



# **ULUSAL BİLGİ SİSTEMLERİ GÜVENLİK PROGRAMI**

**Hayrettin Bahşı**

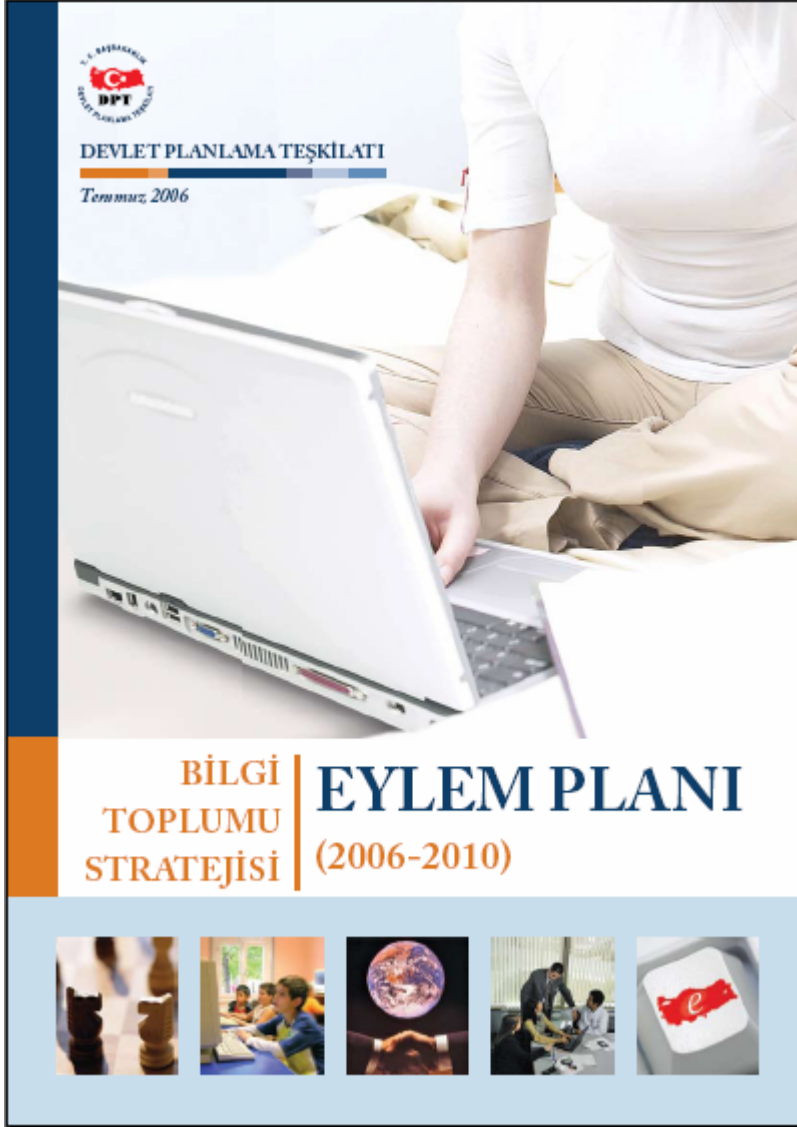
**[bahsi@uekae.tubitak.gov.tr](mailto:bahsi@uekae.tubitak.gov.tr)**

**6 HAZİRAN 2008**

Ulusal Bilgi Sistemleri Güvenlik Programı nedir?

Programın ana hedefleri

Programın alt projelerinin tanıtımı



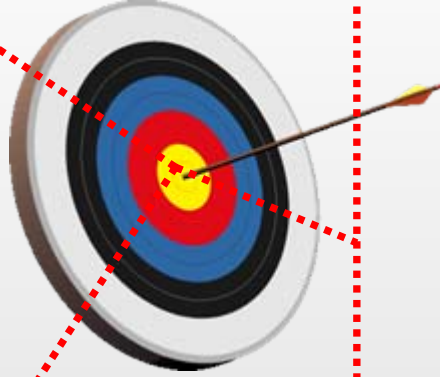
## 88 numaralı madde: Ulusal Bilgi Sistemleri Güvenlik Programı

