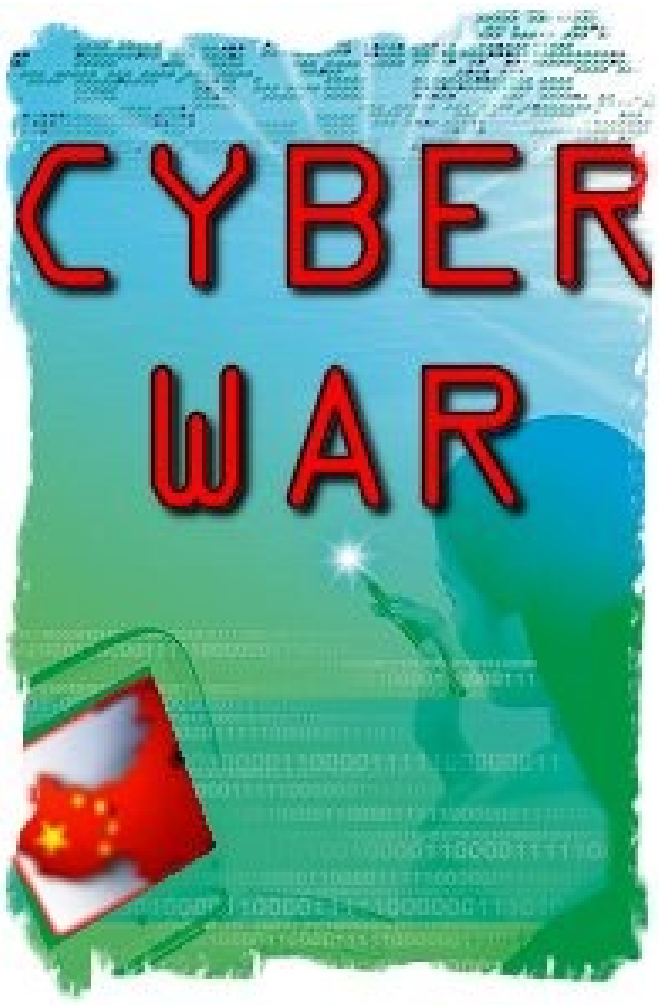


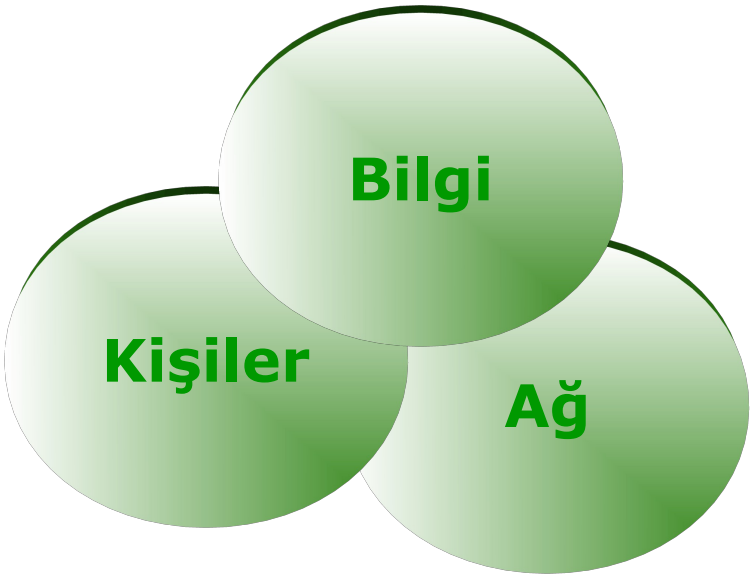
aselsan

Güvenli Bilgi Paylaşımı ve SAHAB

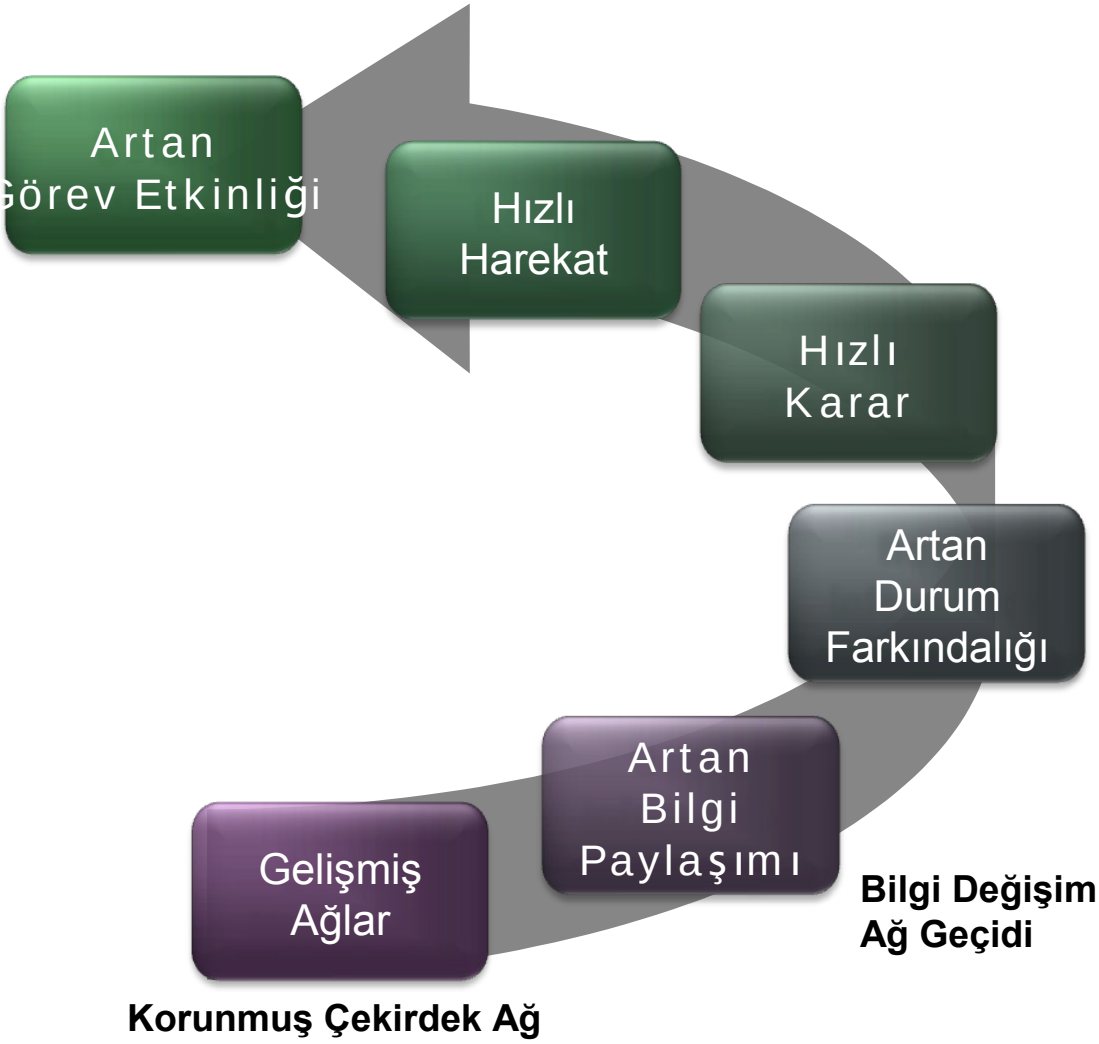
Ali YAZICI

Ağ Destekli Yetenek (NEC) Tanımı

"Stratejik seviyeden taktik seviyeye kadar, bir bilgi ve ağ altyapısı kullanılarak, askeri / sivil harekat ortamının yönetilmesi yeteneği"



Ağ Destekli Yetenek Gelişme Halkası

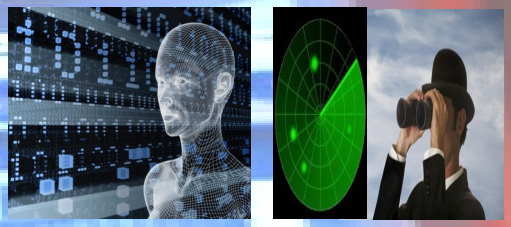


Ağ Destekli Yetenek

- Güvenli bilgi paylaşımı
  - Doğru bilgi,
  - Doğru zaman,
  - Doğru yer,

Bilgi Güvencesi

Siber Savaş

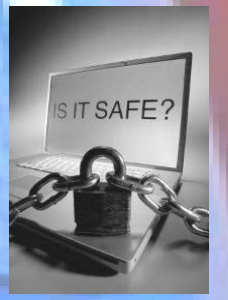


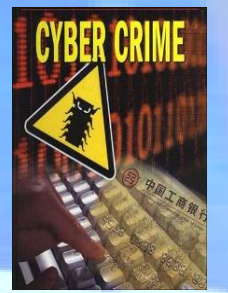
- **Siber Savaş,**
