



**T.C. ULAŖTIRMA VE
ALTYAPI BAKANLIĐI**



**BİLGİ
TEKNOLOJİLERİ
VE İLETİŖİM
KURUMU**

**ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ
(USOM)
FAALİYETLERİ**



ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ



1. SİBER GÜVENLİK ÇALIŖMALARARI

- Bakanlar Kurulu Kararı- Ekim 2012

<https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>

Ulusal siber güvenlik çalışmalarının yürütülmesi, koordinasyonu ve yönetimi

- Bu kararla Siber Güvenlik Kurulu kuruldu
 - Dışışleri Bakanlığı,
 - İçişleri Bakanlığı,
 - Milli Savunma Bakanlığı,
 - Ulaştırma ve Altyapı Bakanlığı,
 - Milli İstihbarat Teşkilatı,
 - Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanlığı,
 - Bilgi Teknolojileri ve İletişim Kurumu,
 - Türkiye Bilimsel ve Teknolojik Araştırma Kurumu,
 - Mali Suçları Araştırma Kurulu
- 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı onaylandı.
- TR-CERT/USOM 27 Mayıs 2013 tarihinde kuruldu.



1. ULUSAL SİBER GÜVENLİK STRATEJİLERİ

- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı
 - 2013-2014 (<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/actionplan2013-2014.pdf>)
 - 2016-2019 (<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf>)
 - 2020-2023 (<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plan-2020-2023.pdf>)



1. ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM)

- TR-CERT / USOM 27 Mayıs 2013 tarihinde kurulmuŖtur.
- 15 AĐustos 2016'da yeni yetkiler verilmiŖtir.
- Yeni tesisinin aılıŖı 10 Ŗubat 2020'de yapılmıŖtır.



ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM)

USOM, 2013 yılında kurulmuş olup, 2016 yılından bu yana doğrudan BTK bünyesinde yer almaktadır. USOM, ülke kapsamında yurtiçi ve yurtdışı kaynaklı siber tehditleri önlemek amacıyla alarm, uyarı ve duyurulara ilişkin faaliyetler yürütmekte, kritik durumlarda yerinde müdahale ekipleriyle olayın kontrolünün sağlanmasında önemli bir rol üstlenmektedir.