Sorumlu ve İlgili Kuruluşlar:

TÜBİTAK-UEKAE (S)  
Kamu Kurum ve Kuruluşları (İ)  
Üniversiteler (İ)

2007 Ocak – 2008 Aralık

Bilgi sistem güvenliği ile ilgili bilgi ihtiyacının karşılanması



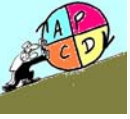
Ülkemizin bilgisayar olaylarına acil müdahale koordinasyon merkezini kurmak

Kamu kurum ve kuruluşları için:

1. Minimum güvenlik gereksinimlerini belirlemek
2. Bilgi sistem güvenliği ile ilgili tehditleri tespit etmek
3. Bilgi sistem güvenliği eksiklikler konusunda önerilerde bulunmak
4. Bilgi sistem güvenliği ile ilgili acil uyarılar yapmak
5. Bilgi güvenliği yönetim sistemi konusunda pilot kurumlara danışmanlık vermek
6. Bilgi sistem güvenliği ile ilgili eğitimler vermek



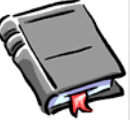
Bilgisayar Olayları Müdahale Koordinasyon Merkezi



Bilgi Güvenliđi Yönetim Sistemi Danışmanlık Projeleri



Sanal Ortam Savunma Merkezi Kurma Projesi



Bilgi Sistemleri Güvenliđi Dokümantasyon



Ulusal Bilgi Güvenliđi Kapısı



Bilgi Sistemleri Güvenlik Eđitimleri

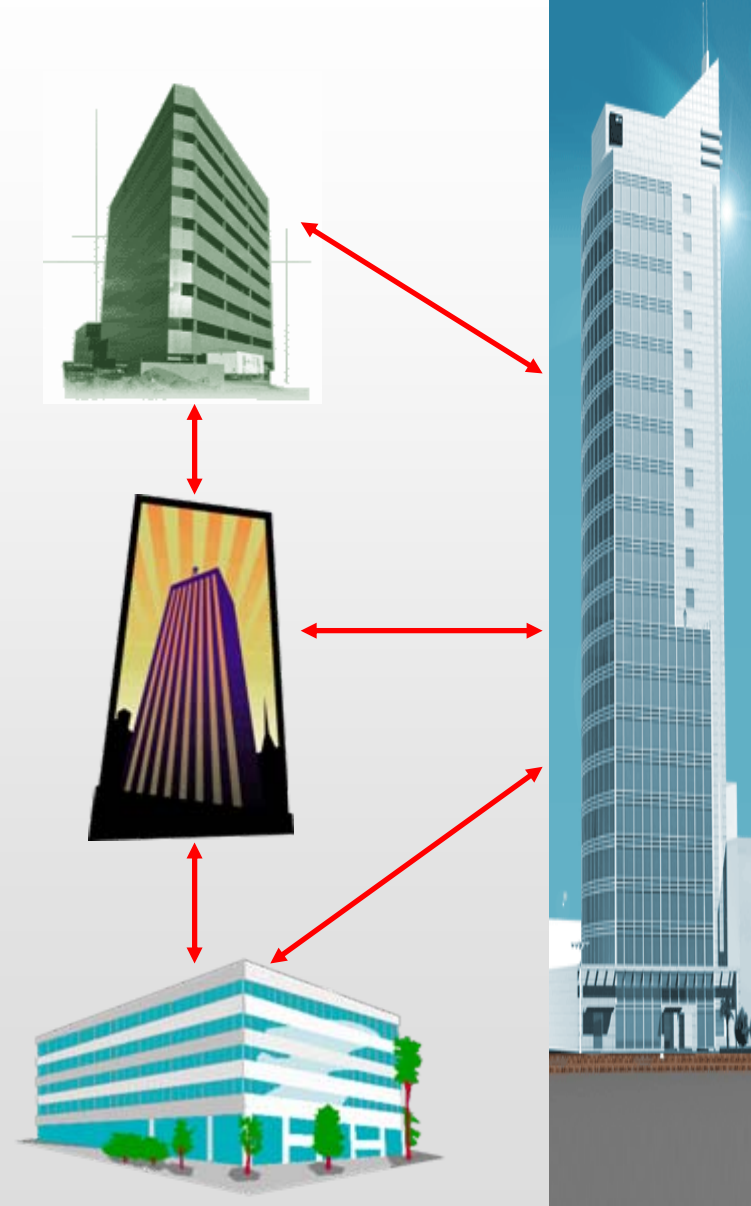


- Bilgi güvenliği olayı yaşama olasılığı
- Bilgi güvenliği olaylarına müdahale yeteneği
- Kurumda,
  - Bilgisayar olay müdahale takımı oluşturma
  - Bilgisayar olay müdahale süreci oluşturma
    - Olay tespiti ve kayıt altına alma
    - Olay müdahale