  - **Saldırı:** Ekonomik, politik veya askeri nedenlerle hedef seçilen ülkeye bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılardır.
  - **Savunma:** Ülkede yerleşik sivil, askeri ve hükümete ait bilgi ve iletişim sistemlerinin siber saldırılara karşı savunulması,

Çoğrafi sınırlardan bağımsız olarak gerçekleşir

Siber Saldırılar

- Hizmet dısı bırakma, (DoS/DDoS)
- Web sayfalarının ele geçirilmesi,
- Gizlilik dereceli bilgilerin ele geçirilmesi, değiştirilmesi, silinmesi,
- Kritik sistemlere yönelik saldırılar (enerji, iletisim, finans, güvenlik altyapısı vb.)



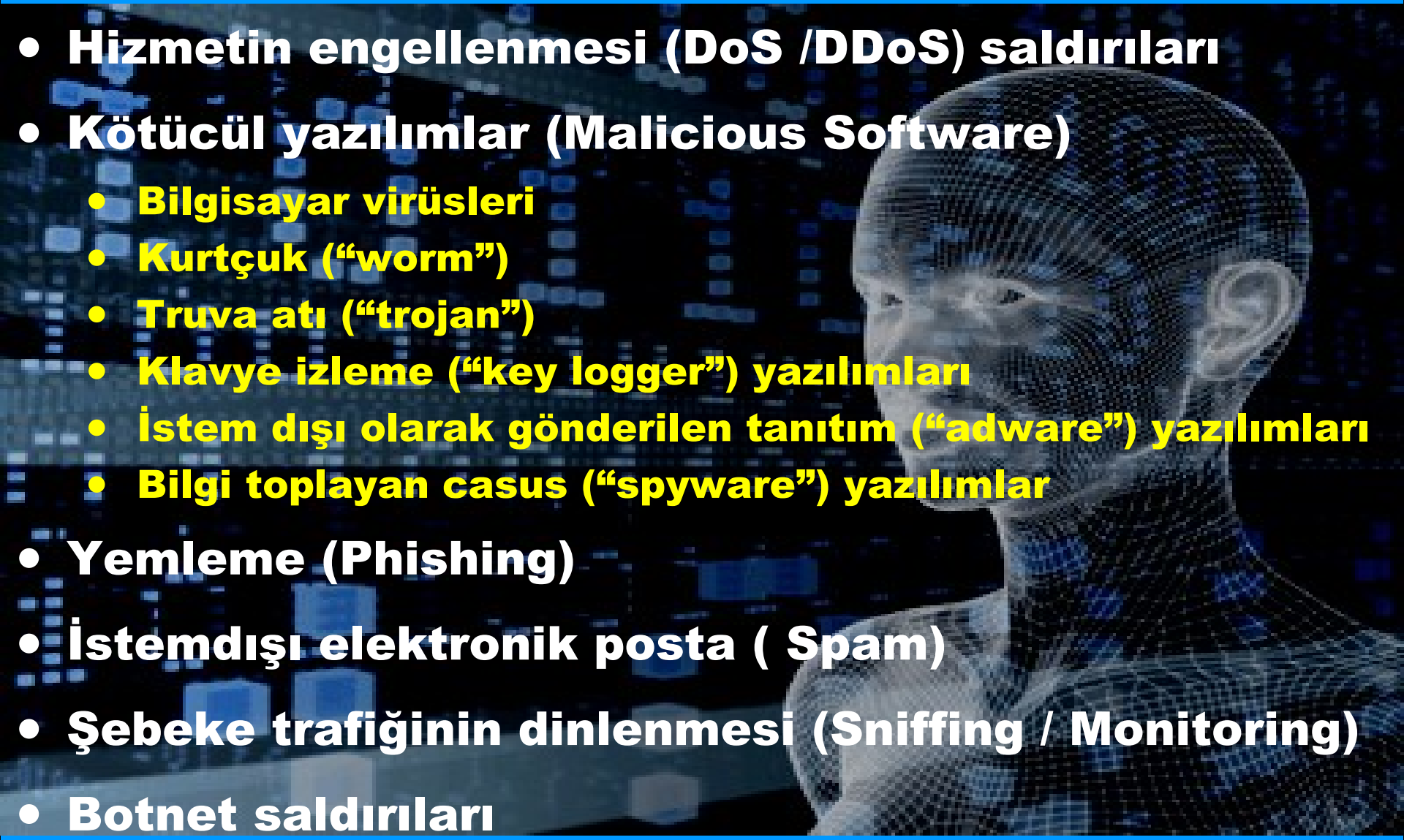


Siber Savaşlara Örnek

- 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.