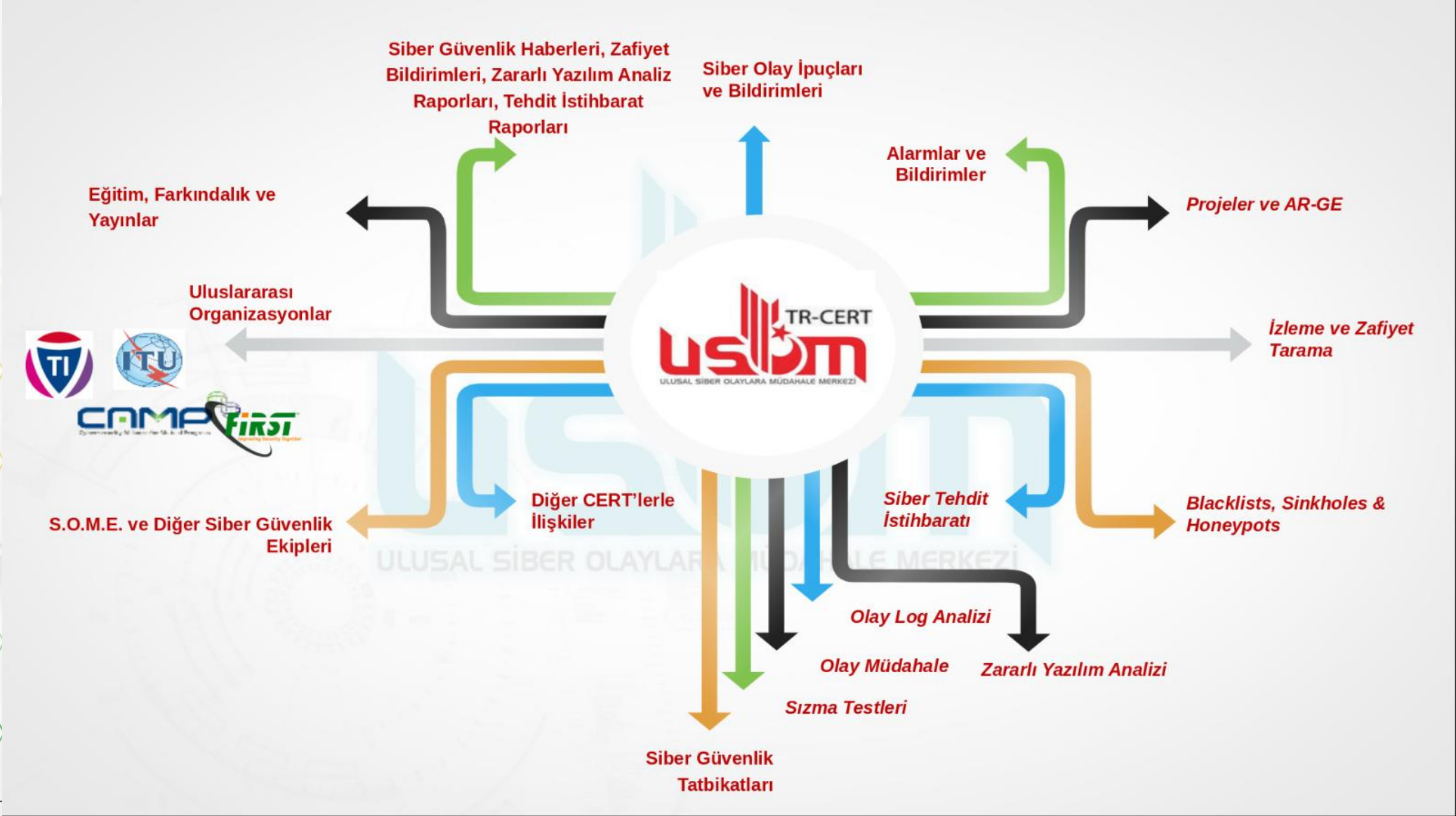


1. SİBER GÜVENLİK – 5809 Elektronik Haberleşme Kanunu / Kurumun Görevleri

- 60/11: Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin **siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için** her türlü tedbiri alır veya aldırır.
- 60/12: Kurum, görevi kapsamında ilgili yerlerden **bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir**; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkroda belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkroya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir.
- 60/13: Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar. İşletmeciler dışında Kurumun görevleri ile ilgili yükümlülüklerini yerine getirmeyenlere bu maddenin ikinci fıkrasındaki **yaptırım** uygulanır. (bin liradan bir milyon liraya kadar idari para cezası)



ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM)





Siber Gvenlik Yapılanması

Siber Olaylara Mdahale Ekipleri (SOME'ler) kurumların ve kritik altyapı sektörlerinin korunmasına yönelik olarak USOM'un koordinasyonunda 7/24 grevlerini gerçekleŖtirmektedir. Teknik seviyede USOM, Sektrel SOME'ler ve Kurumsal SOME'ler olarak Ŗekillenen siber gvenlik yapılanmasında halihazırda toplam 2100'n zerinde SOME ile USOM bnyesinde iŖletilen SOME İletişim Platformu'na kayıtlı 7.300'den fazla siber gvenlik uzmanı lkemizin siber sahasını korumaktadır.





Hızlı Tespit ve Önleme Sistemleri

- **Avcı:** zararlı yazılım bulaşmış sistemler ve komuta kontrol merkezlerinin tespiti.
- **Azad:** Makine öğrenmesi ve yapay zeka imkanları ile botnetlere dahil olmuş bilgisayarların tespiti.
- **Kasırga:** Başta kritik altyapılar olmak üzere ülkemizin internete açık kaynaklarına ilişkin zafiyet taraması ve hizmet sürekliliğine yönelik izleme faaliyetlerinin gerçekleştirilmesi.
- **Atmaca:** Kasırga ve farklı taramalardan gelen sonuçların sorgulanması sonucu zafiyet taraması faaliyetleri gerçekleştirilir.





Siber Gvenlik Bildirimleri / Zararlı BaĐlantı Engelleme

lkemizdeki kritik kurum ve kuruluŖların tehditler ve zafiyetlere karŖı uyarılarak gerekli nlemlerin alınması amalanmıŖtır. USOM alıŖmaları kapsamında, 250.000'in zerinde zararlı baĐlantı tespit edilerek altyapı seviyesinde eriŖimi engellenmiŖtir. Ayrıca USOM tarafından 25.000'in zerinde siber gvenlik bildirimini yapılarak gerekli nlemlerin alınması saĐlanmıŖtır.





