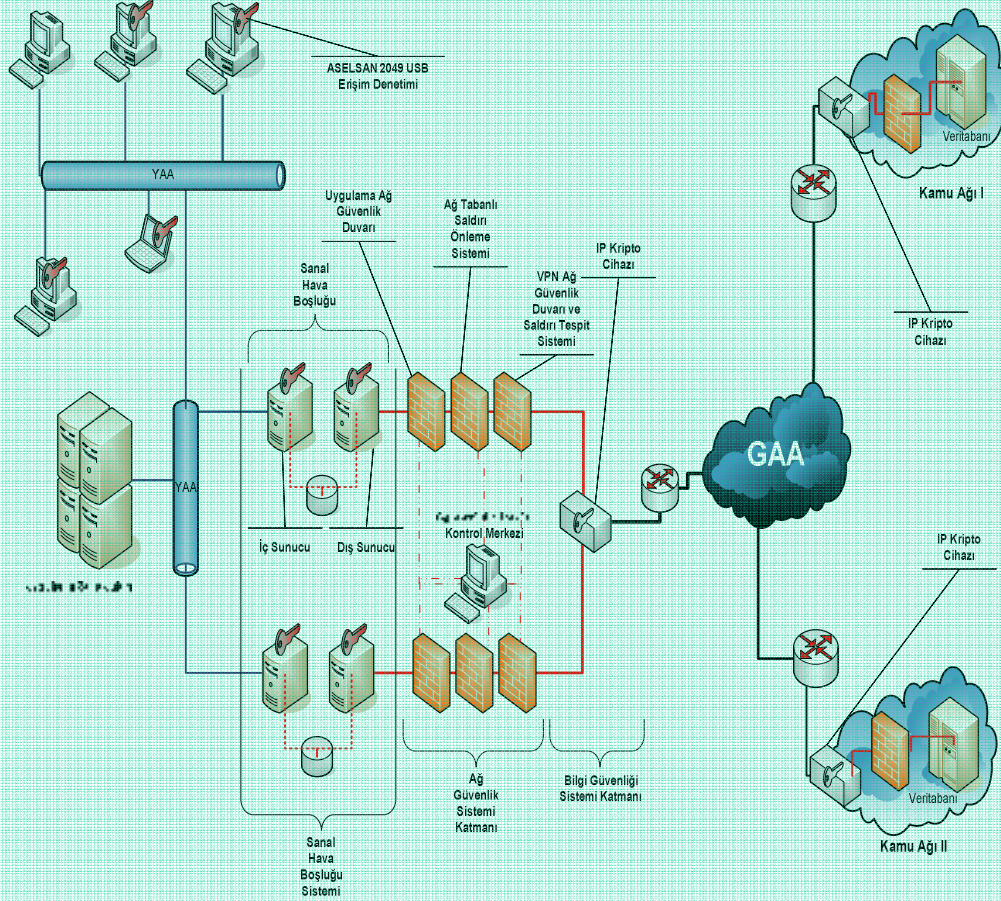
# 2195 Emniyetli Sabit Disk



- Diske yazılan tüm verilerin fiziksel seviyede kriptolanması
- Veri Diski ve/veya İşletim Sistemi Diski olarak kullanılabilme özelliği,
- Donanım yapıları kriptolama
- IDE, SATA ve USB arayüz desteği
- 2.5 inch ve 3.5 inch boyutlarına uygunluk
- Harici ve Dahili Kullanım özelliği



# Sanal Hava Boşluğu - SAHAB

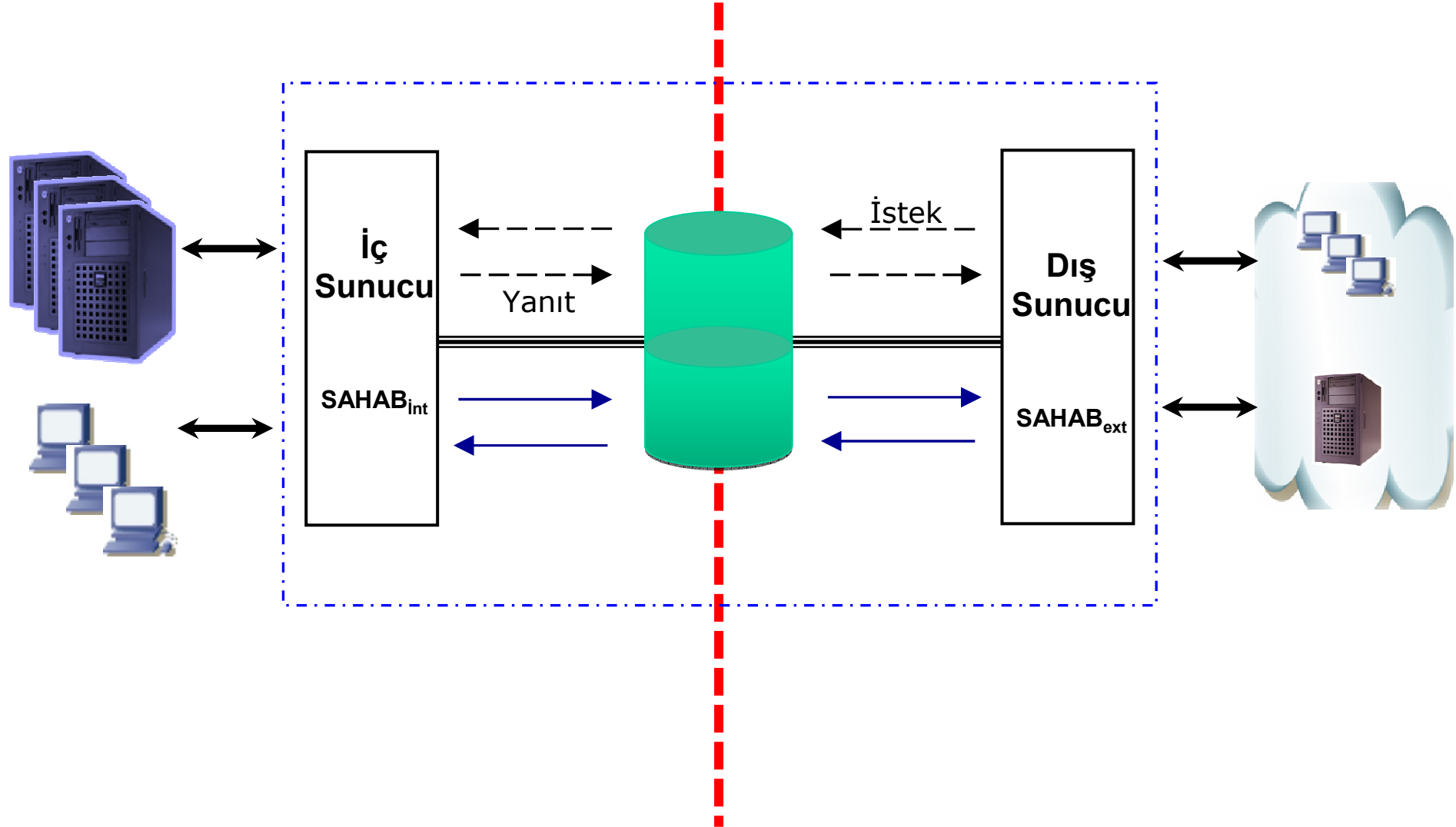


- Gizlilik seviyesi daha düşük bir ağdan gizlilik seviyesi daha yüksek bir ağa gerçek zamanlı güvenli iletişim sağlamak

- Denetimsiz doğrudan veya dolaylı yoldan erişime izin vermemek

- Gizlilik Derecesi yüksek olan ağın güvenliğini korumak

# SAHAB İletişim Modeli



# 2064 Serisi IP Ağ Kripto Cihazları



**aselsan**

**2064**  
**2064E**  
**2064Mini**

**IP Ağ Kripto**  
**Cihazları**

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

# 2064 Serisi IP Ağ Kripto Cihazları

- Yeni Nesil IP Kripto Cihazı (PCN Mimaride Çalışabilme)
- NATO NINE Standartlarına Uyumlu
- Yüksek Güvenlik Özellikleri
- IPSec Standartlarına Uyumlu
- Mobil IP (Dinamik Keşif Protokolleri) Desteęi
- İki Algoritma Desteęi (GİZLİ /ÖZEL)
- IPv6 Desteęi





# 2064 Serisi IP Ağ Kripto Cihazları

- IPSec Standartlarında Tanımlı
  - IKE
  - ESP
  - AH, özelliklerinin yanı sıra,
- Aselsan tasarımı milli algoritmaların kullanımı,
- IPSec'le sağlanmayan kullanıcı doğrulama özellikleri mevcuttur.



# 2064 Serisi IP Ağ Kripto Cihazları

- Elektronik Kimlik Modülü (EKIM) Erişim Denetimi
- 3-yönlü Güçlü Kimlik Doğrulama
- SDIP-27 A TEMPEST Uyumlu
- Manuel ve Elektronik Anahtar Yükleme



## Aksesuarlar

- Fillgun Cihazı
- Elektronik Kimlik Modülü, EKIM
- Yönetim Sistemi

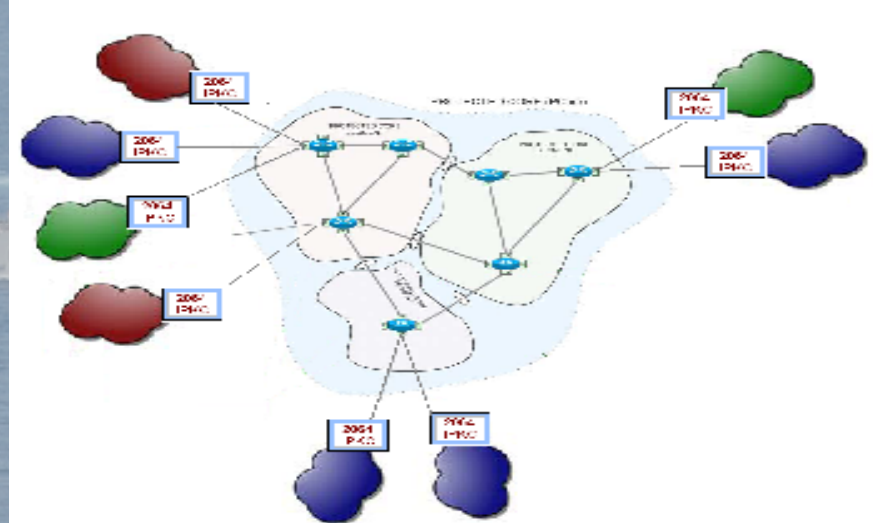




# 2064 Serisi IP Ağ Kripto Cihazları

## Mobil IP Desteği

- Güvenli ağların Dinamik Keşif Protokollerine izin verir.
  - OSPF, BGP
- IPKC cihazları birbirlerini dinamik olarak bulabilirler.
  - Tünel Keşif Protokolü
- Aynı anda farklı güvenlik seviyelerinde iletişim kurabilmektedir.



# 2064 Serisi IP Ağ Kripto Cihazları

## 2064 IPKC



10/100 Mbit/s ethernet arayüzü

60 Mbit/s işlem hızı

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011

# 2064 Serisi IP Ağ Kripto Cihazları

## 2064E IPKC



10/100/1000 Mbit/s ethernet arayüzü

300 Mbit/s işlem hızı

**aselsan**

Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

Eylül 2011



# 2064 Serisi IP Ağ Kripto Cihazları

## 2064Mini IPKC



10/100Mbit/s ethernet arayüzü

Taşınabilir boyut

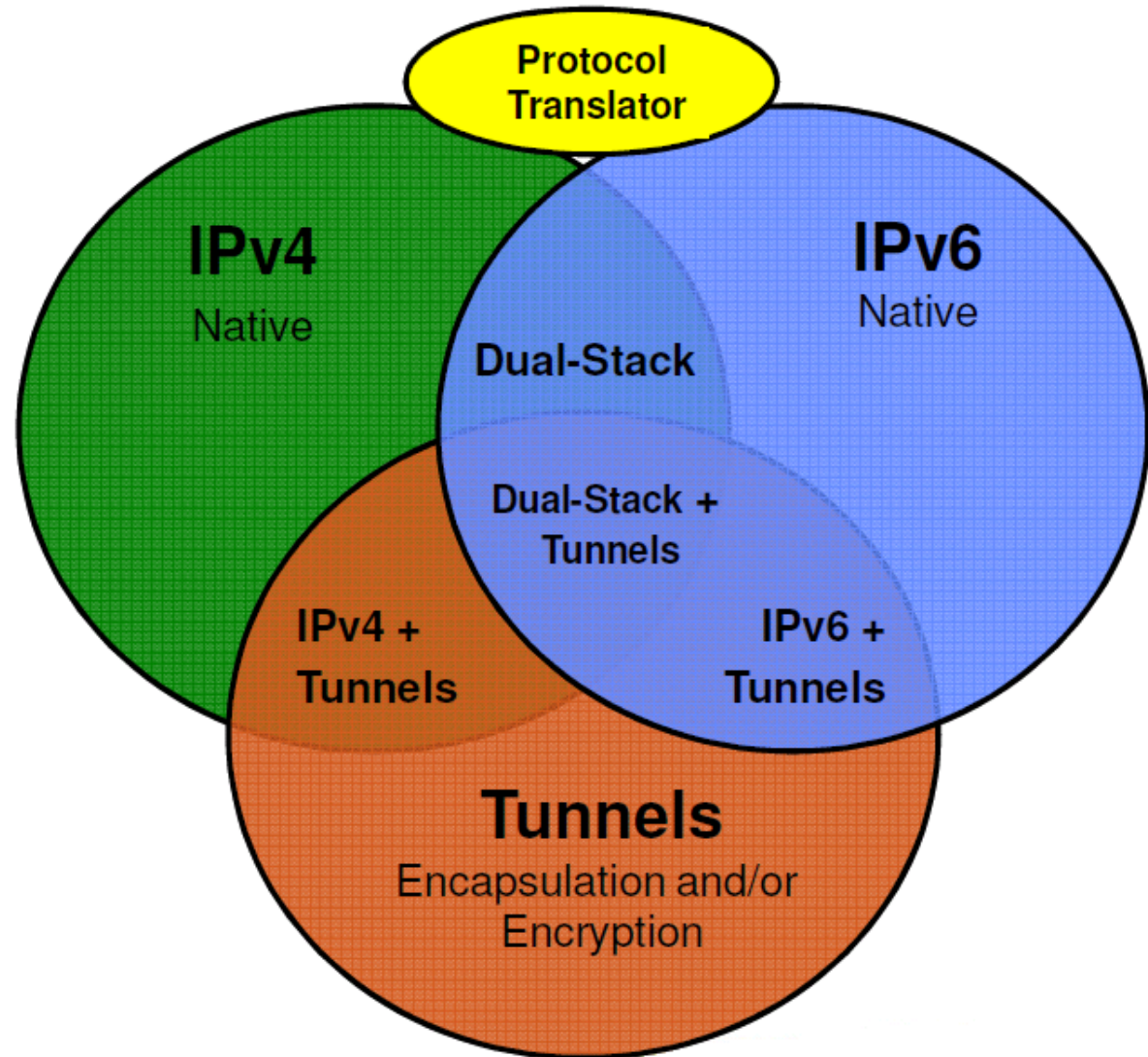
# IPv6 GeçiŖi

- Son IPv4 adresleri Ŗubat 2011 tarihinde IANA tarafından verildi.
- IPv6'ya geçiŖ zorunluluk halini almıŖ durumda.
- IPv6'ya geçiŖin gvenlikle ilgili avantajları ve dezavantajları olacak.
- IPv6 destekleyen cihazların v4 – v6 geçiŖinde alması gereken nlemler bulunuyor.



# 2064 IPv6 Geçişi

- 6in4
- 6to4
- Dual Stack



Teşekkürler...  
M. Özgür ŞAHİN  
Aselsan A.Ş.

[mosahin@aselsan.com.tr](mailto:mosahin@aselsan.com.tr)



## Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Sistemi

Kerim Göztepe

Ahmet Ejder

## Takdim Planı

- ❖ Bulanık ve Klasik Mantık
- ❖ Siber terörizm
- ❖ Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Sistemi
- ❖ Sonuç

2/16

## Siber Terörizm

- ❖ Stanford Taslağı
- ❖ Siber terör “hukuken yetkili kılınmış görevlilerinin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü ya da yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdididir”

## Klasik (Aristo) Mantık

- ❖ Murat'ın boyu 158cm dir.
- ❖ 100, 1'den 99 fazladır.
- ❖ Bu yaprak %56 kırmızıdır.
- ❖ Düşman tanklarının bize mesafesi 312m.
- ❖ Hedefin 78m ötesi.

Bu ifadeler bulanık değildir

## Bulanık Mantık

- ❖ Murat uzun bir çocuk.
- ❖ 100, 1'den çok daha büyük bir sayıdır.
- ❖ Kırmızı bir yaprak.
- ❖ Düşman tankları bize çok yakın.
- ❖ Hedefin hemen ötesi.
- \* Bu cümleler, klasik mantık sistemleriyle net olarak tanımlanması güç cümlelerdir.

Bu ifadeler bulanıktır.

## Bulanık Mantık

Uzun Güzel Derhal Büyük

- ❖ Açık bir şekilde tanımlanmamış, belirsizlik içeren sözcükler.

Açıkça tanımlanmamış kavramlar insanın düşünmesinde önemli rol oynar.

## Bulanık Mantık

- ❖ *Bulanık mantık, insan düşüncesinin ortaya koyduğu sözel bilgileri matematiksel verilere çevirmekte ve bunları bulanık küme teorisi ile ifade edebilmektedir.*

## Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Sistemi

- ❖ Bu çalışmada siber terör saldırıları karşısında daha bilinçli hareket etmek, kritik sistemlere yapılacak siber saldırılar karşısında neler yapılabileceğini önceden görmek maksadıyla bulanık mantık tabanlı karar destek sistemi geliştirilmiştir.



## Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Sistemi

- ❖ Model dört adımdan oluşmaktadır.

Adım 1: Siber saldırı önleme grubunun oluşturulması



Adım 2: Bulanık karar destek sistemi kriterlerinin belirlenmesi



Adım 3. Uygulama kuralları ve çıkarım yönteminin belirlenmesi



Adım4. Siber tehdit engelleme bulanık karar destek sisteminin uygulanması

| Girdi                     | Tanım                          | Kısaltma | Bulanık Değer         |
|---------------------------|--------------------------------|----------|-----------------------|
| Teknikler                 | Aç saldırısı                   |          | (0, 0, 1)             |
|                           | DoS saldırısı                  |          | (0, 0, 0, 1, 0, 2)    |
|                           | Virüs                          |          | (0, 1, 0, 3, 0, 5)    |
|                           | E-mail virüs                   |          | (0, 1, 0, 5, 0, 2)    |
|                           | Truva atı                      |          | (0, 0, 0, 7, 0, 3)    |
|                           | Sosyal mühendislik             |          | (0, 8, 0, 9, 1)       |
|                           | Zararlı yazılım                |          | (0, 5, 1, 1)          |
| Amaç                      | Mantık bombası                 |          | (0, 5, 0, 6, 0, 65)   |
|                           | Hizmet dışı bırakmak           |          | (0, 0, 0, 2)          |
|                           | Web sayfasını ele geçirmek     |          | (0, 1, 0, 3, 0, 6)    |
|                           | Küçük düşürmek                 |          | (0, 3, 0, 5, 0, 65)   |
|                           | Gizli bilgileri ele geçirmek   |          | (0, 4, 0, 85, 0, 9)   |
|                           | Kritik sistemleri ele geçirmek |          | (0, 4, 0, 6, 0, 8)    |
|                           | Kontrol etmek                  |          | (0, 85, 1, 1)         |
| Saldırı yapılan yerler    | Haberleşme                     |          | (0, 0, 0, 3, 0, 6)    |
|                           | Banka ve finans                |          | (0, 2, 0, 3, 0, 4)    |
|                           | Elektrik santralleri           |          | (0, 8, 0, 85, 0, 9)   |
|                           | Petrol ve doğalgaz dağıtım     |          | (0, 45, 0, 9, 1)      |
|                           | Su şebekesi                    |          | (0, 5, 0, 8, 0, 85)   |
|                           | Ulaştırma                      |          | (0, 5, 0, 6, 0, 7)    |
|                           | Acil hizmetler                 |          | (0, 45, 0, 55, 0, 65) |
| Siber terör yapan gruplar | Kamu kuruluşları               |          | (0, 4, 0, 65, 0, 85)  |
|                           | Bilgisayar korsanları          |          | (0, 0, 4, 0, 8)       |
|                           | Siber aktivistler              |          | (0, 7, 0, 85, 1)      |
|                           | Sistem düşmanları              |          | (0, 2, 0, 8, 0, 3)    |
| Çıktı                     | Özel personel                  |          | (0, 0, 1, 0, 3)       |
|                           | Tanım                          |          |                       |
| Yazılım                   | Mali yazılım                   |          | (0, 6, 25, 0, 5)      |
|                           | Güncelleme                     |          | (0, 2, 0, 5, 0, 7)    |
|                           | Ulusal bilgi merkezi           |          | (0, 5, 0, 75, 1)      |
| Donanım                   | Fiziksel kontrol               |          | (0, 0, 25, 0, 5)      |
|                           | Kritik bilgisayarlar           |          | (0, 3, 0, 6, 0, 3)    |
|                           | Teknik destek                  |          | (0, 6, 0, 8, 1)       |
| Eğitim                    | Kullanıcı eğitimi              |          | (0, 0, 3, 0, 6)       |
|                           | Farkındalık                    |          | (0, 3, 0, 5, 0, 7)    |
|                           | Kullanıcı kontrolü             |          | (0, 6, 0, 8, 1)       |

## Kriterlerin Açıklanması

- ❖ **Teknikler:** Siber saldırı yapan kişi veya gruplar farklı teknikler kullanmaktadır.



- ❖ **Amaç:** Siber saldırıların genellikle bir amacı vardır.

- ❖ **Saldırı yapılan yerler:** Siber saldırıları gerçekleştirenler amaçları doğrultusunda ki hedeflere saldırı düzenlerler.



## Kriterlerin Açıklanması

- **Siber terör yapan gruplar:** En tehlikeli kişiler profesyonel bilgiye sahip, belirli hedefler için saldırı düzenleyenlerdir.



- ❖ **Çıktı:** Elde edilen sonuçlar yazılım, donanım ve sistem kullanıcılarının eğitimi açısından incelenmelidir



## Modelin Uygulanması

- ❖ “Ağa saldırı ( $\delta = \delta_1$ )” tekniği kullanılan, saldırı amacının “hizmet dışı bırakma ( $\beta = \beta_1$ )” ve saldırı yapılan bölgenin haberleşme sistemleri ( $\gamma = \gamma_1$ ) olduğu bir siber saldırının kuralı aşağıda verilmiştir.

if  $[(\delta \text{ is } \delta_1) \text{ and } (\beta \text{ is } \beta_1) \text{ and } (\gamma \text{ is } \gamma_1)]$   
then  $[(\rho_d \text{ is } \rho_6)]$

- ❖ Bu durumda sisteme “teknik destek ( $\rho_d = \rho_6$ )” sağlanmalıdır.

## Modelin Uygulanması

- ❖ “Özel eğitilmiş ( $\theta = \theta_4$ )” kişilerce “zararlı yazılım ( $\delta = \delta_7$ )” kullanılarak “kontrol ( $\beta = \beta_6$ )” edilmek istenen bir “kamu kuruluşu ( $\gamma = \gamma_8$ )” sistemine organize siber saldırılar yapılmaktadır. Bu tip bir saldırıya karşı “milli yazılım ( $\rho_y = \rho_1$ )” kullanılmalı özel üretim “kritik bilgisayarlar” ( $\rho_d = \rho_5$ ) temin edilmeli ve bu bilgisayarların “kullanıcıları ( $\rho_e = \rho_7$ )” eğitilmelidir”.

if  $[(\delta \text{ is } \delta_7) \text{ and } (\beta \text{ is } \beta_6) \text{ and } (\gamma \text{ is } \gamma_8) \text{ and } (\theta \text{ is } \theta_4)]$   
then  $[(\rho_y \text{ is } \rho_1) \text{ and } (\rho_d \text{ is } \rho_5) \text{ and } (\rho_e \text{ is } \rho_7)]$

## Sonuç

- Siber terör, saldırı yapılan kamu veya özel kuruluşlara çok ciddi zararlar verebilmektedir. Bu nedenle bilişim teknolojilerini yoğun olarak kullanan kurum ve kuruluşlar;
- personel eğitimine önem vermelidir.
- milli yazılım kullanılmalıdır (özellikle kritik kamu sistemleri)
- siber saldırılar konusunda uzman teknik personel temin etmelidir
- ve en önemlisi siber tehdidi ciddiye almalıdır.

• İlginiz için teşekkür ederiz....





# SİBER GÜVENLİK ve TÜRKİYE

Prof. Dr. Şeref SAĞIROĞLU

Bilgi Güvenliği Derneği YK Üyesi  
Gazi Üniversitesi Mühendislik Fakültesi  
Bilgisayar Mühendisliği Bölümü  
[ss@gazi.edu.tr](mailto:ss@gazi.edu.tr)

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



## SUNUM ÖZETİ



- Genel Bakış ve Terminoloji
- Gündemdekiler
- Mevcut Durum Analizi
- Güncel Tehdit ve Tehlikeler
- Nasıl bir SG? Öneriler
- Sonuç ve Değerlendirmeler

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## TANIM?



### Siber Güvenlik?

“Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü” olarak tanımlanıyor.

Kaynak: ITU-T Recommendation X.1205 "Overview of Cybersecurity"

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## TANIM?



### Siber Güvenliğin Temel Hedefi?

Kurum ve kuruluşların bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, varlıkların ve kaynakların başlarına **KÖTÜ BİR ŞEYLER GELMEDEN** korumaktır.

Kaynak: <http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%208%20Cybersecurity.pdf>

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Siber Güvenlik Tanımı (ABD Başkanı Obama)



“Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir husustur.”

“Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir.

**"America's economic prosperity in the 21st century will depend on cybersecurity." May 2009**

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Ülkemizdeki Tanımlar..



### Ulaştırma Bakanı Sn. Binali Yıldırım

- “bilgi sistemi güvenliğinde **ortak akıl** ve ortak hareketle hattı müdafaa yerine sathı müdafaanın başarılı bir şekilde gerçekleştirilme girişimi”,
- “devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz.”



25-28 Ocak 2011

“siber savaş tehdidine karşı hazırlıklı olmanın, kurumların **bilgi sistemi** güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin artırılmasını amaçlamak”

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## İNTERNET

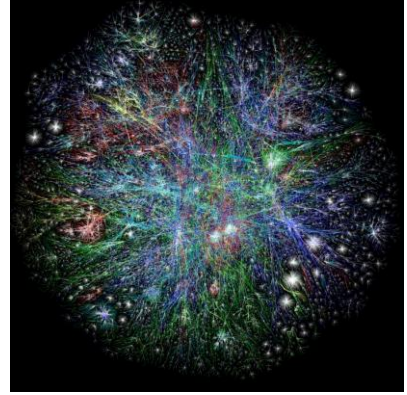


Eylül 1971

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



38 yılda  
gelenen  
nokta  
(2009)



Kaynak: <http://www.physorg.com/news151162452.html>

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

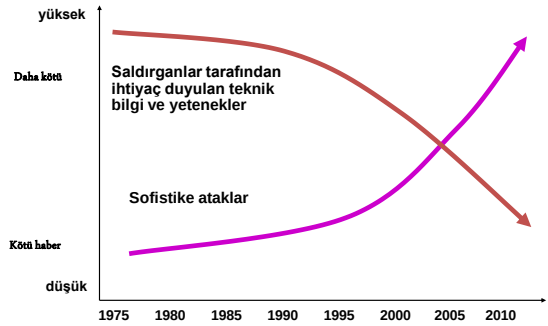
## GÜNDEMDEKİLER - 1

1. e-li ve m-li ortamlar yaygınlaşıyor..
2. Uygulamalar artıyor..
3. Tehdit, tehlikeler, saldırılar artıyor..
4. Yeni çözümler geliştiriliyor..
5. Bilinmesi gerekenler çoğalıyor..
6. Yapılacak ve kontrol edilecek parametreler sürekli artıyor.

