Cyber Security at Smallsats

Ali YAZICI

Türkiye Bilişim Derneği Genel Başkan Yardımcısı

Siber Güvenlik Stratejisti

Uzayda Siber Güvenlik Neden Önemli?

Uydular küçüldü, otonom araçlar haline dönüştü ve uydular arası haberleşme link ihtiyacı arttı

Görev Yükleri: Yazılım Tabanlı çözümlere evrildi, Tedarik zincirleri genişledi

Yer İstasyonları: BT alanındaki yenilikçi çözümleri yaygın olarak kullanmakta (Bulut / Uç Bilişim, YZ)

SALDIRI YÜZEYİ GENİŞLEDİ

Siber Tehditlerin Amacı

- Veriye Erişim
- Veriyi Değiştirme
- Veriyi Silme
- Veriyi Rehin Alma
- Hizmet Engelleme

Siber Güvenlik Tehditleri (2030)

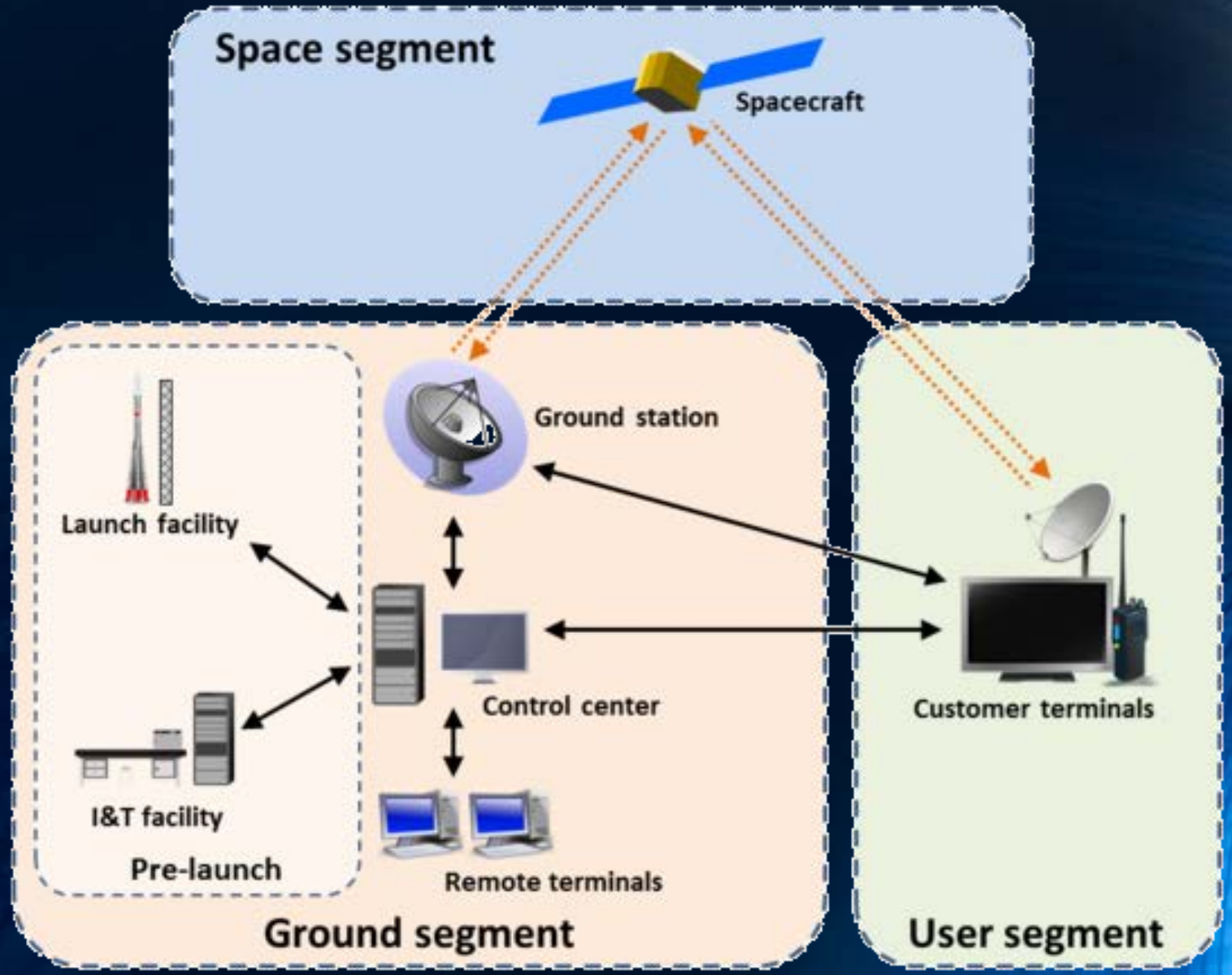
Küçük Takım Uydular

Küçük Uydulara Yönelik Siber Saldırılar

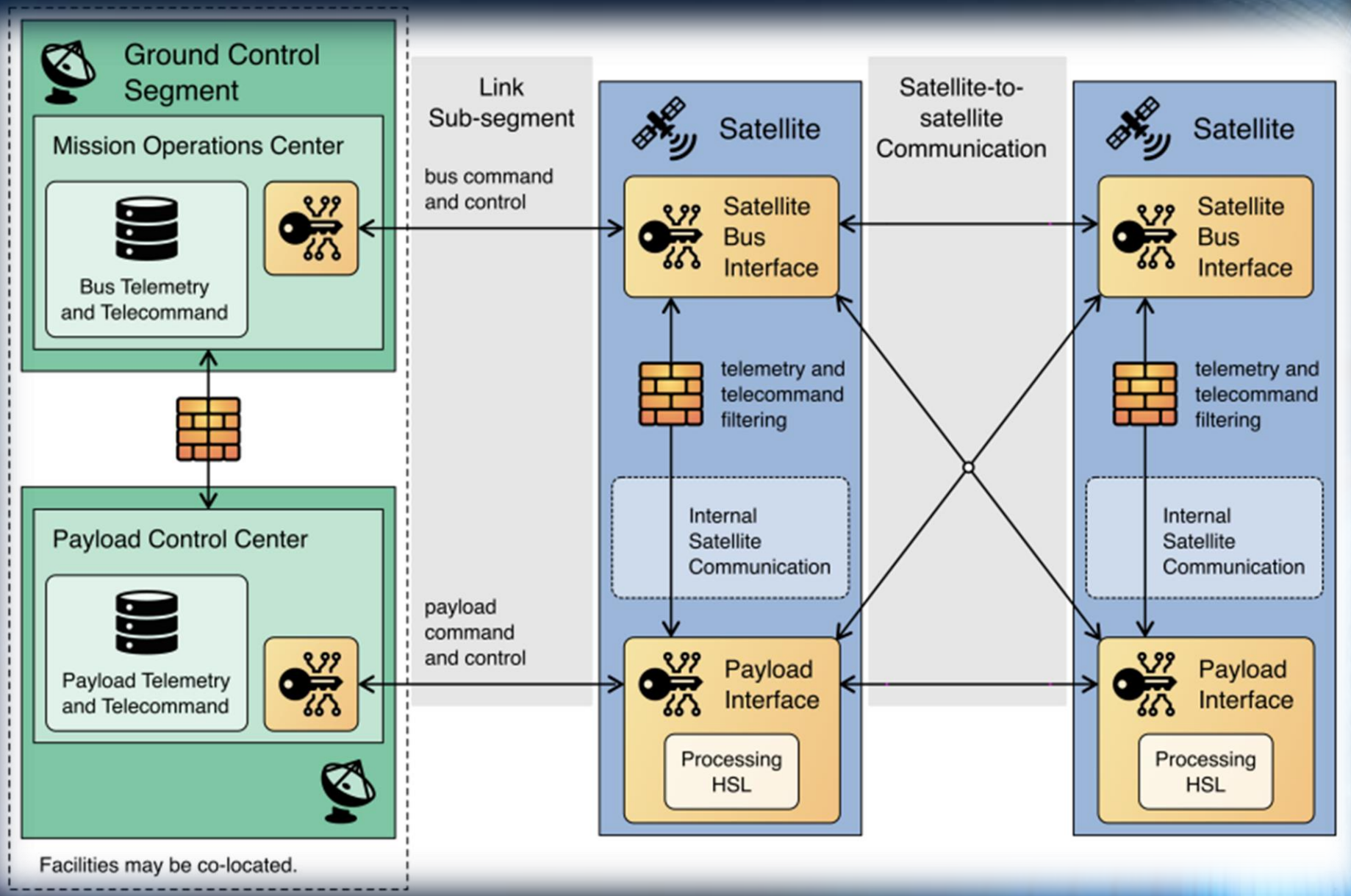
Uydulara Yönelik Siber Saldırılar

- Denial of Service Hizmet Dışı Bırakma
  - Aşağı / Yukarı Link Bastırma, (Jam Uplink, Downlink & inter-satellite Link)
  - Yukarı Link Aşırı Yükleme (Overpower Uplink)
- Attack to Orbital Positioning & Collision Avoidance System Yörünge Konumlandırma ve Çarpışma Önleme Sistemine Saldırı
  - Doğrudan Komut Verme (Direct Commanding)
  - Komut Tekrarı (Command Replay)
  - Ekleme (Insertion)
- Unauthorized Access to Data Veriye Yetkisiz Erişim
  - Aldatma / Araya Girme
  - Dinleme
  - Rehin Alma