Güvenlik Operasyonları Merkezi

Siber Güvenlik Operasyon Merkezi ile USOM ve operatörler arasındaki iş ve işlemlerin 7/24 kesintisiz olarak izlenebilmesi ve gerekmesi halinde aksiyonların zaman kaybetmeksizin alınmasına imkan sağlanmıştır. Siber Güvenlik Operasyon Merkezi faaliyetlerinin etkin ve verimli bir şekilde yürütülmesi amacıyla en yeni teknolojiler kullanılarak altyapı kurulum çalışmaları tamamlanmış, farklı kaynaklardan gelen veriler konsolide edilerek görselleştirilmiş ve bu amaçla izleme ekranları kurulmuş durumdadır. Siber Güvenlik Operasyon Merkezi Cumhurbaşkanı Recep Tayyip Erdoğan'ın teşrifiyle 10 Şubat 2020 tarihinde açılmıştır.





Farkındalık & Kapasite GeliŖtirme



- 2011 yılından bu yana 4 ulusal ve 2 uluslararası siber gvenlik tatbikatı gerekleŖtirilmiŖtir.
- 2019 yılında “Cyber Shield” uluslararası tatbikatı UlaŖtırma ve Altyapı Bakanlığı ve BTK-USOM iŖbirliđinde gerekleŖtirilmiŖtir. Aynı zamanda ITU ve CAMP tarafından desteklenmiŖtir.
- Cyber Shield tatbikatına 17 farklı lkeden 87 katılımcı dahil olmuŖtur.
- 2021 yılında “Ulusal Siber Kalkan” tatbikatı UlaŖtırma ve Altyapı Bakanlığı ve BTK-USOM iŖbirliđinde gerekleŖtirilmiŖtir.
- Tatbikat, 36 kurumdan 135 uzmanın katılımıyla gerekleŖmiŖtir.



Farkındalık & Kapasite GeliŖtirme



- Siber Yıldız yarışması ile ÷lkemizde siber güvenliđe ilgi duyan ve yetenekli kiŖilere kendilerini geliŖtirme fırsatı sunulmaktadır. Ayrıca bu alandaki farkındalıđı artırmaktadır.
- Yođun katılımıla dñzenlenen yarışmalar sonucunda başarılı olan katılımcılara istihdam, eđitim ve para öd÷lü gibi fırsatlar sađlanmaktadır.



Farkındalık & Kapasite GeliŖtirme

SİBER TALİMHANE
FETİH

<https://fetih.gov.tr/>

Siber Yıldız yarışmamızın bir sonraki aşaması olan ve genç yeteneklerimizin profesyonelleşme yolunda ilerlemesine imkan vererek, Ülkemizin ihtiyacı olan siber güvenlik uzmanlarının yetiştirilmesine yönelik Fetih Siber Talimhane projesi ile uygulamalı siber güvenlik eğitim laboratuvarı altyapısı USOM bünyesinde tamamlanmıştır.



Farkındalık & Kapasite GeliŖtirme



BTK bünyesinde kurulan BTK-Akademi, Türkiye'nin insan kaynađının uzmanlık düzeyinin artırılmasına katkı sađlamak amacıyla siber güvenlik ve diđer ilgili alanlarda halka açık çevrimiçi eđitimler vermektedir. Eđitim içerikleri BTK-Akademi resmi web portalında mevcuttur.

<https://www.btkakademi.gov.tr/portal>



Uluslararası İŖbirliĐi



USOM, siber tehdit istihbaratı edinimi, üretimi ve paylaşımı noktasında ulusal ve uluslararası paydaşlarıyla koordinasyon sağlanmasında önemli görevler üstlenmektedir. İnternet aktörleri, uluslararası kuruluşlar, adli makamlar, araştırma merkezleri, üniversiteler ve özel sektör kuruluşları ile birlikte hareket ederken aynı zamanda uluslararası alanda ülkemizin temas noktası olma görevini de yerine getirmektedir.



ITU Küresel Siber Güvenlik Endeksi (ITU-GCI)

2020	Dünya:	11
	Avrupa:	6
2018	Dünya:	22
	Avrupa:	11
2017	Dünya:	43
	Avrupa:	22