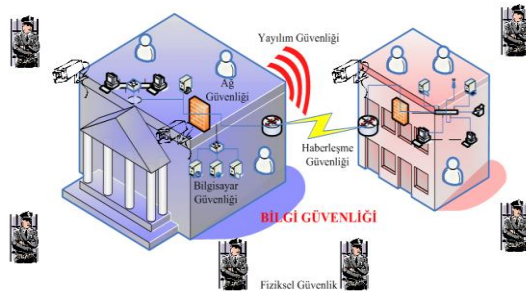
Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



## GÜNDEMDEKİLER - 2



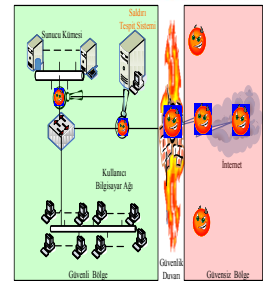
## GÜNDEMDEKİLER - 3



## GÜNDEMDEKİLER - 4

- Fiziksel Güvenlik
- Haberleşme Güvenliği
- Yayılım Güvenliği
- Bilgisayar Güvenliği
- Ağ Güvenliği
- Bilgi Güvenliği
- Donanım Güvenliği
- Yazılım Güvenliği
- İşletim Sistemi Güvenliği
- Sosyal Ağ Güvenliği
- Mobil Cihaz Güvenliği
- Veri Tabanı Güvenliği
- Web Teknolojileri Güvenliği
- Web Uygulama Güvenliği
- Protokol Güvenliği
- Sunucu Güvenliği
- IPv6 Güvenliği
- Algoritmik Güvenlik
- Siber Güvenlik
- Kritik Altyapı Güvenliği
- Şifre Güvenliği
- ...

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



## GÜNDEMDEKİLER - 5



- Savaşlar internete kaydı..
  - Ayyıldız TİM, Cyber Warrior, RedHack, Coldhacker
  - Anonymous
  - LulzSec (ABD Senatosu),
  - Estonya
  - Gürcistan
- Wikileaks
- İyilerin ve Kötülerin amansız savaşı
  - Saldıran Taraf
  - Savunan Taraf

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## GÜNDEMDEKİLER - 6



- Saldıran Taraf
  - Saldırıların artmakta saldırı bilgi seviyesi hızla azalmakta
  - Kötücül kodlar gelişerek ve değişerek hızla yayılmakta
  - Organize olarak sanal suç örgütlerini kurma
  - İyilerden hep bir adım önde

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## GÜNDEMDEKİLER - 7



- Savunan Taraf
  - Güvenliğiniz en zayıf halkanız kaddır.
  - **%99,9 Korunma + %0,1 Korunmasızlık = %100 güvensizlik**
  - Bilgisizlik, ilgisizlik, hafife alma
  - Korunma maliyetleri (Yatırım, Eğitim)
  - Kişilere güven duygusu
  - E-dünyanın doğasında olan güvensizlik

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## GÜNDEMDEKİLER - 8



- Siber Bilgi Güvenliği?

- Üretim
- Erişim
- İşleme
- Depolama
- Aktarma
- Yok etme

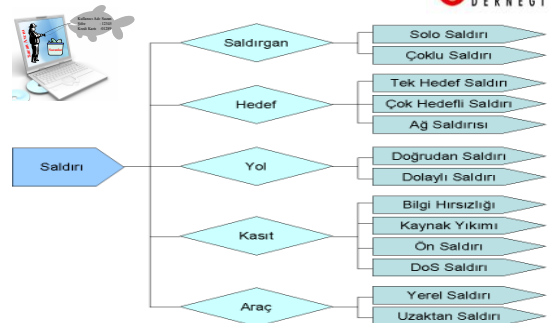


Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

GÜNDEMDEKİLER - 9  
(SALDIRILAR – 1)

- Saldırıların artık kapsamlı
- Çoklu saldırılar popüler
- Senaryoları yazılmış ve denenmiş,
- Karma yapıları içeriyor..
- Bilinmeyenler /düşünülmeyenler..
- Sürekli yenilikler içeriyor..
- Takip gerektiriyor..
- Yüksek bilgi birikimi gerektiriyor..

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

GÜNDEMDEKİLER - 9  
(SALDIRILAR – 2)

**GÜNDEMDEKİLER - 9****(SALDIRILAR – 3)**

1. Casus yazılım sayısı artıyor.
2. Farklılaşıyorlar.
3. Kendilerini saklayabiliyorlar, görünmez olabiliyorlar.
4. Silseniz bile tekrar kopyalayabiliyorlar
5. Belirli bir süre var olup sonra kendilerini yok edebiliyorlar.
6. 38 grupta bunları sınıflandırdık.

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

**GÜNCEL GELİŞMELER - 11****WIKILEAKS**

- Dünyanın güvenlik açısından çok iyi dersler çıkaracağı en iyi örnek
- ABD'nin sanal savaş denemesi
- Kendisini/diğer ülkeleri nasıl etkileyecek
- Geliştirilen teknolojileri test etme
- Facebook ve Google gibi teknolojilerini ne kadar iyi kullanabiliyor testi
- İnternet ne kadar kontrol edebilir / edilemez..

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

**GÜNCEL GELİŞMELER - 12****GOOGLE -2**

- Dünyanın en iyi casus yazılım sistemi
- Dünyanın bilgisini topluyor..
- Ülkesine hizmet eden en iyi yazılımlardan birisi..
- Bizi bizden (ülkeleri, ülkelerden) daha iyi analiz edebiliyor..
- Kelime/Cümle/Resim/Ses araması yapabiliyor..
- İstihbarat için vazgeçilmez bir ortam..
- Tabii ki bu sistemi iyi kullananlar için..
- encrypted.google.com hizmete giriyor..
- Güvenlik açığı oluşturabilecek hususları kapatıyor..

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

**GÜNCEL GELİŞMELER - 10**

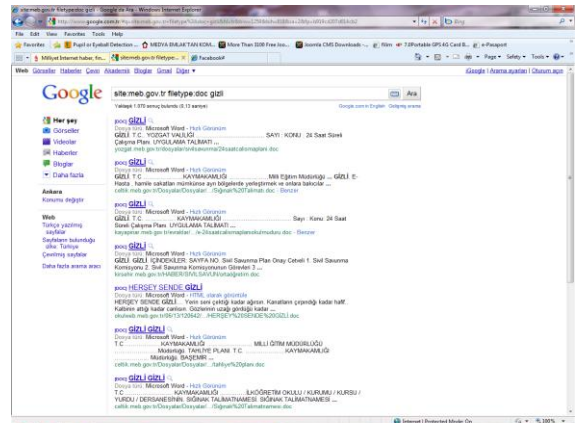
- Standartlar daha da spesifik.
- Kritik yapıların güvenliği mercek altında..
- Yeni çözümler kullanılıyor (Diyot Yaklaşımı)
- Kısıtlı kullanım sunan işletim sistemleri (JeOS)
- “Şifre (password)” yerini “Deyim veya Cümle Şifre (Pass-sentence)”..
- Sıfır gün / saat yaklaşımı
- 360 derece güvenlik.
- “Bilgi Güçtür!” yerine “Bilgi Güvenliği Sağlandı”
- Ölçüde Güçtür!” “Bilgi üretmeden korunulamaz.”

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

**GÜNCEL GELİŞMELER - 12****GOOGLE - 1**

- Mükemmel bir arama motoru
- En çok tercih edilen arama motoru
- Mükemmel hizmetler veriyor
  - Academics, books, translation, blogs, gmail, documents, mobil, talk, maps, IPv6, Google+, .....
  - Değeri 200 Milyar Dolar
- FAKAT...

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara







## Bilgi Güvenliği Standartları ?



- Bilgi güvenliği yönetim standartları (ISO/IEC 270XX ailesi)
- Kriptografik standartlar (PKCS)
- Güvenlik Değerlendirme standartları
- Güvenlik Denetimleri ve Hizmetleri
- Kimlik yönetimi ve gizlilik
- IT hizmet yönetimi

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## ISO/IEC Bilgi Güvenliği Standartları

| Standart Adı       | Açıklaması                                                              |
|--------------------|-------------------------------------------------------------------------|
| ISO/IEC 27000:2009 | Teknik terimler ve açıklamaları içeren genel bir sözlük                 |
| ISO/IEC 27001:2005 | BGYS ihtiyaçları (BS7799 Bölüm-2)                                       |
| ISO/IEC 27002:2005 | BGYS uygulama ilkeleri                                                  |
| ISO/IEC 27003      | BGYS uygulama rehberi                                                   |
| ISO/IEC 27004      | BGYS metrikleri ve ölçüm                                                |
| ISO/IEC 27005:2008 | BGYS risk yönetimi                                                      |
| ISO/IEC 27006:2007 | BGYS belge kaydı ve belgelendirme süreçleri kılavuzu                    |
| ISO/IEC 27007      | BGYS izleme/Denetim için kılavuz                                        |
| ISO/IEC 27008      | BGYS bilgi güvenliği güvenlik kontrollerini izleme/Denetim için kılavuz |
| ISO/IEC 27010      | Sektörden sektöre iletişimde BGYS kılavuzu                              |

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## ISO/IEC Bilgi Güvenliği Standartları

| Standart Adı       | Açıklaması                                                                                                                                                     |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27011:2008 | Haberleşme organizasyonları için BGYS kılavuzu (ITU X.1051).                                                                                                   |
| ISO/IEC 27012      | E-devlet hizmetlerinin uygulanması için BGYS rehberi                                                                                                           |
| ISO/IEC 27013      | BGYS ve ITIL dan türetilen Bilgi teknolojileri servis yönetim sisteminin entegrasyonunu tarif eden bir rehberdir. Bu yıl yayımlanacağı tahmin edilmektedir.    |
| ISO/IEC 27014      | Bilgi Güvenliği Yönetişimi.                                                                                                                                    |
| ISO/IEC 27015      | BGYS'nin finans sektöründe uygulanması rehberidir. Taslak halinde olan bu rehberin, son olarak kanunlara uyum hakkında görüş toplanması aşamasına gelinmiştir. |
| ISO/IEC 27016      | Bilgi Teknolojileri ve Güvenlik teknolojileri, BGY ve Organizasyon ekonomisi                                                                                   |

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## ISO/IEC Bilgi Güvenliği Standartları

| Standart Adı  | Açıklaması                                                                                                                                                                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27031 | Bilgi Teknolojileri odaklı İş Sürekliliği                                                                                                                                                                                                                                         |
| ISO/IEC 27032 | Siber Güvenlik Rehberi Servis olarak Yazılım ve Güvenlik, Web 2.0, Noktadan noktaya ağ, Blogging ve türevleri, Anlık mesajlaşma, VoIP ve VideoIP, sanal dünya, online oyunlar, ortalama vb olayları                                                                               |
| ISO/IEC 27033 | ISO/IEC 18028 Ağ güvenliği standardı yerine hazırlanmış henüz taslak halinde olan bir çalışmadır. Ağ güvenliği ve içeriği, tasarlama ve uyarılma rehberi, senaryoları, ağlar arasındaki güvenlik, IP yakınsaması, kablosuz ağ, VPN güvenliği rehberi ve diğer yapıların güvenliği |
| ISO/IEC 27034 | Uygulama güvenliğine yönelik olarak, organizasyon çerçevesi, uygulama güvenlik yönetimi işlemi, uygulama güvenlik geçerliliği, protokoller ve uygulama veri yapıları güvenlik kontrolleri, özel uygulama güvenlik kontrolleri                                                     |

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## ISO/IEC Bilgi Güvenliği Standartları

| Standart Adı  | Açıklaması                                                                                                                                                                                                                                       |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27035 | Halen yürürlükte olan ISO TR 18044 üzerinde küçük değişiklikler yapan, ISO/IEC 27035 güvenlik kazaları yönetimi standardı üzerine de çalışmalar devam etmektedir. ENISA'nın ülkeler arası bilgi paylaşımı apsamda değerlendirilmektedir.         |
| ISO/IEC 27036 | Güvenliğin dış kaynaklı olmasına istinaden kullanılabilecek bir rehber olarak tasarlanmaktadır. Bu taslak içinde COBIT ve ITIL/ISO 20000 gibi COSO yapısını da düşünme yönünde bir eğilim bulunmakta ve önerilmektedir. Şu an taslak halindedir. |
| ISO/IEC 27037 | Dijital kanıt toplama, belirleme ve korumaya yönelik bilgi güvenliği rehberi                                                                                                                                                                     |
| ISO/IEC 27038 | Bilgi Teknolojileri ve Güvenlik teknolojileri                                                                                                                                                                                                    |

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Bilgi Güvenliği Standartları (TR)



- Bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır.
- TSE ISO/IEC 17799:2000 standardını tercüme ederek 11 Kasım 2002 tarihinde TS ISO/IEC 17799 standardını yayınlamıştır.
- Bilgi güvenlik yönetimi ile ilgili tavsiyeleri içeren belgelerdir.
- TS 17799-2 standardı olarak 17 Şubat 2005 tarihinde kabul edilmiş ve yürürlüğe girmiştir. Ancak ISO/IEC 27001 standardı TS ISO/IEC 27001:2006 Türk standardı olarak kabul edildiğinden TS 17799-2 standardı TSE tarafından iptal edilmiştir
- ISO/IEC 27001:2005 standardın tercümesidir. TS 17799-2 Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgelendirme hizmetine Mart 2005 tarihi itibarı ile başlamıştır.
- [TS ISO/IEC 27001](#) 02.03.2006 Bilgi teknolojileri – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## DÜNYADA SİBER GÜVENLİK



- Genel durum pek iç açıcı değil..
- Bilgi varlıklarına değer veren ülkeler ülke stratejilerini geliştiriyorlar..
- Tehditleri belirleme ve durdurmaya yönelik çözümler üzerinde çalışılıyor..
- Politika ve stratejileri belirleme ve bunları yürürlüğe koyma..
- Farkındalık oluşturma çabaları..
- Uluslararası işbirliklerini geliştirme..



Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Siber Güvenlik Stratejisi (ABD)



- Kamu kurumları ağlarını tek bir ağ altında güvenli internet bağlantıları ile yönetme
- Kamu kurumları genelinde saldırıları tespit eden sensörler kurma
- Kamu kurumları genelinde saldırı önleme sistemleri kurulumunun sürdürülmesi.
- Ar-Ge çabalarının artırılmasını koordine etmek ve yönlendirme
- Güvenilen internet bağlantıları ile tek bir ağ kuruluş olarak kamu kurumları hizmetlerinin yönetilmesi.
- Durumsal farkındalığı geliştirmek için mevcut siber merkezleri birbirine bağlama.
- Hükümet çapında karşı siber casusluk planı geliştirilmesi ve uygulanması.
- Sınıflandırılmış ağların güvenliğini artırma.
- Siber eğitim çalışmalarını genişletme.
- Kalıcı bir "sıçrama-ilerleme" teknolojisi, stratejiler ve programlar tanımlayınız ve geliştiriniz.
- Kalıcı ve caydırıcılık stratejileri ve programları tanımlama ve geliştirme.
- Küresel tedarik zinciri ve risk yönetimi için çok yönlü yaklaşımlar geliştirme.
- Kritik altyapı alanları içine alan ve devletin sorumluluklarını tanımlayan genişletilmiş siber güvenlik çalışmaları yapma

Kaynak: <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## CNCİ Merkezin Temel Hedefi



- Kamu ve özel sektöre siber güvenlik eğitimleri ve etkinlikleri konusunda destek ve sponsor olmak, koordinasyonu sağlamak,
- Siber güvenlik danışma, kontak ve ortak bilgi toplama ve paylaşma noktası olmak,
- Siber güvenlik eğitim merkezi olmak ve akademik dereceler sağlamak.
- Siber güvenlik araştırmalarını için altyapı oluşturmak ve desteklemek

CNCİ: comprehensive national cybersecurity initiative

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

39

## Siber Güvenlik Stratejisi (Hindistan)



- Güvenlik Politikası, Uyum ve Güvence (Yasal Çerçeve)
- Güvenlik Olayı – Erken Uyarı ve Müdahale
- Kapasite geliştirme
- Dijital Adli Tıp Merkezleri Kurma
- Araştırma ve Geliştirme
- Uluslararası İşbirliği



Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Siber Güvenlik Stratejisi (Almanya)



Stratejik Hedefler ve Ölçütler

- Kritik Bilgi Altyapılarını Koruma
- Almanya BT Sistemleri Güvenliğini Sağlama
- Kamu Yönetiminde BT Güvenliğinin Güçlendirilmesi
- Ulusal Siber Müdahale Merkezi
- Ulusal Siber Güvenlik Konseyi
- Siber Güvenlik İçin Etkili Suç Kontrolü
- Avrupa Ve Dünya Çapında Siber Güvenliği Sağlamak İçin Etkin Koordinasyon
- Güvenilir Ve Sağlam Bilgi Teknolojisi Kullanımı
- Federal Kurumlardaki Personellerin Eğitimi Ve Gelişimi
- Siber Saldırıların Müdahale Araçları

Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara



## Siber Güvenlik Stratejisi (Hollanda)



- Bağlama ve güçlendirme girişimleri
- Kamu-Özel Ortaklığı
- Bireysel sorumluluk
- Departmanlar arasındaki sorumluluk Bölümü
- Aktif uluslararası işbirliği
- Alınması gereken önlemler orantılı olmalı
- Öz-denetim



Siber Güvenlik Çalıştay, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## SİBER GÜVENLİK ETKİNLİKLERİ

- BOME 2008 Tatbikatı, 20-21 Kasım 2008
- Sayısal Ortamda Savaş, 10 Aralık 2009
- Siber Savunma Çalıştayı, 6-8 Mayıs 2010  
(www.iscturkey.org)



- **Siber Güvenlik Tatbikatı 25-28 Ocak 2011**
- TMMM, Genel Kurmay Başkanlığı, 2011
- Siber Güvenlik Yaz Kampı, Ağustos 2011
- Siber Güvenlik Çalıştayı, 29 Eylül 2011

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## SİBER GÜVENLİK TATBİKATI

“siber savaş tehdidine karşı hazırlıklı olmanın, kurumların [bilgi sistemi](#) güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin artırılmasını amaçlamak”

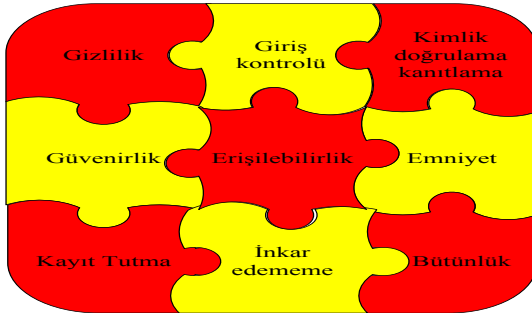
Ulusal Siber Güvenlik Tatbikatı (41 kamu ve [özel sektör](#))

- Enerji,
- Finans,
- Telekom,
- Savunma,
- Sağlık ve
- [Sosyal güvenlik](#)

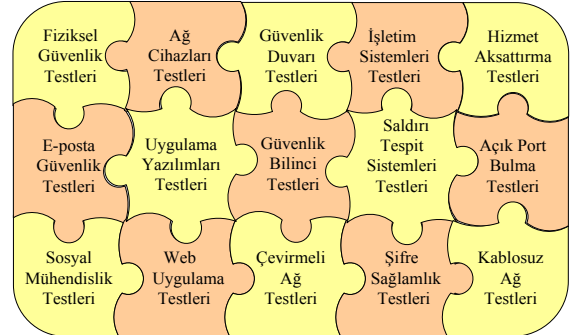


Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Nasıl bir Siber Bilgi Güvenliği?



## Nasıl bir Siber Bilgi Güvenliği?



## Nasıl Bir Siber Bilgi Güvenliği ?

### ÖNCELİKLE..

- Bilgi sistemleri güvenliği **ciddi olarak ele alınması** gerekiyor.
- **Neyin korunacağını** bilmek en önemli adım.
- **Nasıl korunacağını** veya korunamayacağını bilmek (risk yönetimi) **işin özü**.
- Uygulama safhası doğru yolda olduğunun, **gözleme, izleme ve denetim** de etkinliği ve **başarının anahtarıdır**.
- **İnsan-Eğitim-Teknoloji** birlikteliğini sağlamada işin **püf noktasıdır**.

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Nasıl Bir Siber Bilgi Güvenliği ?

### DAHA SONRA..

- Bu işlemleri koordine edecek bir birimin kurulması,
- Siber suçlarla mücadele biriminin kurulması
- Ulusal stratejilerin belirlenmesi ve kısa sürede hayata geçirilmesi
- Farkındalık-eğitim çalışmalarının artırılması
- Uluslararası BYGS standartlarının BT hizmeti veren devlet kurumlarında zorunlu hale getirilmesi
- Uluslararası işbirliğinin artırılması
- Bu konuda yapılacak olan ar-ge çalışmaları desteklenmeli
- Güncel tehditleri takip edip, duyuracak ve giderecek ekiplerin güçlendirilmesi veya bir yapı altında toplanması

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara

## Nasıl Bir Siber Bilgi Güvenliği?

### KISACA...

- Konunun sahibinin bilinmesi
- Standartların takip edilmesi ve uygulanması
- Farkındalık eğitimlerin artırılması
- Sızma testlerine önem verilmesi
- Güncel tehditlerin takip edilmesi ve mevcut sistemlerdeki açıkların giderilmesi
- Tüm kurumları mümkün olduğunca siber güvenlik tatbikatların katılması
- Güvenli yazılım geliştirme teknikleri kullanılarak yazılımların geliştirilmesi
- Saldırı tespitlerinin yapılması ve engellenmesi
- Veri kurtarma yaklaşımlarının bilinmesi
- Ulusal ve uluslararası işbirliğinin artırılması

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



**TEŞEKKÜR EDERİM.**

Adres:

[Gazi Üniversitesi Mühendislik Fakültesi](#)

[Bilgisayar Mühendisliği Bölümü](#)

[ss@gazi.edu.tr](mailto:ss@gazi.edu.tr)

Siber Güvenlik Çalıştayı, TNB Konferans Salonu, 29 Eylül 2011, Ankara



# **Philosophy** of Information Security

September 29<sup>th</sup> 2011, CYBER SECURITY WORKSHOP

Aysun TUNCER

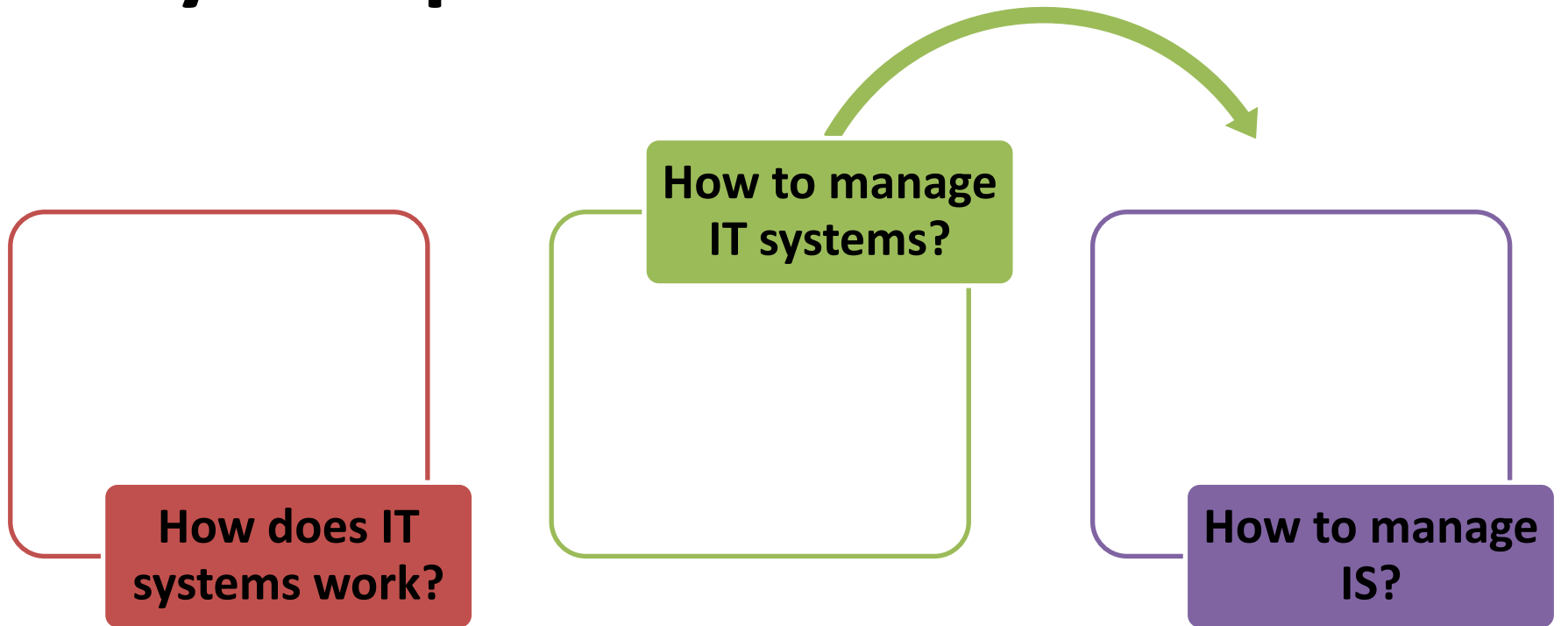
Information Security Consultant

Managing Director @ Armones

CISSP, CEH, ISO 27001 Lead Auditor



# Why this presentation?



**CURIOSITY**

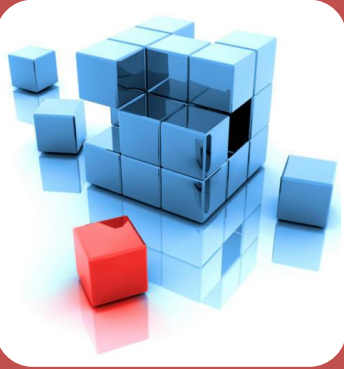




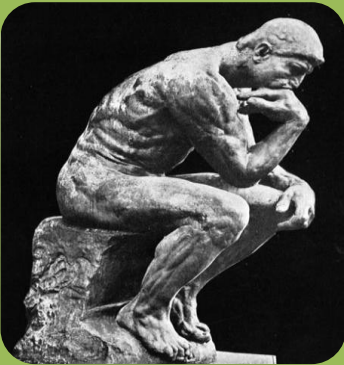


Curiosity **kills** the cat?

# I'm curious about what?



What is the **philosophy** of IS?



OK but, what is philosophy?

# What is philosophy?

## Φιλοσοφία

**Phileo**: Love, seek, search

**Sophia**: knowledge, wisdom



Aristoteles

“All humans naturally want to know” Metaphysics

# CURIOSITY



# So ...

We can **ask** fundamental questions

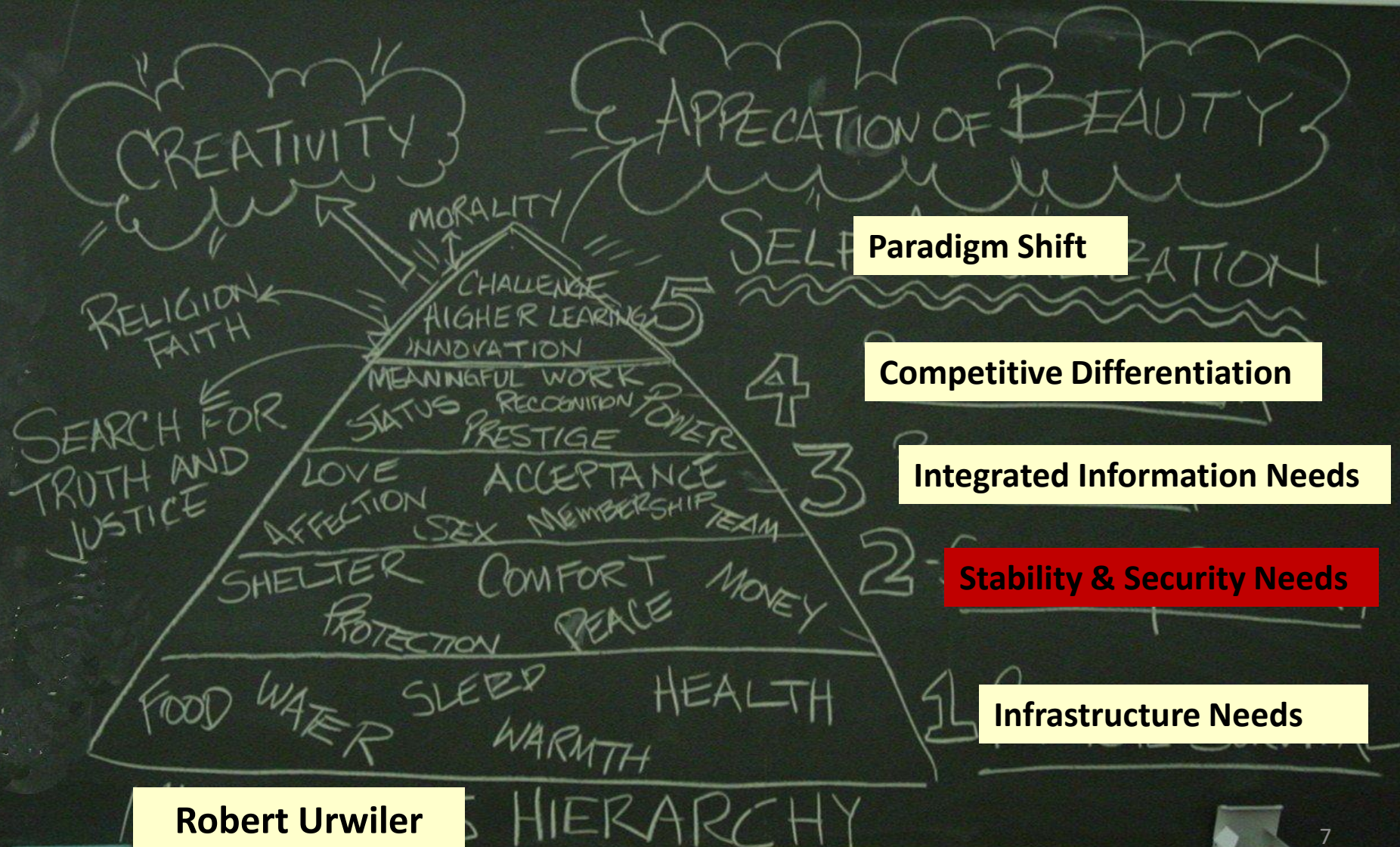
We can **question** fundamental concepts

Even try to **redefine** fundamental concepts





# What is the source of security need?



# Security of what?

We are trying to secure what?