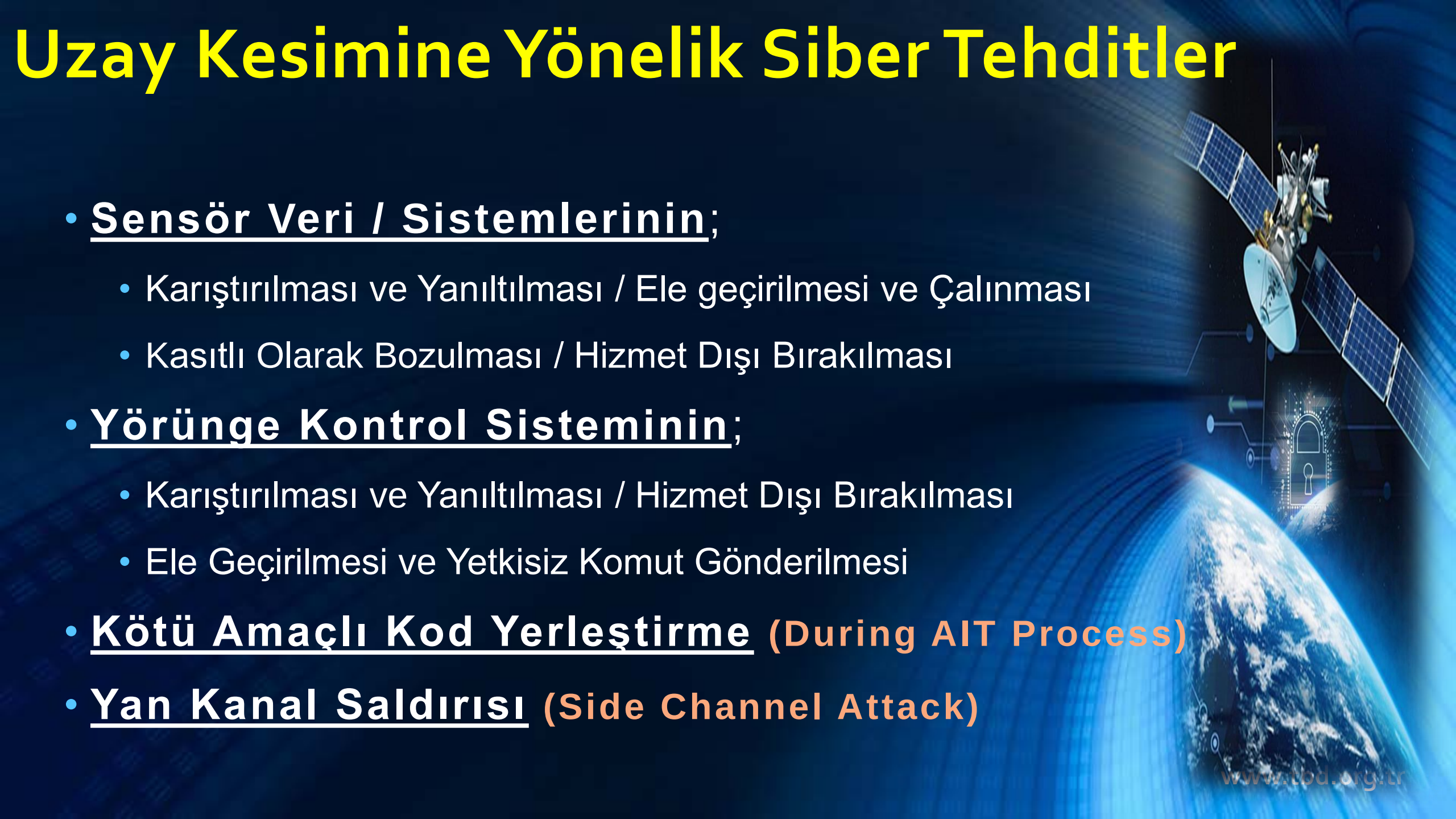
Uydu Sistemi Mimari Yapı



Uzay Kesimine Yönelik Siber Tehditler

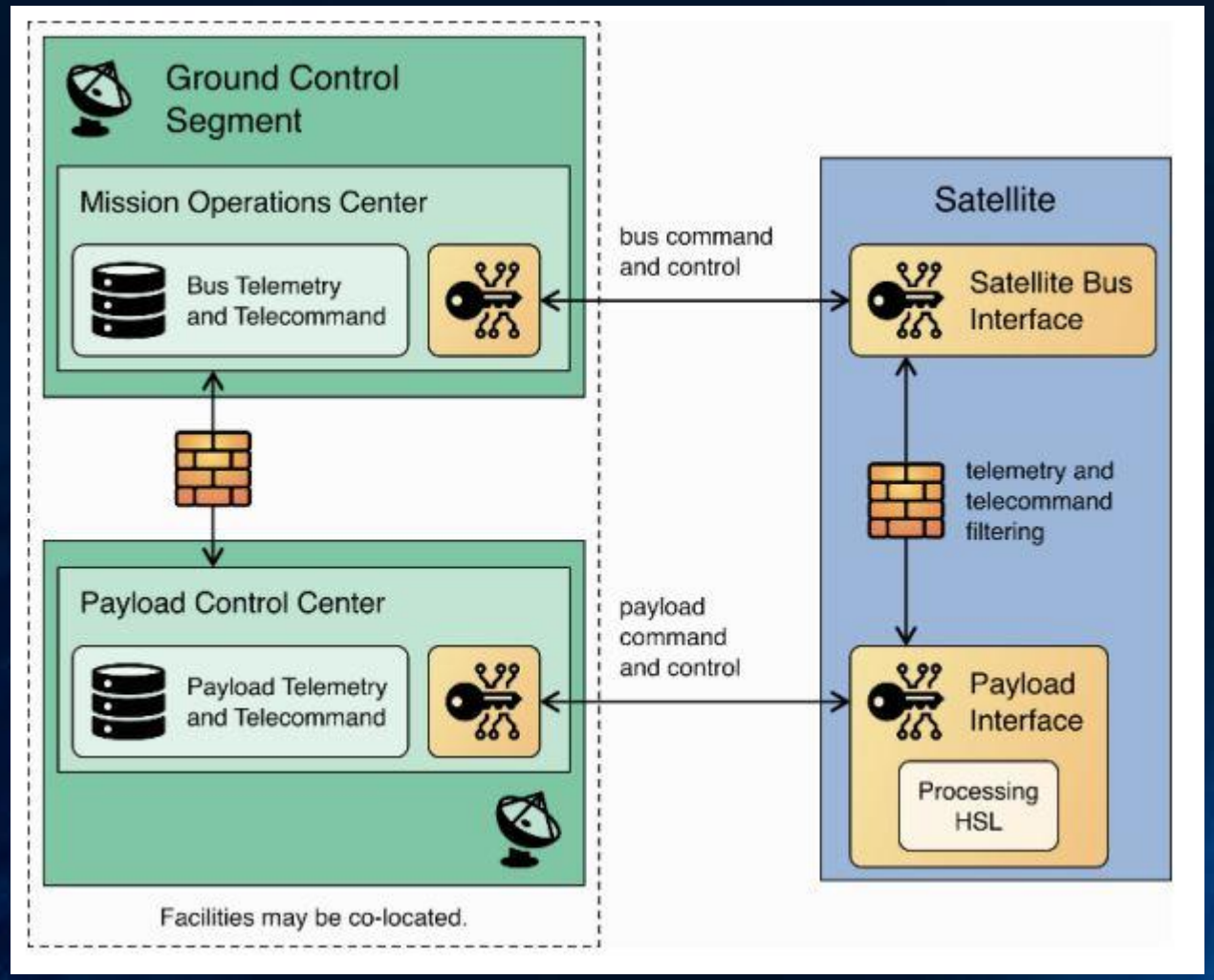


Uzay Kesimine Yönelik Siber Tehditler



- **Sensör Veri / Sistemlerinin**;
  - Karıştırılması ve Yanıltılması / Ele geçirilmesi ve Çalınması
  - Kasıtlı Olarak Bozulması / Hizmet Dışı Bırakılması
- **Yörünge Kontrol Sisteminin**;
  - Karıştırılması ve Yanıltılması / Hizmet Dışı Bırakılması
  - Ele Geçirilmesi ve Yetkisiz Komut Gönderilmesi
- **Kötü Amaçlı Kod Yerleştirme** (During AIT Process)
- **Yan Kanal Saldırısı** (Side Channel Attack)

Yer Kesimine Yönelik Siber Saldırılar



Yer Kesimine Yönelik Siber Tehditler

- Physical Attacks / Fiziksel Saldırı
- IT Network Exploitation / BT Ağından Yaralanma
  - Cloud Infrastructure / Bulut Altyapısı
  - On Premise / Tesiste
  - Unpatched Attack Surface / Yamalanmamış Saldırı Yüzeyi
- Data Corruption & Modification / Veri Bozulması ve Değiştirilmesi
- Supply Chain Attacks / Tedarik Zinciri Saldırıları
  - Malware insertion / Kötü Amaçlı Kod Yerleştirme