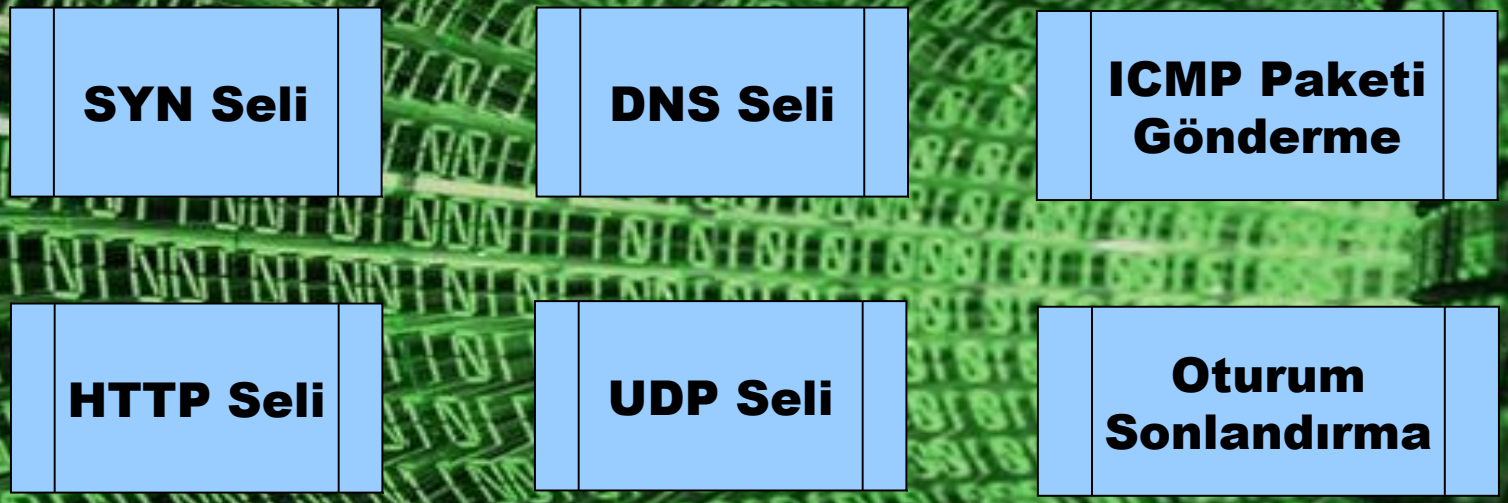
Siber Saldırı Araçları



- 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 / Monitoring)
- Botnet saldırıları

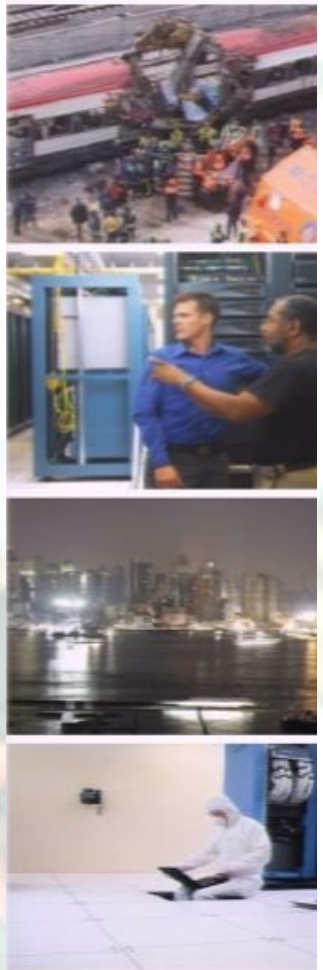
DDoS Saldırıları

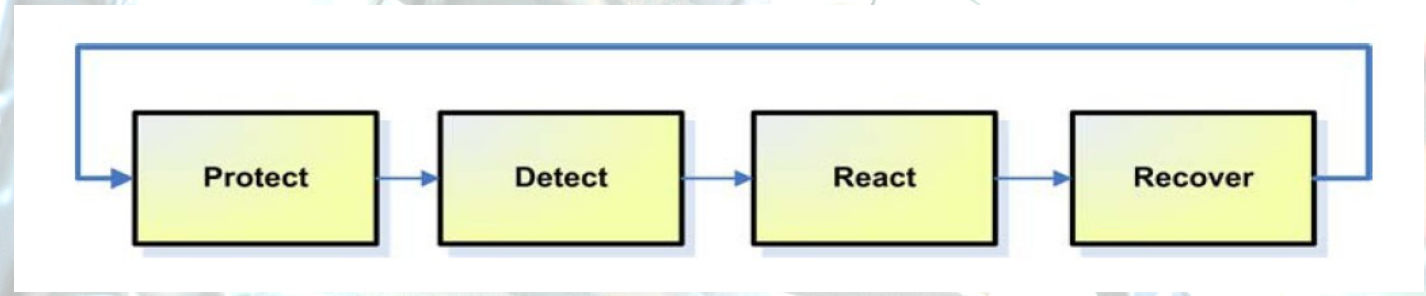
- **DDoS-Dağıtık Hizmet Dışı Bırakma Saldırıları;**
  - Bandgenişliği Doldurma,
  - Kaynak Tüketimi,



Siber Saldırı Amaçları

- **Sistemlere 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
  - İnkar Edilemezlik
  - Kimlik Doğrulama
  - İletişim Güvenliği