How “value” is defined?

*“If information does not have any value, then who cares about protecting it?”*

*Shon Harris, CISSP Guide*





# Protect from what/whom?

合気道

Enemy, bad people?

Good people?

Yourself???

UKE

TORI



# Is there a threat/danger?

Threat perception\* of person answering the question?

- Information level
- Past experiences
- Selective perception?



\* Managers` perception of security directly effects IS strategy, organization, business plans and investment amounts

# Information Security lessons from Aikido



(Steven Seagal, 1993 All-Japan Aikido Demonstration)

# How are they protected in past?



# LETS PLAY A GAME 😊

## Find the common point in 2 pictures





# Border concept in cyberspace

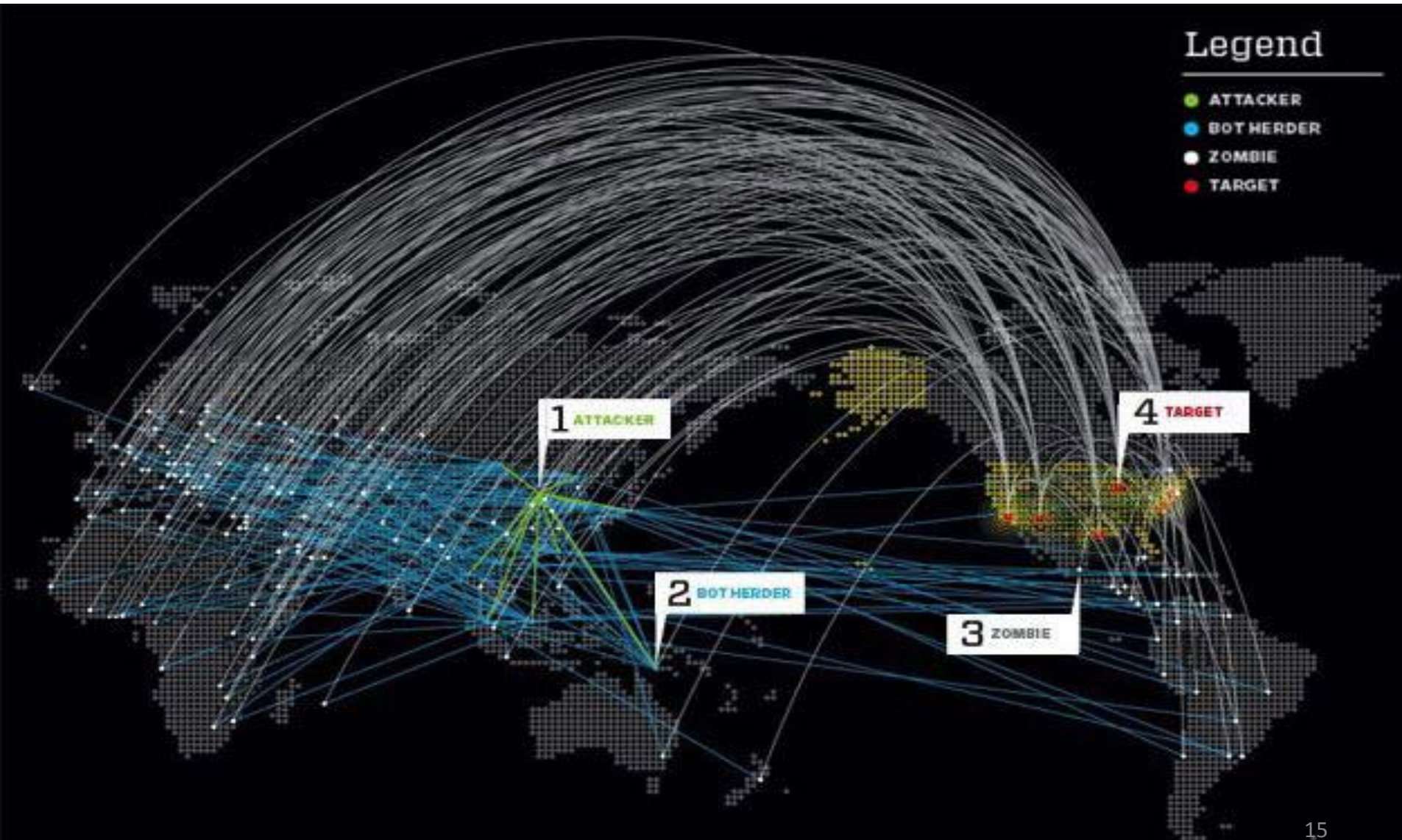
Border of economic relations

Nation`s border

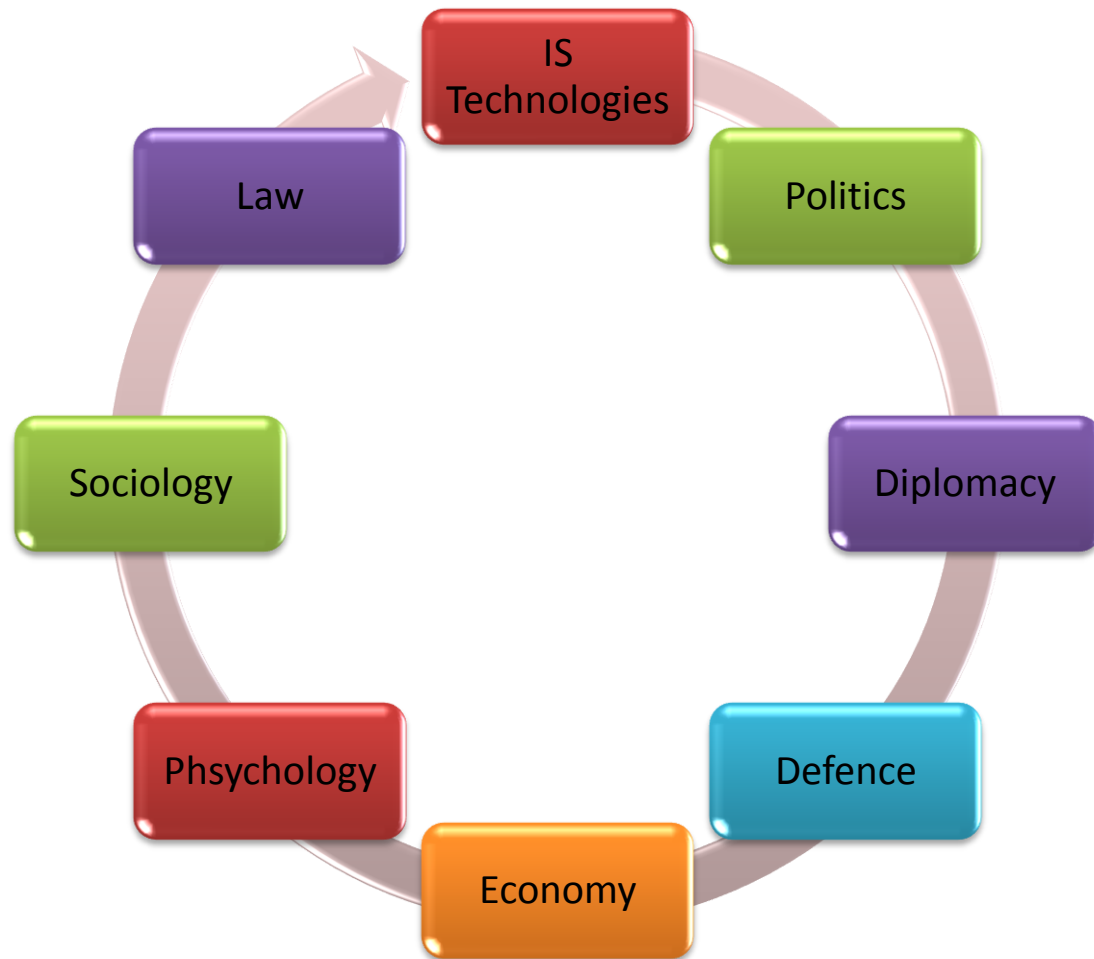




# Who serves whom?



# Security in a borderless world?



# Harmony, communication ...





**Thank you :)**

September 6<sup>th</sup> 2011, TUBAV

Aysun TUNCER

Information Security Consultant

Managing Director @ Armones

CISSP, CEH, ISO 27001 Lead Auditor

**ARMONES**



# **KRİTİK ALTYAPILARA YÖNELİK SİBER TEHDİTLER VE TÜRKİYE İÇİN SİBER GÜVENLİK ÖNERİLERİ**

**Bilge KARABACAK**

**Siber Güvenlik Çalıştayı**

**29 Eylül 2011**

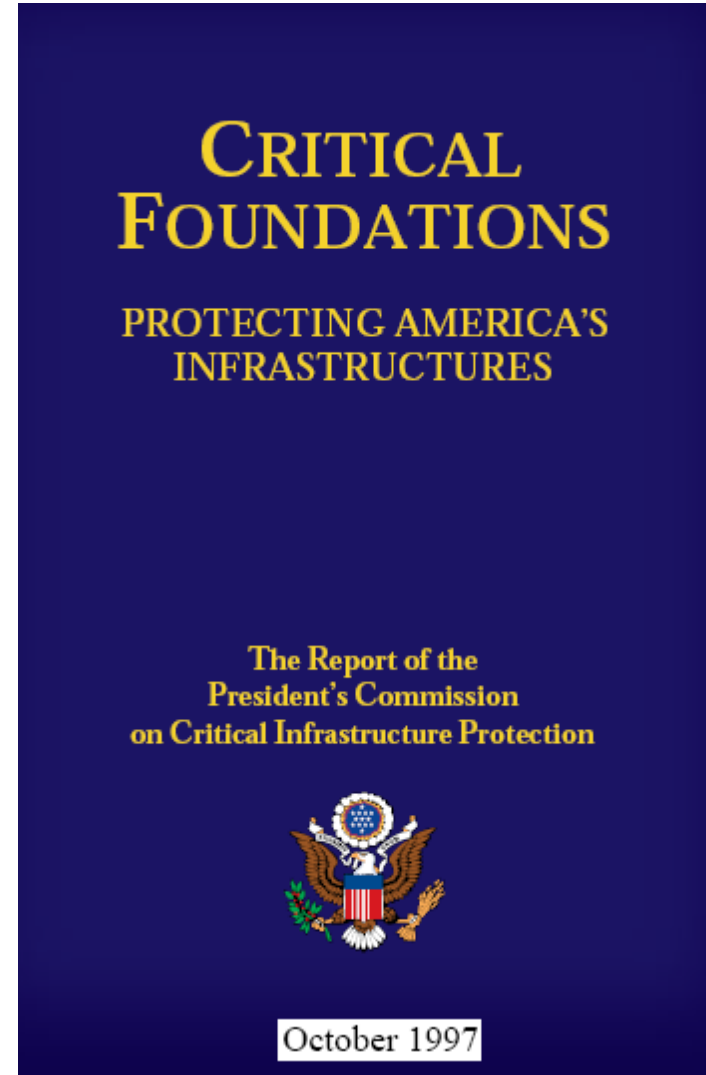


- Kritik Altyapılar
- SCADA Sistemleri
- Kritik Altyapılara Yönelik Siber Tehditler
- Karşı Önlemler

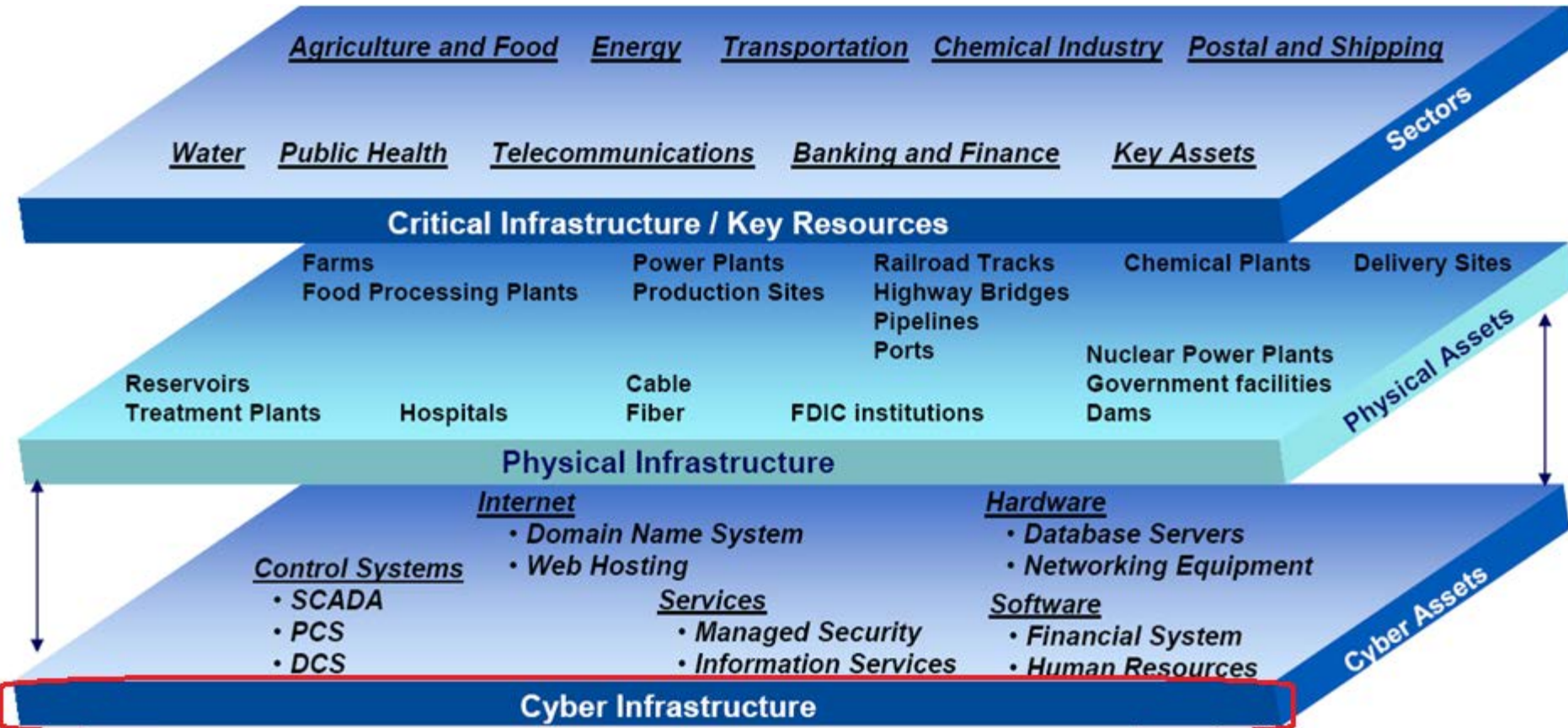
Ekonominin ve devletin işlemesi için gerekli olan fiziksel ve **siber** sistemler.

Kritik altyapılar kamu ve özel sektör tarafından işletilen iletişim, enerji, finans, ulaşım, su sistemleri, acil durum servislerini kapsar ancak bu sistemlerle de sınırlı olmayabilir.

Geçmişte kritik altyapılar fiziksel ve mantıksal olarak ayrıldı. **Bilgi teknolojilerindeki** gelişmeler, kritik altyapıların **otomasyonunu**, birbirilerine olan **bağımlılıklarını** ve **ilişkilerini** gün geçtikçe artırmaktadır.



# Siber Altyapı ve Kritik Altyapılar



## BT'yi kullanan kritik altyapılar:

- Ulaşım
- Bankacılık ve finans
- Sağlık ve acil durum servisleri
- Kritik kamu servisleri

## Tamamen BT'den oluşan kritik altyapılar:

- Telekomünikasyon

## SCADA ile kontrol edilen ve izlenen kritik altyapılar:

- Kritik üretim tesisleri
- Enerji ve su

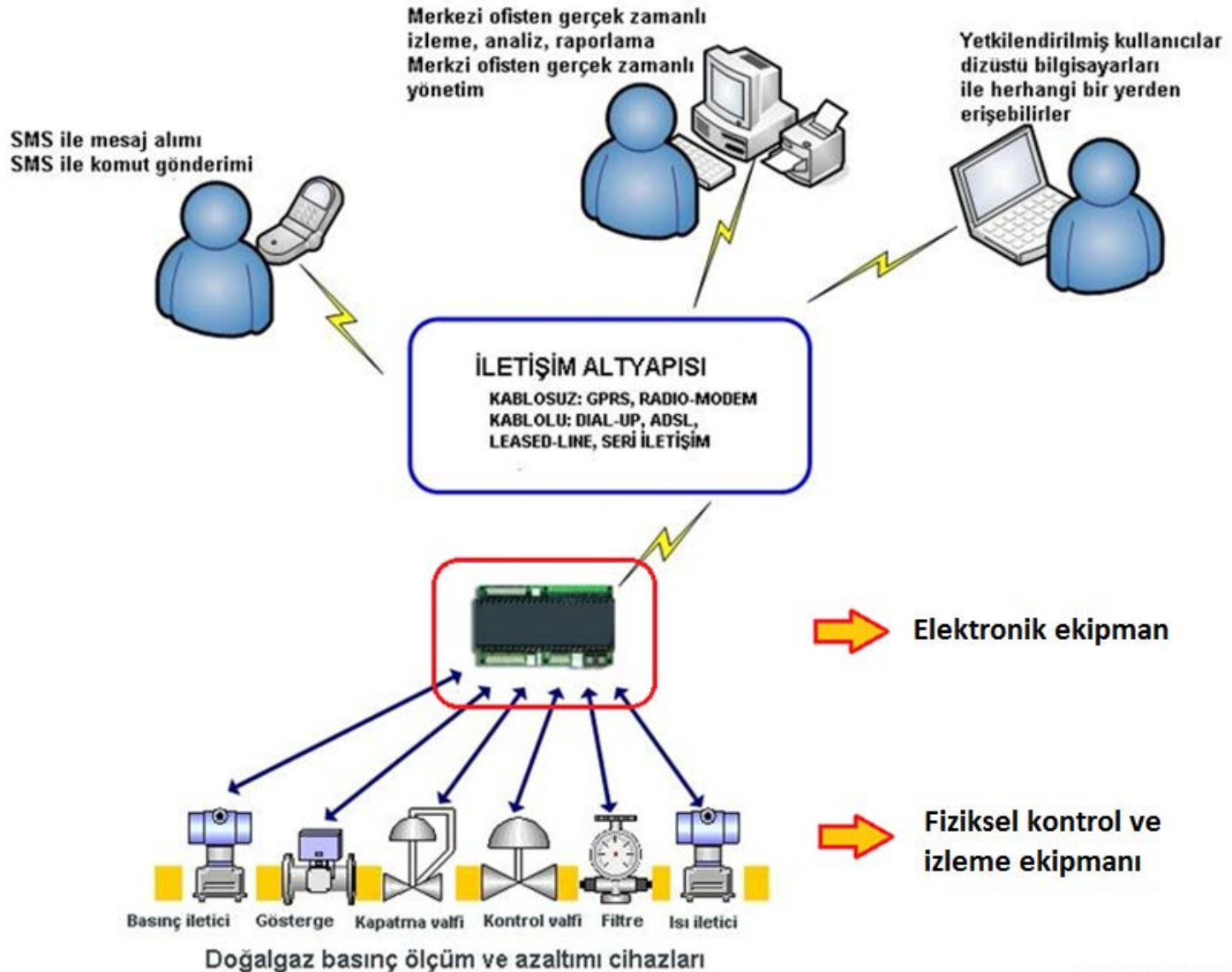
## Endüstriyel sistemlerin izlenmesi ve kontrolü:

- Barajlar
- Sulama sistemleri
- Elektrik üretim ve dağıtım sistemleri
- Petrol rafinerileri
- Gaz iletim sistemleri
- Fabrikalar

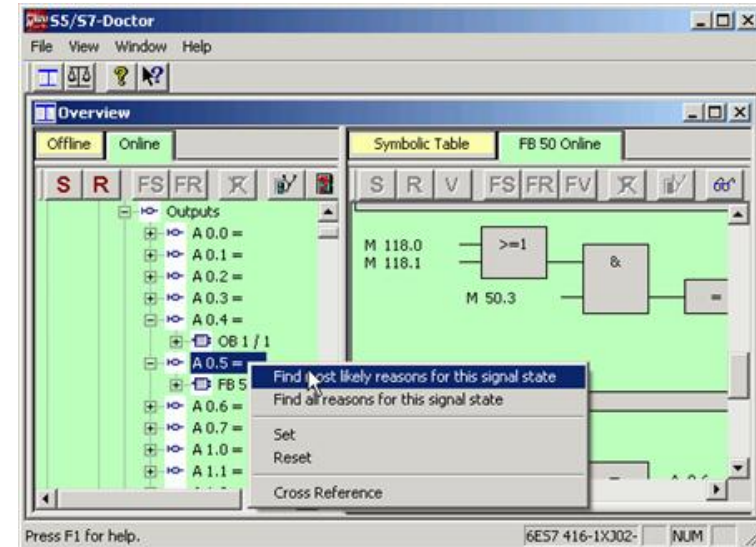




## DOĞALGAZ DAĞITIM ŞEBEKESİ İZLEME VE KONTROL SİSTEMİ

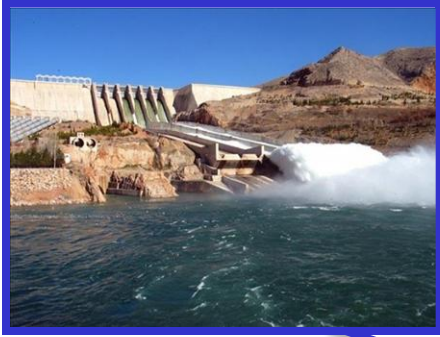


- 1970 - 1990
  - Özelleşmiş
  - İzole
- Bugün
  - Standart donanım
  - Standart işletim sistemi
  - Standart protokol
  - Dokümante
  - Bağlantılı
    - Kablosuz
    - İnternet
  - Ethernet, TCP/IP, Windows, RPC, SMB, 802.11b, HTTP/HTTPS, Unix/Linux/Solaris, SQL









**INTERNET = Siber Uzay**

Fiziksel olarak dağıtık ...

Mantıksal olarak tek ...







## Dijital savaş çağı

**Bir ülkenin başta su ve elektrik şebekesi olmak üzere kritik altyapı sistemini bilgisayar ağları üzerinden vuran sanal saldırıların ciddiyeti artıyor. Hükümetler büyük mali kayba yol açan saldırılara karşı önlem arıyor.**

Bir ülkenin başta su ve elektrik şebekesi olmak üzere kritik altyapı sistemini bilgisayar ağları üzerinden vuran sanal saldırıların ciddiyeti artıyor. Hükümetler büyük mali kayba yol açan saldırılara karşı önlem arıyor.

Siber savaş, sanal saldırı ve dijital muharebe... Bunlar, [İnternet](#)'in hızlı

gelişimiyle birlikte son yıllarda giderek daha fazla işittiğimiz kavramlar. Tanımlamak gerekirse; ekonomik, politik veya askeri amaçlar için bir ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırıların tamamına siber savaş adı veriliyor. Bu saldırılarda bir ülke açısından son derece kritik altyapı tesisleri hedef alındığından hükümetler de bu konuya artık daha fazla ağırlık veriyor.

Güvenlik uzmanı Kevin Coleman, sanal saldırı yöntemlerini tatbik etmeyen ülkenin kalmadığını belirtiyor. Coleman'a göre [İnternet](#) ağına bağlı olmayan az sayıdaki ülke dışında hemen bütün dünyada bu yönetime başvuruluyor:

"Sanal dünyada her an milyonlarca saldırı düzenleniyor. Bir ay içinde Çin'den dakikada 128 adet sanal saldırı girişi kaydedildi. Bu saldırılar, askeri birimlerin dışında, kamu ve özel sektöre ait kuruluşları hedef alıyordu. Mali ve ekonomik alanın dışındaki saldırıları da hesaba katarsanız karşınıza muazzam büyüklükte bir sorun çıkıyor."



## İlk siber savaşın galibi 'Kızıl Ordu'

Geçtiğimiz ay sessiz sedasız ve yöntem olarak benzersiz bir savaş yaşandı. Rusya, Estonya'ya organize bir saldırı düzenledi ve ülkenin ticaret ve kamu düzenini dize getirmeyi başardı

04/06/2007 (6756 defa okundu)

1918 yılında Alman ordularına yenilen Rusya'dan bağımsızlığını ilan eden Estonya, aynı Almanya'nın Rusya ile yaptığı gizli bir anlaşmanın ardından 1940 yılında Rus askerlerinin işgaliyle başlayan süreçte Sovyet Sosyalist Cumhuriyetler Birliği'nin bir üyesi olmak zorunda kalmıştı. 1989'da şarkılarla başlayan kıpırdanmanın ardından 1991 yılında sonunda Estonya yeniden bağımsızlığını kazandı. Ancak bu yeni süreçte Rusya'nın Estonya üstündeki hâkimiyet arzusunun söndüğü de söylenemez. Bunun son örneklerinden biri de geçtiğimiz günlerde internette yaşandı.



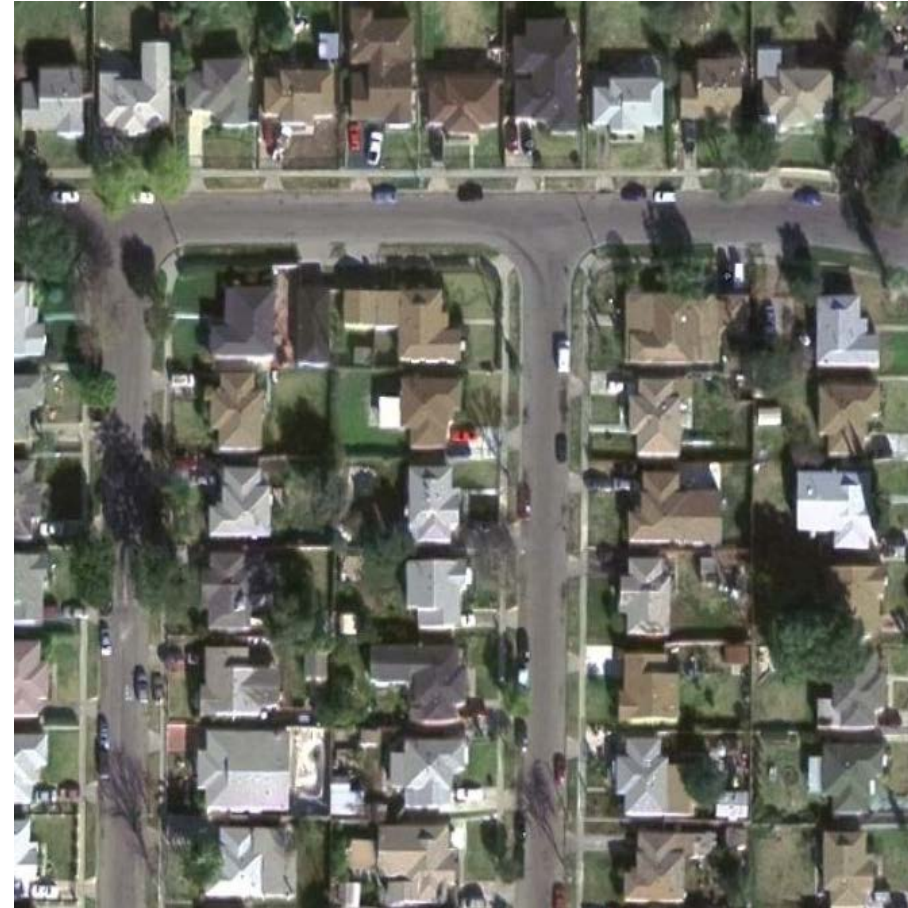
Tanklar eşliğinde yeri göğü inleterek bir ülkeyi dize getirmek hâlâ mümkün. Ama artık başka yollar da var.