Uzay Kesiminde Siber Güvenlik Tedbirleri-1

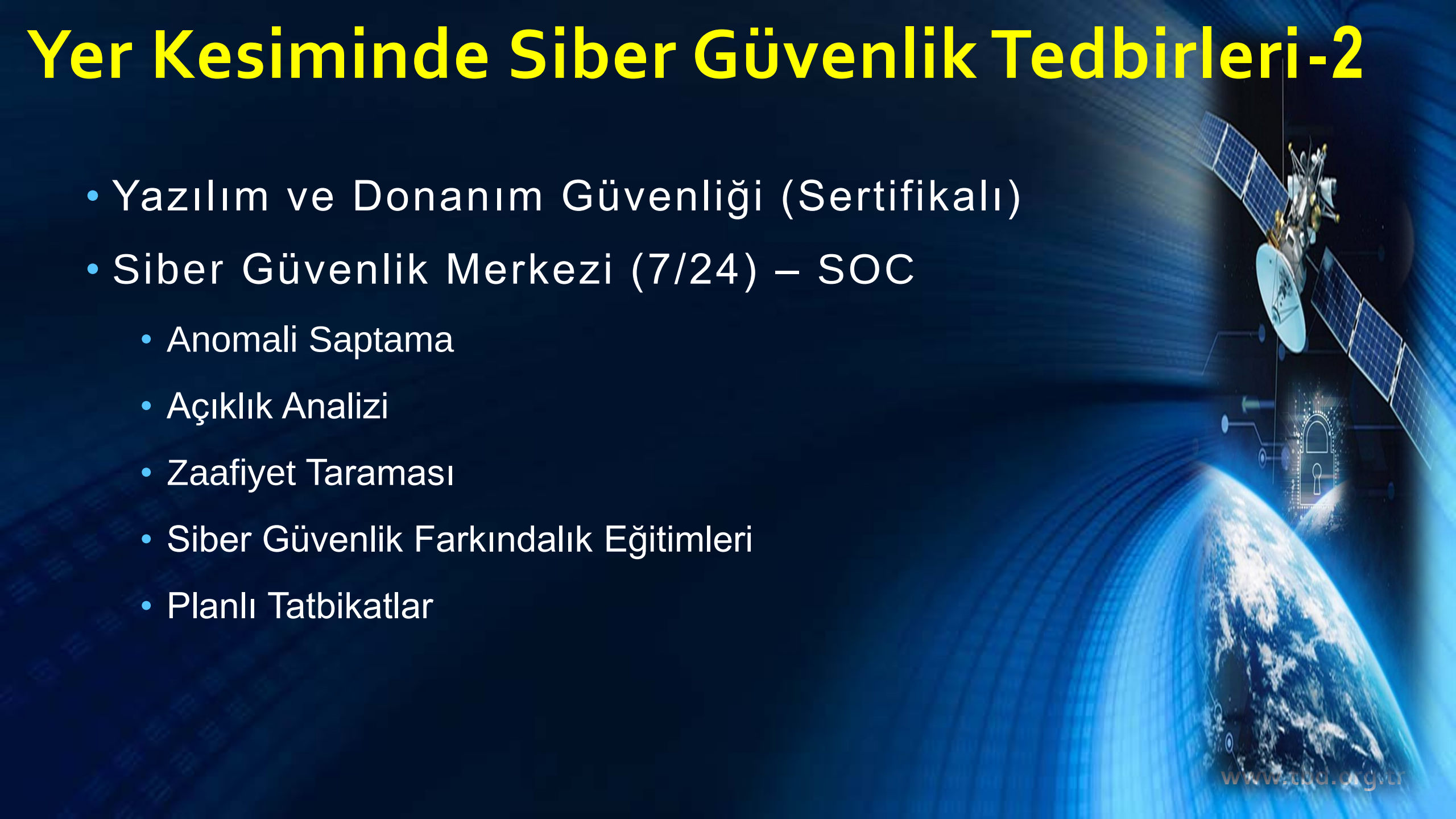
- **Erişebilirlik**
  - Güvenli Donanım Kullanımı (Sertifikalı)
  - Güvenli Yazılım Kullanımı ve Yama Yönetimi
  - Anomali Saptama
- **Bütünlük Kontrolü**
  - Tüm Yazılım ve Konfigürasyon Kontrol Dosyaları Sayısal İmzalı olmalı
- **Gizlilik**
  - Kontrol Kanalı (TMTC) ve Görev Yükü Verileri Kriptolanmalı

