# Siber Güvenlik Teknoloji Yol Haritası – Sektörel Uygulamalar

## Öncelikli Sektörel Uygulamalar

| 1:5G ve ötesi haberleşme teknolojileri, IoT protokolleri ve baz istasyonları için yerli siber güvenlik teknolojileri ve ürünleri | 2: Akıllı üretim sistemlerinde ağ trafiğinin yönetimi, güvenli haberleşme, siber saldırı önleme teknolojileri | 3: Otomotiv ve Ulaşım sektörleri | 4: Enerji sektörü | 5: Kamu ihtiyaçlarına yönelik siber güvenlik çözümleri |
|---|---|---|---|---|
| 1.1. 5G ve ötesi için fiziksel katman güvenliği | 2.1. Akıllı üretim sis. ağ trafiği yönetimi ve anomali tespiti | 3.1. Otomotiv ve Ulaşım için temel güvenlik ürünleri | 4.1. Enerji sektörü için saldırı önleme, veri şifreleme, veri kaçağı önleme | 5.1. Kamu için güvenlik duvarı, saldırı tespit, veri kaçağı önleme, vb. |
| 1.2. 5G ve ötesi, IoT ve baz istasyonları için siber güvenlik (SDN/NFV tabanlı güvenlik ve SDN/NFV güvenliği) | 2.2. Akıllı üretim sis. güvenli haberleşme, itibar sis., veri kaçağı önleme, siber saldırı önleme | 3.2. Akıllı ve otonom araçlar siber saldırı önleme | | 5.2. Kamuda kullanılan milli işletim sis. güvenliğini artırıcı çözümler |

| 6: Kamu ve özel sektör verileri için güvenli bulut teknolojileri ve ürünleri | 7: Finans ve Ticaret sektörleri | 8: Kamuda (kritik kamu hizmetleri, e-devlet ve sağlık) veri şifrelemesinde güvenli kriptografi teknolojilerini kullanan ürünler | 9: E-ticaret ve sanal alışveriş için dijital varlıkların kullanımına yönelik kriptografik çözümler ve bu sistemlere yönelik siber güvenlik çözümleri | 10: Savunma, Havacılık ve Uzay sektörleri |
|---|---|---|---|---|
| 6.1. Kamu ve özel sektör verilerinin ve servisleri için bulut mimarilerinde güvenlik | 7.1. Finansal hizmet sağlayıcılarını ataklara karşı koruyacak bulut tabanlı sistem | 8.1. Kamuda verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojileri | 9.1. E-ticaret ve sanal alışverişte dijital varlıklar için kriptografi | 10.1. Savunma sistemlerinde merkezi olmayan otonom siber güvenlik çözümleri |
| 6.2. Eğitim sektörü için çevrim içi eğitim sis. siber güvenlik ve kriptoloji teknolojileri | 7.2. Finans ve Ticaret sektörleri için veri kaçağını engelleme/mahremiyeti koruma | 8.2. Biyometrik ve çok aşamalı kimlik doğrulama | 9.2. E-ticaret ve sanal alışverişte dijital varlıklar siber güvenlik çözümleri | 10.2. İHA'lar için EPM teknolojileri ve ürünleri |
| | | 8.3. Büyük veri dahil, veri koruma ve kriptoloji | | 10.3. Savunma sektörü ürünleri ve uygulamaları için siber güvenlik çözümleri |

* Teknolojik Hedeflere ilişkin konular bir önceki yansıdadır.

DijitalTeknolojiler

# Siber Güvenlik - Ağ ve İletişim Güvenliği

**Öncelikli Ürün ve Teknolojiler**

**Temel Ağ ve İletişim Güvenliği Ürünleri**

**Öncelikli Ar-Ge ve Yenilik Konusu**

**Ağ Anahtarı (Switch), Kablolu/Kablosuz Yönlendirici (Router)**

Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«Ağ anahtarı (switch), kablolu/kablosuz yönlendirici (router)»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir.

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
|---|---|

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

Büyük Ölçekli Sanayi, Üniversite, Kamu Araştırma Merkezleri, Kamu Kurumları

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması
- Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi
- Sahte IP değişikliklerinin en kısa sürede algılanması
- Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi
- Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi
- Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi
- Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- İlgili ulusal ve uluslararası standartlara uygun olması
- Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması
- Şifrelenmiş trafiklerde inceleme yapabilmesi
- Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştiril(ebil)meli
- SDN ve NFV uyumlu olması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Ağ ve İletişim Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«Derin paket inceleme altyapısı, ağ izleme sistemi, (DDoS) saldırı tespit ve önleme sistemi, e-posta ağ geçidi»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Temel Ağ ve İletişim Güvenliği Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **7-9** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>KOBİ'ler, Teknopark Firmaları, Üniversiteler | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi | |
| **Derin Paket İnceleme Altyapısı, Ağ İzleme Sistemi, (Ddos) Saldırı Tespit Ve Önleme Sistemi, E-posta Ağ Geçidi** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması
- Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi
- Sahte IP değişikliklerinin en kısa sürede algılanması
- Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi
- Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi
- Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi
- Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- İlgili ulusal ve uluslararası standartlara uygun olması
- Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması
- Şifrelenmiş trafiklerde inceleme yapabilmesi
- Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştiril(ebil)meli
- SDN ve NFV uyumlu olması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Ağ ve İletişim Güvenliği

**Öncelikli Ürün ve Teknolojiler**

**Temel Ağ ve İletişim Güvenliği Ürünleri**

Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«Uygulama katmanı destekli Web/VoIP/IoT/Database»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir.

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
|---|---|

**Öncelikli Ar-Ge ve Yenilik Konusu**

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

KOBİ'ler, Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları

**Uygulama Katmanı Destekli Web/Voıp/Iot/Data base**

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması
- Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi
- Sahte IP değişikliklerinin en kısa sürede algılanması
- Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi
- Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi
- Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi
- Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- İlgili ulusal ve uluslararası standartlara uygun olması
- Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması
- Şifrelenmiş trafiklerde inceleme yapabilmesi
- Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştiril(ebil)meli
- SDN ve NFV uyumlu olması
-

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Ağ ve İletişim Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«İleri seviye veri sızıntısı önleme (DLP) ürünü,»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Temel Ağ ve İletişim Güvenliği Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>KOBİ'ler, Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları | |
| | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi | |
| **İleri Seviye Veri Sızıntısı Önleme (DLP) Ürünü** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması
- Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi
- Sahte IP değişikliklerinin en kısa sürede algılanması
- Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi
- Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi
- Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi
- Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- İlgili ulusal ve uluslararası standartlara uygun olması
- Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması
- Şifrelenmiş trafiklerde inceleme yapabilmesi
- Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştiril(ebil)meli
- Merkezi politika yönetimi
- Farklı cihazlarda kaçak/sızıntı önleme desteği
- Fiziki ağ dışında sızıntı önleme desteği

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler

Teknoloji

# Siber Güvenlik - Ağ ve İletişim Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«Antivürüs, fidye yazılımları önleme sistemleri, loglama sistemi»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Temel Ağ ve İletişim Güvenliği Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>KOBİ'ler, Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları | |
| **Antivürüs, Fidye Yazılımları Önleme Sistemleri, Loglama Sistemi** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması
- Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi
- Sahte IP değişikliklerinin en kısa sürede algılanması
- Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi
- Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi
- Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi
- Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- İlgili ulusal ve uluslararası standartlara uygun olması
- Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması
- Şifrelenmiş trafiklerde inceleme yapabilmesi
- Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştirilebilmeli

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Ağ ve İletişim Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle önleme (*prevention*) bertaraf yöntemine yönelik olarak, temel ağ güvenliği ürünlerinin yerli olarak güçlendirilmesi / geliştirilmesi ve geliştirilen teknolojiler ile ürünlerin ulusal güvenliği ilgilendiren sektörlerden (kamu, haberleşme, vb.) başlanarak kullanımının yaygınlaştırılması hedefine yönelik olarak **«Güvenli haberleşme gereken kullanım alanları ile 5G ve ötesi yeni haberleşme teknolojilerinde (SDN dahil) güvenlik çözümleri, GTP/Diameter ve 5G güvenlik duvarları (*firewall*)»** geliştirilmesi amacıyla **Temel /Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Temel Ağ ve İletişim Güvenliği Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** — **3-7** | • Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde ağ, donanım ve yazılım seviyelerinde test edilmiş olması<br>• Yazılım seviyesinde, yazılım yoğun stratejik sistemlere (hava/kara/deniz aracı, nükleer santral, sağlık, ekonomi, enerji üretim ve dağıtım ağları, telekom, finans, eğitim, bulut altyapıları) yönelik kazanılan kabiliyetlerin tekrar kullanılabilir, biribiri ile entegre olabilir, ulusal siber güvenlik mimarisi oluşturabilir şekilde geliştirilmesi<br>• Sahte IP değişikliklerinin en kısa sürede algılanması<br>• Ağ seviyesinde haberleşme protokollerinin ve altyapılarının zafiyetlerinden faydalanan saldırıların önlenebilmesi için IPv6 adresleme altyapısına geçilmesi<br>• Sosyal mühendislik saldırılarını engelleyebilecek nitelikte içerik analizinin yapılabilmesi<br>• Güvenlik duvarı ürünleri arasındaki entegrasyon standartlarını desteklemesi<br>• Uluslararası veritabanlarının yanı sıra ulusal siber tehdit istihbaratı veritabanları ile entegre olması<br>• İlgili ulusal ve uluslararası standartlara uygun olması<br>• Altyapıda kullanılan kriptolojik yaklaşımların uzman kontrolünden geçmiş olması<br>• Şifrelenmiş trafiklerde inceleme yapabilmesi<br>• Gerekli/mümkün olan hallerde sistemler yapay zekâ ve makine öğrenmesi yöntemleri ile zenginleştiril(ebil)meli<br>• SDN ve NFV uyumlu olması<br>• 3GPP R16 desteği olması |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversite, Sanayi ve ilgili STK'lar | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar ve Ağ Haberleşme, Veri Analizi, Trafik Analizi, Karar Destek Sistemleri, Matematik, Yapay Zekâ ve Makine Öğrenmesi | |
| **Güvenli Haberleşme Gereken Kullanım Alanları İle 5G ve Ötesi Yeni Haberleşme Teknolojilerinde (SDN Dahil) Güvenlik Çözümleri, GTP/Diameter ve 5G Güvenlik Duvarları (Firewall)** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** — **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Kimlik ve Erişim Yönetimi