## Nükleer Silah Tesisi



## Siber Silah Tesisi





Uçak maliyeti:

100.000.000 dolar



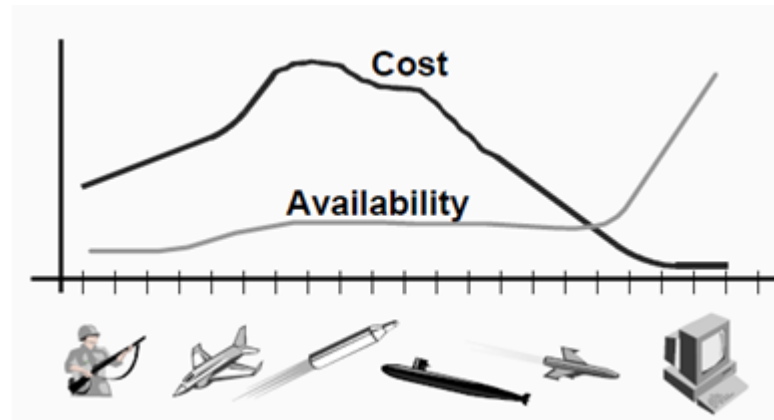
Kruz füzesi maliyeti:

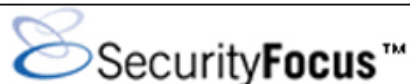
1.000.000 dolar



Siber silah maliyeti:

10 – 50,000 dolar





19 August 2003

## Slammer worm crashed Ohio nuke plant network

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

The breach did not pose a safety hazard. The troubled plant had been offline since February, 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common, and is permitted by federal safety regulations.



## Aussie hacker gets two year sentence

A Queensland court has sentenced a local computer hacker to two years jail. A Maroochydore District Court jury convicted Vitek Boden of hacking into the computer-controlled sewerage system of the local council and deliberately releasing raw sewerage into local creeks and parks.

He was sentenced for 12 months for wilfully causing serious environmental harm, and also received a two year sentence for several computer hacking and theft charges.

The sentences will be served concurrently.

31 October 2001

Los Angeles Times

13 August 2001

## Power Grid Vulnerable to Hackers

For two weeks last spring, hackers wormed their way inside a computer system that plays a key role in moving electrical power where it is needed around the state. The computers belong to the California Independent Service Operator, an agency that oversees much of the state's electricity transmission grid—including the massive complex of power plants and transmission lines.

Cal-ISO patched the flaw that allowed hackers to roam through portions of its network before power supplies were affected. But the episode sent shock waves throughout the energy industry.



## Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes

Technology reporter, BBC News



23 September 2010 Last updated at 10:46 GMT

**One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.**

Stuxnet's complexity suggests it could only have been written by a "nation state", some researchers have claimed.

It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

It was first detected in June and has been intensely studied ever since.



Some have speculated the intended target was Iran's nuclear power plant

## Stuxnet Worm Still Out of Control at Iran's Nuclear Sites, Experts Say

By Ed Barnes

Published December 09, 2010 | FoxNews.com



Iran International Photo Agency, via AFP

Aug 21: The first fuel is loaded into the reactor building at the Russian-built Bushehr nuclear power plant in Iran.

**EXCLUSIVE:** Iran's nuclear program is still in chaos despite its leaders' adamant claim that they have contained the computer worm that attacked their facilities, cybersecurity experts in the United States and Europe say.

The American and European experts say their security websites, which deal with the computer worm known as Stuxnet, continue to be swamped with traffic from Tehran and other places in the

Islamic Republic, an indication that the worm continues to infect the computers at Iran's two nuclear sites.

The Stuxnet worm, named after initials found in its code, is the most sophisticated cyberweapon ever created. Examination of the worm shows it was a cybermissile designed to penetrate advanced security systems. It was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran's uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bashehr.

Stuxnet was designed to take over the control systems and evade detection, and it apparently was very successful. Last week President Mahmoud Ahmadinejad, after months of denials, admitted that the worm had penetrated Iran's nuclear sites, but he said it was detected and controlled.

- Sadece belli SCADA sistemlerini hedef alan bir solucandır. (Siemens SCADA sistemi)
- Windows işletim sisteminin dört adet bilinmeyen açıklığını kullanmıştır.
- Kötücül yazılımların programlanmasında yaygın olarak kullanılmayan bir programlama dili kullanılmıştır.
- Güney Kore'deki iki adet firmaya ait sayısal sertifikaların gizli anahtarları ile imzalanmıştır.
- Siemens'in ilgili yazılımı yok ise kendisini etkisiz hale getirmektedir.



## HABER TÜRK

### Atatürk Havalimanı'nda virüs kabusu

Bilet ve bagaj işlemleri aksadı!



TÜBİTAK'ın uyardığı "downadup" adındaki "networm" virüsü Atatürk Havalimanı Dış Hatlar Terminali'ndeki sistemleri de etkiledi. Bilet ve bagaj işlemlerinin yapıldığı SITA-CUTE sistemleri bozulunca işlemler elle yapıldı.

Birçok yolcunun bagajları havalimanında kaldı. TAV, virüs nedeniyle sistem problemi yaşandığını doğruladı.

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde faaliyet gösteren Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME), bilgi sistemlerinde hızla yayılan yeni bir solucanı "acil" koduyla bildirdi.





## Batman Barajı şifrelendi

28.5.2003

**Alman firması, parasını alamadığı gerekçesiyle bilgisayarları kilitledi**

Bilgisayarların şifrelenerek kilitlenmesi nedeniyle Batman Barajı'nda enerji üretimi yapılamadığını söyleyen DSI yetkilileri, bu nedenle Batman'ın bazı ilçeleri ile Şırnak ve Cizre'ye kesintili olarak elektrik verebildiklerini belirttiler. Barajın yeniden elektrik üretimine başlaması için şifreyi çözmek üzere Türkiye Elektromekanik Sanayi uzmanları da yoğun çalışmalarını sürdürüyor. Uzmanlar bir yandan şifreyi çözmeye, bir yandan da Alman firması yetkililerine ulaşmaya çalışıyor. Batman Barajı Hidroelektrik Santralі'nin yapımını üstlenen Alman Noel Şirketi, 1 milyon dolar alacağını tahsil edemediğı gerekçesiyle şirketin bilgisayarlarını şifre ile kilitleyip, kenti terketti. Şifreleme nedeniyle santralin üç ünitesinde de enerji üretimi durdu.





## 260 milyar dolarlık borsa bir kepçe darbesiyle çöktü

Yol çalışmasında bir kepçe veri kablolarını kopardı. Borsa idaresi hasardan işlem saati yaklaşırken haberdar oldu. Taşeron tamircileri grevdeki sendika durdurdu

29 Kasım 2007





Gönen HES gerek mimari gerekse ergonomik kullanım yönünden Türkiye' deki santralle içinde en modern olarak inşa edilmiş Bölgemizin ilk Hidroelektrik Santralidir. Yap - İşlet - Devret Modeli ile kurulup üretime geçen ilk Hidroelektrik Santrali olan Gönen HES manuel olarak kumanda edilebildiği gibi PLC sistemi ile yarı otomatik olarak veya SCADA sistemi ile kontrol odasından tam otomatik olarak veya uzaktan (başka bir şehirden) kumanda edilerek, bilgisayarla insansız çalıştırılabilen ilk santral olma özelliğini de taşımaktadır.

- En gelişmiş güvenlik sistemleri:
  - Sayısal imzalar
  - Kriptografik önlemler
  - Biometrik güvenlik
  - Güvenlik duvarları
  - Saldırı engelleme sistemleri
  - Erişim kontrol sistemleri
  - İnternet erişimine kapalı ağ !!!
- **En zayıf halka: İnsan**
  - **USB bellekler !!!**



USB thumb drives are convenient, popular and often free--and they're spreading viruses like sailors on shore leave.\*

The US-CERT (Computer Emergency Response Team) issued a warning on Thursday that malicious code is increasingly propagating via USB flash drive devices.

Meanwhile, the U.S. Department of Defense has temporarily banned the use of thumb drives, CDs, and other removable storage devices because of the spread of the Agent.bzt virus, a variant of the SillyFDC worm, according to Wired.

We've seen this before with portable external storage devices. Floppy disks were the culprit in the early 1990s, followed by CDs. The fact that USB thumb drives are being used by so many people makes them an attractive target for virus writers.

"The bad guys are intentionally developing new flavors of malware designed to propagate through USB devices," said Gunter Ollmann, chief security strategist for IBM's ISS security division. "They are today's floppy drives."

# WIRED

## Under Worm Assault, Military Bans Disks, USB Drives

By Noah Shachtman  November 19, 2008 | 3:12 pm | Categories: [Info War](#)

The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.

The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret [SIPR](#) and unclassified [NIPR](#) nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services.



- İlk üçte yer alan kritik karşı önlemler:
  1. Kullanıcı bilinci
  2. Kullanıcı bilinci
  3. Kullanıcı bilinci

(Kullanıcı = bilgisayar operatörü, sistem yöneticisi, kurum yöneticisi = herkes)

- Eğitim (Ne?)
- Kurs (Nasıl?)
- Bilinçlendirme (Niçin?)



1. Üst seviye yürütmeden (Örn: Başbakanlık) destek ve katılım
2. Destekleyen mevzuatın hazırlanması ve yürürlüğe girmesi
3. Kritik altyapıların korunması ile ilgili politika belgesi hazırlanması
4. Çalışmalar için yeterli seviyede bütçe ayrılması

- Kritik altyapılarla ilgili çalışmalarını koordine eden merkezin kurulması
- Hükümet birimleri ve kritik altyapı işletmecileri (özel, kamu) arasında ilişkilerin kurulması
- Özel sektör ile işbirliği ve koordinasyon
- Diğer ülkeler ve uluslararası organizasyonlarla işbirliği

- Güncel kalma
  - Açıklıkların yamalarının yapılması
  - Son teknoloji karşı önlemlerin tedariki ve kurulması
- Güvenlik ve teknoloji tasarımı
  - Güvenliğin bir tasarım konusu olması, sonradan ek yapılmaması
  - COTS ürünlerin kullanımının kısıtlanması
  - Sertifikalı yazılım ve donanım kullanımı
  - Erişim kontrol sistemlerinin kullanımı
- USB belleklerin kullanımının kısıtlanması !

- Internet bağlantısı
  - Gerçekten gerekli mi?
- Periyodik güvenlik testleri ve denetimleri
- Aktif siber güvenlik takımları
  - Siber istihbarat ve önleyici faaliyetler
  - Aktif bilgisayar olaylarına müdahale takımı
- Araştırma ve geliştirme faaliyetlerini desteklenmesi

- SCADA'ya yönelik siber ataklar devam edecek:
  - Stuxnet sadece bir başlangıçtı (bildiğimiz kadarıyla)
- Hükümetler tarafından desteklenen siber ataklar
- Kiralık siber uzmanlar
- Gönüllü siber gruplar (örn: *Anonymous* hacker grubu)





## TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

[bilge@uekae.tubitak.gov.tr](mailto:bilge@uekae.tubitak.gov.tr)

0 312 427 73 66

[www.bilgem.tubitak.gov.tr](http://www.bilgem.tubitak.gov.tr)

[www.bilgiguvenligi.gov.tr](http://www.bilgiguvenligi.gov.tr)

[www.bilgimikoruyorum.org.tr](http://www.bilgimikoruyorum.org.tr)



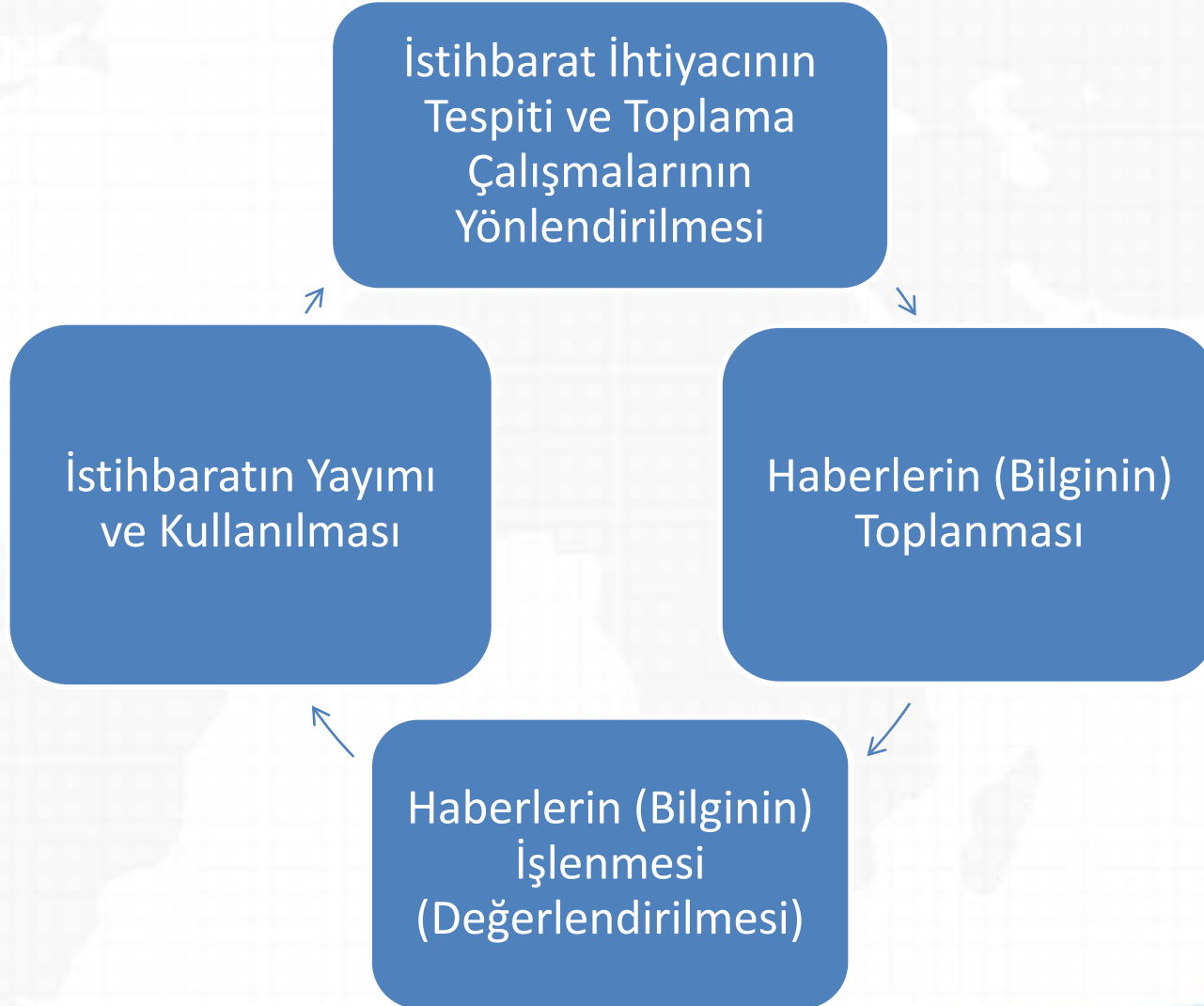
**AÇIK KAYNAK İSTİHBARAT ve  
SİBER GÜVENLİK**  
İlkay ÜNAL

- ▶ İstihbarat Tanımı
- ▶ Açık Kaynak İstihbarat
- ▶ Açık Kaynaklar ve Güvenlik İkilemi
- ▶ Güvenlik ve Mahremiyet
- ▶ Bilgi Casusluğu ve Siber Güvenlik
- ▶ Alınabilecek Önlemler
- ▶ Sonuç

► İstihbarat:

- Haber alma
- Devlet tarafından belirlenen ihtiyaçlara karşılık olarak açık ya da kapalı kaynaklardan derlenen haber, bilgi ve dokümanların sürekli bir şekilde işleme tabi tutulması sonucu elde edilen üründür.







## ► İstihbarat Kaynakları:

- Kapalı kaynaklar: Yetkili kurumların sorumluluğunda
- Açık kaynaklar: Herkes tarafından erişilebilir



► Açık kaynak istihbarat:

- Topluma açık kaynaklardan bilgilerin bulunması, seçilmesi ve toplanması suretiyle bilginin yönetilmesi ve analiz edilerek istihbarat üretilmesidir.



- Uzmanlar, yararlı olduğunu ve bu tür bilgilerin gizli kaynaklardan elde edilen veriler gibi toplanması ve analiz edilmesi gerektiğini kabul ederler.



- ▶ Bilgi devriminin başlangıcından bu yana, özellikle kamu bilgilerine açık kaynaklarda erişim oldukça kolaylaşmıştır.
  - ▶ Rusya'da Soğuk Savaş sonrasında açık bilginin gizli bilgiye oranının 20:80 değerinden 80:20 olarak değiştiği tahmin edilmektedir.
- ▶ Devlet kurumlarının açık kaynaklara bakış açısı sonuç olarak değişmiştir.



## ► Neden açık kaynak?

- Sürekli değişen bilgiye hızlı şekilde ulaşma imkanı
- Gizli bilgilerin anlaşılmasına temel oluşturması
- Kaynak ve yöntemlerin savunulabilir olması
- Bir tarihçeye sahip olması





- ▶ Açık kaynakların gruplandırılması:
  - ▶ Yaygın olarak bulunabilen veri ve bilgi
  - ▶ Hedeflenen ticari veri
  - ▶ Bireysel uzmanlar
  - ▶ “Gri” kaynak; özel sektör, devlet kurumları veya akademik kurumlar tarafından sınırlı sayıda kopyası üretilen, ulaşımı kısıtlı kaynaklar



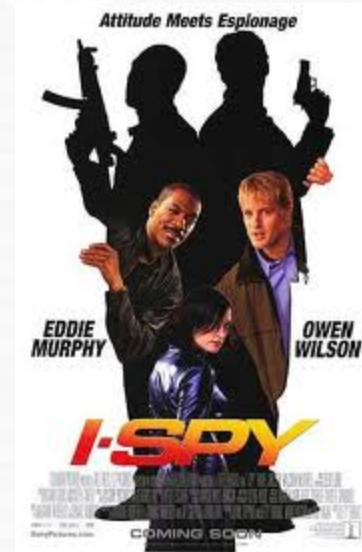
## ► Açık kaynaklara örnekler:

- Medya
- İnternet
- Kamusal veriler
- Gözlem ve raporlama
- Gri edebiyat
- Meslek örgütleri ve akademi



## ► Kullanıcılar:

- Hükümet
- İstihbarat servisleri
- Askeri
- Kolluk kuvvetleri
- İş dünyası
- Diğer



- ▶ Güvenlik problemi
  - ▶ Google Earth uygulaması



## ► Google Earth uygulaması

- Hindistan'ın hassas noktaların sergilenmesi
  - Hindistan'daki hassas noktaları sergileyen uygulamanın, ülke güvenliğini tehdit ettiği ifade edildi.
- Güney Kore'nin itirazı
  - Hükümet, başkanlık sarayı ve kritik askeri tesisler gibi yerlerin görüntülerinin rahatsızlık verdiğini belirtti.



## ➤ İsrail'in rahatsızlığı

- İsrail'in savunma güçlerini, gizli hava üslerini, Arrow hava savunma sistemlerini, Tel Aviv'deki Savunma Bakanlığına ait yerleşkeleri, Aşkelon'daki enerji tesislerini, Negev çölündeki nükleer tesisleri gösteren yüksek çözünürlüklü görüntüleri yayınlamaya başladı.

## ➤ Avustralya'daki nükleer tesisler

- Sydney yakınlarında bulunan Lucas Heights nükleer reaktörünün işletmecileri, Google yetkililerinden tesise ait görüntülerin çözünürlüğünün düşürülmesini talep ettiler

- Gazze'den yapılan roket saldırıları
  - ▶ Gazze'den gerçekleştirdikleri roket saldırılarında Google Earth görüntülerinden faydalandıkları raporlandı.
- İngiltere'deki kilise hırsızlıkları
  - ▶ İngiltere'de hırsızların Church of England kilisenin kurşun tavanını Google Earth ile tespit edip çaldıkları ve sattıkları ortaya çıktı.

- ▶ Açık kaynaklar güvenlik sorununun yanında kişilerin mahremiyetine tehdit oluşturmaktadır.
- ▶ Google Earth Streetview uygulaması
- ▶ Facebook ve benzeri paylaşım siteleri



## ► Olası tehditler

- Kimlik hırsızlığı
- Hakaret
- Reklamveren endişesi
- Soykırım inkarı
- Örgütlenme



## ► Siber güvenlik:

- Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür.



## ► Siber güvenlik:

- Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

## ► Siber güvenlik:

- Kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır.
- Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizlilik.

- ▶ Günlük işlerimizin bir çođu siber ortamda yürütölmektedir.
- ▶ İyi korunmayan bilgiler, istenmeyen kişilerin eline geçebilir:
  - ▶ Wikileaks
  - ▶ Estonya'ya yapılan saldırılar
  - ▶ Kişisel bilgilerin çalınması
  - ▶ Kurumsal bilgilerin çalınması

## ► TÜBİTAK - Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)

- Bilinçlenmenin sağlanması
- Bilgisayar Olayları Müdahale Ekibi
- Tedbirlerin belirlenmesi
- Kamu kurumlarını hedef alan tehditlerin tespit edilmesi  
→ **Siber Güvenlik Tatbikatı**

- ▶ Kurumların siber güvenlik konusunda bilinçlenmesi, kurumsal önlemleri alması
- ▶ Kişilerin bilinçlenmesi, gizlilik konusunda gerekli önlemleri alması
- ▶ Uygulama geliştiricilerin konuya özen göstermesi (Google Earth, Facebook gibi)



- ▶ Açık kaynak istihbarat, herkes tarafından kullanılmaktadır.
- ▶ İnternet, günlük hayatımızın vazgeçilmezlerindendir.



- Siber güvenlik konusunda bilinçlenmenin sağlanması kritiktir öneme sahiptir.
- Gerekli önlemlerin önce kişilerden başlayıp kurumlar düzeyinde gerçekleştirilmesi gerekmektedir.



**Teşekkürler**

**SORULAR???**



ANKARA TEKNOLOJİ GELİŞTİRME BÖLGESİ,  
BİLKENT CYBERPARK, E BLOK 5.CADDE NO: 6/A  
06800, ANKARA, TÜRKİYE

TEL : 0 312 266 35 50 FAKS : 0 312 266 35 51

[www.stm.com.tr](http://www.stm.com.tr)

© STM 2011  
All Rights Reserved

Bu doküman ve içerdiği tüm bilgiler STM AŞ'nin fikri mülkiyetidir. Bu dokümanın dağıtımı veya sunumu ile bu haklar ortadan kalkmış olmaz. STM AŞ'nin yazılı izni olmadan bu dokümanın ve içerdiği bilgilerin üçüncü kişilere aktarımı, çoğaltımı ve dağıtımı yapılamaz. Bu doküman ve içeriği hazırlanma amacının dışında kullanılamaz.

This document and all information contained herein is the sole property of STM AŞ. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of STM AŞ. This document and its content shall not be used for any other purpose other than for which it is supplied.

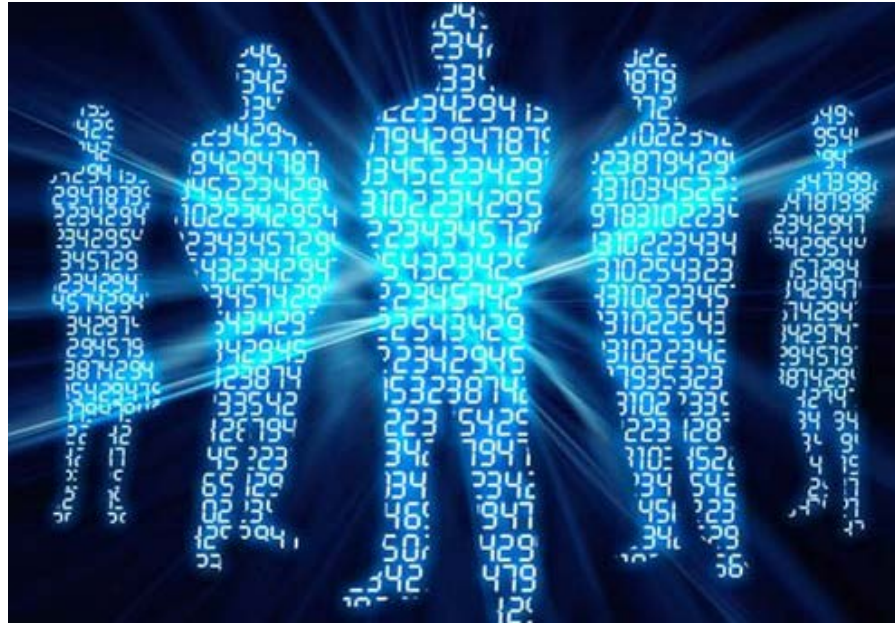
# SİBER GÜVENLİK & YEREL AĞ GÜVENLİĞİ

A.Uğur Duman - TAI

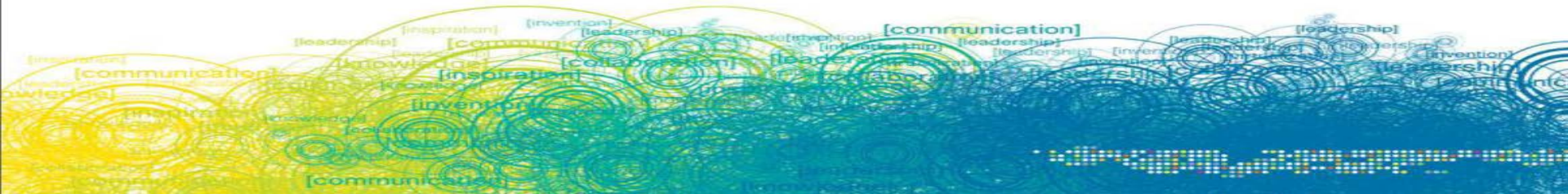




# SİBER GÜVENLİK



Günümüzde hemen her türlü sistemin BT teknolojileri üzerinden yönetilmesi sonucunda bu sistemler bir yandan hayatımızı kolaylaştırmakta ancak kontrollerini sağladıkları sistemlerin kesintiye uğramasının ya da hatalı çalışmasının çok büyük etki yaratacak bir gücünün olması sebebiyle de kaçınılmaz olarak birer hedef durumuna gelmektedirler.



BT sistemlerine yapılan saldırıların yoğunluk, saldırı tipleri, amaçları ve nedenleriyle çok fazla çeşitlik kazandığı günümüzde, organize bir şekilde düzenlenen ve adına “**Siber Savaşlar**” denilen uluslararası çapta büyük saldırılar dönemi yaşanmaktadır.

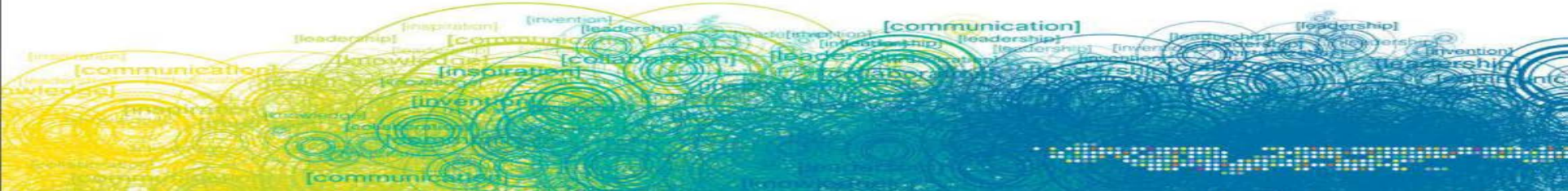




Ülkelerin ticari, ekonomik, sivil ve askeri sistemlerinin kontrolleri büyük ölçüde dijital ortam üzerinde olması nedeniyle bu siber saldırılara karşı güvenlik önlemleri geliştirme ihtiyacı her geçen gün artmaktadır.