Siber Tehditlerin Gelişimi

Basit Sistemler

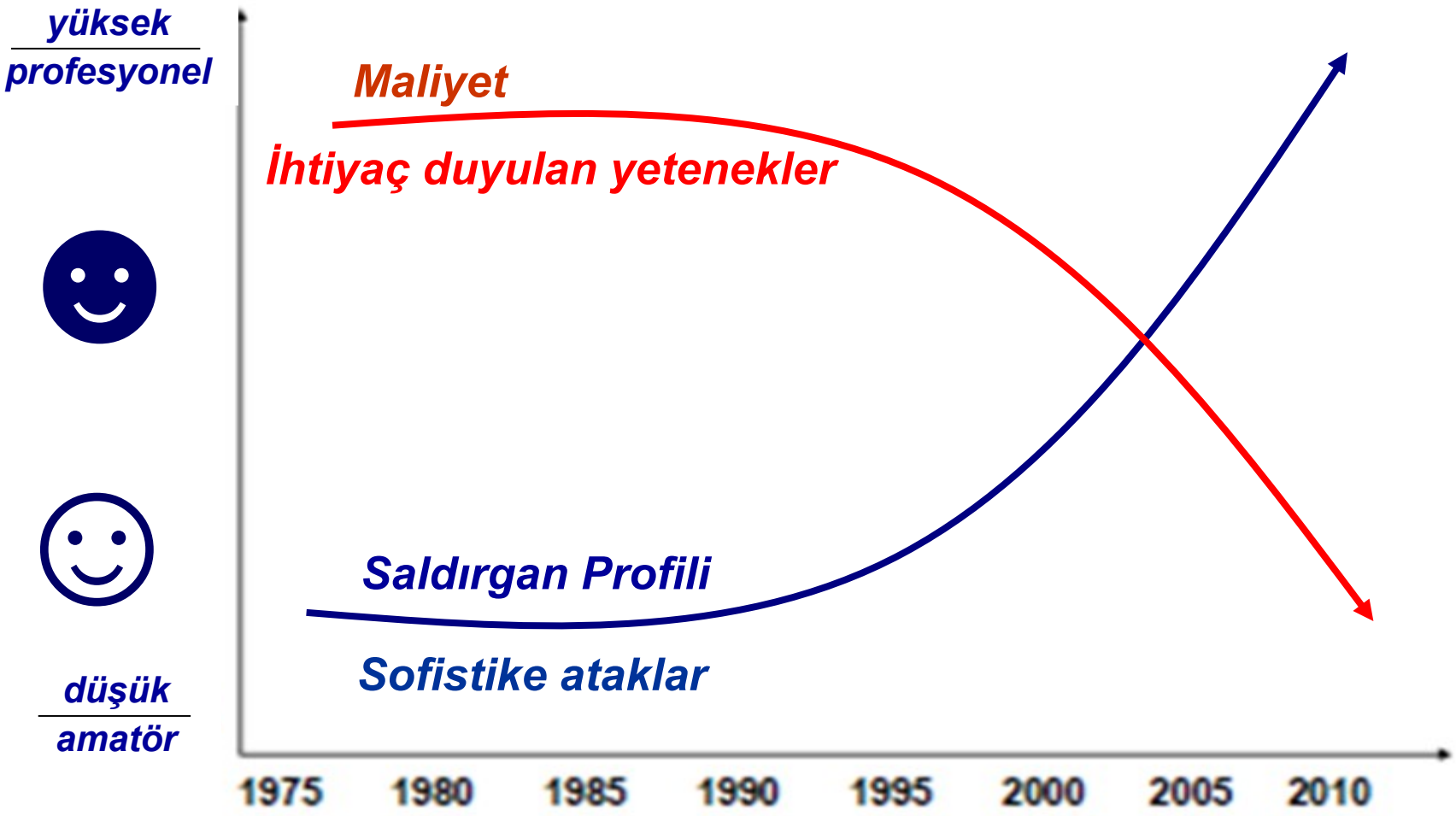
Kompleks Sistemler

DÜN	BUGÜN	YARIN
Hedefler: **İşletim Sistemleri** •Microsoft •Linux •Solaris	**Hedefler:** **Uygulamalar** •Veritabanları •Yazılım paketleri •WEB tabanlı uygulamalar	**Hedefler:** **Yeni Nesil Teknolojiler** •Sanal Sistemler •Ağlar •Yazılım Hizmetleri (SaaS/ ITSaas)
Saldırgan Profili: •Az eğitimli •Şöhret amaçlı **Saldırı Çeşitleri** •E-mail sistemleri aracılığıyla virüs yaymak	**Saldırgan Profili:** •İyi eğitimli •Maddi kazanç elde etmek **Saldırı Çeşitleri** •Web siteleri aracılığıyla malware yaymak	**Saldırgan Profili:** •Deneyimli •Servis sağlayıcılara yönelik saldırılar •Bot saldırıları **Saldırı Çeşitleri** •Polimorfik saldırılar