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*) ve önleme (*prevention*) bertaraf yöntemlerine yönelik olarak, ağ ortamındaki cihazların farklı yöntemlerle (parmak izi çıkarılarak, sertifika yükleyerek vb.) kimlik tespitinin yapılabilmesini ve yetkisiz erişim açısından ağ cihazlarının yetkilerinin yönetilebilmesini sağlayacak teknolojilerin geliştirilmesi hedefine yönelik olarak **«Ağ cihazlarında yetki yönetimi ve kimlik doğrulama yapabilecek teknolojiler»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Ağ Ortamındaki Cihazların Kimlik Tespiti ve Yetkisiz Erişim Yönetimi** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **5-8** | • Cihazların kimliklerinin kayıt altına alınmasının sağlanması<br>• IPv6 ve güncel adresleme teknolojilerini desteklemesi<br>• Merkezi ve dağıtık kimlik doğrulama teknolojilerini desteklemesi<br>• Çok faktörlü doğrulamayı desteklemesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>KOBİ'ler, Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri konsorsiyumu | | |
| **Ağ Cihazlarında Yetki Yönetimi ve Kimlik Doğrulama Yapabilecek Teknolojiler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği ve alt alanları, Yapay Zekâ Mühendisliği, Sistem Mühendisliği, Yazılım Mühendisliği, Matematik.,Kriptoloji, Ağ ve Protokol | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Güvenlik Yönetimi

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*), etki azaltma (*mitigation*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine ve ağ, yazılım, donanım seviyeleri ile fiziksel saldırılar, yetkisiz erişim, veri kaçağı, ifşa/mahremiyet siber tehdit unsurlarına yönelik olarak, kurumsal ağlarda BT sistemlerinde tespit edilen saldırılar için ağ seviyesinde otomatik önlemlerinin alınabilmesini ve güvenlik çözümlerinin orkestrasyonunu sağlayacak yerli çözümlerin ve dağıtık güvenlik yönetim teknolojilerinin yapay zekâ ve makine öğrenmesi destekli olarak geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Ağ seviyesinde otomatik önlemlerinin alınabilmesini ve güvenlik çözümlerinin orkestrasyonunu sağlayacak çözümler»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Kurumsal Ağlarda BT Sistemleri Güvenlik Yönetimi Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri**: **5-9** | • Yapay zekâ ve makine öğrenmesi destekli<br>• Dış cihazlarla iletişim kuracağı standart entegrasyon desteklerinin olması<br>• Diğer ürünlerle çalışabilirliği/birlikte çalışabilirliği sağlayacak API desteğinin olması<br>• Yüksek yük değerlerinde performanslı çalışmanın sağlanması<br>• Kesinti gibi acil durumlarda trafik akışı için buffer desteği sunulması ve güvenlik ihlaline imkân verilmemesi<br>• Hataya karşı dayanıklılık (fault tolerance) ve yedekli çalışabilecek sistemle desteklenmesi (özellikle büyük kurumlarda önemlidir)<br>• Orkestrasyonu yapılan ağı izleyebilmesi (Orkestrasyonu yapılan/yönetilen ağı izleyip sistemi oluşturan varlıkların anormal davranışlarını algılayabilmesi. Bu otomasyonu sağlamak için orkestrasyon “(SOAR - Security Orchestration Automation Response)” ile birlikte kullanılan bir yaklaşım olan “User Entity Behavior Analitics (UEBA)”dan faydalanılması.)<br>• “İleri seviye veri sızıntısı önleme (DLP) ürünü” ile bağlantılı olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Ölçekli Sanayi Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, İlgili Kamu Kurum ve Kuruluşların Yer Aldığı Konsorsiyumlar | |
| **Ağ Seviyesinde Otomatik Önlemlerinin Alınabilmesini ve Güvenlik Çözümlerinin Orkestrasyonunu Sağlayacak Çözümler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Donanım Üretim Teknolojileri, Yapay Zeka ve Makine Öğrenmesi, Ağ İzleme, Kriptoloji, Ofansif Güvenlik, Dağıtık Güvenlik Yönetimi | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu**: **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Güvenlik Yönetimi

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*), etki azaltma (*mitigation*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine ve ağ, yazılım, donanım seviyeleri ile fiziksel saldırılar, yetkisiz erişim, veri kaçağı, ifşa/mahremiyet siber tehdit unsurlarına yönelik olarak, kurumsal ağlarda BT sistemlerinde tespit edilen saldırılar için ağ seviyesinde otomatik önlemlerinin alınabilmesini ve güvenlik çözümlerinin orkestrasyonunu sağlayacak yerli çözümlerin ve dağıtık güvenlik yönetim teknolojilerinin yapay zekâ ve makine öğrenmesi destekli olarak geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Dağıtık güvenlik yönetim teknolojileri»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Kurumsal Ağlarda BT Sistemleri Güvenlik Yönetimi Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** — **5-7** | • Yapay zekâ ve makine öğrenmesi destekli olması<br>• Dış cihazlarla iletişim kuracağı standart entegrasyon desteklerinin olması<br>• Diğer ürünlerle çalışabilirliği/birlikte çalışabilirliği sağlayacak API desteği olması<br>• Yüksek yük değerlerinde performanslı çalışmanın sağlanması<br>• Kesinti gibi acil durumlarda trafik akışı için buffer desteği sunulması ve güvenlik ihlaline imkân verilmemesi<br>• Hataya karşı dayanıklılık (fault tolerance) ve yedekli çalışabilecek sistemle desteklenmesi (özellikle büyük kurumlarda önemlidir)<br>• Orkestrasyonu yapılan ağı izleyebilmesi (Orkestrasyonu yapılan/yönetilen ağı izleyip sistemi oluşturan varlıkların anormal davranışlarını algılayabilmesi. Bu otomasyonu sağlamak için orkestrasyon "(SOAR - Security Orchestration Automation Response)" ile birlikte kullanılan bir yaklaşım olan "User Entity Behavior Analitics (UEBA)"dan faydalanılması.)<br>• İleri seviye veri sızıntısı önleme (DLP) ürünü" ile bağlantılı olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Ölçekli Sanayi Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, İlgili Kamu Kurum ve Kuruluşların Yer Aldığı Konsorsiyumlar | |
| **Dağıtık Güvenlik Yönetim Teknolojileri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Donanım Üretim Teknolojileri, Yapay Zeka ve Makine Öğrenmesi, Ağ İzleme, Kriptoloji, Ofansif Güvenlik, Dağıtık Güvenlik Yönetimi | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** — **3 Yıl** | |