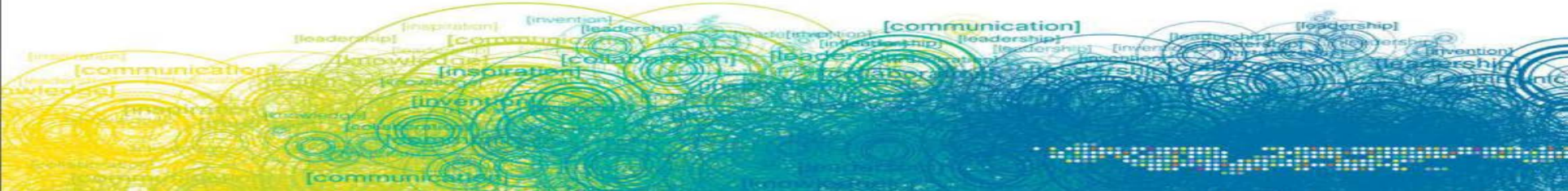
Siber Saldırıların sebepleri incelendiğinde;

- bir devlete, kuruma, ya da çeşitli güç merkezlerine tepki göstermek ,
- bilgi casusluğu yaparak çıkar sağlamak ,
- güç gösterisi yaparak sesini duyurmak,
- hedef bir kitlenin çalışmalarını engellemek  
gibi sebeplerle yapılmakta olduğu gözlenmektedir.



Söz konusu siber saldırılara karşı alınması gereken önlemler ve çözümler “**Siber Güvenlik**” kavramı olarak karşımıza çıkmaktadır.

Siber Saldırılarına karşı ne tür güvenlik önlemlerinin alınabileceğini incelediğimizde ise konunun çok yönlü yapısı sebebiyle bilgi güvenliği ve ağ güvenliği kavramlarının bir arada ele alınması gerektiği ortaya çıkmaktadır.



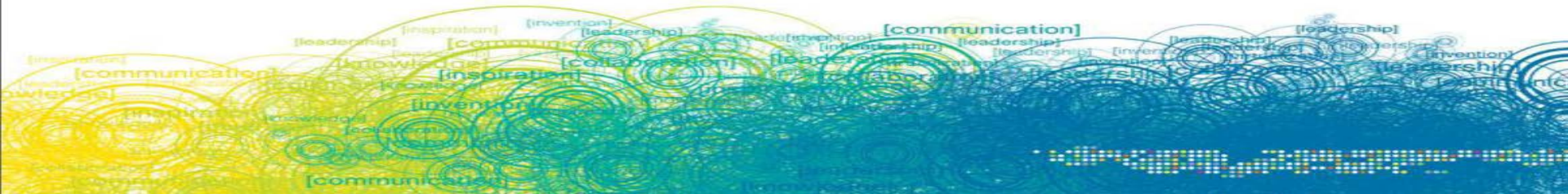


# AĞ GÜVENLİĞİ RİSK DEĞERLENDİRMESİ

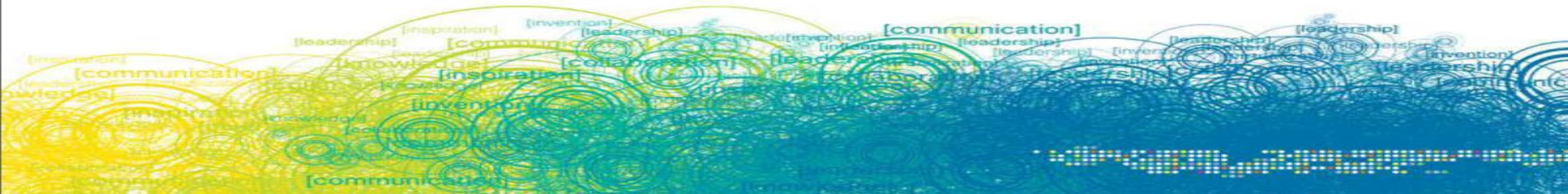


Ağ güvenliği kavramından bahsedilirken genel eğilim İnternet üzerinden gelen saldırı ve tehditlere göre önlemler almaktan yanadır.

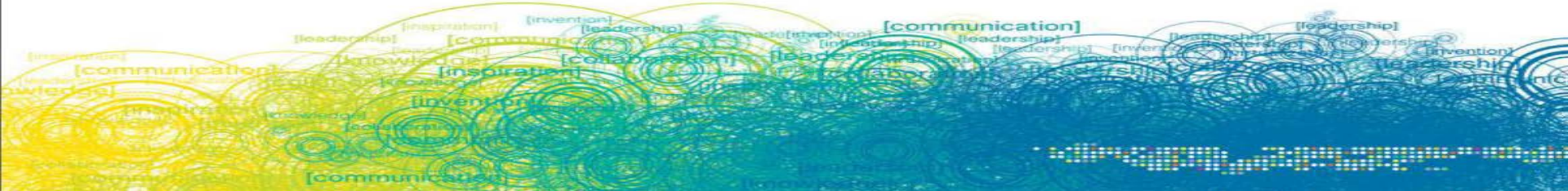
İnternet üzerinde açık kaynaklara ulaşılabilirliğin bir yerel ağa ulaşmaya nazaran çok daha kolay olması nedeniyle “**Siber Saldırılar**” yoğun olarak İnternet’e açık kaynaklara yapılmakta ve ağ güvenliği söz konusu olduğunda genellikle bu tür dış saldırılara karşı önlemler alınmasına öncelik verilmektedir.



Ancak ađ gvenliđi konusuna yaklařırken internet'e ađık kaynakları korumak ve dıřarıdan gelecek tehditlere karřı nlem almak yanında yerel ađ zerinden gelebilecek saldırılara karřı korumanın da zenle planlanması gerekmektedir.

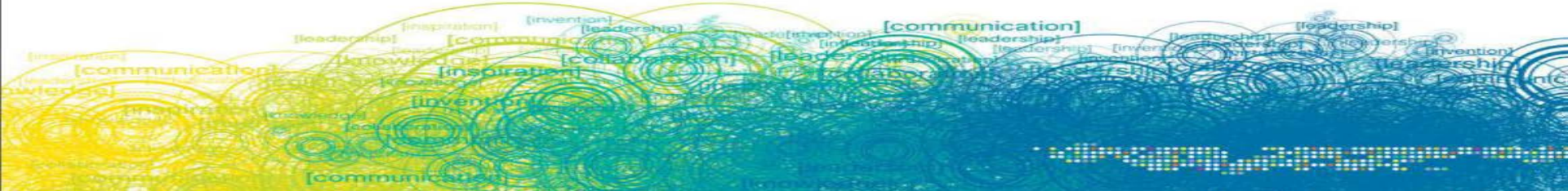
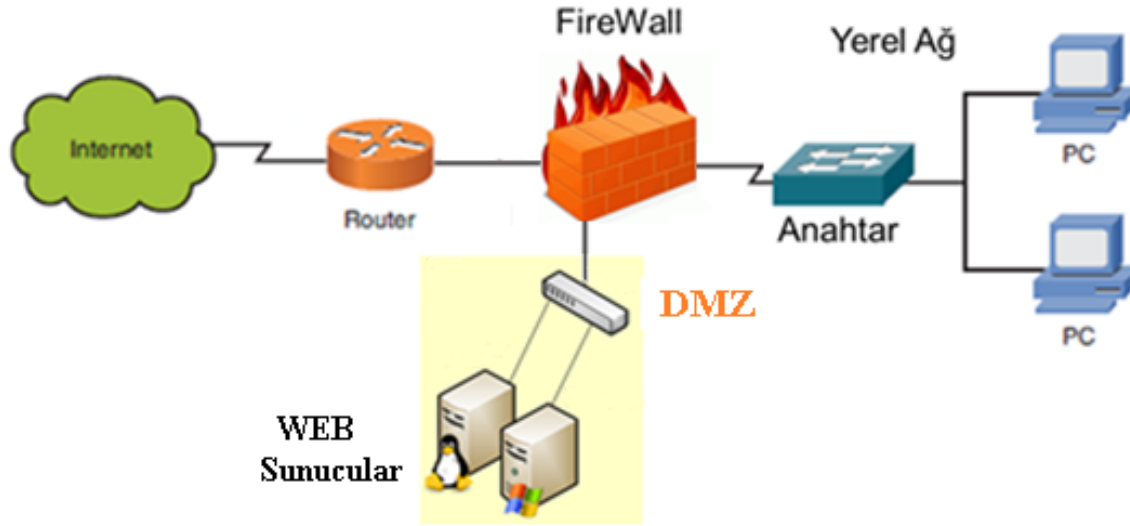


2009 yılında Microsoft firması tarafından yapılan bir araştırmaya göre saldırıların yaklaşık %40'lık bir oranının yerel ağ'dan gelen saldırılar olduğu sonucu ortaya çıkmıştır.



## Tipik Ağ Koruma yaklaşımı :

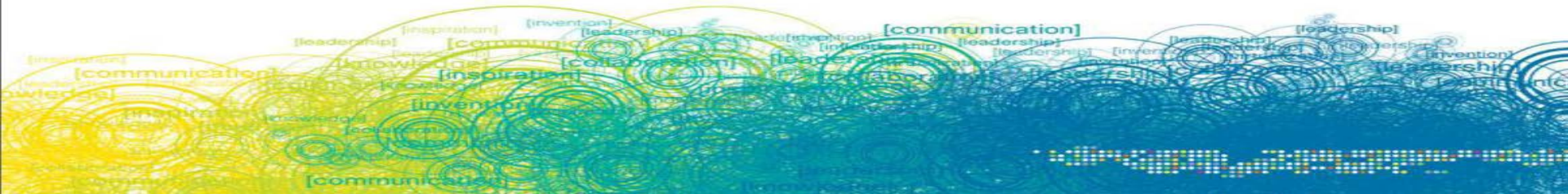
Yerel Ağ'ların güvenliği en genel anlamda dış dünyadan çeşitli güvenlik katmanlarıyla korunmaya alınarak dışarıya karşı izole etme yöntemleriyle çözülmeye çalışılmaktadır.





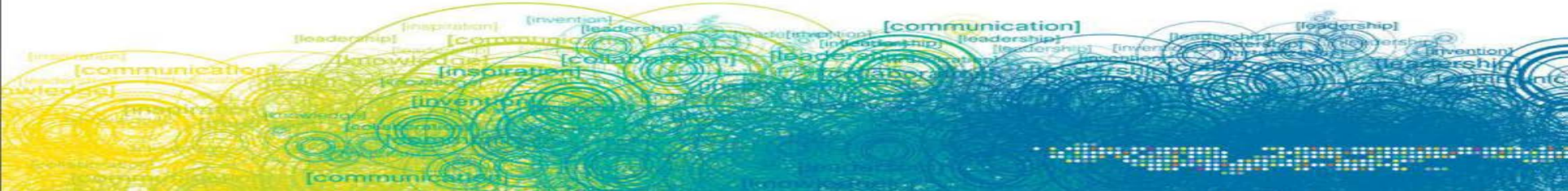


Bu risklere karşı gelen güvenlik gerekleri yerine getirilirken aynı zamanda kullanıcıların ihtiyaç ve beklentilerinin de karşılanması gereği bu konuda her sistem için kendine özgü en uygun çözümlere karar verilip bunların devreye alınmasını zorunlu kılmaktadır.



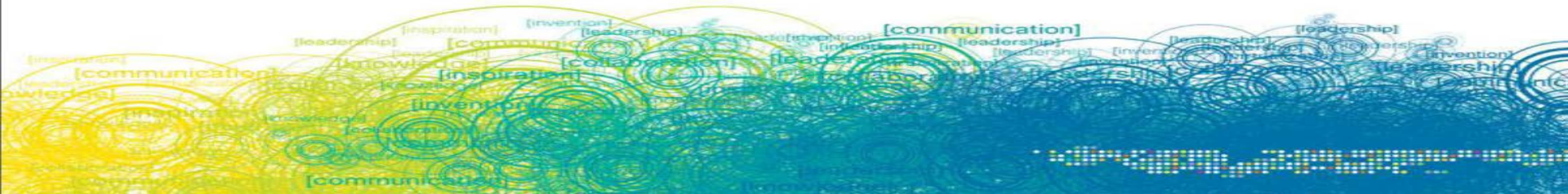
Sonuç olarak; yerel ağı koruma yöntemlerinde klasik izole yöntemlerine göre daha gelişmiş, bu konu üzerinde uzmanlaşmış “dinamik” sistemlere ve “akıllı” çözümlere ihtiyaç duyulmaktadır.

Bu yaklaşım “**Kontrollü Ağ Erişimi**” kavramını karşımıza çıkarmaktadır.



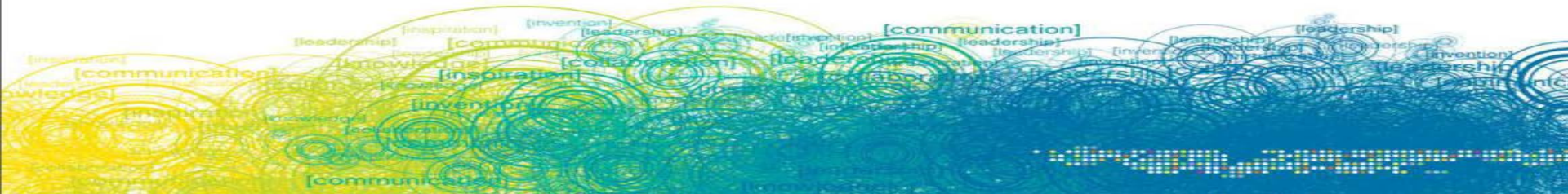


***Kontrollü Ağ Erişimi*** ya da BT dünyasında bilinen adıyla **NAC** (Network Access/Admission Control) genel anlamda bir ağa bağlanacak uç sistemleri kontrollü ve istenilen kural ve standartlara göre söz konusu ağa dahil etmek ve ağı gerçek zamanlı olarak denetim altında tutmak amacıyla kurulmuş bir alt yapı sistemi olarak tanımlanabilir.





*“Kontrollü Ağ Erişimi”* ile ağ kaynaklarına erişmek isteyen birbirinden çok farklı uç sistemlerin bu isteklerini değerlendirip, girişlerinin o ağ için belirlenmiş güvenlik politikalarına uygunluğunu belirlemek ve sakıncalı bulunan cihazları yada bilgisayarları ağa dahil etmeme işlemleri yapılabildiği gibi, bir yazılım eksikliğinden dolayı girişleri uygun bulunmayan uç sistemler için gerekli yönlendirmeler yapıp eksikliklerini tamamlaması ve gerekli düzeltmeler sonrası ağa alınması da sağlanabilmektedir.



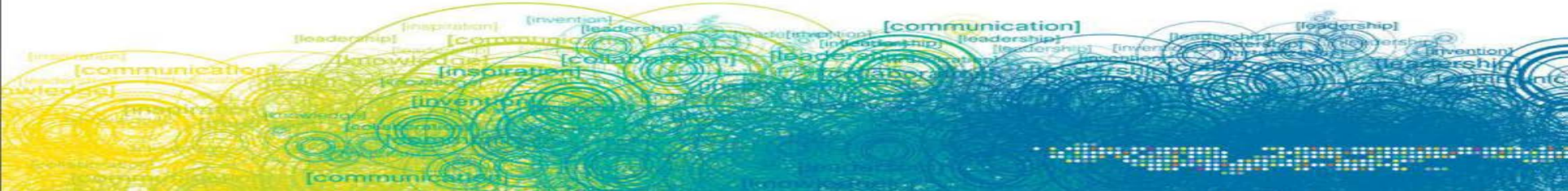
Bu sisteme göre örneğin bir yerel ağda bulunan son kullanıcılar çalışma ihtiyaçlarına göre aşağıdaki şekilde gösterildiği şekilde gruplandırılarak ve bu gruplamalara göre rol tanımlamaları yapılarak değişik seviyelerde yetkilendirilerek ağa dahil edilebilirler.

Rol Tanımları :



NAC genel anlamda; ađ yapısına dahil edilen tm cihaz ve bilgisayar'ların nceden belirlenmiř gvenlik standartlarına uygun olmasını sađlamak ve tm sistemin bu standartların dıřına çıkmadan alıřmasını garantilemek iin zmler sunan bir teknolojidir.

NAC hem yerel ađ zerinden hem de uzak lokasyonlardan ađ'a bađlanma isteđi olan u noktalar iin farklı zmleri olan ve her kurumun yerel ađ gvenliđi iin deđiřik seviyelerdeki ihtiyalarına uygun olarak řekillenebilen esnek bir zm olarak tasarlanmıřtır.







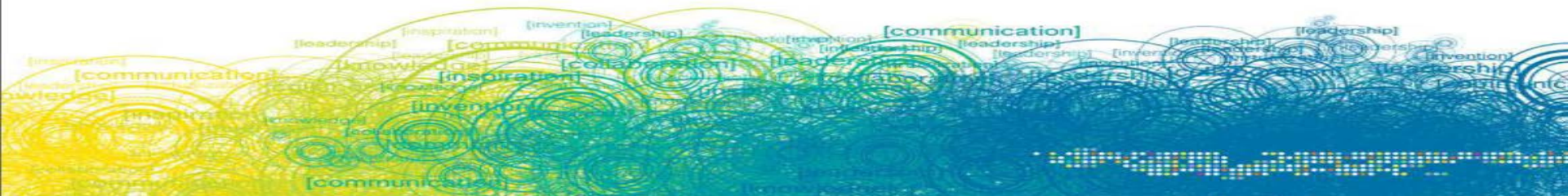
Yetkisiz veya ağı dahil olması sakıncalı bulunan bir uç sistem giriř yaptığında, ağı üzerinde bulunan bilgi kaynaklarının hem bütünlüğü hem de gizliliğı tehlikeye girer.

Örneğın; ağı dahil edilmiş kötü amaçlı bir misafir veya yetkisiz kullanıcı ağı trafiğini çeřitli programlarla dinleyerek ağı hakkında bilgi toplayabilir ve bu bilgileri kullanarak yetkisiz giriř denemeleri yapabilir, çeřitli yöntemlerle ağı trafiğini yanlış yönlendirebilir, çeřitli saldırı teknikleriyle sistemlerin çalışmalarını engelleyebilir yada kritik bilgileri, şifreleri ele geçirebilir.

Bu saldırı çeřitlerini aşığıdaki gibi genelleyebiliriz.

Hedef kaynaklarını ele geçirme → Haklama (Hacking)

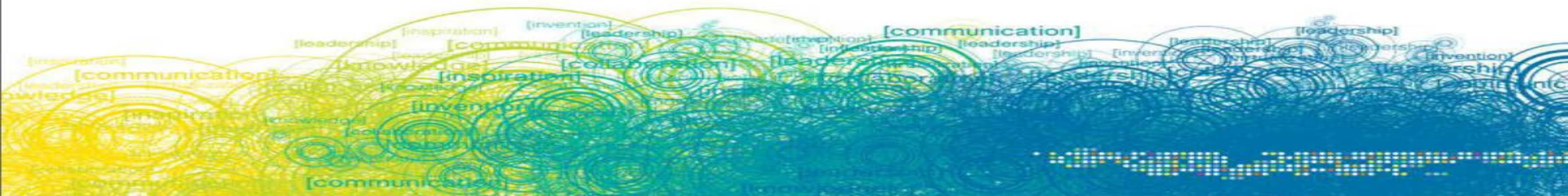
Hedefin çalışmasını engelleme → Ağı (Network) saldırıları





Öte yandan yetki açısından uygun bulunan kuruma ait bir bilgisayar'ın üzerinde AntiVirus/ AntiSpam/AntiMalware vb. gibi koruyucu program kurulumları olmadan ağa dahil edilmesi içeride potansiyel bir risk noktası oluşturur. Söz konusu bilgisayar Virus/Trojan gibi programlar aracılığıyla kullanıcısından bile habersiz şekilde ağ kaynaklarına saldırı noktası (örn: *Zombi PC*) haline getirilebilir.

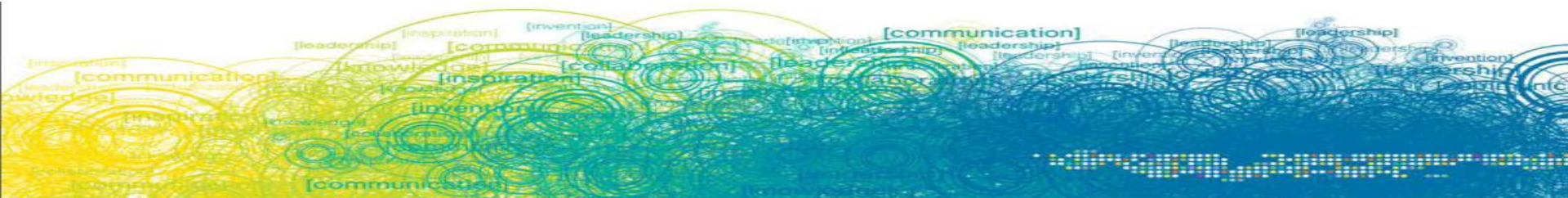
NAC çözümü bu tür istenmeyen durumları engellemek için kullanılabilen bir teknolojidir.



NAC uygulaması kablolu veya kablosuz yerel ağa, ağ içerisinde yada internet üzerinden herhangi bir uç sistemin bağlanması durumunda; ağda uygulanması istenen güvenlik politikalarına göre otomatik olarak bu kuralların işletilmesini sağlayabilir ve söz konusu uç sistem için gerekli görülen kontrolleri yaptıktan sonra ağa dahil edilip edilmeyeceğine karar vererek işlemi gerçekleştirebilir.

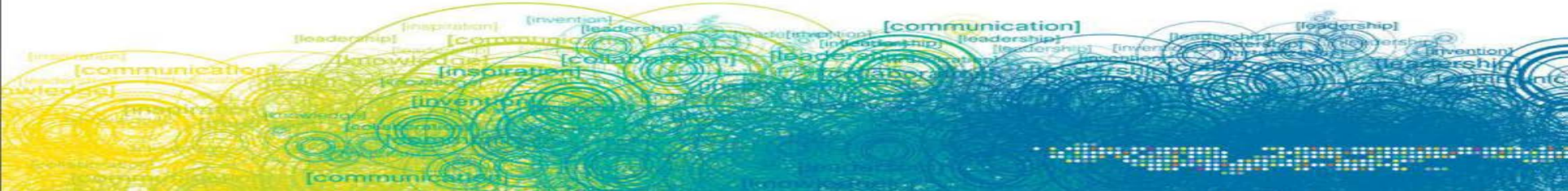


Yerel Ağ girmek isteyen bir uç kullanıcıyı karşılama görevini üstlenen NAC sistemleri bir ara katman oluşturarak, ağa giriş için yeterlilik kontrol işlemlerini yürütür.



Sonuç olarak NAC; bir yerel ağın belirlenmiş olan güvenlik standartlarına uygun çalışmasını sağlamasını garanti edebilen önemli bir seçenek olarak karşımıza çıkmaktadır.

En önemli avantajı hem internet üzerinden hem de yerel ağdan gelebilecek saldırılara karşı değişik çözümler ve önlemler sunabilmesi ve böylece “**Siber Güvenlik**” açısından önemli bir savunma politikası geliştirebilme olanağı sağlamasıdır.



# NAC UYGULAMALARININ GENEL MANTIĐI



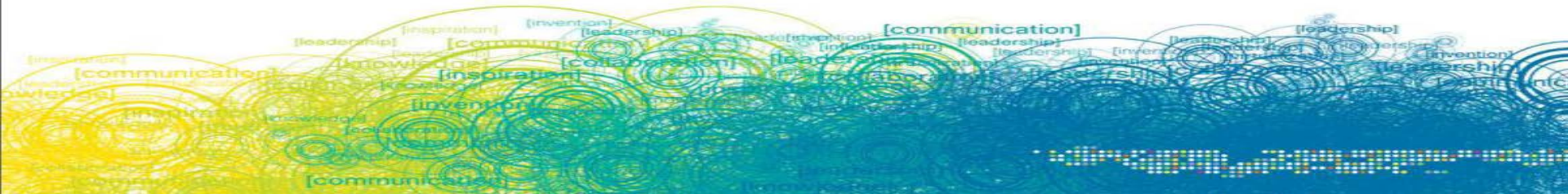


NAC uygulanılan bir ağa bağlanma girişiminde bulunan bir bilgisayar gerekli kontrolleri yapıp onaylanma aşamalarından geçinceye kadar ağ'da bulunan kaynaklara ulaşamazlar.



Bu durumu; iş yerine gelen ziyaretçileri önce bir bekleme odasına alma sonra uygun görülürse içeriye kabul etme gibi düşünebiliriz.

Bu bekleme odasında uç sistemler sadece kontrollü bir trafik sistemi aracılığıyla onay işlemleri için kendilerini tanıtmaya izin verecek düzeyde ve önceden belirlenmiş portlar üzerinden belirlenmiş noktalara kontrollü olarak kimlik bilgilerini gönderebilirler ve burada onay işlemlerinin sonuçlarını beklerler.





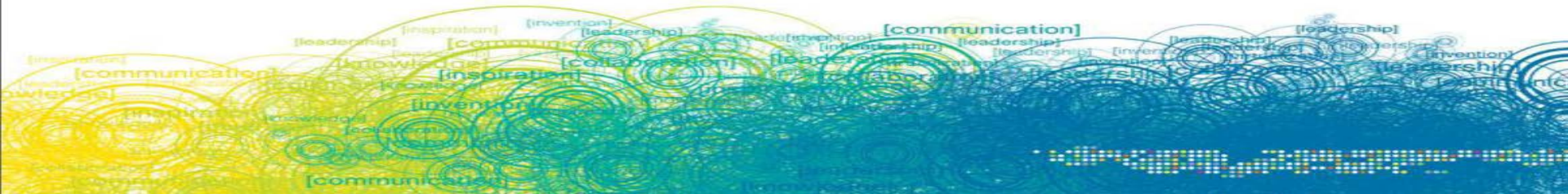
Örneğin; onay sistemi olarak AD Etki Alanı onayı (AD SSO) kontrolü kullanılıyorsa uç kullanıcılar; AD yöneticisi konumundaki DC sunucular ile izin verilmiş belirli portlar üzerinden haberleşebilir ve kendini tanıtmak için gereken login bilgilerini ağ içerisindeki bu DC sunucularına gönderebilirler.

Bu sırada DHCP, DNS gibi ağ hizmetleri veren sunucular ile izin verilmiş belirli port'lar üzerinden haberleşebilir, yerel ağa henüz dahil olmamalarına karşın yerel ağda hizmet veren DHCP sunucusundan IP alabilirler.



Onay işlemleri için gereken şartları sağlayan uç sistemler yerel ağa dahil edilirler, bu aşamada geçersiz kullanıcı bilgisi veya başka herhangi bir uyumsuzluk yüzünden sisteme kabul işlemi sonlanmamış uç kullanıcılar ise yerel ağ'a giremezler.

Eğer söz konusu uyumsuzluk “düzeltilebilir hata” seviyesinde tanımlanmış bir eksiklikten kaynaklanıyor ise bu eksikliğin tamamlanması amacıyla bu bilgisayar'lar belirli bir süre için karantina bölgesine alınır ve istenen düzeltmeleri yapabilmeleri için bu işlemler için hazırlanmış sunuculara (Remediation Servers) gene kontrollü olarak yönlendirmeleri yapıp güncellemelerini tamamlama işlemleri sonrasında yapılan kontroller sonucu onay alabilirlerse ağa dahil olmalarına izin verilir.



## NAC İLE KONTROL EDİLEBİLEN ÖZELLİKLER







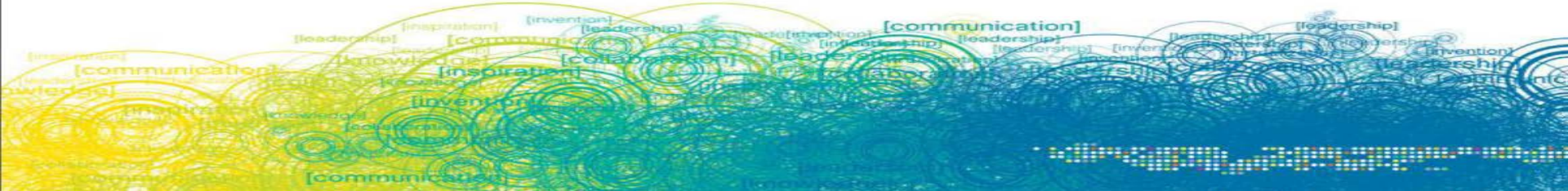
NAC sistemleri aşağıdaki gibi kontrolleri yapabilmektedirler.