Az eğitimli

Profesyonel

Siber Tehditlerin Gelişimi



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.**

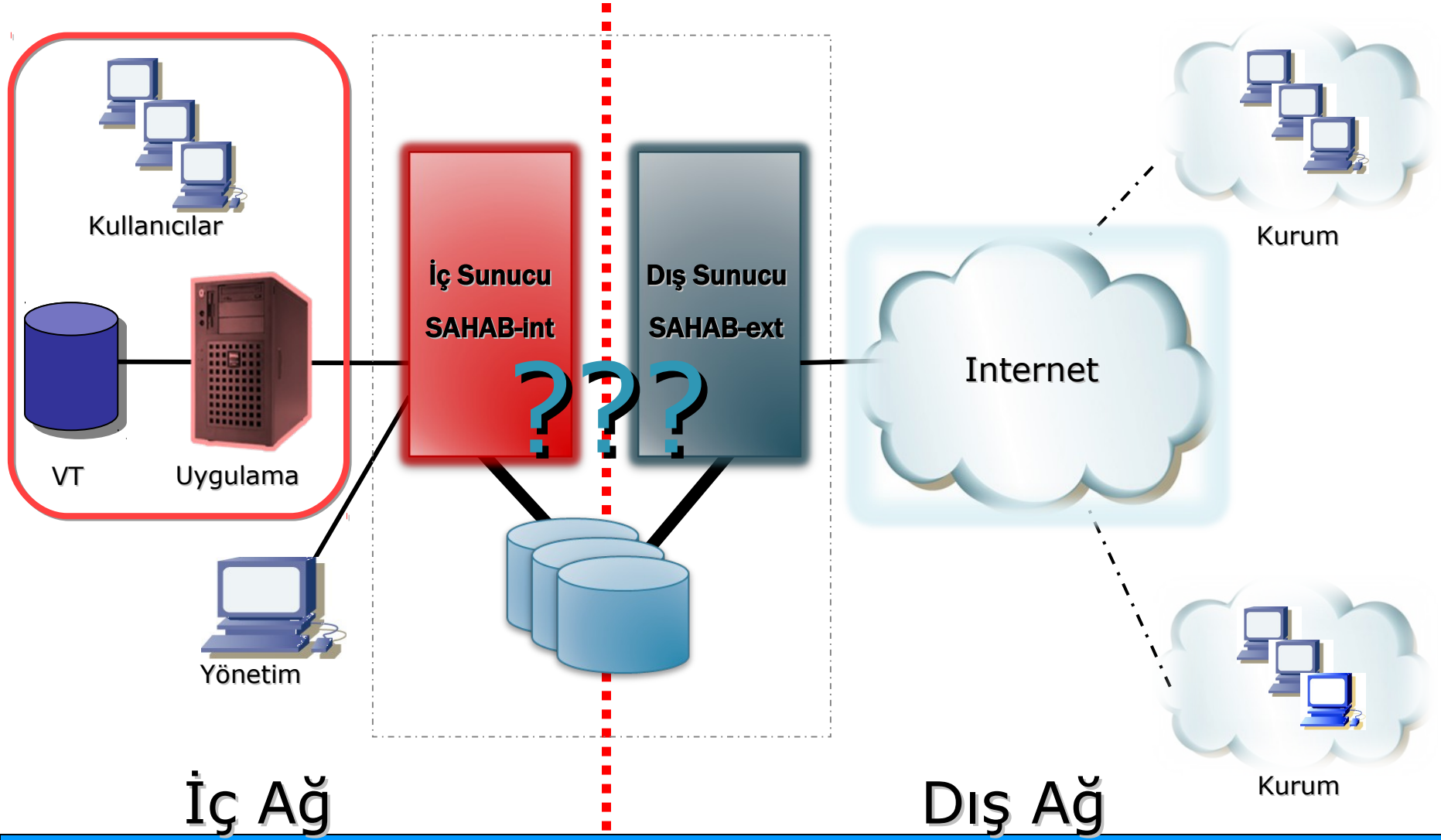
Siber Saldırılara Milli Çözümler

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

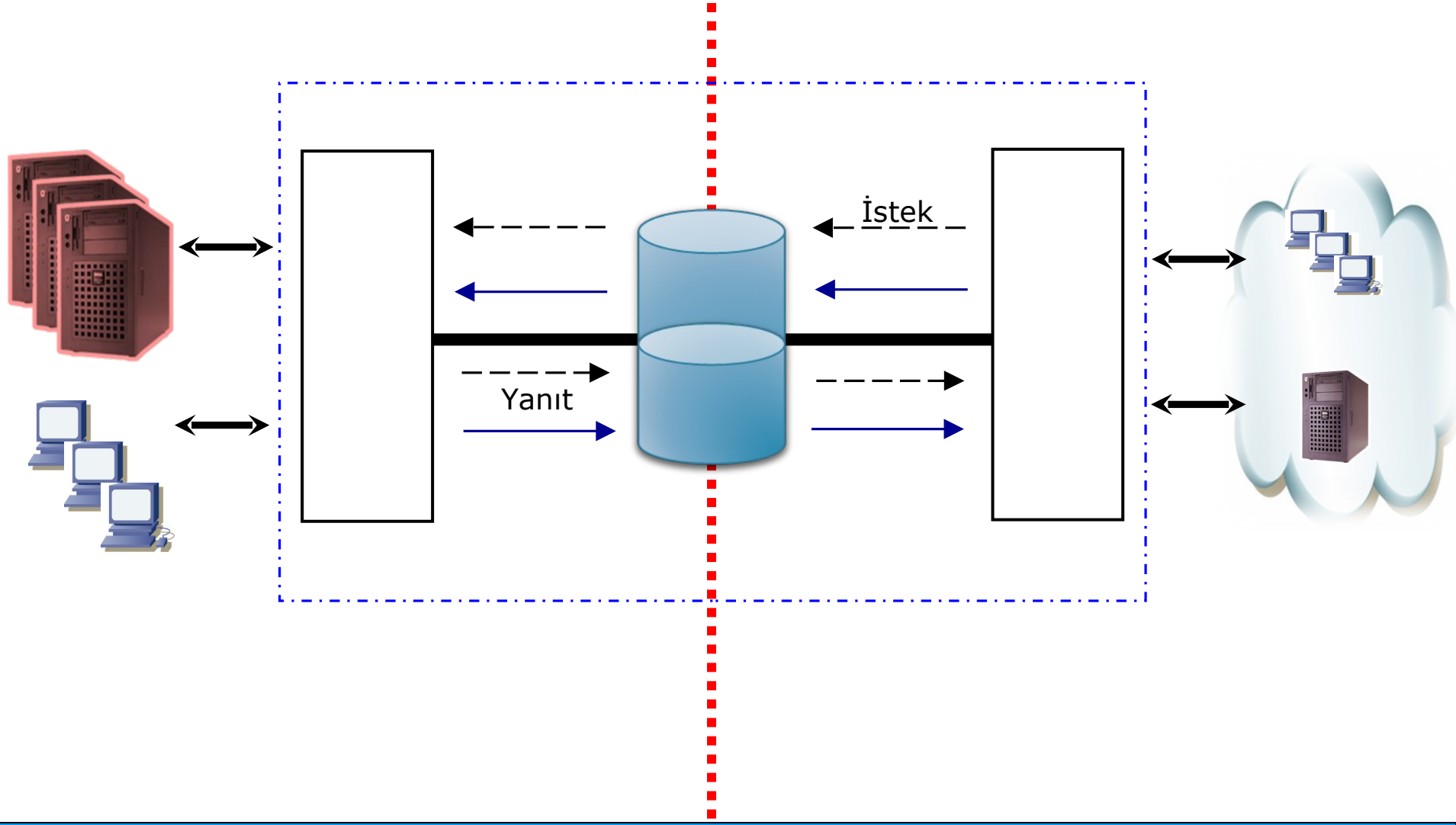
Sanal Hava Boşluğu - SAHAB