Tüm Sektörler | Teknoloji

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

# Siber Güvenlik - OT, IoT Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine yönelik olarak, endüstriyel sistemler (OT) cihazları ile nesnelerin interneti (IoT) cihazlarının bulunduğu ağlardaki trafiğin izlenebilmesine, yönetilebilmesine (güvenlik duvarı, erişim kontrolü vb.) ve siber saldırıların tespit edilerek önlenmesine yönelik teknolojilerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«OT, IoT cihazlarının bulunduğu ağlardaki trafiği izleyebilen, yönetilebilen (güvenlik duvarı, erişim kontrolü vb.) ve siber saldırıları önleyen teknolojiler»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **OT, IoT Cihazlarının Bulunduğu Ağlardaki Trafiği Yönetebilen, Siber Saldırıları Önleyen Teknolojiler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **7-9** | • Kablolu ve kablosuz ağ trafiğini takip edebilen, dinleyen; bu protokolleri anlamlandıran sistemler geliştirilmesi<br>• Bu protokollere yönelik saldırı tiplerinin anlamlandırılıp trafik dinleme yöntemlerine entegre edilmesi<br>• Protokol bazlı koruma yerine IoT için donanım bazlı güvenlik çözümleri geliştirilmesi (Smart NIC vb.)<br>• Donanımın yükünü azaltan, donanım hızlandırıcı özellikte olması<br>• Ürün paketten çıktığında güvenlik önlemlerinin alınmış olmasına yönelik çalışmalar |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>IoT Sistemlere Sahip Üretim Merkezleri, Elektronik Kart ve Donanım Üretebilecek Firmalar, Üniversiteler | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | | | |
| **OT, IoT Cihazlarının Bulunduğu Ağlardaki Trafiği İzleyebilen, Yönetebilen (Güvenlik Duvarı, Erişim Kontrolü vb.) ve Siber Saldırıları Önleyen Teknolojiler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Kablosuz Ağ Güvenliği, Kriptoloji, Ofansif Güvenlik, Donanım Üretim Teknolojileri, Yapay Zekâ ve Makine Öğrenmesi | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - OT, IoT Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine yönelik olarak, endüstriyel sistemler (OT) cihazları ile nesnelerin interneti (IoT) cihazlarının bulunduğu ağlardaki trafiğin izlenebilmesine, yönetilebilmesine (güvenlik duvarı, erişim kontrolü vb.) ve siber saldırıların tespit edilerek önlenmesine yönelik teknolojilerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Uygulama katmanında ara haberleşme (middleware olarak tanımlanan) protokollerinin güvenlik kontrol modülü (Publish Subscribe)»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **OT, IoT Cihazlarının Bulunduğu Ağlardaki Trafiği Yönetebilen, Siber Saldırıları Önleyen Teknolojiler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-7** | • Kablolu ve kablosuz ağ trafiğini takip edebilen, dinleyen; bu protokolleri anlamlandıran sistemler geliştirilmesi<br>• Bu protokollere yönelik saldırı tiplerinin anlamlandırılıp trafik dinleme yöntemlerine entegre edilmesi<br>• Enerji problemi olan cihazlar açısından IPS<br>• M2M haberleşme protokolleri |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>IoT Sistemlere Sahip Üretim Merkezleri, Elektronik Kart ve Donanım Üretebilecek Firmalar, Üniversiteler | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Kablosuz Ağ Güvenliği, Kriptoloji, Ofansif Güvenlik, Donanım Üretim Teknolojileri, Yapay Zekâ ve Makine Öğrenmesi | | |
| **Uygulama Katmanında Ara Haberleşme (*Middleware* Olarak Tanımlanan) Protokollerinin Güvenlik Kontrol Modülü (*Publish Subscribe*)** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Otonom Hareketli Sistemleri Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine yönelik olarak, otonom hareketli sistemlere ve yönetim ara birimlerine uzaktan gerçekleştirilebilecek, siber saldırıları tespit edebilecek ve bu saldırıları engelleyebilecek teknolojilerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Otonom hareketli sistemlere ve yönetim ara birimlerine uzaktan gerçekleştirilebilecek siber saldırıları tespit edebilecek ve bu saldırıları engelleyebilecek teknolojiler»** geliştirilmesi amacıyla **Temel /Uygulamalı Araştırm, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Otonom Hareketli Sistemlere ve Yönetim Ara Birimlerine Yönelik Siber Saldırıları Önleyici Teknolojiler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-7** | • Yanıltma sinyali (*spoofing*) saldırılarına karşı sürekli algılama yapması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerini sürekli takip edip algılaması<br>• Kara deilk (blackhole) saldırılarını algılaması<br>• Mesh networklerde karşılaşılabilecek saldırıların algılanması<br>• Gerekli durumlarda sistemler yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması ve ulusal kripto sistemleri de desteklemesi<br>• Güvenli güncelleme ve bakım özelliği olması |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Ölçekli Sanayi Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurumları, STK'lar, Uluslararası İş Birlikleri | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>• Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | | |
| **Otonom Hareketli Sistemlere ve Yönetim Ara Birimlerine Uzaktan Gerçekleştirilebilecek Siber Saldırıları Tespit Edebilecek ve Bu Saldırıları Engelleyebilecek Teknolojiler** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Son Kullanıcı Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle tespit (*detection*) ve önleme (*prevention*) bertaraf yöntemlerine yönelik olarak, son kullanıcı cihazlarının güvenliğini sağlamak amacıyla zararlı yazılım, oltalama, veri kaçağı tespitine ve önlenmesine yönelik teknolojiler ile EDR (Uç Nokta Tehdit Algılama ve Yanıt) ve tarayıcı izolasyonu gibi teknolojilerin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Son kullanıcı cihazlarının güvenliğini sağlamak amacıyla zararlı yazılım, oltalama, veri kaçağı tespitine ve önlenmesine yönelik teknolojiler»** geliştirilmesi amacıyla **Temel /Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | |
| **Son Kullanıcı Cihazlarının Güvenliği İçin Teknolojiler** | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-9** |
| **Son Kullanıcı Cihazlarının Güvenliğini Sağlamak Amacıyla Zararlı Yazılım, Oltalama, Veri Kaçağı Tespitine ve Önlenmesine Yönelik Teknolojiler** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Özel Sektör, Teknopark Firmaları, Üniversite, Kamu Araştırma Merkezleri | |
| | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Matematik | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Yazılım seviyesinde Kimlik ve Erişim Yönetimi standartlarına uyumun gözetilmesi ve ulusal kullanıma alınacak yazılımların tescillenerek uyumunun denetlenmesi, uyum seviyesini sağlamayan yazılımların tescil edilmemesi ve ulusal olarak kullanıma alınmaması
- Yetkisiz erişim seviyesinde Kimlik ve Erişim Yönetimi standartlarında sistem kritiklik seviyelerinin tanımlanması, yetkisiz erişim tespiti anında verinin yok edilmesi
- Kimlik ve Erişim Yönetimi sistemlerinde saldırılarda ele geçirilebilecek bilgilerin en aza indirilmesi amaçlı çeşitli kriptolojik yöntemlerin uygulanması (örn. veri anonimleştirme, anonim sertifikalar, eş biçimli şifreleme ile hesaplama yöntemleri)
- Makine öğrenmesi ile desteklenmiş, daha isabetli zararlı yazılım tespiti yapabilecek uygulamalar geliştirilmesi.
- Kullanıcının cihazlarını kullanırken kaynak kullanımı, performans kaybı, yavaşlık, hizmet kesintisi gibi kullanıcı deneyimini ve verimliliğini olumsuz etkileyecek faktörlerin kabul edilebilir endüstri standartlarının seviyesinde olması
- Kullanıcı cihazlarında, kullanıcı ya da yönetici onayı olmadan işletim sistemi seviyesinde ve kritik dosyalarda yapılan güncellemelerin ve konfigürasyon değişikliklerinin tespit edilmesi ve engellenmesi
- Kullanıcılara gereğinden fazla verilmiş olan veya artık ihtiyaç duyulmayan ve kullanılmayan yetkilerin belirlenerek kaldırılması
- Kullanıcı cihazlarına kullanıcıların her zaman en düşük yetki seviyesi ile giriş yapması ve daha yüksek yetkilere ihtiyacı olan faaliyetleri gerçekleştirmesi gerektiğinde sadece ihtiyacı olduğu süre boyunca ve ihtiyaç duyduğu kadar yetki seviyesinin yükseltilmesi
- Küresel zararlı yazılım tespit uygulamaları ve veritabanları ile entegre çalışabilecek altyapının kurulması
- Ülkemizde tespit edilmese dahi uluslararası alanda tespit edilen zararlı yazılım imzalarının hızlıca tespiti ve proaktif önlem alınmasının kolaylaştırılması
- Oltalamaların önlenmesine ilişkin saldırganların en sık kullandığı sözcük öbekleri ve ifadeler göz önünde bulundurularak davranış temelli sistemlerin geliştirilmesi

Tüm Sektörler | Teknoloji

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

# Siber Güvenlik - Son Kullanıcı Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle tespit (*detection*) ve önleme (*prevention*) bertaraf yöntemlerine yönelik olarak, son kullanıcı cihazlarının güvenliğini sağlamak amacıyla zararlı yazılım, oltalama, veri kaçağı tespitine ve önlenmesine yönelik teknolojiler ile EDR (Uç Nokta Tehdit Algılama ve Yanıt) ve tarayıcı izolasyonu gibi teknolojilerin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«EDR (Uç Nokta Tehdit Algılama ve Yanıt) ve tarayıcı izolasyonu gibi teknolojiler»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | |
| **Son Kullanıcı Cihazlarının Güvenliği için Teknolojiler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-9** |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Özel Sektör, Teknopark Firmaları, Üniversite, Kamu Araştırma Merkezleri | |
| **EDR (Uç Nokta Tehdit Algılama ve Yanıt) ve Tarayıcı İzolasyonu Benzeri Teknolojiler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilişim Teknolojileri, Bilgisayar Mühendisliği, Bilgi Güvenliği Mühendisliği, İstatistik, Matematik | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Ağ seviyesinde zararlı kullanıcı hareketlerinin tespitinde veri bilimi uygulamaları kullanılması
- Uluslararası veritabanlarının yanında ulusal siber tehdit istihbaratı veritabanları ile entegre olması
- Tanımlanan politikalara ve kurallara uygun olarak işlevleri yerine getirdiğini doğrulayacak şekilde test edilmiş olması
- Makine öğrenme teknolojileriyle (derin ağ) uç nokta cihazları için yapay zekâ destekli saldırı destek sistemleri için son ürün geliştirilmesi
- Gerektiği taktirde kural tabanlı yöntemlerle hibrit bir sistemin inşa edilmesi