Yer Kesiminde Siber Güvenlik Tedbirleri-1

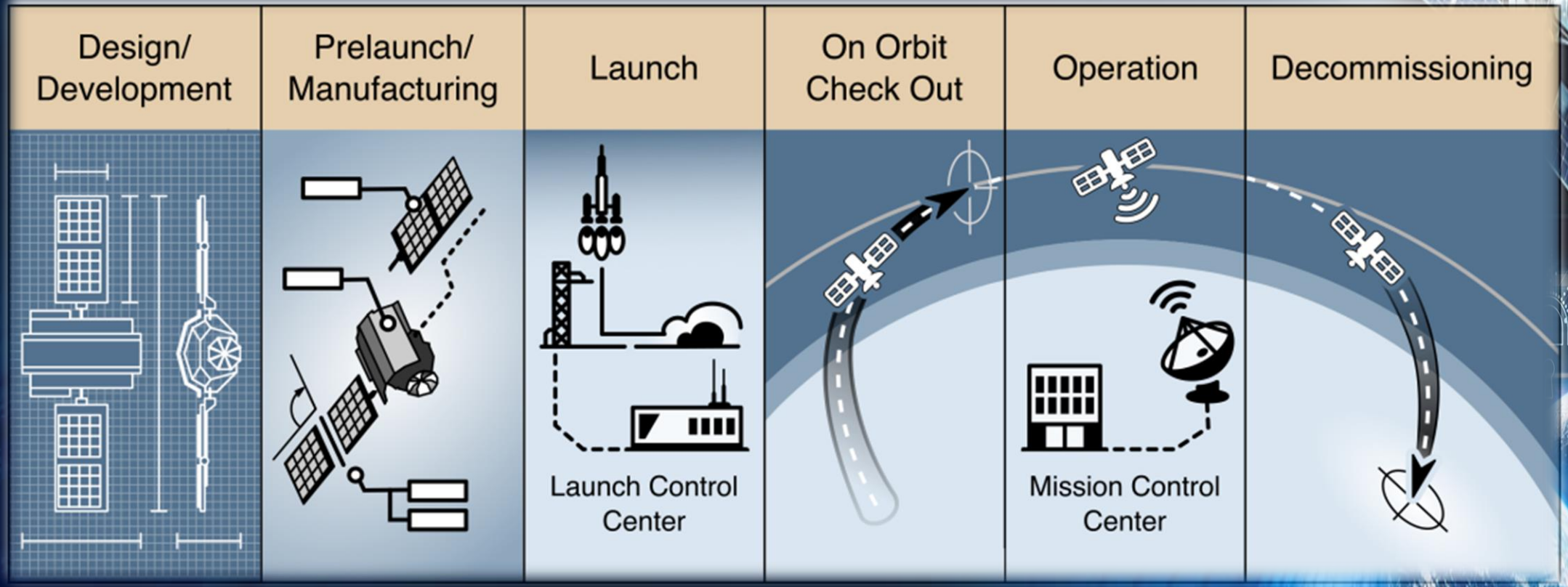
- Güvenli BT Mimari Yapısı / Altyapısı
  - Farklı Güvenlik Seviyesine Sahip Ağlar
  - Erişim Kontrolü / 2 Faktörlü Doğrulama
  - Veri Diyodu / Güvenlik Duvarı
  - Ağ Güvenliği (Kriptolama/Güvenlik Duvarı)
  - Saldırı Tespit ve Önleme Sistemleri (AI based & DDOS Mitigate)
  - Yama Yönetimi
  - Güvenli Veri Saklama (Kriptolu)
  - Yedek Alma (Kriptolu)

Yer Kesiminde Siber Güvenlik Tedbirleri-2

- Yazılım ve Donanım Güvenliği (Sertifikalı)
- Siber Güvenlik Merkezi (7/24) – SOC
  - Anomali Saptama
  - Açıklık Analizi
  - Zaafiyet Taraması
  - Siber Güvenlik Farkındalık Eğitimleri
  - Planlı Tatbikatlar



Uydu Yaşam Döngüsü



Secure by Design

Teşekkürler...

ali.yazici@tbd.org.tr