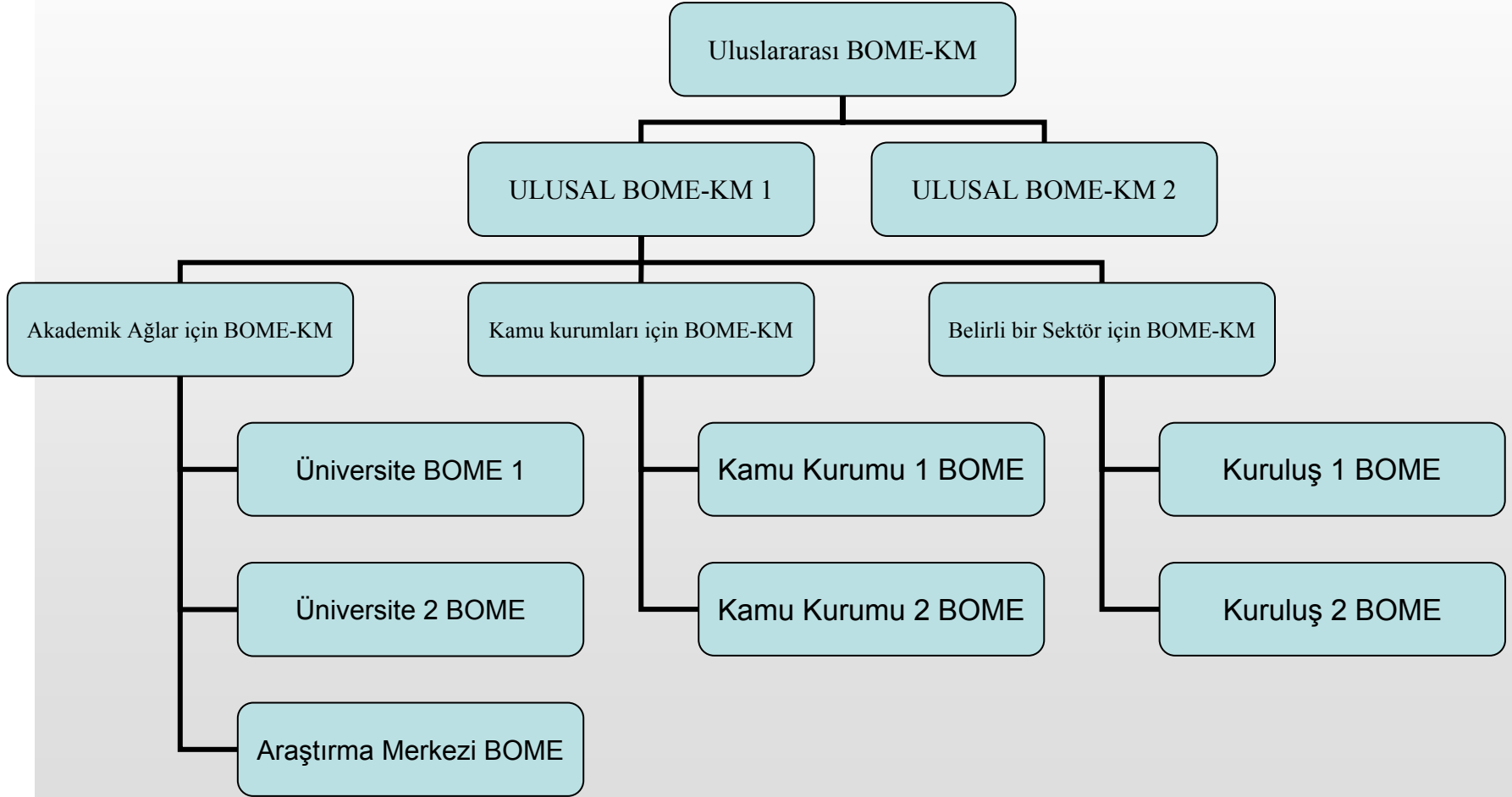


- Kurumlararası ilişkiler
  - Korunmak için iş birliği
  - Diğer kurumlarla koordinasyon gereksinimi
    - Güven ilişkisi oluşturma
    - Ulusal ve uluslararası
    - Olay engelleme imkanının başka kurumlarda olabilmesi
  - Acil bilgi güvenliği ikazları oluşturma ve paylaşma





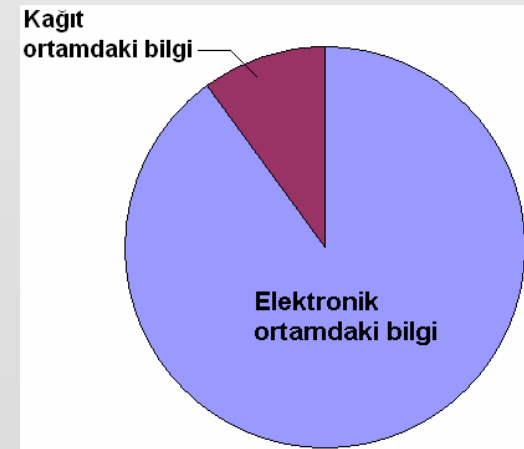
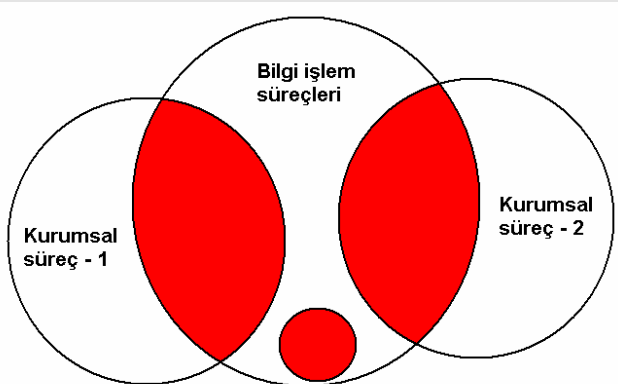
- Bilgisayar olayları müdahale ekipleri koordinasyon merkezleri (BOME-KM) hiyerarşisi





- Ulusal BOME-KM kurulması çalışması
  - Kamu kurumlarına BOME kurulum danışmanlığı
    - Başbakanlık
    - Sayıştay Başkanlığı
    - Adalet Bakanlığı
    - Maliye – Muhasebat Genel Müdürlüğü
    - Tapu Kadastro Genel Müdürlüğü
    - Sermaye Piyasası Kurulu
    - Merkez Bankası
    - Dış Ticaret Müsteşarlığı
    - Hazine Müsteşarlığı
  - Diğer ulusal BOME-KM'ler ile ilişkilerin geliştirilmesi faaliyetleri
  - Olay ihbarı koordinasyonu
- Akademik ağ (Ulak-Net) için Ulak-CSIRT
  - TÜBİTAK-Ulusal Akademik Ağ ve Bilgi Merkezi bünyesinde