EDR için ek olarak aşağıdaki kabiliyetleri desteklemelidir:

- Uç nokta verilerinin toplanması
- Kötü amaçlı yazılım analizi
- Davranış analizi - şüpheli davranışları ortaya çıkarmak için görünüşte zararsız olaylar zincirini birbirine bağlama yeteneği
- Veri korelasyonu ve zenginleştirme
- İlgili uyarıların olaylarla ilişkisi
- Olayların güvenirliği ve ciddiyetine göre önceliklendirme
- Tıklama zincirlerini görselleştirme araçları
- Ağ izolasyonu, dosya karantinası, dosya kaldırma, yeniden görüntüleme
- Süreç öldürme ve davranış engelleme dahil olmak üzere iyileştirme
- Politikalara veya önceden tanımlanmış kurallara dayalı otomatik aksiyon alan ve düzelten iş akışları

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Son Kullanıcı Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle tespit (*detection*) ve önleme (*prevention*) bertaraf yöntemlerine yönelik olarak, son kullanıcı cihazlarının güvenliğini sağlamak amacıyla zararlı yazılım, oltalama, veri kaçağı tespitine ve önlenmesine yönelik teknolojiler ile EDR (Uç Nokta Tehdit Algılama ve Yanıt) ve tarayıcı izolasyonu gibi teknolojilerin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Gerçek dışı çoklu ortam içeriklerin (görüntü, video ve ses) son kullanıcı cihazlarında tespit edilebilmesine ve bu içeriklerin önlenebilmesine yönelik teknolojiler»** geliştirilmesi amacıyla **Teknoloji Geliştirme Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Son Kullanıcı Cihazlarının Güvenliği için Teknolojiler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-8** | • Görüntü ve ses işleme yazılımlarındaki artış ve kolay kullanılabilirlikleri<br>• Son kullanıcı güvenliğinin tehlikeye girmesi durumunda kullanıcı özelinde kötü niyetli video, görüntü veya ses dosyası oluşturulabilmesi<br>• Görüntü, video ve ses sahteciliği tespit yöntemleri geliştirilmesi |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversite, Özel Sektör, Kamu Araştırma Merkezleri, Teknopark Firmaları | | Görüntü, video ve ses doğru tespit oranı ve yanlış tespit oranı, yöntemlerin performansını belirlemekte kullanılabilir:<br>• Görüntü sahteciliği alanında, tespit oranları gerek piksel seviyesinde gerekse görüntü seviyesinde gerçekleştirilebilir.<br>• Video sahteciliğinde ise video bazında veya çerçeve bazında doğru tespit ve hatalı tespit oranları elde edilebilir.<br>• Ses dosyaları üzerinde de örnek ve dosya seviyesinde, doğru ve hatalı tespit oranlarını belirlenebilir. |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği | | |
| **Gerçek Dışı Çoklu Ortam İçeriklerin (Görüntü, Video ve Ses) Son Kullanıcı Cihazlarında Tespit Edilebilmesine ve Bu İçeriklerin Önlenebilmesine Yönelik Teknolojiler** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Mobil Güvenlik

**Öncelikli Ürün ve Teknolojiler**

**Güvenilir İşletim Sistemi ve TEE Teknolojilerinde Kullanılan Yeni Mobil Cihaz Güvenlik Çözümleri**

Önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine yönelik olarak, yazılım tabanlı beyaz kutu kriptografi ve donanım destekli özellikler içeren güvenilir çalışma ortamı (Trusted Execution Environment, TEE) destekleyen güvenilir işletim sisteminin ve TEE teknolojilerini kullanılan yeni mobil cihaz güvenlik çözümlerinin yerli olarak geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«TEE teknolojilerini destekleyen güvenilir işletim sistemi»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir.

**Öncelikli Ar-Ge ve Yenilik Konusu**

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-9** |
|---|---|

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları, Özel Sektör

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Bilgisayar Mühendisliği, Yapay Zekâ, Veri Mühendisliği, İstatistik

**TEE Teknolojilerini Destekleyen Güvenilir İşletim Sistemi**

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6 Yıl** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- İşletim sistemi üzerinde sızma testleri uygulanması
- Sayfalama ve tarifeleme algoritmalarının msn cinsinden ölçülmesi
- Dosya sisteminde uygulanacak olan güvenlik algoritmalarının güvenlik analizinin yapılması
- Dosya sisteminde uygulanacak olan güvenlik algoritmalarının donanım destekli güvenilir kriptografik çözümler ile geliştirilmesi
- Hataya toleransının ölçülmesi
- İşletim sisteminde farklı kaynaklardan gelen ve kriptorafik yöntemler ile doğruluğu kanıtlanamayan uygulamalar için sosyal kontrol mekanizmaları destekli güven yöntemleri geliştirilmesi

Açıklıkların tespiti için:

- Erişim güvenliği yöntemleri
- Sosyal kontrol yöntemleri (insanların duygularını ölçen, değerlendiren, yönlendiren) uygulanması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Mobil Güvenlik

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine yönelik olarak, yazılım tabanlı beyaz kutu kriptografi ve donanım destekli özellikler içeren güvenilir çalışma ortamı (*Trusted Execution Environment*: TEE) destekleyen güvenilir işletim sisteminin ve TEE teknolojilerini kullanılan yeni mobil cihaz güvenlik çözümlerinin yerli olarak geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«TEE teknolojileri kullanılan yeni mobil cihaz güvenlik çözümleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Güvenilir İşletim Sistemi ve TEE Teknolojilerinde Kullanılan Yeni Mobil Cihaz Güvenlik Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-9** | • Yenilikçi teknolojilerle zararlı yazılım tespiti (makine öğrenmesi gibi yöntemlerle)<br>• Tespitlerin başarı oranlarının belirleyecek metrikler geliştirilmesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları, Özel Sektör | | |
| **TEE Teknolojileri Kullanılan Yeni Mobil Cihaz Güvenlik Çözümleri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Yapay Zekâ, Veri Mühendisliği, İstatistik | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Uygulama Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine yönelik olarak, uluslararası standartlara (ISO/IEC 13335, ISO/IEC 12207) uyumlu kod güvenlik analiz ve test teknolojileri ile mevcut kullanımdaki uygulamaların zafiyet yönetimini yapacak ve güvenli işletilmesini sağlayacak teknolojilerin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmekredir. Buna yönelik olarak **«Kod güvenlik analiz ve test teknolojileri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Uygulama Güvenliği Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | • Yazılım seviyesinde yazılımsal açıkları tespit edebilmesi<br>• Yazılım seviyesinde tersine mühendislik saldırılarına karşı kod karıştırma, vb. tekniklerin kullanılması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları, Özel Sektör | | |
| **Kod Güvenlik Analiz Ve Test Teknolojileri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Yapay Zeka, Veri Mühendisliği, İstatistik | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Uygulama Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine yönelik olarak, uluslararası standartlara (ISO/IEC 13335, ISO/IEC 12207) uyumlu kod güvenlik analiz ve test teknolojileri ile mevcut kullanımdaki uygulamaların zafiyet yönetimini yapacak ve güvenli işletilmesini sağlayacak teknolojilerin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Uygulamaların zafiyet yönetimini yapacak ve güvenli işletilmesini sağlayacak teknolojiler»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Uygulama Güvenliği Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | • Mevcut işletim sistemlerinin güvenirliğini arttırmak için zafiyetleri mümkün olduğu kadar otomatik tespit edip hızlı ve dinamik önlem alabilen yöntemlerin geliştirilmesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Teknopark Firmaları, Üniversiteler, Kamu Araştırma Merkezleri, Kamu Kurumları, Özel Sektör | | |
| **Uygulamaların Zafiyet Yönetimini Yapacak ve Güvenli İşletilmesini Sağlayacak Teknolojiler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Yapay Zeka, Veri Mühendisliği, İstatistik | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Bulut Güvenliği

**Öncelikli Ürün ve Teknolojiler**

**Bulut Güvenliği Teknolojileri**

Tespit (*detection*), önleme (*prevention*), etki azaltma (*mitigation*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine ve ağ, yazılım seviyeleri ile veri kaçağı, yetkisiz erişim, yetki yükseltme siber tehdit unsurlarına yönelik olarak, bulut sistemlerinin siber güvenlik kontrollerinin gerçekleştirilmesini ve gerekli güvenlik önlemlerinin uygulanabilmesini sağlayacak, 5G altyapı bileşenlerinin ihtiyaçlarını karşılayacak, bulut ortamında yönetilen verilerin güvenliği ve mahremiyeti ve bulut altyapılarına güvenli entegrasyon sağlayacak teknolojiler ile bu altyapılardan faydalanmak için bulut tabanlı siber güvenlik teknolojilerinin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Bulut ortamında yönetilen verilerin güvenliği ve mahremiyeti ile bulut altyapılarına güvenli entegrasyonunu sağlayacak teknolojiler»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir.