Active Directory Computer Membership  
Active Directory Computer Name  
Active Directory Computer OS  
Active Directory Computer OS Version  
Active Directory Computer Service Pack  
Active Directory Distinguished Name  
Cisco Discovery Protocol  
Comment  
DHCP Host Name  
DHCP Options  
DHCP Requested Options  
DHCP Vendor Class  
DNS Name  
IP Address Rule  
MAC Address/MAC Vendor  
Open TCP Port Rule  
RADIUS User Name  
SMTP Server Banner  
SNMP System Description  
TCP Stack or Network Stack Info  
Traffic Rule  
Web Server Type  
Web URL Rule  
Web User Agent Rule  
Web User Agent Rule

&

- “bilgisayar kimlik” veya “kullanıcı kimlik” doğrulama
- İşletim sistemi, yama veya servis paketi
- AntiVirüs, AntiSpyware, Antimalware
- Güncellik kontrolleri
- Kayıt Defteri (Registry) değerlerini
- Çalışan “Servis”ler

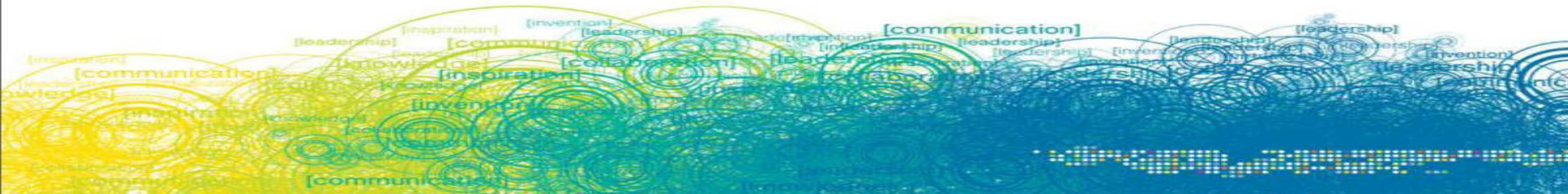
NAC çözümleri yukarıdaki kontrolleri kullanarak yapılandırılan kurallarla uygulandıkları ağ sistemlerinde güvenlik kapıları oluşturabilmektedirler.





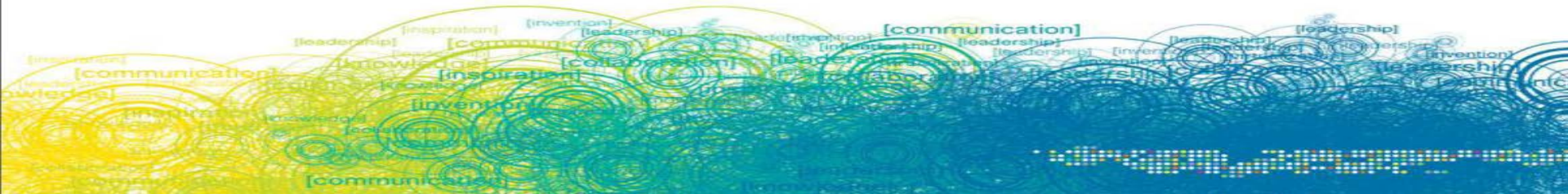
*Bilgisayarlar açısından getirileri;*

- Yerel ağa dahil olma girişiminde bulunan bilgisayarların tanımlanan güvenlik politikalarıyla uyumundan emin olunmasını sağlayarak ağın standartlarını belirler.
- Güvenlik politikalarıyla uyumsuz bilgisayarların yerel ağa dolayısıyla ağdaki bilgi kaynaklarına erişimini engeller.



## *Cihazlar açısından getirileri ;*

- Yerel Ağ'da çalışan yönetilebilen ve yönetilemeyen tüm cihazların (IP /MAC-ID üzerinden) izlenmesi, tanımlanması, gruplanmasını sağlar. Oluşturulan gruplamalara göre bu cihazların ağa dahil edilip edilmemeleri konusundaki kuralları uygulayarak erişim kontrolleri yaparak güvenli bir ağ altyapısı sağladığı için olası riskleri azaltır.
- Cihazlar için tanımlanmış rollere göre işlemleri otomatik olarak yürütebilir, böylece ağın sürekli olarak denetlenmesini ve güncel takibini sağlar.
- geçmişe dönük kontrollerle gerçek zamandaki farklılıkları karşılaştırarak değişiklikleri raporlar, şüpheli ağ trafiği hareketleri için uyarılar oluşturur, böylece “Yerel Ağ” güvenliğinin arttırılmasına önemli bir katkı sağlar.



## NAC KONTROL ADIMLARI

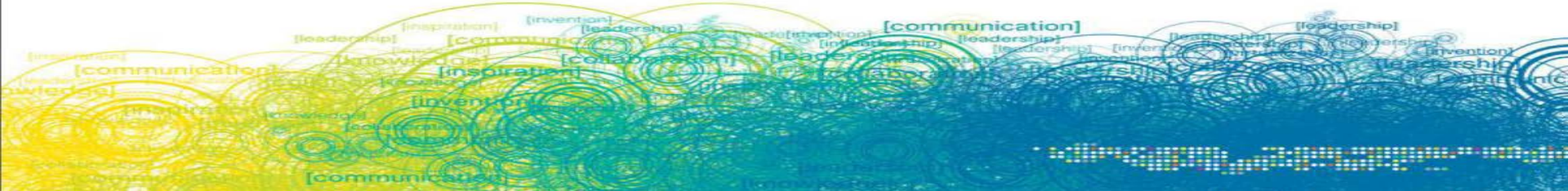
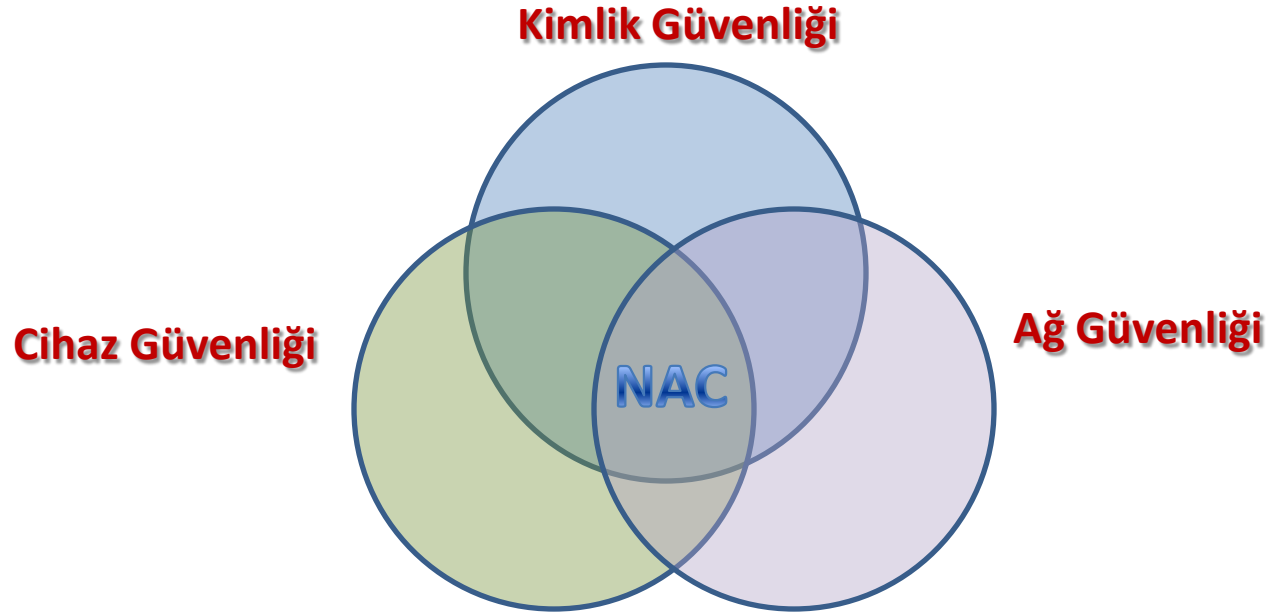


NAC ile ađ güvenliđi temel olarak 5 ařamada sađlanır.

- Tespit
- Kimlik Dođrulama
- Deđerlendirme
- Onaylama
- Düzeltme
  - Güvenlik Taraması
  - İyileřtirme
  - Karantina
  - İzleme



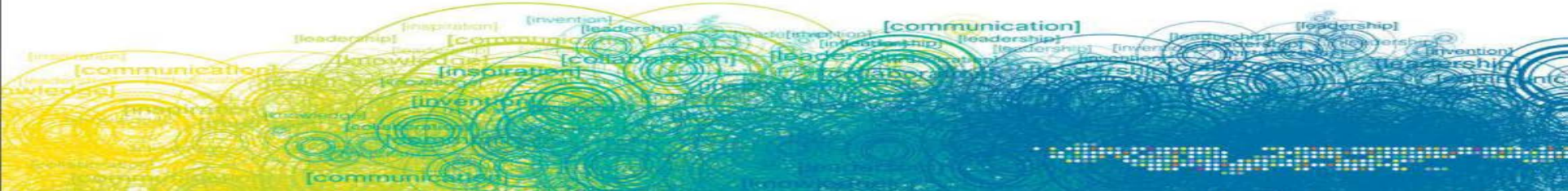
Bu kontrol adımlarını uygulayarak kim, hangi yetkiyle, hangi kaynaklara, nereden ulaşıyor bilgileri dahilinde kontrollü bir ağ erişimi için kullanılacak araçlar elde edilmiş olur.





Siber saldırılara karşı önlem geliştirme konusunda en önemli faktörlerden birisi ağda gerçekleşen şüpheli ağ hareketlerinden, sisteme izinsiz yada yetkisiz erişme girişimlerinden ya da sakıncalı bulunan cihazlardan haberdar olunması yani tehditlerin farkına varılmasıdır.

NAC Sunucuları aracılığı ile tespitleri, sınıflandırmaları, rol atamaları yapılan uç sistemler için istenilen seviyede kurallar ve politikalar oluşturularak bu politikaların belirlenen uç sistemlere uygulanmasıyla dinamik bir güvenlik döngüsü yaratılabilmektedir.

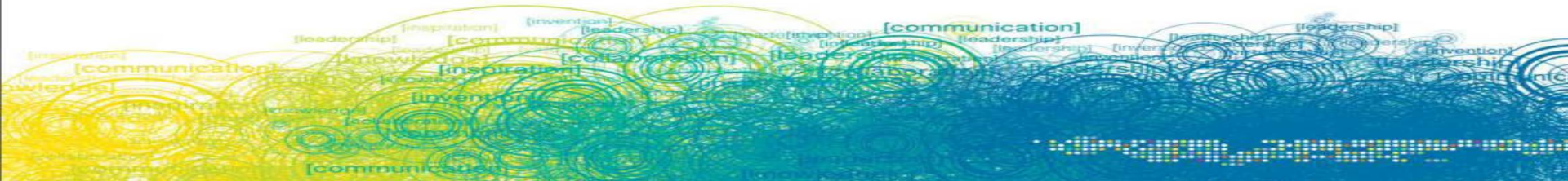
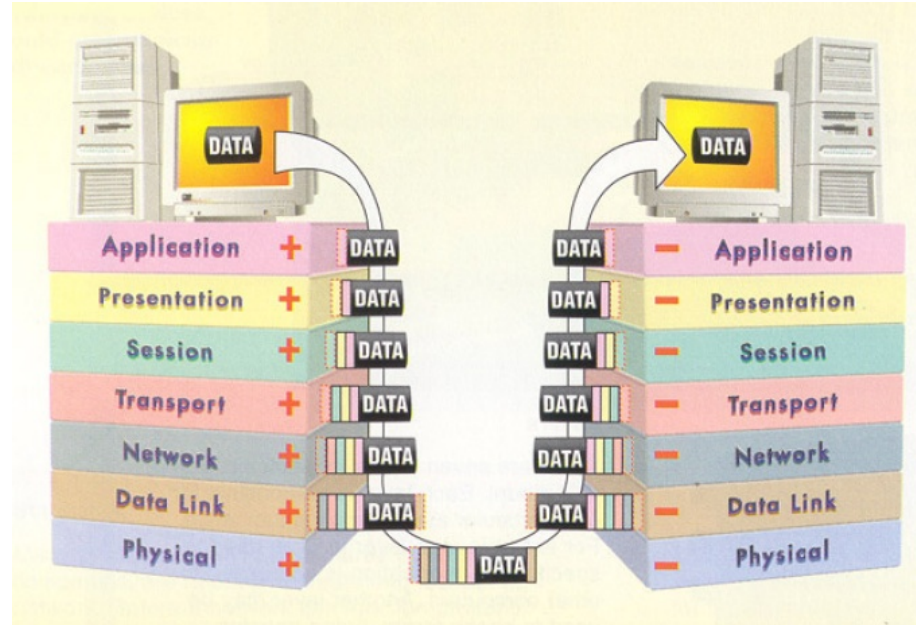


# NAC UYGULAMA TEKNOLOJİLERİ



NAC teknolojilerinin genel çalışma prensipleri incelendiğinde ağ haberleşme katmanlarının (**OSI katmanları**) birbirleriyle ilişkileri ve bu katmanlarda çalışan cihazların özelliklerinin kullanılarak işlemlerin yürütüldüğü görülmektedir.

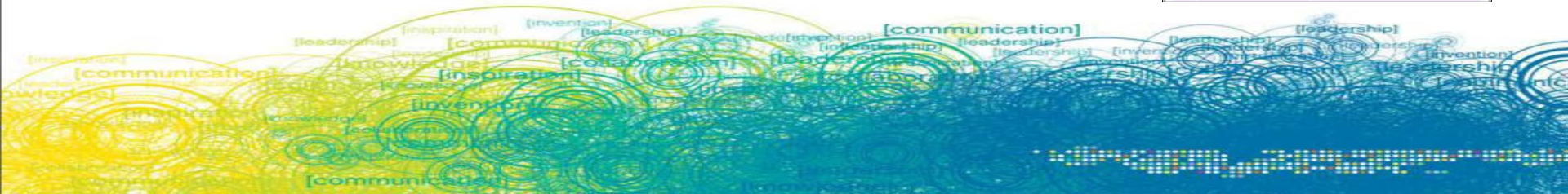
Cihazlar ve bilgisayarlar birbirleriyle OSI katmanları standartlarına uygun olarak haberleşirler.



NAC çözümleri; monitor, tespit ve kontrol işlemlerini gerçekleştirirken OSI katman yapısı standartlarını, ve haberleşme mantığını, haberleşmede kullanılan portlar ve protokollerin özelliklerini, MAC\_ID, IP, ARP, DHCP, VLAN, SNMP vb. bilgileri kullanarak ağ yapısını tanıma ve ağ trafiğine müdahale etme yöntemleri oluştururlar.

Bu yöntemler yazılım yada donanım bazlı olabilmektedirler. Sistemlere müdahale etme açısından daha etkin çözümler sunabildikleri için bu çalışmamızda “Donanım” bazlı (Appliance) çözümler incelenecektir.

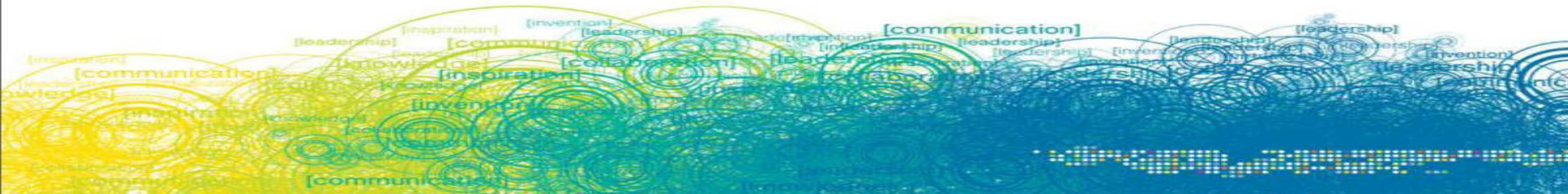
| OSI Modeli                 |                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------|
| Katman                     | İletişim kuralları                                                                   |
| 7. Uygulama katmanı        | HTTP, HTTPS, SMTP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ... |
| 6. Sunum katmanı           | ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...                           |
| 5. Oturum katmanı          | NFS, SMB, ISO 8326, ISO 8327, ITU-T T.6299, ...                                      |
| 4. Ulaşım katmanı          | TCP, UDP, SCTP, DCCP, ...                                                            |
| 3. Ağ katmanı              | IP, IPv4, IPv6, ICMP, ARP, IGMP, ...                                                 |
| 2. Veri bağlantısı katmanı | Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...                                    |
| 1. Donanım katmanı         | ISDN, RS-232, EIA-422, RS-449, EIA-485, ...                                          |





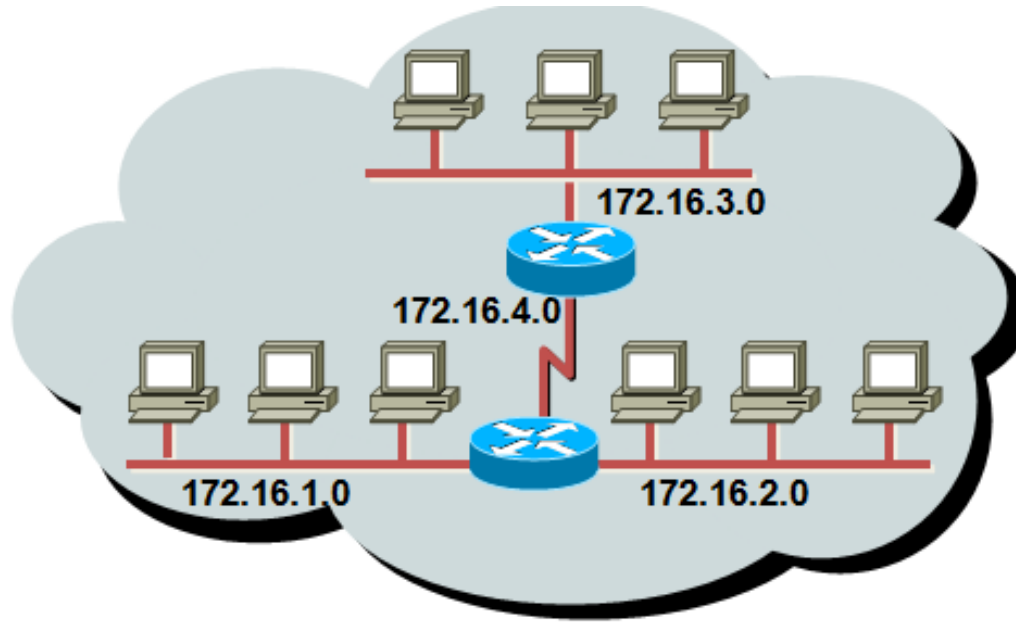
Donanım bazlı NAC çözümlerinin mantığının daha iyi anlaşılması için kullanılan temel teknolojilerden biri olan VLAN (Sanal Yerel Alan Ağ) çalışma ve Vlan'lar arası haberleşme mantığından kısaca bahsetmemiz gerekmektedir.

VLAN; bir yerel ağı mantıksal olarak (sanal) bölümlere ayırma yöntemi olarak tanımlanabilir.



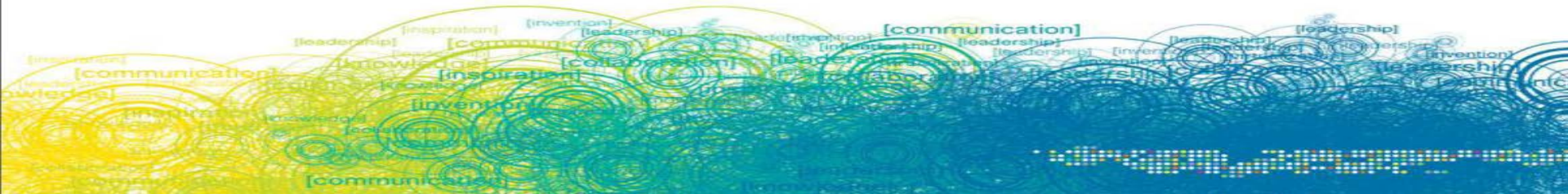


Vlan kullanılan bir ağda, aynı Vlan'da bulunan uç kullanıcılar sadece kendi yayın alanlarına (broadcast domain) sahip olacaklarından birbirleri ile haberleşebilirler, ancak farklı Vlan'larda bulunan uç kullanıcılar ile gerekli konfigürasyonlar yapılmadığı sürece iletişim kuramazlar.

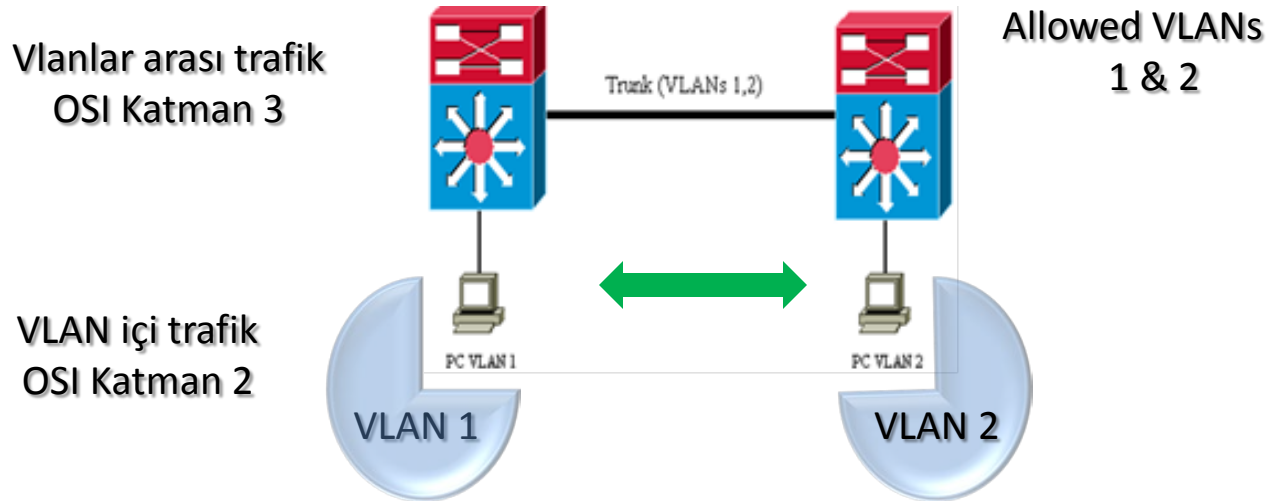


Bir yerel ağ'da bir "Vlan" oluşturulduktan sonra bu Vlan'a ağ içerisindeki başka Vlan'lardan ulaşabilmek için üzerlerinde bir Interface tanımlanır ve bu interface için bir adresleme bilgisi (IP ve subnet) verilir, böylece bu Vlan dışarıdan erişilebilir hale gelir, eğer böyle bir interface tanımı yapılmazsa söz konusu Vlan ile dış bağlantı kurulamaz.

Bir Vlan'a (sistem yöneticileri tarafından) dahil edilen uç kullanıcılar DHCP sunucu üzerinden söz konusu Vlan için ayrılmış bulunan IP bloğundan IP ve Gateway bilgilerini alarak diğer Vlan'larla haberleşecek duruma gelirler.



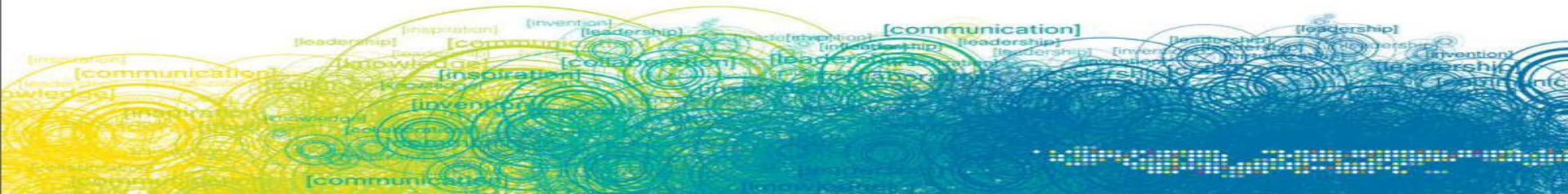
Aşağıdaki şekilde örneği verilen VLAN1 ve VLAN2 Vlanları üzerinde interface ve adresleme bilgileri tanımlanmaz ise veya bu Vlan'ları birbirine bağlayan Switchlerin birbirlerine bağlandıkları "Trunk" portları üzerinde bu Vlan'lar için karşılıklı izin tanımlamaları yapılmazsa bu iki farklı Vlan'daki PC'ler birbirleriyle haberleşemezler.



NAC programları yukarıda bahsedilen VLAN tanımlamalarını dinamik olarak değiştirip, kontrol ederek ağ trafiğini durdurabilir ve Vlan'lar arası kontrollü geçiş olanağı yaratabilirler.

NAC sunucularının kontrol sonuçlarına göre uç kullanıcı trafiğini tasarım aşamasında tanımlanan politikalara uygun VLAN'lara yönlendirebilirler.

Örneğin; uç kullanıcıları belirlenen Rol profillerine göre ilgili "Rol Vlan"larına, ağa girmesi uygun olmayan uç kullanıcıları "Karantina Vlan"ına, misafir kullanıcıları ise "İnternet Vlan"ına alabilirler.



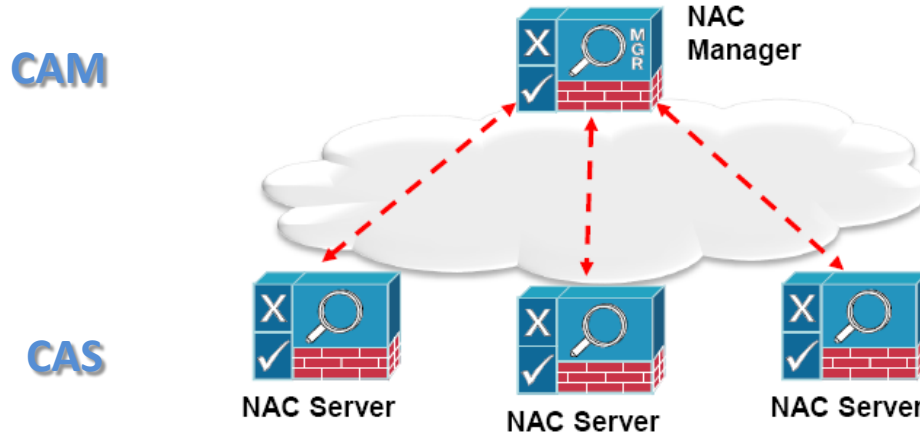


## NAC BİLEŞENLERİ





NAC sisteminin bileşenlerini yaygın kullanılan bir NAC uygulaması üzerinden incelemek uygun olacaktır. NAC Sistemi farklı görevler yapan sunucuların bir arada çalışması ile oluşturulur, bu sunuculardan Yönetici (CAM) ve Uygulayıcı (CAS) sunucuları sistemin temel işlemleri yerine getirirler, son kullanıcıların ağa dahil edilip edilmeyeceği kararları, gereken kontrollerin yapılması ve sonuçların uygulanmasından sorumludurlar. Ayrıca “Gruplayıcı” (Profiler) ve “Bilgi Toplayıcı” (Collector) sunucuları diğer önemli bileşenlerdir.



Ağın ihtiyaçlarına uygun sayıda CAS sunucu kullanılabilmektedir.