- Bilgi güvenliđi yönetim sistemi (BGYS) ihtiyacı
  - Bilgi güvenliđine kurumsal yaklaşım
  - Yazılı bilgi güvenliđi politika ve prosedürler
  - Kurumsal bilgi güvenliđi – kullanılabilirlik dengesi
    - Risk odaklı koruma
- ISO 27001 temelli yaklaşım
- Pilot kurumlara BGYS danışmanlıđı





- Pilot kurumlar
  - Başbakanlık
  - Sayıştay Başkanlığı
  - Adalet Bakanlığı
  - Maliye – Muhasebat Genel Müdürlüğü
- Yapılan çalışmalar
  - BGYS kapsamının belirlenmesi
  - Varlık envanterinin oluşturulması
  - Bilgi güvenliđi koordinasyon kurullarının oluşturulması ve işlerlik kazanması
  - Risk analizi çalışmaları



- Tehditlerin profilinin deęişmesi
- Siber savař beklentisi
- Estonya örneęi
- Kamu kurumlarına ait kritik sistemlerini hedef alan tehditlerin tespiti
  - Birden fazla kurumu hedef alan koordineli saldırıların tespiti
  - Bir kamu kurumunu hedef alan tehditlerin tespiti

- Tehditlerin genel profilinin belirlenmesi
  - Genel tehdit gözlem raporlarının oluşturulması
    - Tehdit türleri, dağılımı, etki analizi
  - Genel tedbirler alınarak uygulanması
    - Eğitim
    - Acil uyarı mekanizmaları
    - Teknik tedbirler



- Sistemin teknolojik altyapısı
  - Farklı bilgi sistem kaynaklarının ilişkilendirilmesi
    - Güvenlik duvarı (Firewall) kayıtları
    - İşletim sistemi kayıtları
    - Saldırı tespit sistemlerine ait kayıtlar
  - Dağıtık balküpe (honeypot) sistemleri
- Gerçekleştirilen çalışmalar
  - Kullanılacak temel sistemin belirlenmesi
    - Açık kaynak kodlu sistemler
  - Test ortamında bir prototip oluşturulması
  - Merkez sistem kuruldu
- Yapılacak çalışmalar
  - Gönüllü kamu kurumlarının sisteme dahil edilmesi





- Bilgi sistem unsurlarının en zayıf halkası sistemin güvenliđini belirler
  - İşletim sistemi güvenliđi, uygulama güvenliđi, ağ güvenliđi vs
- Tüm unsurların “yeterince” güvenliđinin sağlanması
- Sistem güvenliđi ile ilgili teknik bilgi ihtiyacı
- Sistem güvenliđi ile ilgili Türkçe doküman azlığı



- BGYS ile ilgili doküman ihtiyacı
  - Bilgi güvenliđi politikası dokümanı nasıl yazılır?
  - İş sürekliliđi planlaması nasıl yapılır?
- Bilgi sistem güvenliđi ile ilgili yayın yapan kuruluşlar
  - NIST (National Institute of Standards and Technology)
  - NSA (National Security Agency)



- Proje kapsamında
  - Bilgi sistem güvenliđi ile ilgili teknik dokümanlar
  - Bilgi güvenliđi yönetim sistemi ile ilgili dokümanlar
  - Yayınlanan doküman sayısı: 25
- Bitirilen teknik dokümanlarına örnekler
  - Kablosuz Ağ Güvenliđi Kılavuzu
  - Web Uygulama Güvenliđi Kılavuzu
  - Yönlendirici (router) Güvenliđi Kılavuzu
- Bitirilen BGYS dokümanlarına örnekler
  - Bilgi Güvenliđi Risk Yönetim Süreci Oluşturma Rehberi
  - Erişim Kontrol Politikası Oluşturma Rehberi
  - Bilgi Güvenliđi Bilinçlendirme Süreci Oluşturma Rehberi



# Ulusal Bilgi Güvenliği Kapısı Projesi

- www.bilgiguvenligi.gov.tr
- Bilgi güvenliği ile ilgili bilgi kaynağı
- Herkesin katkısına açık
  - Bilgi güvenliği ile ilgili makaleler
  - Yayınlanan dokümanlara yorum verebilme
- Bilgi güvenliği dokümanları