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-8** |
|---|---|

**Öncelikli Ar-Ge ve Yenilik Konusu**

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

Bulut Altyapısını Kurmak için Büyük Ölçekli Veri Hizmeti Sunan Kuruluşlar, ISP (*Internet Service Provider*), Bulut Sistemi Yöneticilerine Sahip KOBİ'ler, Teknopark Firmaları, Kamu Araştırma Merkezleri, Üniversiteler; Müşteri Olarak Büyük Ölçekli Veri Merkezi İşleyen veya İşleten Kamu Kurumları

**Bulut Ortamında Yönetilen Verilerin Güvenliği ve Mahremiyeti İle Bulut Altyapılarına Güvenli Entegrasyonunu Sağlayacak Teknolojiler**

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Makine Öğrenmesi, Ağ Uzmanlığı, Donanım Programlama ve Geliştirme, Kriptoloji, Yazılım Geliştirme, Bulut Sistemi Uzmanlığı

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Mevcut bulut sağlayıcılarının üzerinde kullanılabilecek güvenlik servislerinin geliştirilmesi (*App store* ürünü gibi. Platform kurulana kadar tekno)
- Bulut ortamında çalışan güvenlik hizmeti verilmesi (örn. bulut imaj sunucusu olarak FaaS)
- Bulut hizmetinin sağlanmasında sanal makinelerinin yerine kullanılan konteynerların güvenliği de önemlidir. Konteynır güvenliği (aralarındaki ağ ve imajlalarının güvenliği)
- Konteynerlerin üzerinde çalıştığı hostların güvenliği
- FaaS güvenliğini sağlayacak bulut teknolojilerin geliştirilmesi (bu tip teknolojiler neredeyse tamamen bulut sağlayıcıya bağlıdır)
- SaaS güvenliğini sağlayacak bulut teknolojilerin geliştirilmesi
- Donanım bazlı kriptografik yapıları da içerecek Smart NIC gibi güvenlik çözümleri içermesi
    - Donanımsal güvenlik öncelikli olması
    - Hızlandırıcı kartlar içermesi
    - İlgili standartları destekleyecek donanımlar geliştirilmesi
    - Yan kanala karşı dayanıklı ürünler olması
    - Altyapının kurulması için bu donanımların öncelikli olarak bulunması
    - Yeni kanal saldırıları çok hızla gelişen bir alan olduğundan çiplerin üretimi ve güncellenmesi
- Yeni gelişen atakları takip edip sistemi sürekli güncel tutması, Homomorfik Şifreleme kullanılması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Bulut Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*), etki azaltma (*mitigation*) ve saldırı (*cyber warfare*) bertaraf yöntemlerine ve ağ, yazılım seviyeleri ile veri kaçağı, yetkisiz erişim, yetki yükseltme siber tehdit unsurlarına yönelik olarak, bulut sistemlerinin siber güvenlik kontrollerinin gerçekleştirilmesini ve gerekli güvenlik önlemlerinin uygulanabilmesini sağlayacak, 5G altyapı bileşenlerinin ihtiyaçlarını karşılayacak, bulut ortamında yönetilen verilerin güvenliği ve mahremiyeti ve bulut altyapılarına güvenli entegrasyon sağlayacak teknolojiler ile bu altyapılardan faydalanmak için bulut tabanlı siber güvenlik teknolojilerinin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Bulut altyapılarından faydalanmak için bulut tabanlı siber güvenlik teknolojileri (kötücül yazılım analiz araçları, aykırılık tespiti, DDoS karşıtı önlemler, vb.)»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma ve Teknoloji Geliştirme Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Bulut Güvenliği Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **3-6** | • Mevcut bulut sağlayıcılarının üzerinde kullanılabilecek güvenlik servislerinin geliştirilmesi (App store ürünü gibi. Platform kurulana kadar tekno)<br>• Bulut ortamında çalışan güvenlik hizmeti verilmesi (örn. bulut imaj sunucusu olarak FaaS)<br>• SDN ve NFV teknolojileri kullanılarak bulut güvenlik servislerinin geliştirilmesi<br>• DDoS saldırılarına karşı bulut teknolojisi destekli ölçeklenebilir güvenlik çözümlerinin geliştirilmesi<br>• DDoS saldırılarına karşı hız ve güvenlik önemli olduğu için linux kennel tarafından desteklenen özelliklere (eBPF,XDP, vb.) sahip olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Bulut Altyapısını Kurmak için Büyük Ölçekli Veri Hizmeti Sunan Kuruluşlar, ISP (*Internet Service Provider*), Bulut Sistemi Yöneticilerine Sahip KOBİ'ler, Teknopark Firmaları, Kamu Araştırma Merkezleri, Üniversiteler; Müşteri Olarak Büyük Ölçekli Veri Merkezi İşleyen veya İşleten Kamu Kurumları | | |
| **Bulut Altyapılarından Faydalanmak için Bulut Tabanlı Siber Güvenlik Teknolojileri (Kötücül Yazılım Analiz Araçları, Aykırılık Tespiti, Ddos Karşıtı Önlemler, vb.)** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Makine Öğrenmesi, Ağ Uzmanlığı, Donanım Programlama ve Geliştirme, Kriptoloji, Yazılım Geliştirme, Bulut Sistemi Uzmanlığı | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler Teknoloji

# Siber Güvenlik - Kriptoloji

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine ve özellikle yazılım seviyesi siber tehdit unsurlarına yönelik olarak, kuantum kriptografi ve kuantum sonrası kriptografi teknolojilerini kullanan siber güvenlik teknolojilerinin geliştirilmesi, açık kaynaktan geliştirilen kriptografik yazılımların güvenlik açıklarının tespitini yapacak teknik altyapıların oluşturulması hedeflenmektedir. Buna yönelik olarak **«Kuantum kriptografi teknolojileri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Kuantum Kriptografi ve Kuantum Sonrası Kriptografi Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **7-8** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, KOBİ'ler, Araştırma Merkezleri, Kamu Kurumları (DDO vb.) | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Makina Mühendisliği | |
| **Kuantum Kriptografi Teknolojileri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- "Kuantum Bilgi, Kuantum Bilgi İletim ve Kuantum Hesaplama Teknolojileri"nin geliştirilmesi
  - Kuantum mesajları bir yerden bir yere güvenli şekilde aktarımının yapılmasına yönelik teknoloji ve tekniklerin geliştirilmesi
  - Kuantum bilgi şifreleme ve bilgi aktarım teknolojileri ve algoritmaları
  - Bu alanda teorik araştırmalar- Kuantum bilgi şifreleme ve bilgi aktarım algoritmaları
- Mevcutta var olan ürün ve sistemlerin kuantum sırası ve sonrası gizlilik ve güvenliğinin sağlanması
- Anahtar dağıtımını güvenli olarak (fiber, uydu ve otonom araçlar ile bağlantılı anahtar dağıtım sistemi gibi) gerçekleştirebilen Hibrit Sistemlerin tasarlanması
- Kuantum anahtar geliştirilmesi ve anahtar dağıtım sistemlerinin uydu ve otonom araçlar bazlı sistemleri üzerinden tasarlanması
- Kuantum bilgisayarlarda polinom zamanda (veya yakın karmaşıklık) kriptoanaliz algoritmalarının geliştirilmesi
- Kriptoanaliz odaklı kuantum bilgisayar tasarımına odaklanılması
- Kuantum anahtar geliştirilmesi ve anahtar dağıtım sistemlerinin fiber, uydu ve otonom araçlar bazlı sistemleri üzerinden tasarlanması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Kriptoloji