- 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

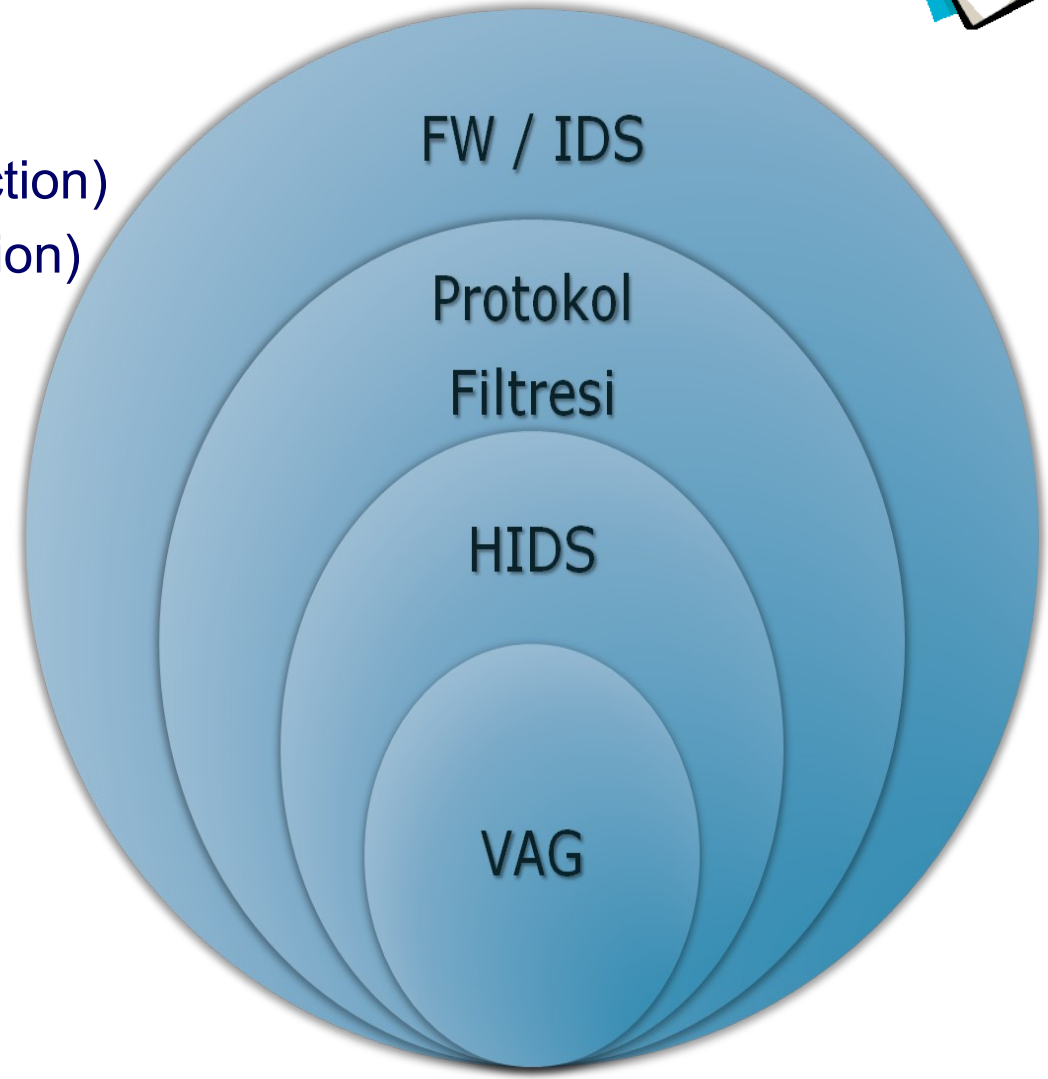


SAHAB İletişim Modeli

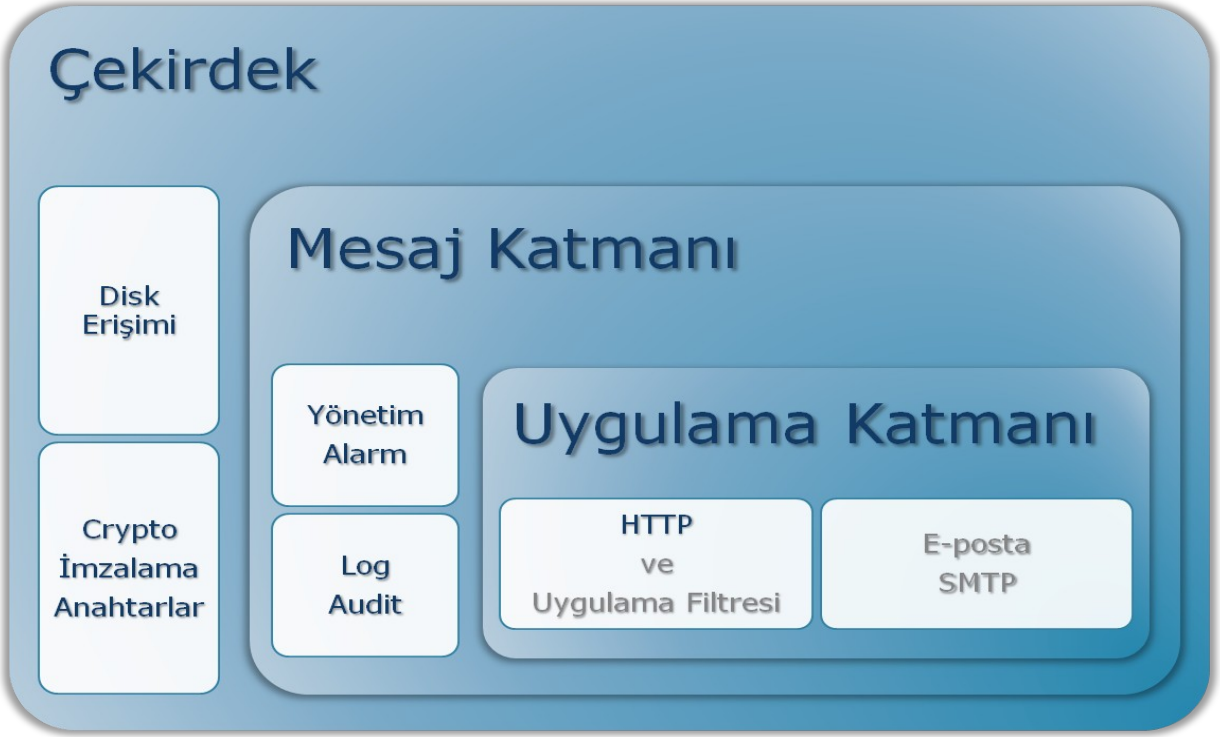


SAHAB Bileşenleri

- **Koruyucu Bileşenler**
  - Güvenlik Duvarı (Firewall)
  - Saldırı Tespit (Intrusion Detection)
  - İmzalı kodlar (Trusted Execution)