***NAC Manager (CAM):*** Tüm NAC sisteminin yöneticisi durumundadır.

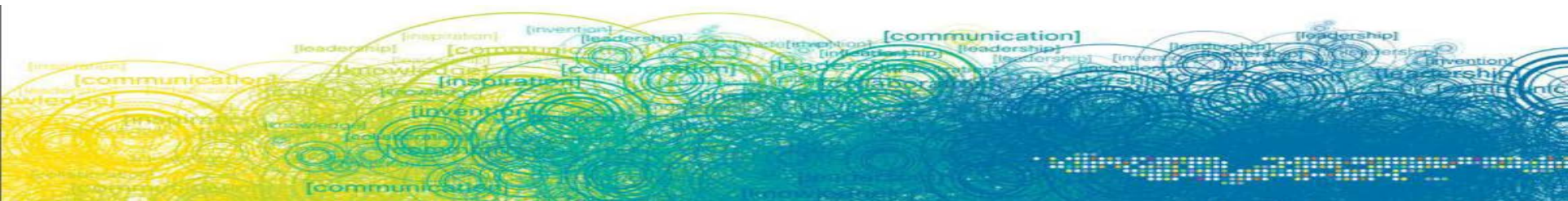


***NAC Server (CAS) :*** Ağa erişim kontrolünü gerçekleştiren uygulama sunucusudur.



***NAC Agent***

***NAC Agent (NA) :*** İstemci tarafında çalışan NAC ajanıdır.





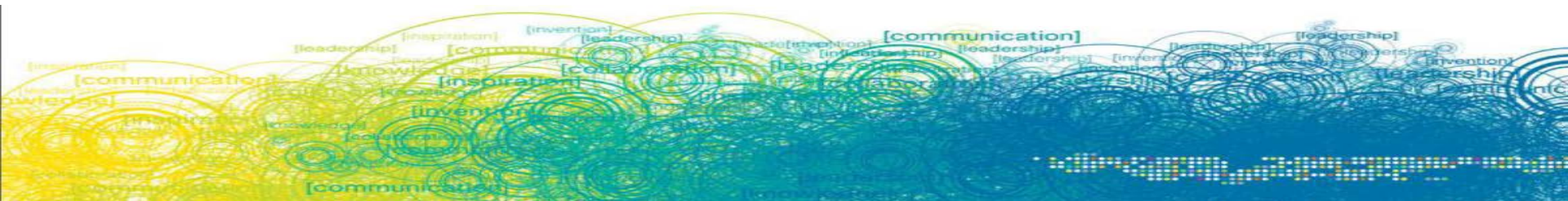
**NAC Collector Server :** Ağ içerisinde bulunan tüm cihazları gerçek zamanlı olarak tarayarak; topladığı bilgileri Profiler sunucusuna aktarır.

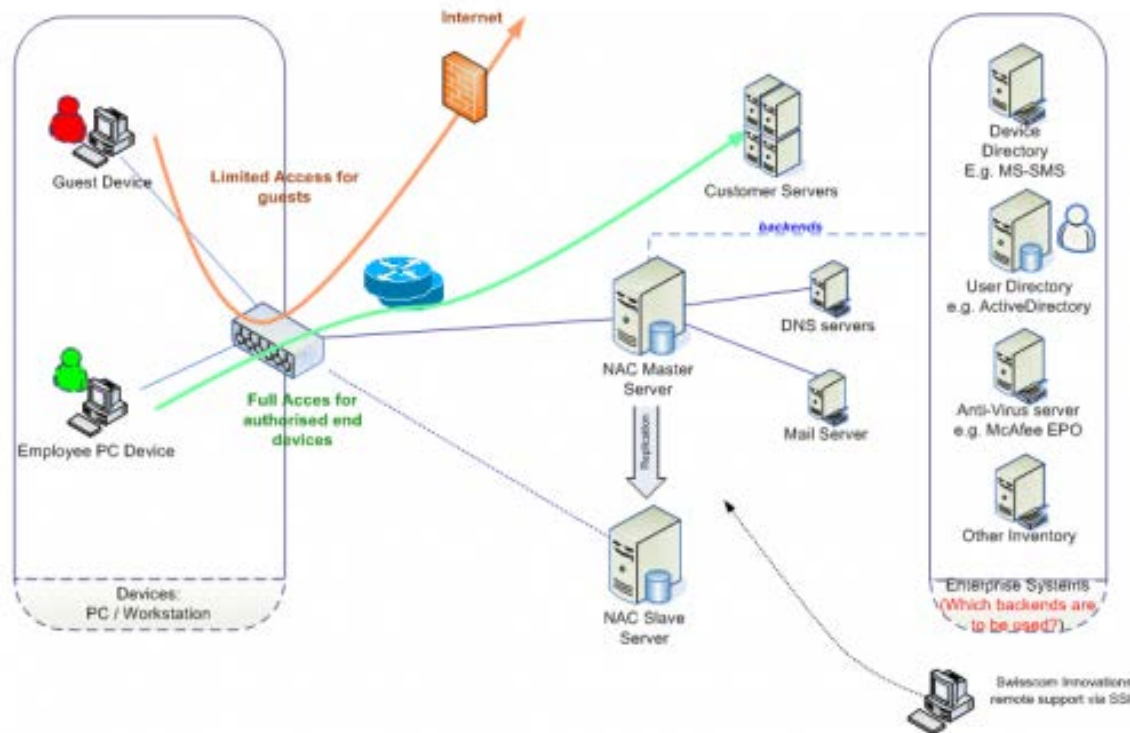


**NAC Profiler Server :** Collector sunucularından gelen bilgilerin analizlerini yaparak özelliklerine göre cihazları tanımaya yönelik kontroller ve sınıflamalar yapar, son kullanıcıların tanımlanmış grup ya da “Roller”e “dinamik” atamalarını yapar, sonuçları CAM sunucusuna bildirir.



**Guest Server :** Ağ üyesi olmayan ziyaretçi sistemlerin, örneğin; ziyaretçi dizüstü bilgisayarların sadece Internet’e çıkma ihtiyaçlarını sağlamak için kullanılan bileşendir.



[illegible]



# CAS SUNUCU UYGULAMA TASARIMI

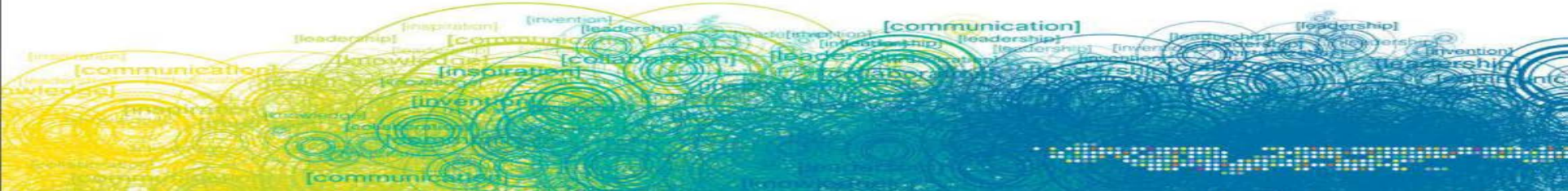




### CAS Modları:

NAC uygulanması planlanan ağ yapıları ve uygulama ihtiyaçları çeşitlilik gösterdiğinden ilk adım olarak NAC uygulaması yapılacak ağ için analiz yapılarak NAC'ın hangi seçeneklerine uygun olduğuna karar vermek gerekmektedir. Bu aşamada son kullanıcı tarafında uygulayıcı sunucu rolündeki CAS sunucu üzerinde ağın yapısına göre aşağıdaki *Tablo* 'da gösterilen modları ve seçeneklerini kullanarak NAC tasarımını ihtiyaca uygun yapmak son derece önemlidir.

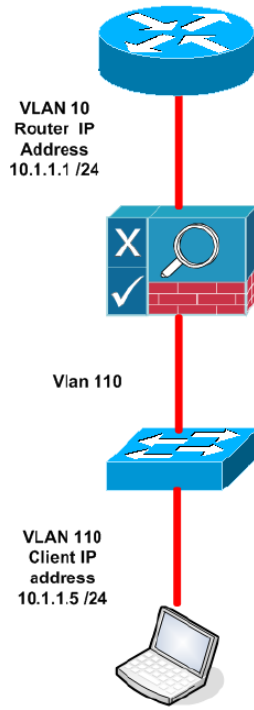
| CAS Uygulama Modları     | Seçenekler                   |
|--------------------------|------------------------------|
| Trafik Modları           | Virtual veya Real_IP Gateway |
| Trafik Akış Modları      | In-Band veya Out-of-band     |
| Kullanıcı ulaşım Modları | Layer 2 veya Layer 3         |



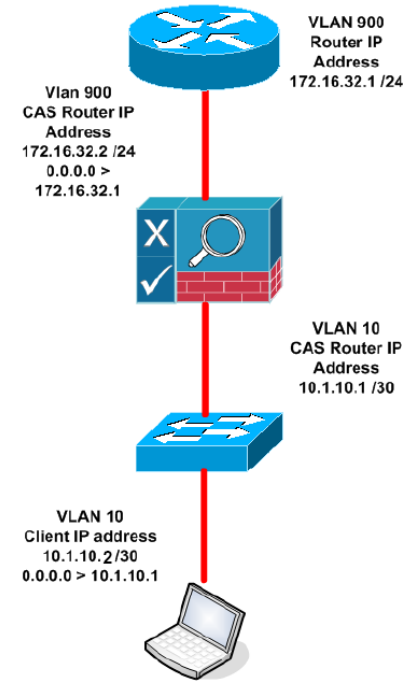
## Trafik Modu:

CAS sunucu paketleri uçtan uca doğrudan aktaracak şekilde (Bridged) çalışacaksa **Virtual Gateway**, IP yönlendirmeleri yapacak şekilde (IP Routing) çalışacak ise **Real IP Gateway** Modu olarak ayarlanmalıdır.

### Virtual Gateway



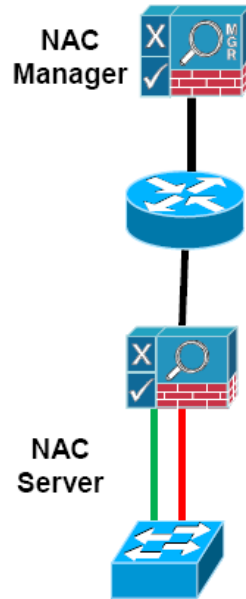
### Real IP Gateway



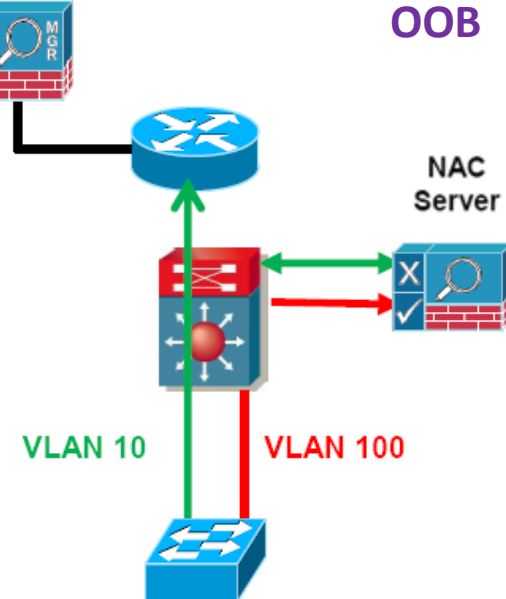
## Trafik Akış Modu:

CAS sunucu üzerinde eth0 ve eth2 olmak üzere 2 adet ethernet çıkışı bulunmaktadır, bu 2 çıkışın ağa bağlanma yöntemine göre **In-band** ve **Out-of-Band** olmak üzere 2 farklı seçenekle ağ trafiğini kontrol edebilmektedir.

### In- Band Modu



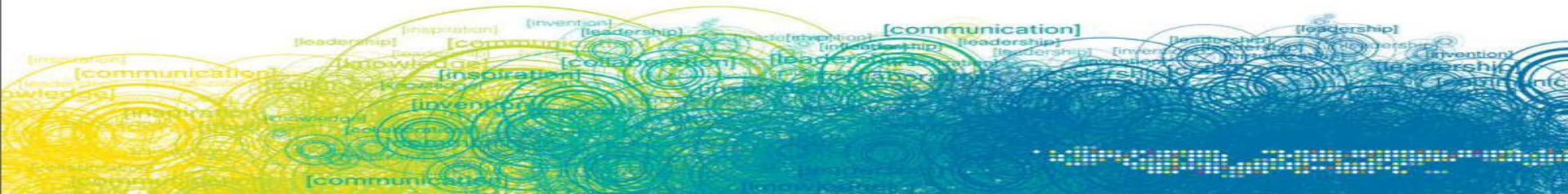
### Out-of Band Modu OOB



### *Trafik Akış Modu (devam)*

Tüm ağ trafiği CAS sunucu üzerinden geçirilerek trafiğin her an kontrol edebilir durumda olması istenirse “**In-Band**” modu seçilmelidir.

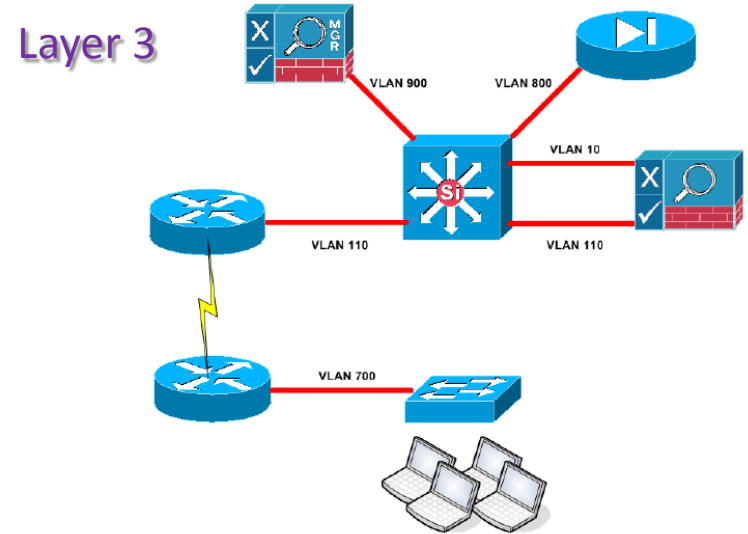
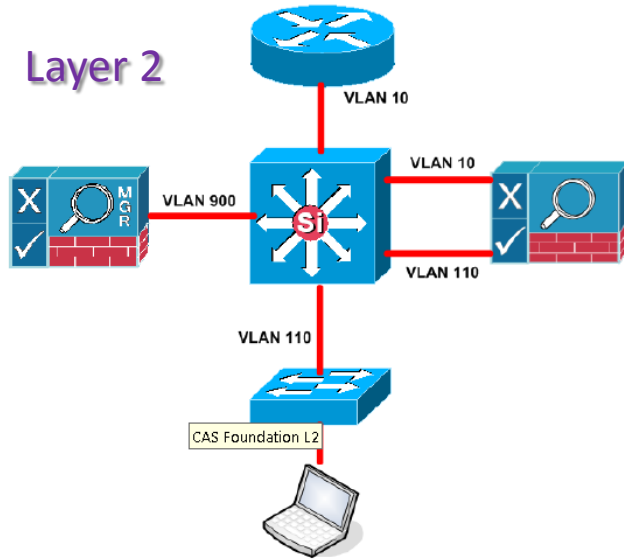
Eğer CAS ethernet çıkışları söz konusu ağa mantıksal olarak bağlanır ve trafiği sadece uç kullanıcıları onaylama işlemi sırasında kontrol edilmesi yeterli bulunur ise “**Out-of-Band**” modu seçilir.





### Kullanıcı Ulaşım Modu:

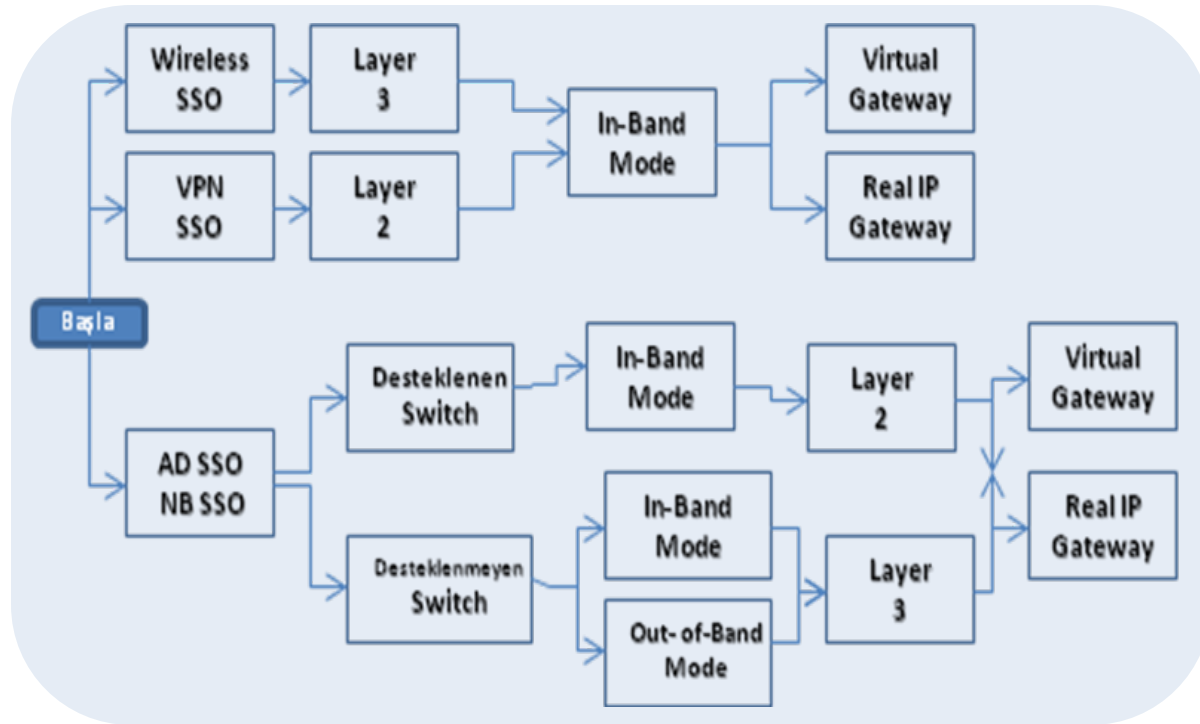
- Uç kullanıcılar yerel ağ içerisinde bulunuyorlar ise yani uç noktalar MAC-ID'leri üzerinden kontrol edilebilecek ise CAS “**Layer 2**” modunda çalıştırılır.
- Uzak lokasyonlardan ulaşacak kullanıcıların kontrollerinin yapılması isteniyor ise kontroller IP'ler üzerinden yapılacağından bu durumda “**Layer 3**” modu seçilir. *(Bu 2 mod bir arada kullanılabilir)*





Yukarıda verilen bilgiler ışığında NAC uygulaması yapılması planlanan bir ağın fiziksel yapısına, lokasyonların birbirleriyle bağlantı koşullarına, kullanılan ağ cihazlarına ve ağ için uygulanacak güvenlik politikalarına göre aşağıda gösterilen algoritma kullanılarak uygun olacak seçeneklere göre CAS sunucularının uygulama modlarına karar verilir.

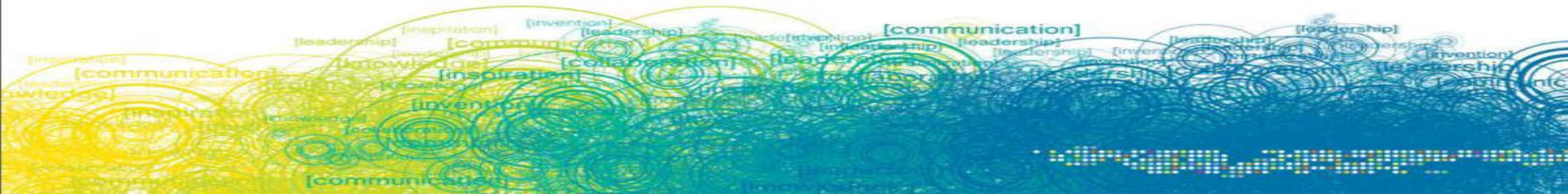
### Trafik Modları İçin Algoritma



Bu modlar farklı kombinasyonlarla bir arada kullanılabilirler.

Örneğin; yerel ağ tarafını kontrol edecek CAS sunucusu “Out-of-band” ve “Layer 2” modunda çalıştırılırken uzak bağlantıları karşılayacak CAS sunucusu ise “In-Band” ve “Layer 3” modunda çalıştırılarak yerel, geniş yada uzak tüm uç kullanıcılar NAC kontrollü olarak ağa alınabilmektedirler.

Bu açıdan NAC uygulanacak ağın fiziksel yapısı ve güvenlik ihtiyaçlarına uygun olarak özenli bir analiz ve tasarım çalışması yapılması ve sonrasında uygulamayı devreye almadan önce hazırlık ve pilot aşamalarının dikkatle planlanarak her durum için testlerinin yapılması son derece önemlidir.



# NAC TASARIM ÖRNEĞİ

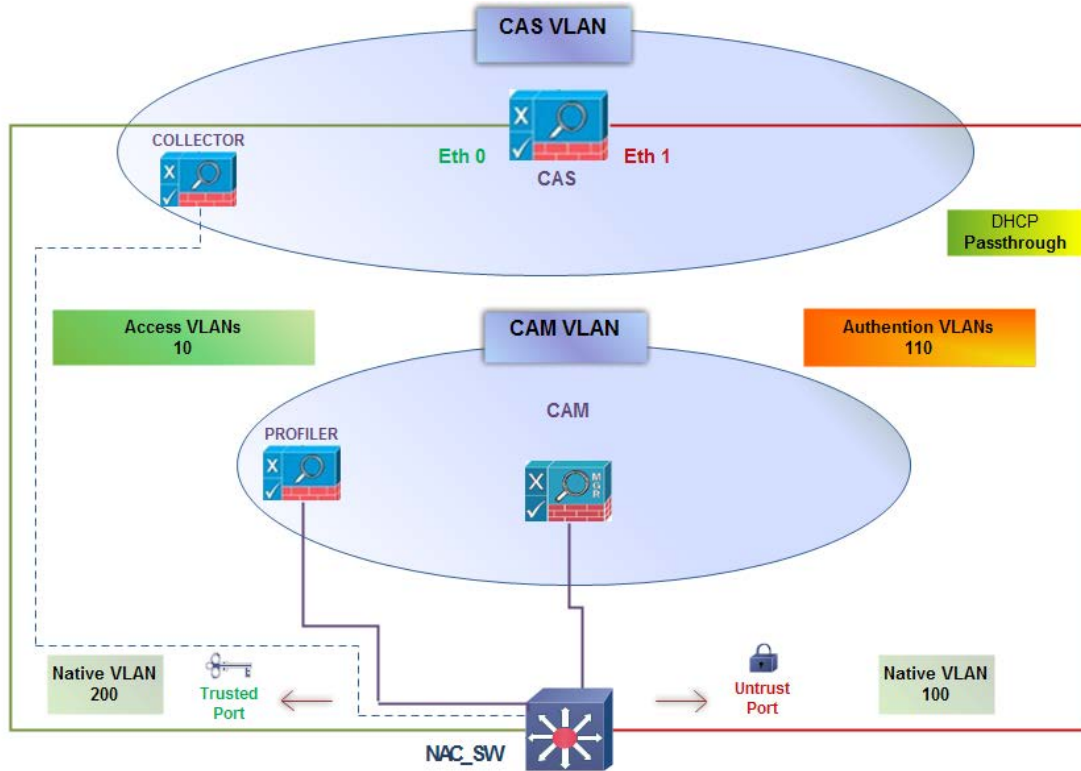
## TAI - TUSAŞ NAC UYGULAMASI



NAC uygulama örneği olarak inceleyeceğimiz TAI yerel ağında daha önce bahsedilen NAC teknolojileri kullanılarak kontrollü ağ erişimi sağlanmıştır.

- TAI yerel ağında yaklaşık 5000 uç sistem bulunmaktadır, ağa bağlı tüm bilgisayarlar ve cihazlar NAC tarafından kontrol edilmektedirler.
- Yerel ağ içerisinde şirket kullanıcıları için hizmet veren bir Windows AD Domain yapısı bulunmakta ve kurulan NAC sistemi bu domain ile entegre edilmiş durumdadır.
- Ağa girme isteğinde bulunan bilgisayarlar ancak TAI AD SSO onayını alabilirlerse giriş yapabilmektedirler.
- Şirkete ait yazıcılar, Cihazlar ve sunucular kendileri için hazırlanmış özel VLAN'lara alınmış durumdadırlar.
- Cihazlar, yazıcılar ve sunucular Profiler sunucu üzerinde özel "xml" formülleri kullanılarak ve bu sonuçlar IP/MacID bilgileriyle eşleştirilerek sistem yöneticileri tarafından NAC denetlemeleri için onaylı duruma getirilmekte ve güvenli bir şekilde ağa girebilmektedir.

TAI NAC sistemi yapısı ve kullanıcılar bileşenler basitleştirilmiş bir şekilde aşağıda gösterilmiştir. CAS sunucusu Virtual Gateway, Out-of-Band, Layer 2 seçenekleri ile kurulmuştur.

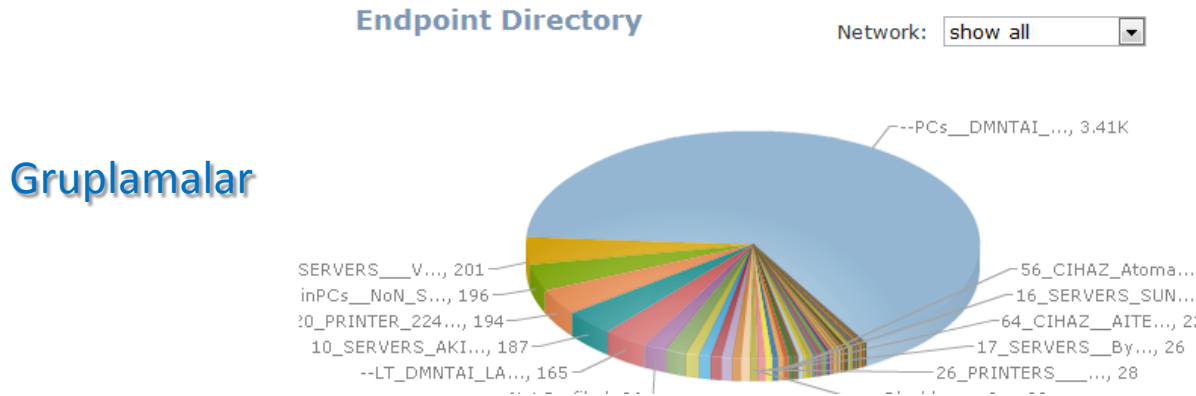


Yerel ağ Profiler ve Collector sunucuları tarafından gerçek zamanlı olarak denetlenmektedir.



NAC Collector sunucuları tarafından Profiler sunucularına iletilen bilgiler NAC sistem yöneticisi tarafından derlenir, uç cihazlar özel “xml” fomülleriyle birbirinden ayrıştırılır ve gruplanır.

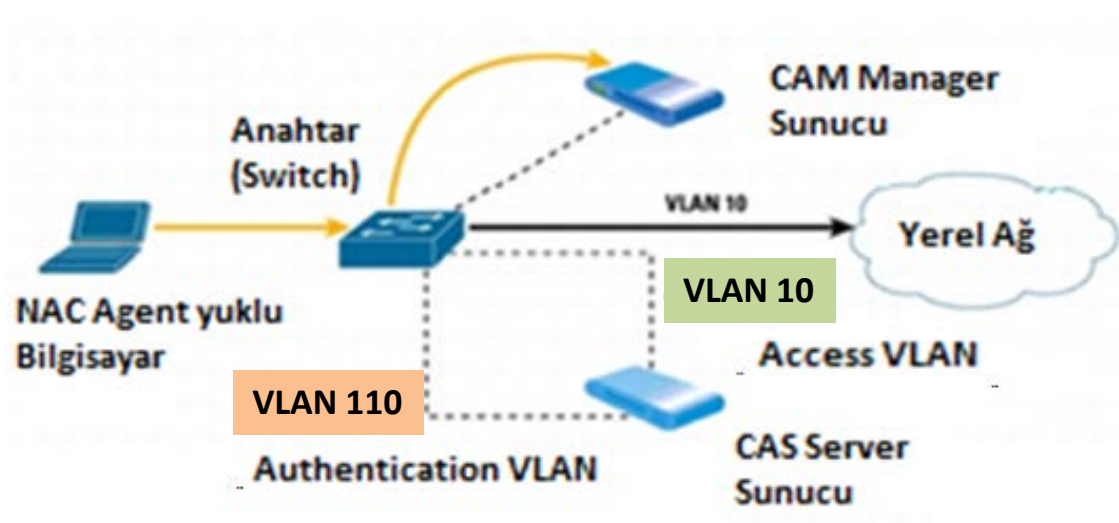
Bu gruplamalara göre uç sistemler için roller tanımlanır, bu rollere uyan yeni bir uç sistem ağa giriş yapmak istediğinde otomatik olarak kendisine uyan role atanır ve o rol için tanımlanmış politika kendisine uygulanır. (Rol atamaları için hazırlanan “NAC Event” kuralları aracılığıyla Profiler Sunucu yeni uç kullanıcının rolünü CAM sunucuna bildirilir, CAM sunucu da bu rol için uygun politikanın uç kullanıcı için uygulanmasını sağlar, böylece sistem kuralları ve politikalar dinamik olarak işletilir.



Uygulanan yapının çalışması sadeleştirilmiş bir yapıda aşağıda gösterilmektedir.