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine ve özellikle yazılım seviyesi siber tehdit unsurlarına yönelik olarak, kuantum kriptografi ve kuantum sonrası kriptografi teknolojilerini kullanan siber güvenlik teknolojilerinin geliştirilmesi, açık kaynaktan geliştirilen kriptografik yazılımların güvenlik açıklarının tespitini yapacak teknik altyapıların oluşturulması hedeflenmektedir. Buna yönelik olarak **«Kuantum sonrası kriptografi teknolojileri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Kuantum Kriptografi ve Kuantum Sonrası Kriptografi Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, Araştırma Merkezleri | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Makina Mühendisliği | |
| **Kuantum Sonrası Kriptografi Teknolojileri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- "Kuantum Bilgi, Kuantum Bilgi İletim ve Kuantum Hesaplama Teknolojileri"nin geliştirilmesi
  - Kuantum mesajları bir yerden bir yere güvenli şekilde aktarımının yapılmasına yönelik teknoloji ve tekniklerin geliştirilmesi
  - Kuantum bilgi şifreleme ve bilgi aktarım teknolojileri ve algoritmaları
  - Bu alanda teorik araştırmalar- Kuantum bilgi şifreleme ve bilgi aktarım algoritmaları
- Uzun süre gizli kalması gereken bilgilerin kuantum hesaplamaya karşı güvenliği için acil çözümler geliştirilmesi ve mevcut sistemlere entegre edilmesi
- Simetrik şifrelemeyi desteklemesi:
  - Mevcut anahtar boyutlarının/ blok uzunluklarının güncellenmesi ve yeni tasarımların geliştirilmesi
  - Mevcut mimari/sistemlere yakın performans (anahtar boyutu, hız vb. bakımlardan) gösterebilen ve/veya performansı iyileştirilmiş
- Asimetrik şifrelemeyi desteklemesi:
  - Yenilikçi tasarımların geliştirilmesi
  - Algoritmik alt modüllerin güncellenmesi
  - Haberleşme protokollerinin güncellenmesi/iyileştirilmesi
  - Belirli ihtiyaçlara uygun alt işlemci tasarımları
  - Mevcuda yakın performans (anahtar boyutu, hız vb.) gösterebilen ve/veya performansı iyileştirilmiş olması
  - Yapılacak tasarımların güvenlik analizlerinin tasarlanması ve ilgili gerçek zamanlı algoritmaların eşzamanlı olarak tasarlanması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Kriptoloji

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Tespit (*detection*), önleme (*prevention*) ve etki azaltma (*mitigation*) bertaraf yöntemlerine ve özellikle yazılım seviyesi siber tehdit unsurlarına yönelik olarak, kuantum kriptografi ve kuantum sonrası kriptografi teknolojilerini kullanan siber güvenlik teknolojilerinin geliştirilmesi, açık kaynaktan geliştirilen kriptografik yazılımların güvenlik açıklarının tespitini yapacak teknik altyapıların oluşturulması hedeflenmektedir. Buna yönelik olarak **«Açık kaynaktan geliştirilen kriptografik yazılımların güvenlik açıklarının tespitini yapacak teknik çözümler»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | |
| **Kuantum Kriptografi ve Kuantum Sonrası Kriptografi Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, Araştırma Merkezleri | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Makina Mühendisliği | | |
| **Açık Kaynaktan Geliştirilen Kriptografik Yazılımların Güvenlik Açıklarının Tespitini Yapacak Teknik Çözümler** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1 Yıl** | |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- "Kuantum Bilgi, Kuantum Bilgi İletim ve Kuantum Hesaplama Teknolojileri"nin geliştirilmesi
  - Kuantum mesajları bir yerden bir yere güvenli şekilde aktarımının yapılmasına yönelik teknoloji ve tekniklerin geliştirilmesi
  - Kuantum bilgi şifreleme ve bilgi aktarım teknolojileri ve algoritmaları
  - Bu alanda teorik araştırmalar- Kuantum bilgi şifreleme ve bilgi aktarım algoritmaları

- Yazılım zayıflık ve zafiyetlerinin giderilmesi ve test edilmesi ve test edilebilmesine yönelik yerli yazılım araçlarının geliştirilmesi
- Zararlı yazılımların test edilmesi ve test edilebilmesine yönelik yerli yazılım araçlarının geliştirilmesi
- İlgili tersine mühendislik yazılımlarının geliştirilmesi
- Yan kanal analizleri için var olan yöntemlerin gerçek zamanlı uygulanması
- Yan kanal analizleri için yenilikçi yöntemlerin tasarlanması (özellikle donanımsal özel ihtiyaçları karşılayabilecek)
- Özellikle gizli ve çok gizli güvenlik seviyeleri için kritik olan donanımsal çözümlerin, yazılım çözümleri ile eşzamanlı olarak geliştirilmesi

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Siber Güvenlik - Dijital Adli Analiz

**Öncelikli Ürün ve Teknolojiler**

**Dijital Adli Analiz Teknolojileri**

**Öncelikli Ar-Ge ve Yenilik Konusu**

**Olay Müdahale (DFIR) Teknolojileri**

Tespit (detection) bertaraf yöntemine ve donanım seviyesi ile veri kaçağı, yetkisiz erişim, yetki yükseltme, ifşa/mahremiyet siber tehdit unsurlarına yönelik olarak, dijital ortamlarının (telefon, sabit disk) kopyasını alabilecek, kopya ortamlar üzerinde inceleme, sayısal delil ayrıştırma ve raporlama yapabilecek; siber saldırılarda son kullanıcı cihazlarından delil toplama gibi özelliklere sahip, olay müdahale (DFIR) teknolojilerinin yerli olarak geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Olay müdahale (DFIR) teknolojileri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir.

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
|---|---|

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

Üniversiteler, Teknopark Firmaları, Başlangıç Firmaları, KOBİ'ler, Büyük Ölçekli Firmalar, Araştırma Merkezleri, Kamu Kurumları

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Adli Bilişim, Bilgisayar Mühendisliği, Yazılım Mühendisliği, Elektrik ve Elektronik Mühendisliği, İstatistik, Matematik, Yapay Zekâ ve Makine Öğrenmesi, Hukuk, Adli Tıp

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1 Yıl** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Masaüstü, dizüstü, tablet, cep tel benzeri mobil cihazlar vb. sunucu tip bilgisayarlarda kullanıcı şifrelerinin kırılması için yerli donanım ve ilgili yazılımlarının geliştirilmesi
- Adli kopyalama donanımları/yazılımları (Veri yazma-koruma donanım ve yazılımları dahil)
- Ağ izleme donanım ve yazılımları
- Veri kurtarma donanım ve yazılımları
- Güvenli veri silme donanım ve yazılımları
- Ram bellek (uçucu bellek) görüntü alma donanım ve yazılımları
- Yapay zeka tabanlı yazılımların geliştirilmesi– Özellikle Yapay zeka ve makine öğrenmesi tabanlı Senaryo analizleri, analitik yazılımlar vb.
- Adli bilişim analizi amaçlı biyometrik veri ve ses analizlerinin donanım ve yazılımları
- Adli süreçlerde uzun vadeli dijital veri ve görüntü saklamaya/arşivlemeye yönelik bulut ve blokzincir tabanlı yazılımlar
- Adli bilişim analizlerinde kullanılacak, dijital para üzerinde geriye dönük suç analizi ve transfer takibi yapabilen yazılımlar
- Mobil uygulamalar özelinde, adli bilişim analizler yapılabilmesine yönelik kullanıcı hareketleri yazılımları
- Büyük veri sistemlerinin adli bilişim analizlerinin/incelemelerinin yapılmasına yönelik yazılımlar
- Ulusal/Uluslararası hukuk altyapılarının uyumluluk takibini gerçekleştirecek yazılımlar
- Olay müdahalede son kullanıcı cihazlardan gerçek zamanlı çoklu veri toplayabilecek yazılım ve sistemlerin geliştirilmesi
- EDR/XDR sistemlerin yerli geliştirilmesi ve yaygınlaştırılması
- Derin paket analizi yapabilecek donanım ve yazılımlar
- Ağ seviyesinde veri toplanabilmesi ve gerçek zamanlı adli bilişim analizleri için NDR teknolojilerinin geliştirilmesi
- Nesnelerin internetine yönelik adli bilişim inceleme yazılımları

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Telekomünikasyon ve Haberleşme Sektörleri ile Dijital Altyapılar Sektörü - Ağ ve İletişim Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Yeni geliştirilen 5G ve ötesi benzeri haberleşme teknolojilerinin, nesnelerin interneti haberleşme protokollerinin, baz istasyonlarının ve ilgili siber güvenlik teknolojilerinin ve ürünlerinin yerli olarak geliştirilmesi hedefine yönelik olarak **«5G ve ötesi haberleşme teknolojileri için fiziksel katman güvenliği teknolojileri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **5G ve Ötesi Haberleşme Teknolojileri, IoT Protokolleri ve Baz İstasyonları için Yerli Siber Güvenlik Teknolojileri ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-3** |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları, KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar; Uluslararası İşbirlikleri | • Ağ seviyesinde yüksek band genişliği ve hızın desteklenmesi<br>• Veri kaçağı açısından DLP teknolojilerinin kullanılması<br>• Daha az işlem gücü ve daha az enerji gerektiren donanımsal işlemlerde (özellikle buluttan edge yönelimi olduğu için) siber saldırıları yapay zekâ destekli ve otomatik olarak tespit edip engelleyecek sistemler geliştirmesi<br>• Hizmet kesintisi saldırılarını engelleyebilir nitelikte olması<br>• Maliyet etkin kriptolojik yaklaşımların kullanılması, ayrıca buna yönelik uzman denetimi yapılması<br>• Ağ seviyesinde uydu haberleşme cihazlarında transec/netsec ve comsec vb. özellikli yerli cihazlar kullanılması<br>• Yapay zekâ tabanlı uç düğüm (Edge AI) çözümleri geliştirilmesi<br>• Hiyerarşik Uç ve Üst Seviye Veri Optimizasyonu, DNS ve Web Bellekleme ve Filtreleme vb. yapabilmesi<br>• "Güvenli haberleşme gereken kullanım alanları ile 5G ve ötesi yeni haberleşme teknolojilerinde (SDN dahil) güvenlik çözümleri, GTP / Diameter ve 5G güvenlik duvarları (*firewall*)" teknik özelliklerini de kapsaması |
| **5G ve Ötesi Haberleşme Teknolojileri için Fiziksel Katman Güvenliği Teknolojileri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik, Bilgisayar Bilimleri, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6 Yıl** |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler — Teknoloji