  - Şaşırtma (Obfuscation)
  - Bütünlük denetimi (HIDS)



SAHAB Bileşenleri

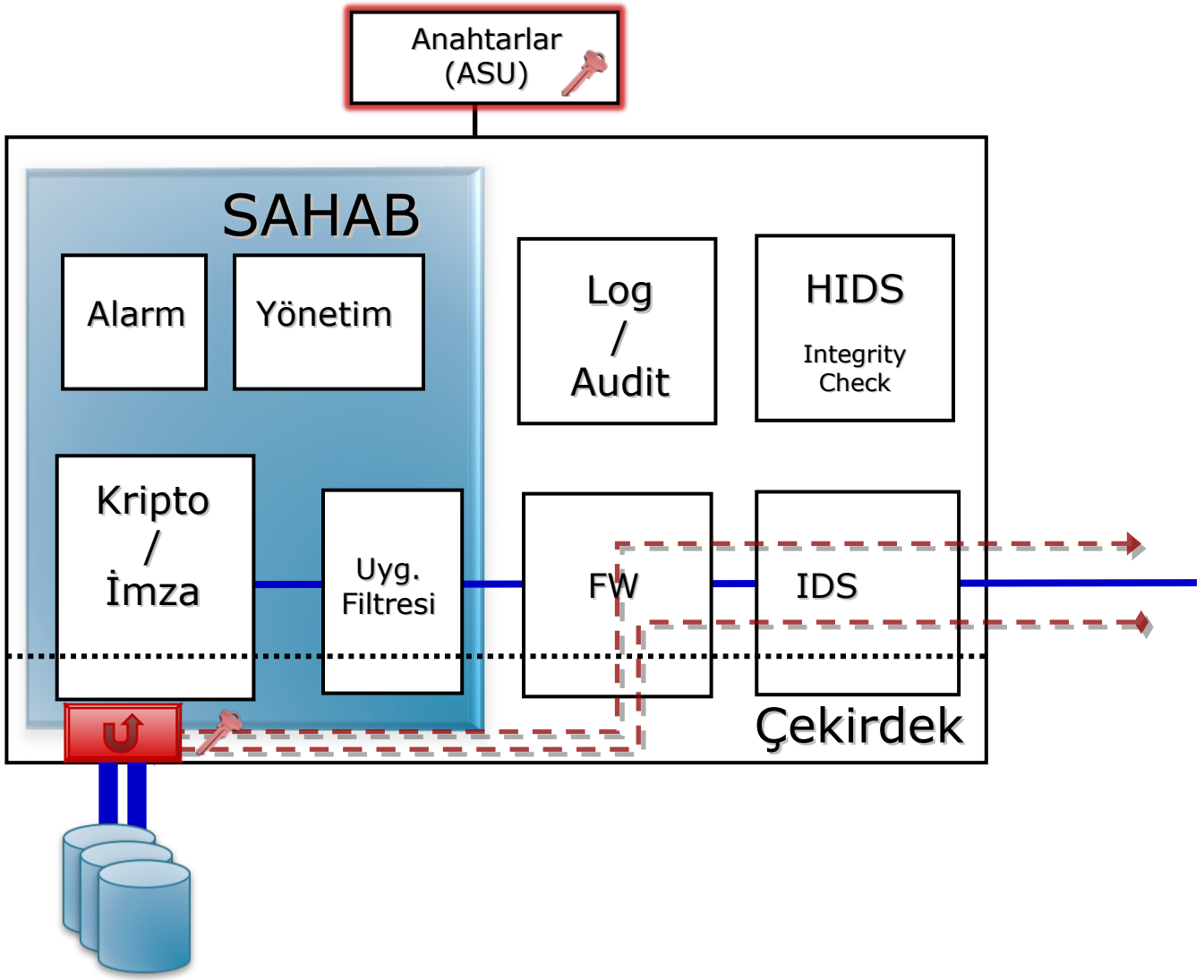


- **3 Katmanlı Yapı**
  - Uygulama katmanında çoklu protokol desteği
    - HTTP, FTP, E-posta, vb.
  - Protokol'den bağımsız mesaj katmanı
  - Güvenli Disk Erişimi ("Air Gap") (Çekirdek)