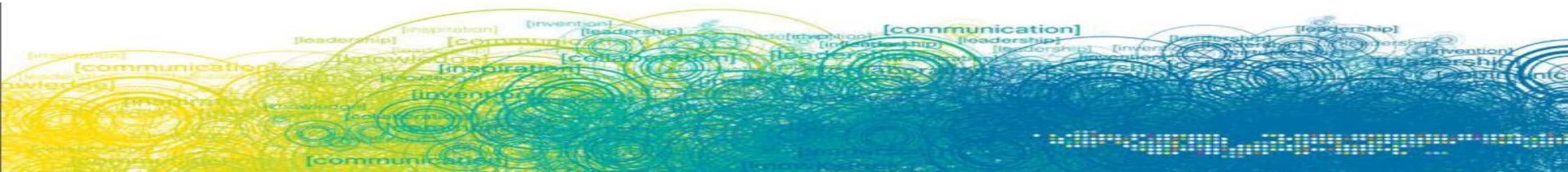
Yerel ağ için NAC tarafından 2 ana mantıksal bölümlenme uygulanmaktadır. Güvensiz taraf olan giriş isteğinde bulunulan taraf **VLAN 110** olarak, yerel ağ tarafı yani güvenilen taraf ise **VLAN 10** olarak gösterilmiştir.

Kullanıcı anahtarının portlarını kontrol eden CAS sunucusu CAM üzerinden AD SSO onay sistemi ile kontrollü ağ erişimini sağlamaktadır.



## Kontrol Adımları;

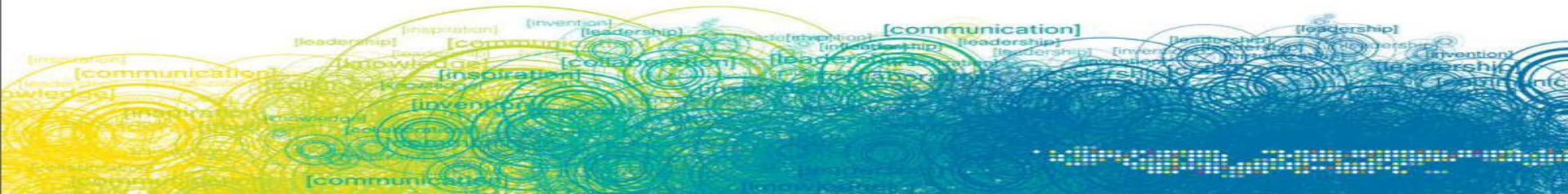
- Ağa giriş isteğinde bulunan bir bilgisayar'ın bağlı bulunduğu Anahtar (switch) port'u CAS sunucu tarafından önce VLAN 110 olarak tanımlanmış "Authentication VLAN"ına yani "güvenilmeyen taraf"a alınır, bu VLAN'da onay işlemleri tamamlanana kadar bekletilir, bu sırada sadece kendisine onay DC sunucularla özel portlar üzerinden haberleşebilir, bu arada örneğin DHCP sunucusundan bağlanma isteğinde bulunduğu güvenilir Vlan tarafı için uygun olan bir IP alır, (*DHCP Passthrough özelliği nedeniyle*), ancak bu aşamada ağdaki diğer kaynaklara ulaşamazlar.
- Bilgisayar üzerindeki kullanıcı login işlemini yaptığında üzerinde ygklğ bulunan Agent aracılığı ile bu bilgi CAS sunucusuna iletilir. CAS sunucusu AD ile entegre çalışan CAM sunucu ile haberleşerek login sonucuna göre CAS sunucuna onay verip vermeyeceğini bildirir. Onay alan bilgisayar'ın bağlı bulunduğu port yerel ağ Vlan'ına değiştirilir.
- Aynı anda Antivirus sürüm kontrolü de yapılır.



Uç kullanıcı NAC üzerinde tanımlanmış kurallara göre onay alırsa (AD\_SSO üzerinden DMNTAI domain üyesi PC/ User çifti olduğunu kanıtlarsa ve istenen diğer şartları da sağlarsa) VLAN10 olarak tanımlı “Access VLAN” ına yani “güvenilir” şirket ağına ait vlan’a kendisine uygun Rol tanımı ile alınır, onaylanmaz ise ağı giremez, “Authentication VLAN”ında kalır.

Sistem yöneticisi tarafından tanınmış ve onaylanmış cihazlar, yazıcılar NAC kontrolünden güvenle geçmekte, onaysız cihazlar ise ağı girememektedir.

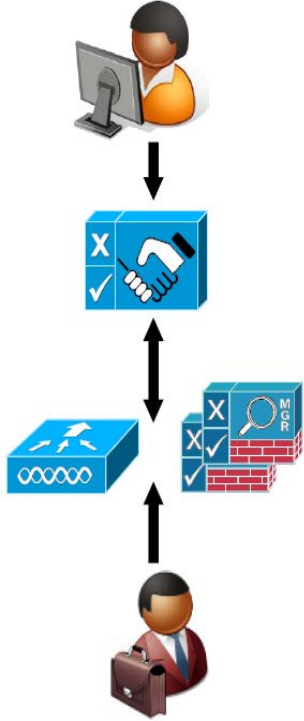
Ağda gerçekleşen tüm hareketler loglanmakta ve NAC yöneticisi CAM ve Profiler sunucusu WEB konsollarından tüm ağ hareketlerini izleyebilmekte ve ağ anahtarlarını NAC üzerinden yönetebilmektedir.





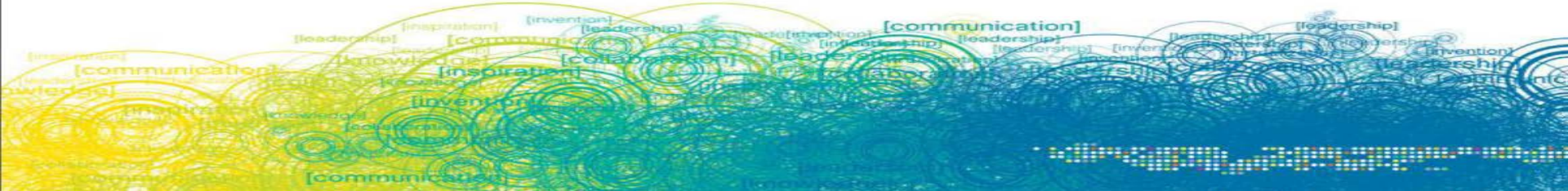
## Ziyaretçi Sistemi

Dışarıdan gelen ziyaretçilerin internet ihtiyaçlarını karşılamak için ise kablosuz (Wireless tabanlı) bir “Guest server” kullanılmaktadır.



Ziyaretçiler kendilerine içeriye girişleri için güvenlik birimi tarafından verilen ziyaretçi giriş kartlarındaki numara ile ilişkilendirilmiş olarak TAI operasyon birimi tarafından kısıtlı süre için geçerli olacak şekilde tanımlanan kullanıcı ID'leri ve password'leriyle giriş yaparak sadece Internet'e çıkış işlemlerini gerçekleştirebilmektedirler.

Ziyaretçi sistemler hiçbir şekilde yerel ağa dahil olamamaktadırlar.



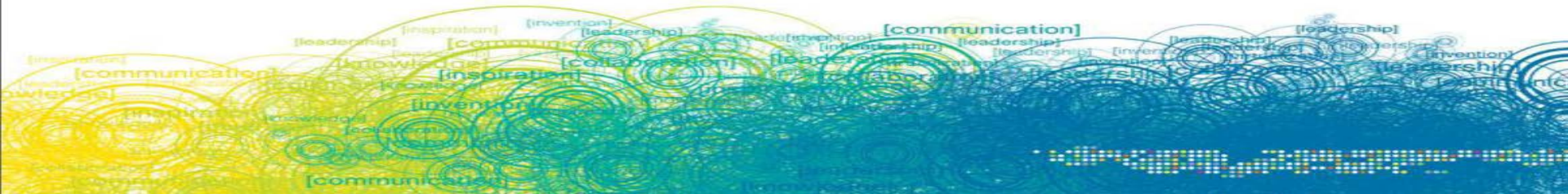


## SONUÇ VE DEĞERLENDİRME



NAC uygulamasının ağ yöneticilerinin ağ üzerindeki kontrol ve yönetim gücünün arttığı ve önemli bir oranda güvenlik iyileştirmesi gerçekleştirilebildiği görülmektedir.

NAC sistemleri “Ağ Güvenliği”nin istenilen standartlara gelmesi ve değişik seviyedeki güvenlik ihtiyaçlarına cevap verebilmesi ve sürekli kontrol sağlayabilmesi açısından Siber saldırılara karşı önlemler alınabilmesi için gerekli bileşenleri ağ yöneticilerine sunmaktadır.



NAC sistemi hazırlanan kurallar geređi sakıncalı bulunan uç sistemlere veya cihazlara giriş izni vermediđi gibi ađa girmesine izin verilmiř bulunan uç noktalar üzerinde řüpheli ađ hareketleri oluřtuđuunda da ađ yöneticilerini uyararak önceden önlem alma olanađı sunmakta ve tüm ađ elemanlarını gerçek zamanlı olarak izlenme olanađı da vermektedir.

Bu deęerlendirmeler ışığında NAC özmleri “Siber Saldırılar”a karşı proaktif önlemler oluşturma alışmaları sırasında önemli bir denetim ve destek mekanizması olarak karşıımıza çıkmaktadır.

NAC özümü savunma sistemlerinde kullanılan dost ve düşman sistemleri ayırt etme yeteneęi bulunan cihazların aę karşılığı olarak nitelendirilebilecek şekilde bir koruma, ayırt etme ve saldırı tespit olanakları sunmaktadır.



Sonuç olarak NAC; Ağ güvenliğini tehdit eden saldırı tiplerine karşı “dinamik” bir koruma kalkanı kurma olanağı sağlamaktadır, ayrıca IDS ve IPS gibi diğer saldırı tespit ve saldırıdan koruma sunucuları ile birlikte kullanıldığında dışarıdan gelebilecek “Siber Saldırıları”a karşı farklı teknolojiler kullanan çok katmanlı bir güvenlik çözümü de yakalanmış olacağından “**Siber Güvenlik**” açısından arzu edilen seviyede standartlar sağlanabilecektir.



Katılımınız  
için  
Teşekkürler...

Sorularınız için  
[uduman@tai.com.tr](mailto:uduman@tai.com.tr)



# aselsan

**KRİTİK ALTYAPI GÜVENLİĞİNE  
YÖNELİK ÖZGÜN ÇÖZÜMLER:**

**SANAL HAVA BOŞLUĞU**

# SUNUM PLANI

## SUNUM PLANI

KRİTİK ALT YAPILAR NELERDİR?

KRİTİK ALT YAPILARA YÖNELİK SALDIRILAR

KRİTİK ALTYAPILARA YÖNELİK SİBER SALDIRILARA KARŞI  
ALINACAK ÖZGÜN GÜVENLİK ÖNLEMLERİ VE SANAL HAVA  
BOŞLUĞU SİSTEMİ ÇÖZÜMÜ

SONUÇ

# KRİTİK ALTYAPI TANIMLARI

Kritik altyapılar ile ilgili ortak uluslararası bir tanım bulunmamaktadır.

USA PATRIOT ACT 2001'e göre kritik altyapı tanımı:

“Hasar görmesi veya etkisizleştirilmesi halinde ulusal halk sağlığını, güvenliği, ekonomik güvenliği veya tümünü olumsuz etkileyecek fiziki veya sanal tüm varlık ve sistemler kritik altyapı sistemleri”

Avrupa Birliği (AB) Meclisine sunulan “Terörist Saldırlara Karşı Kritik Altyapıların Korunması” başlıklı metine göre:

“kesilmesi ve/veya hasar görmesi halinde vatandaşların güvenliği, sağlığı ve ekonomik refahı üzerinde veya üye hükümetlerin etkin ve verimli işleyişi üzerinde ciddi olumsuz etkiler oluşturacak fiziki ve bilgi teknolojileri tesisleri, hizmetleri ve varlıkları”

Ağustos 2009 tarihi itibari ile yayınlanan “e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı” başlıklı metne göre:

“İşlevleri tamamen veya kısmen yerine getirilmemesi halinde kamu güvenliği ve düzenini önemli derecede etkileyen bilgi sistemleri”

# KRİTİK ALTYAPI TANIMLARI

Bu tanımlamalar ışığında:

- Üretimde ve günlük yaşamda sürekli hizmet vermesi gereken;
- Fiziksel ve/veya siber bir saldırıya maruz kaldığında bir ya da birden fazla ülkenin ulusal ve/veya uluslar arası çıkarlarını etkileme,
- Kamu sağlığını tehdit etme,
- Çevre kirliliği,
- Para ve itibar kaybına neden olabilecek potansiyele sahip altyapı unsurları

“Kritik Altyapı” olarak tanımlanabilir.



# KRİTİK ALTYAPI TANIMLARI

- Enerji hatları,
- Bankacılık ve finans,
- Bilgi teknolojileri ve iletişim,
- Ulaşım,
- Kamu sağlığı ve su sevkiyatı

kritik altyapılar için yapılan genel tanım içerisinde yer almaktadır.

# KRİTİK ALTYAPILARA YÖNELİK SALDIRILAR

- Kritik Altyapı tesisleri, stratejik önemleri nedeni ile terörist saldırıların öncelikli hedefleridir.
- Bilgi teknolojilerindeki gelişme ve Internet'in yaygınlaşması kritik altyapı kontrol sistemlerini de etkilemiştir.
- Geçmişte, fiziksel unsurlardan tamamen yalıtılmış kontrol sistemleri; günümüzde, bilgi ve iletişim teknolojileri ile yönetilebilir ve izlenebilir duruma gelmiştir

# KRİTİK ALTYAPILARA YÖNELİK SALDIRILAR

- Kritik altyapıların yönetimi ve izlenmesinde SCADA (Supervisory Control And Data Acquisition) endüstriyel kontrol sistemleri kullanılmaktadır.
- SCADA sistemleri, günümüzde yaygın olarak kullanılan ve bilinen yazılım, donanım ve ağ protokollerini barındırmaktadır.
- SCADA sistemleri kurumsal ağlara ve Internet'e bağlantılı hale gelmeye başlamıştır.
- Sıcak savaş senaryolarının yerini kritik altyapı unsurlarına yönelik siber saldırılar almaktadır.

# KRİTİK ALTYAPILARA YÖNELİK SALDIRILAR

- 2001-2006 yıllarını kapsayan Endüstriyel Güvenlik Olayları Veritabanı (ISID – Industrial Security Incidents Database), 2002 yılı ve sonrasında SCADA sistemlerinde yaşanan güvenlik olaylarında ciddi bir artış olduğunu göstermektedir.

Kaydedilen siber saldırılardan bazıları şunlardır:

- 2000 yılında Avustralya'nın Moroochy eyaletinde 28 Şubat ile 23 Nisan tarihleri arasında arıtma tesisine düzenlenen saldırı.
- 2003 yılında düzenlenen “Northeast Blackout”
- Ağustos 2003'te Ohio'da faaliyet gösteren, Davis-Besse nükleer santralinin izole bilgisayar ağına Slammer solucanının bulaşması.
- Ekim 2003'de ABD'nin en yoğun limanlarından olan Houston Limanı'nın bilgisayar sistemi saldırıya uğraması.
- 2007 Nisan ve Mayıs aylarında, Rus bilgisayar korsanlarının Estonya bilgi sistemlerine sızması.
- 30 Ocak 2009 tarihinde Conficker virüsünün Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarları devre dışı bırakması.

# KRİTİK ALTYAPILARA YÖNELİK SALDIRILAR

- 2010 yılı Temmuz ayında keşfedilen Stuxnet yazılımı
- İran nükleer zenginleştirme programını hedeflediği düşünülen Stuxnet yazılımı, SCADA sistemlerini hedefleyen bilinen en tehlikeli zararlı yazılımdır.
- Daha önce endüstriyel sistemlere yapılan ataklarda genellikle sistemin ele geçirilmesi, yetkinin kötüye kullanılması gibi ataklar yapılmıştı. Bu atak zararlı yazılım sistemlerine fiziksel zarar veriyor olması ile de bir ilktir.



# KRİTİK ALTYAPILARA YÖNELİK SALDIRILARA KARŞI ALINACAK ÖZGÜN GÜVENLİK ÖNLEMLERİ

- Kritik altyapı sistemlerine yönelik elektronik tehditlerin detaylı olarak incelenmesi ve önlemlerin belirlenmelidir.
- Kritik altyapı sistemlerine yönelik elektronik tehditler, bilgisayar sistemlerine uygulanabilecek tehditlerden farklı değildir.
- Kritik Altyapıları korumaya yönelik olarak:
  - Kritik altyapı sistemlerine olan erişim yöntemleri,
  - Kritik altyapı sistemlerinin güncelleme ve destek yönetimleri,
  - Yazılım ve yapılandırma hataları karşısında alınacak tedbirler
- Gerekli güvenlik prosedürleri geliştirilmeli;
- Prosedürler eksiksiz ve periyodik aralıklar ile uygulanmalıdır.

# KRİTİK ALTYAPILARA YÖNELİK SALDIRILARA KARŞI ALINACAK ÖZGÜN GÜVENLİK ÖNLEMLERİ

- Kamu/kurumsal sistem güvenlik duvarları, anti virüs yazılımları ile korunmaktadır.
- Ağlar ihtiyaca göre:
  - Dış ağlardan izole bir yapıda hizmet vermekte,
  - Dış Ağlar ile çevrimiçi bağlantı gerekmektedir.
- İzole ağlar farklı güvenlik prosedürleri ile yönetilebiliyor
- Dış ağlar ile çevrimiçi bağlantı ihtiyacı olan ağlar, saldırılara daha açık olabiliyor.

## Sanal Hava Boşluğu (SAHAB) Sistemi

Yaygın olarak kullanılan güvenlik duvarı anlayışını bir adım öteye taşıyan Sanal Hava Boşluğu Sistemi gerçek zamanlı hizmet alan/veren kuruluşlar için gündemde olan güvenlik tehditlerine karşı durmak ve onları ortadan kaldırmak amacıyla tasarlanmıştır.

SAHAB, yönlendirilebilir bir protokolün doğrudan yüksek güvenlik seviyesine sahip ağa erişmesini engellemektedir.

## Sanal Hava Boşluğu (SAHAB) Sistemi

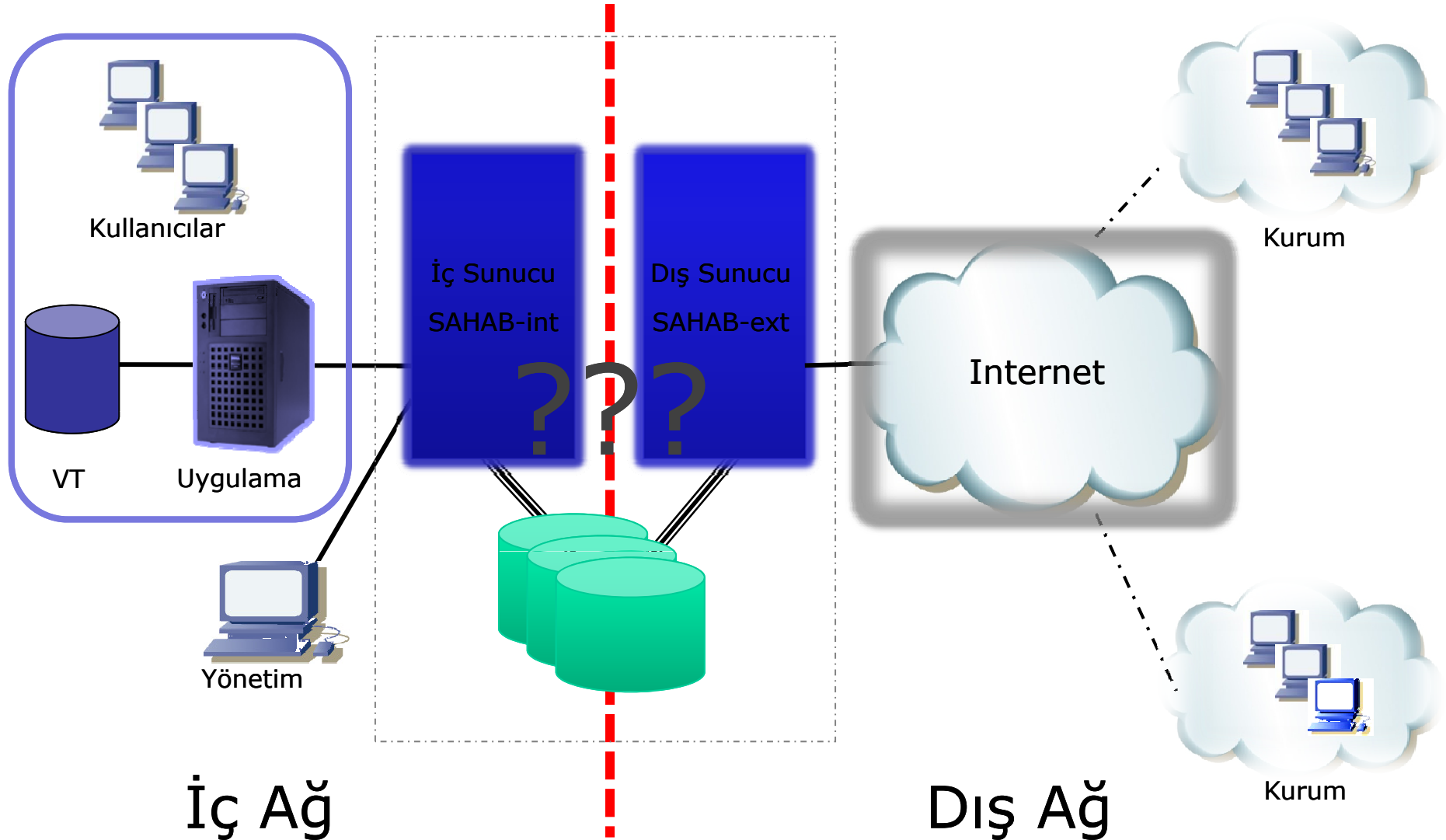
Yaygın olarak kullanılan güvenlik duvarı anlayışını bir adım öteye taşıyan Sanal Hava Boşluğu Sistemi gerçek zamanlı hizmet alan/veren kuruluşlar için gündemde olan güvenlik tehditlerine karşı durmak ve onları ortadan kaldırmak amacıyla tasarlanmıştır.

# Sanal Hava Boşluğu (SAHAB) Sistemi

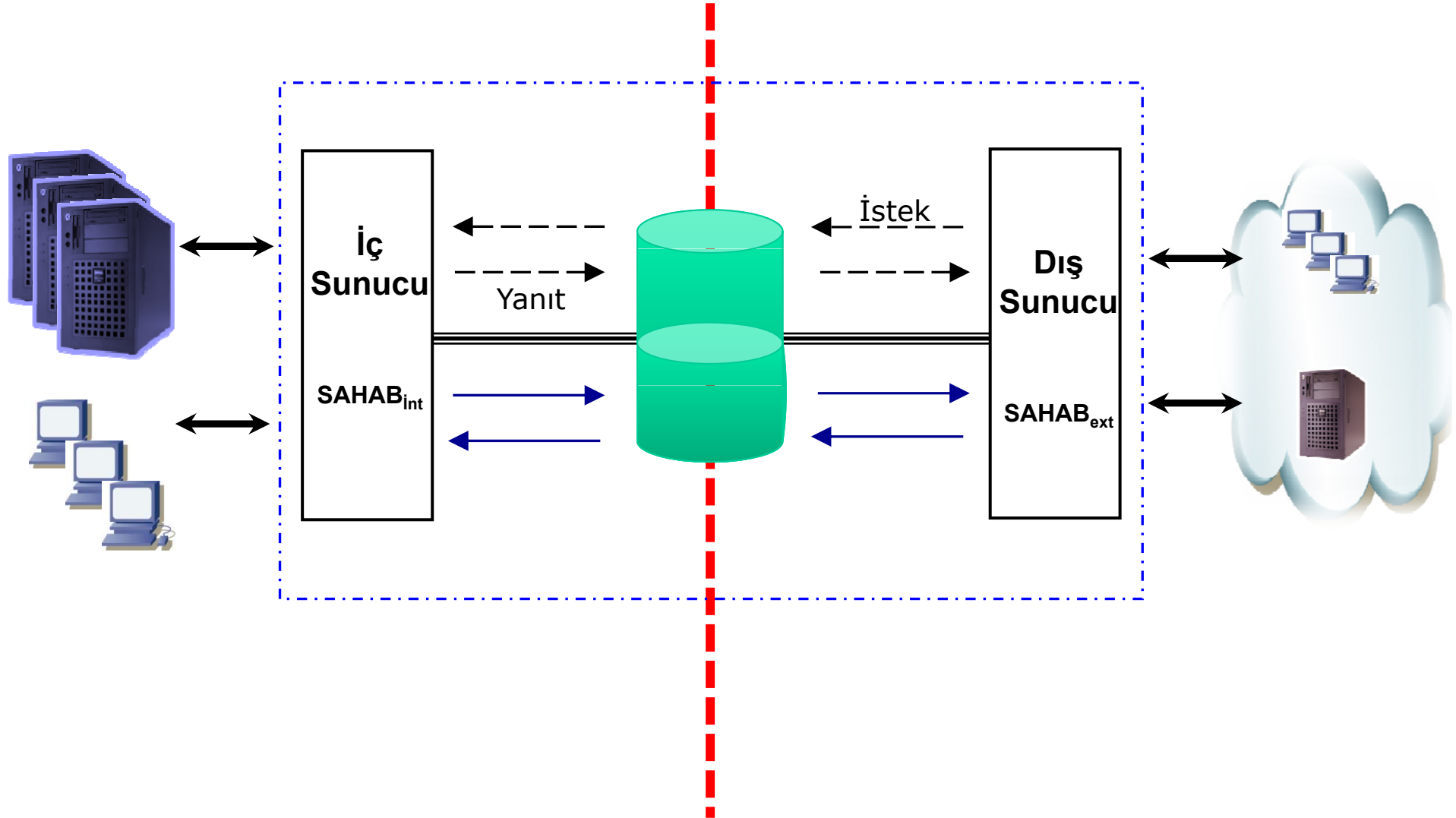
- Gizlilik seviyesi daha düşük bir ağdan gizlilik seviyesi daha yüksek bir ağa gerçek zamanlı güvenli iletişim sağlamak,
- Denetimsiz doğrudan veya dolaylı yoldan erişime izin vermemek,
- Gizlilik Derecesi yüksek olan ağın güvenliğini korumak.



# Sanal Hava Boşluğu - SAHAB



# SAHAB İletişim Modeli



# Sanal Hava Boşluğu (SAHAB) Sistemi

Bir ağ güvenliği çözümü:

- Ağ kullanıcıların kimliklerinin belirlenmesi
- Kayıtlı IP'leri optimize şekilde kullanma
- Ağ trafiğinin tümünün içeriğine güvenlik politikasını uygulama
- Saldırıları gerçek zamanlı olarak belirleme ve önlem alma
- Denetim bilgilerinin tümünün kayıtlarını tutma özelliğine sahip olmalıdır.

# SONUÇ

- Ülkemizde kritik altyapı ve güvenlik bilincinin henüz olgunluk seviyesine ulaşmamıştır,
- Üst düzey devlet yönetimince konu ile ilgili olarak yeterli ve ciddi çalışmalar henüz gerçekleştirilmemiştir.
- Kritik Altyapı Güvenliği'nin yetkili birimlerce sahiplenilmesi, gerekli yasal düzenlemelerin yapılması ve toplumsal bilincin artırılması gerekmektedir.
- Kritik altyapılar belirlenmeli ve bu tesislere yönelik güvenlik riskleri ve tehditler belirlenmelidir.
- Tespit edilecek isk ve tehditler çerçevesinde belirlenecek güvenlik politikaları eksiksiz uygulanmalıdır.
- Kritik altyapıların siber saldırılara karşı korunmasında güvenlik duvarı, anti virüs yazılımlarının yanı sıra sistem yalıtımını sağlayan SAHAB ve haberleşme trafiğini şifreleyen kriptoloji cihazlarının mutlaka yapılandırılması gerekmektedir.
- Güvenlik hedefleri iyi belirlenmiş, güvenlik prosedürleri eksiksiz uygulanan ve temel sayısal güvenlik bileşenleri ile korunan altyapılar, sayısal saldırılara karşı daha dirençli hale gelebilecektir.

## SONUÇ

Kritik altyapıların güvenliğinin sağlanmasında en önemli faktörün ise insan faktörü olduğu hiçbir zaman unutulmamalıdır.



Teşekkürler...