# Telekomünikasyon ve Haberleşme Sektörleri ile Dijital Altyapılar Sektörü - Ağ ve İletişim Güvenliği ve OT, IoT Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Yeni geliştirilen 5G ve ötesi gibi haberleşme teknolojilerinin, nesnelerin interneti haberleşme protokollerinin, baz istasyonlarının ve ilgili siber güvenlik teknolojilerinin ve ürünlerinin yerli olarak geliştirilmesi hedefine yönelik olarak **«5G ve ötesi, IoT ve baz istasyonları için yerli siber güvenlik teknolojileri ve ürünleri (SDN/NFV tabanlı güvenlik uygulamaları ve SDN/NFV güvenliği dahil)»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme Projeleri** desteklenecektir. | |
| **5G ve Ötesi Haberleşme Teknolojileri, IoT Protokolleri ve Baz İstasyonları için Yerli Siber Güvenlik Teknolojileri ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-6** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları, KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar; Uluslararası İşbirlikleri | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik, Bilgisayar Bilimleri, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | |
| **5G ve Ötesi, IoT Ve Baz İstasyonları için Yerli Siber Güvenlik Teknolojileri ve Ürünleri (SDN/NFV Tabanlı Güvenlik Uygulamaları ve SDN/NFV Güvenliği Dahil)** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Ağ seviyesinde yüksek band genişliği ve hızın desteklenmesi
- Veri kaçağı açısından DLP teknolojilerinin kullanılması
- Hizmet kesintisi saldırılarını engelleyebilir nitelikte olması
- Ağ seviyesinde uydu haberleşme cihazlarında transec/netsec ve comsec vb. özellikli yerli cihazlar kullanılması
- Yetkisiz erişim açısından merkezi ve tümleşik izleme/loglama/raporlama araçları kullanılması
- Siber saldırıları yapay zekâ destekli ve otomatik olarak tespit edip engelleyecek sistemler geliştirmesi
- Ağ, yazılım ve donanım seviyelerinde IEC62351 standardına göre ürünlerin tasarlanması (TCP/IP vb.)
- Maliyet etkin kriptolojik yaklaşımların kullanılması, ayrıca buna yönelik uzman denetimi yapılması
- SDN ve NFV uyumlu olması
  - Ağ dilimleri arası izolasyon güvenliği sağlaması
  - 5G Ağ fonksiyonları için Güvenlik Grupları ve Güvenlik Politika Sunucusu geliştirilmesi
  - 3GPP R16 desteği olması
- "Güvenli haberleşme gereken kullanım alanları ile 5G ve ötesi yeni haberleşme teknolojilerinde (SDN dahil) güvenlik çözümleri, GTP / Diameter ve 5G güvenlik duvarları (*firewall*)" teknik özelliklerini de kapsaması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Akıllı Üretim Sistemleri, İmalat Sektörü ve Tedarik Zinciri, Lojistik Sektörü - Ağ ve İletişim Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Ağ, yazılım seviyeleri ile yetkisiz erişim ve veri kaçağı siber tehdit unsurlarına yönelik, imâlat sektörü ve tedarik zinciri ile lojistik sektörlerini ihtiyaçlarını da kapsayacak şekilde akıllı üretim sistemlerine özgü ağ trafiğinin yönetimi ve anomali tespiti, akıllı üretim sistemlerine yönelik güvenli haberleşme, siber saldırıların tespiti ve önlenmesini sağlayacak teknolojilerin geliştirilmesi hedefine yönelik olarak **«Akıllı üretim sistemlerine özgü ağ trafiğinin yönetimi ve anomali tespiti çözümleri»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Akıllı üretim sistemlerinde ağ trafiğinin yönetimi, güvenli haberleşme, siber saldırı önleme teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-8** | • Kablolu ve kablosuz ağ trafiğini takip edebilen, dinleyen, bu protokolleri anlamlandıran sistemler geliştirilmesi ve bu protokollere yönelik saldırı tipleri anlamlandırılıp trafik dinleme yöntemlerine entegre edilmesi<br>• Enerji problemi olan cihazlar açısından IPS olması (Performans metrikleri OT ve IoT olarak değişmektedir.)<br>• M2M haberleşme protokolleri<br>• Gecikme konusunun önemli olduğu durumlarda protokol bazlı koruma yerine AIOT için donanım bazlı güvenlik çözümlerinin geliştirilmesi (Smart NIC vb.) ve donanımın yükünü azaltan, donanım hızlandırıcı ile desteklenmesi<br>• Ürün paketten çıktığında güvenlik önlemlerinin alınmış olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Özel Sektör, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar; Uluslararası İşbirlikler | | |
| **Akıllı üretim sistemlerine özgü ağ trafiğinin yönetimi ve anomali tespiti çözümleri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Kablosuz Ağ Güvenliği, Kriptoloji, Ofansif Güvenlik, Donanım Üretim Teknolojileri, Yapay Zeka ve Makine Öğrenmesi, İtibar Sistemleri, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Akıllı Üretim Sistemleri, İmalât Sektörü ve Tedarik Zinciri, Lojistik Sektörü - Ağ ve İletişim Güvenliği - OT, IoT Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Ağ, yazılım seviyeleri ile yetkisiz erişim ve veri kaçağı siber tehdit unsurlarına yönelik, imâlat sektörü ve tedarik zinciri ile lojistik sektörlerini ihtiyaçlarını da kapsayacak şekilde akıllı üretim sistemlerine özgü ağ trafiğinin yönetimi ve anomali tespiti, akıllı üretim sistemlerine yönelik güvenli haberleşme, siber saldırıların tespiti ve önlenmesini sağlayacak teknolojilerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Akıllı üretim sistemlerine yönelik güvenli haberleşme, itibar sistemleri, erişimin kontrol ve yetkilendirme sistemleri, RFID, IoT, Pick-to-Light gibi ürünlerden veri kaçağının önlenmesi, siber saldırıların tespiti ve önlenmesini sağlayacak teknolojiler»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Akıllı Üretim Sistemlerinde Ağ Trafiğinin Yönetimi, Güvenli Haberleşme, Siber Saldırı Önleme Teknolojileri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-8** | • Kablolu ve kablosuz ağ trafiğini takip edebilen,dinleyen ve bu protokolleri anlamlandıran sistemler<br>• Protokollere yönelik saldırı tiplerinin anlamlandırılıp, trafik dinleme yöntemlerine entegre edilmesi<br>• Enerji problemi olan cihazlar açısından IPS<br>• M2M haberleşme protokolleri<br>• Gecikme konusunun önemli olduğu durumlarda protokol bazlı koruma yerine AIOT için donanım bazlı güvenlik çözümleri (Smart NIC vb.)<br>• Donanımın yükünü azaltan donanım hızlandırıcı<br>• Ürün paketten çıktığında güvenlik önlemlerinin alınmasının sağlanması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Özel Sektör, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar; Uluslararası İşbirlikler | | |
| **Akıllı Üretim Sistemlerine Yönelik Güvenli Haberleşme, İtibar Sistemleri, Erişimin Kontrol ve Yetkilendirme Sistemleri, RFID, IoT, Pick-to-Light gibi Ürünlerden Veri Kaçağının Önlenmesi, Siber Saldırıların Tespiti ve Önlenmesini Sağlayacak Teknolojiler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Kablosuz Ağ Güvenliği, Kriptoloji, Ofansif Güvenlik, Donanım Üretim Teknolojileri, Yapay Zeka ve Makine Öğrenmesi, İtibar Sistemleri, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Otomotiv ve Ulaşım Sektörleri - Ağ ve İletişim Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Özellikle ağ ve yazılım seviyeleri siber tehdit unsurlarına yönelik, otomotiv ve ulaşım sektör ihtiyaçlarına yönelik güvenlik duvarı, kimlik ve erişim yönetimi gibi temel güvenlik ürünlerinin ve çözümlerinin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedefine yönelik olarak **«Otomotiv ve ulaşım sektör ihtiyaçlarına (kara, hava, deniz) yönelik güvenlik duvarı, kimlik ve erişim yönetimi gibi temel güvenlik ürünleri ve çözümleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Otomotiv ve Ulaşım Sektörlerinde Temel Siber Güvenlik Ürünleri ve Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-7** | • Yanıltma sinyali (*spoofing*) saldırılarına karşı sürekli algılama yapılması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerinin sürekli takip edilip, algılanması<br>• Kara delik (*blackhole*) saldırılarını algılama<br>• *Mesh* ağlarda karşılaşılabilecek saldırıların algılanması<br>• Gerekli durumlarda sistemlerin yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması<br>• Güvenli güncelleme ve bakım özelliği olması<br>• Elektromanyetik sızıntılara karşı dayanıklı olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Ölçekli Sanayi Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar, Uluslararası İşbirlikleri | | |
| **Otomotiv ve Ulaşım Sektör İhtiyaçlarına (Kara, Hava, Deniz) Yönelik Güvenlik Duvarı, Kimlik ve Erişim Yönetimi gibi Temel Güvenlik Ürünleri ve Çözümleri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik ve İstatistik, Uygulamalı Veri Bilimi, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Otomotiv ve Ulaşım Sektörleri - Otonom Hareketli Sistemleri Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Özellikle ağ ve yazılım seviyeleri siber tehdit unsurlarına yönelik, otomotiv ve ulaşım sektör ihtiyaçlarına yönelik güvenlik duvarı, kimlik ve erişim yönetimi gibi temel güvenlik ürünlerinin ve çözümlerinin yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedefine yönelik olarak **«Akıllı ve otonom araçlara uzaktan ve her türlü kablosuz iletişim üzerinden gerçekleştirilebilecek siber saldırıları tespit edebilecek ve bu saldırıları engelleyebilecek güvenlik teknolojileri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Otomotiv ve Ulaşım sektörlerinde temel siber güvenlik ürünleri ve çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-7** | • Yanıltma sinyali (*spoofing*) saldırılarına karşı sürekli algılama yapılması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerinin sürekli takip edilip, algılanması<br>• Kara delik (*blackhole*) saldırılarını algılama<br>• *Mesh* ağlarda karşılaşılabilecek saldırıların algılanması<br>• Gerekli durumlarda sistemlerin yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması<br>• Güvenli güncelleme ve bakım özelliği olması<br>• Elektromanyetik sızıntılara karşı dayanıklı olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Ölçekli Sanayi Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurumları, STK'lar, Uluslararası İşbirlikleri | | |
| **Akıllı ve otonom araçlara uzaktan ve her türlü kablosuz iletişim üzerinden gerçekleştirilebilecek siber saldırıları tespit edebilecek ve bu saldırıları engelleyebilecek güvenlik teknolojileri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik ve İstatistik, Uygulamalı Veri Bilimi, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Enerji Sektörü - Ağ ve İletişim Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Enerji sektörü ihtiyaçlarına yönelik saldırı tespit, veri şifreleme ve yedekleme, veri kaçağı önleme sistemi gibi siber güvenlik çözümlerinin yerli olarak geliştirilmesi hedefine yönelik olarak **«Enerji sektörü ihtiyaçlarına yönelik saldırı tespit ve önleme, veri şifreleme ve yedekleme, veri kaçağı önleme sistemi gibi siber güvenlik çözümleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Enerji Sektörü İhtiyaçlarına Yönelik Siber Güvenlik Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **3-7** | • Yazılım seviyesi ve veri kaçağı açısından hem veri güvenliğini sağlayıp, hem de verileri yedekleyip olası saldırı sonrası kurtarılmasının sağlaması<br>• Elektrik dağıtım ve iletim şebekelerinin SCADA sistemleri ile güvenli haberleşmesinin sağlaması<br>• Enerji yönetim sistemlerinin özellikle donanım (kontrol kartları, RTU, PLC, vb.) ve yazılım seviyelerinde güvenli şekilde uzaktan kontrolünü sağlayan ürünlerin uluslararası standartlara uygun olarak geliştirilmesi<br>• Ülke genelindeki enerji aktarımı dijital altyapısına gelebilecek siber saldırıların engellenmesi için saldırı tespit ve önleme sistemlerinin % 100 yerli olarak geliştirilmesi |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları; KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurum ve Kuruluşları, STK'lar, Uluslararası İşbirlikleri | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektrik ve Elektronik Mühendisliği, Enerji Mühendisliği, Temel Mühendislik Alanları, Kontrol Mühendisliği, Ağ, Donanım, Algılama ve Tahmin Etme, SCADA, Hukuk | | |
| **Enerji Sektörü İhtiyaçlarına Yönelik Saldırı Tespit ve Önleme, Veri Şifreleme ve Yedekleme, Veri Kaçağı Önleme Sistemi Gibi Siber Güvenlik Çözümleri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Kamu Hizmetleri Sektörü - Ağ ve İletişim Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Kamuda ihtiyaçlara yönelik güvenlik duvarı, saldırı tespit, veri kaçağı önleme sistemi gibi siber güvenlik çözümlerinin yerli olarak geliştirilmesi ile kamuda kullanılan donanımlarda ve gömülü tüm cihazlarda (açık kaynak kodlu) milli işletim sisteminin güvenliğinin artırılması ve kullanım sürdürülebilirliğinin sağlayacak şekilde yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Kamuda ihtiyaçlara yönelik güvenlik duvarı, saldırı tespit, veri kaçağı önleme sistemi gibi siber güvenlik çözümleri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Kamuda İhtiyaçlara Yönelik Siber Güvenlik Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | • Ağ ve uygulama seviyelerinde güvenlik uygulamalarının yüksek performanslı çalışabilmesi<br>• Yazılım seviyesi ile veri kaçağı ve ifşa/mahremiyet açısından veritabanı korumasının güçlendirilmesi, erişim yetkilerinin sınırlandırılması<br>• Geliştirilen/geliştirilecek açık kaynak kodlu milli işletim sistemleri üzerinde çalışacak ek güvenlik uygulamalarının geliştirilmesi, test edilmesi, yaygınlaştırılması<br>• Kamu bilişim ağlarının en az bir seviye güvenliğinin yerli ürünlerle sağlanabilmesi için ürünlerin sektördeki eşleniklerinin fonksiyonalitesinde olması<br>• Kamunun özel ihtiyaçlarına çözümler oluşturması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurum ve Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları ve Özel Sektörün Yer Aldığı Konsorsiyumlar | | |
| | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Yapay Zeka, Veri Mühendisliği, İstatistik | | |
| **Kamuda ihtiyaçlara yönelik güvenlik duvarı, saldırı tespit, veri kaçağı önleme sistemi gibi siber güvenlik çözümleri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** | |