The screenshot shows the website's interface with the following elements:

- Header:** "ULUSAL BİLGİ GÜVENLİĞİ KAPISI" logo and navigation tabs: "Hakkımızda", "İletişim/Bilgi Edinme", "Sıkça Sorulan Sorular", "Yorumlarımız", "RSS", "Arama".
- Left Sidebar:** "Ana Menü" with links to "Anasayfa", "Etkinlikler", "Güvenlik Bildirileri", "Teknik Yazılar", "Kılavuzlar", "Duyurular", "Terimler Sözlüğü", "Site İçerisinde Arama", "TR-BÖME KM", "TR-CERT". Below is a user login form with fields for "Kullanıcı Adı", "Parola", and a "Beni habirla" checkbox.
- Main Content Area:**
  - Güncel Açıklıklar:** A list of recent news items including "Debian/Ubuntu OpenSSL Anahtar Oluşturma A...", "Adobe Flash Player Uzaktan Kod Çalıştırma A...", "Creative Software AutoUpdate Engine Active...", "IBM Lotus Sametime Community Services Multi...", and "EMC AlphaStor Çoklu Açıklıklar".
  - Polimorfik Solucan Saldırılarının Tespiti:** An article dated 04.06.2008 by Yazarı: Burak Bayoğlu. The text discusses the detection of polymorphic worms and their impact on network security.
  - Duyurular:** A notice titled "WSUS ile Yama Yönetimi Güvenlik Kılavuzu yayınlanmıştır" (WSUS Patch Management Security Guide published).
  - Anket:** A survey titled "Ulusal Bilgi Güvenliği Kapısı'nı nasıl buldunuz?" (How do you find the National Information Security Gate?).
  - Popüler Teknik Yazılar:** A list of popular technical articles such as "ADSL Modem (Yönetici Arayüzü) Güvenliği - Yönetici Arayüzü Güvenliği - Araştırma", "ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi", "İşletim Sistemleri Güvenliği", "Kişisel Bilgisayarlar için Temel Güvenlik Adımları", and "Teknik Açıklık Yönetimi".
  - Popüler Kılavuzlar:** A list of popular guides including "UEKAE BCYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu", "UEKAE BGT-2002 Güvenlik Durum Güvenliği Kılavuzu", and "UEKAE BCYS-0002 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu".



- Güncel bilgi sistem güvenlik açıklıkları
- Bilgi güvenliđi ile ilgili güncel haberler
- Kamu kurumları için e-posta listeleri
  - Bilgi alış verişı
  - Konularına göre farklılaşmış
- E-posta listelerinin aktif halde kullanılması
- Bilgi güvenliđi ile ilgili duyurular
- Yaklaşık 190 üye, 18'i kamu kurumlarından



- 13 farklı alanda eđitimler, toplam 40 gn
- İki gnden altı gne deđişen eđitim sreleri
- Uygulamaların yapıldığı laboratuvar ortamı
- Örnek eđitimler
  - Web Uygulamaları Güvenliđi, 2 gn
  - Microsoft Sistemler Güvenliđi, 3 gn
  - Veritabanı Güvenliđi, 3 gn
  - İş Sürekliliđi/Felaket Kurtarım Planlama, 3 gn
- Yaklaşık 100 kamu bilgi işlem personeli
- Üç periyot halinde eđitimler verildi
- Üniversite bilgi işlem personeline eđitim verilmesi planlandı

- Programda önemli ilerlemeler kaydedildi
- Programın devamlılığının sağlanması
  - Sanal Ortam Savunma Merkezinin yönetilmesi
  - Ulusal Bilgi Güvenliği Kapısının yönetilmesi
  - Bilgi güvenliği dokümanlarının güncellenmesi ve yeni doküman ihtiyaçları
  - Danışmanlık ihtiyaçlarının devam etmesi
  - Bilgisayar olay müdahale çalışmalarının devamlılığı
- Kamu kurumlarının katkısı



# Teşekkürler Sorular?

**Hayrettin Bahşı**

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