Common Criteria

EAL4+

SAHAB Sunucu Mimarisi



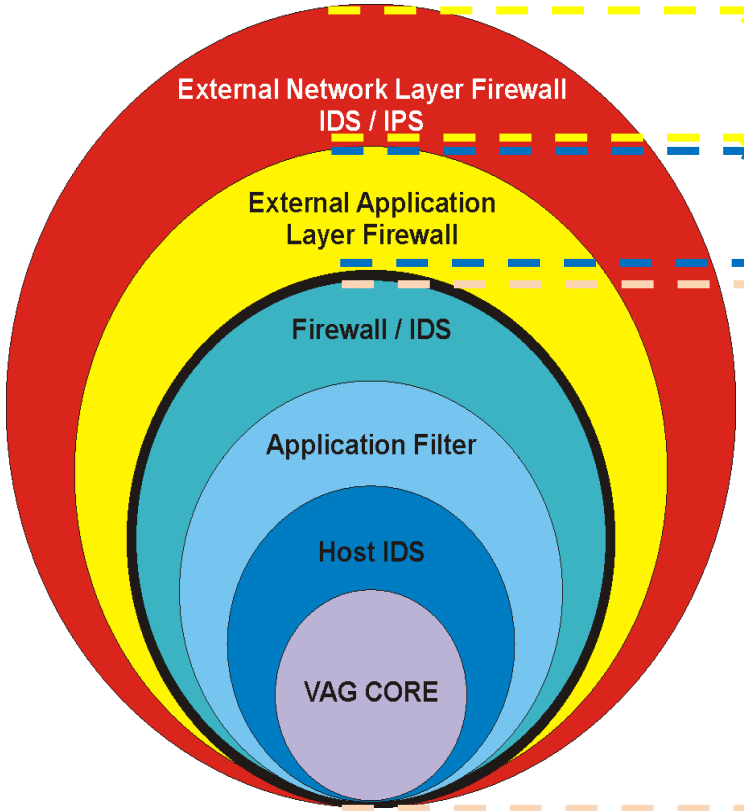
SAHAB Temel Özellikleri

- **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

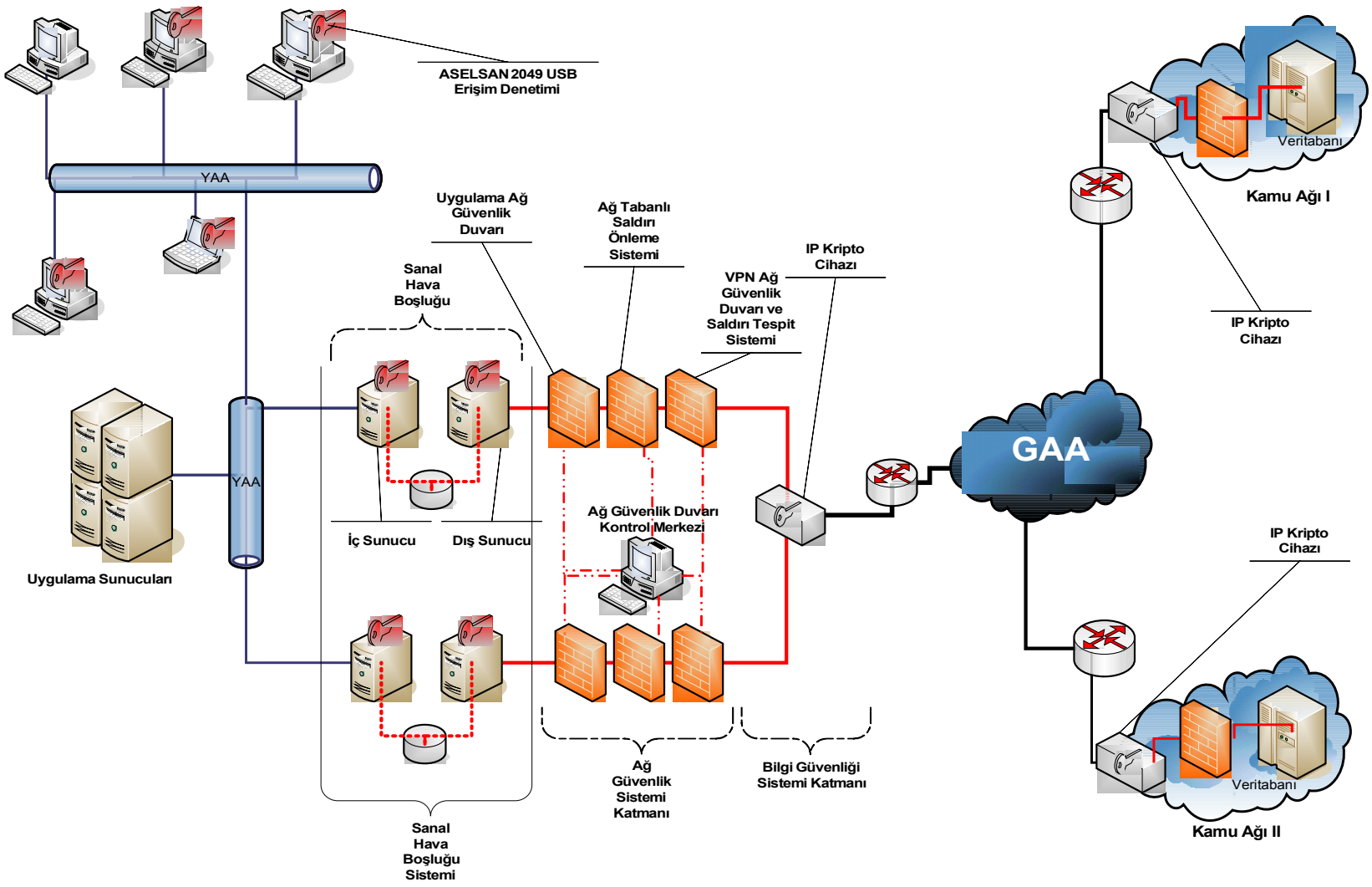
SAHAB Güvenlik Özellikleri



TCP/IP REFERENCE MODEL

- Application Layer
- Transport Layer
- Network Layer
- Host - To - Network

2180 SAHAB Genel Mimari



Siber Saldırılara Milli Çözümler

- Sanal Hava Boşluğu-SAHAB,
- **Yeni Nesil IP Ağ Kripto Cihazı-2064,**
- 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 Mbits Ethernet Arayüzü
- SDIP-27 TEMPEST Uyumlu
- Manual ve Elektronik Anahtar Yükleme
- Web Tabanlı Yerel ve Uzak Yönetim Arayüzü (SNMP)

Desteklenen Protokolleri

- **IP**
- **ARP**
- **ICMP**
- **OSPF**
- **BGP**

2064 IP Ağ Kripto Cihazı

Mobil IP Desteği

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

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

Siber Saldırılara Milli Çözümler

- Yeni Nesil IP Ağ Kripto Cihazı-2064,
- Sanal Hava Boşluğu-SAHAB,
- **Emniyetli Sabit Disk-2195**

2195 Emniyetli Sabit Disk

- Harici ve dahili kullanım,
- Fiziksel seviyede kriptolama,
- Kullanıcıdan saydam olarak gerçekleştirilen kriptolama ve kripto çözme işlemleri,
- İşletim sistemi ve Servis Paketi bağımsız çalışabilme, (Windows / Linux / Unix),
- Donanım yapılı kriptolama,
- Acil silme / kurcalamaya karşı koruma
- IDE, SATA ve USB arayüz desteği,

Sorular…