Tüm Sektörler | Teknoloji

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

# Kamu Hizmetleri Sektörü - Uygulama Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Kamuda ihtiyaçlara yönelik güvenlik duvarı, saldırı tespit, veri kaçağı önleme sistemi gibi siber güvenlik çözümlerinin yerli olarak geliştirilmesi ile kamuda kullanılan donanımlarda ve gömülü tüm cihazlarda (açık kaynak kodlu) milli işletim sisteminin güvenliğinin artırılması ve kullanım sürdürülebilirliğinin sağlayacak şekilde yaygınlaştırılması / güçlendirilmesi / geliştirilmesi hedefienmektedir. Buna yönelik olarak **«Kamuda kullanılan milli işletim sisteminin güvenliğini artırıcı çözümler»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Kamuda ihtiyaçlara yönelik siber güvenlik çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | • Kullanıcının cihazlarını kullanırken kaynak kullanımı, performans kaybı, yavaşlık, hizmet kesintisi gibi kullanıcı deneyimini ve verimliliğini olumsuz etkileyecek faktörlerin kabul edilebilir endüstri standartlarının seviyesinde olması<br>• Kullanıcı cihazlarında, kullanıcı ya da yönetici onayı olmadan işletim sistemi seviyesinde ve kritik dosyalarda yapılan güncellemelerin ve konfigürasyon değişikliklerinin tespit edilmesi ve engellenmesi<br>• Kullanıcılara gereğinden fazla verilmiş olan veya artık ihtiyaç duyulmayan ve kullanılmayan yetkilerin belirlenerek kaldırılması<br>• Kullanıcı cihazlarına kullanıcıların her zaman en düşük yetki seviyesi ile giriş yapması ve daha yüksek yetkilere ihtiyacı olan faaliyetleri gerçekleştirmesi gerektiğinde sadece ihtiyacı olduğu süre boyunca ve ihtiyaç duyduğu kadar yetki seviyesinin yükseltilmesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurum ve Kuruluşları, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları ve Özel Sektörün Yer Aldığı Konsorsiyumlar | | |
| **Kamuda kullanılan milli işletim sisteminin güvenliğini artırıcı çözümler** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Bilgisayar Mühendisliği, Yapay Zeka, Veri Mühendisliği, İstatistik | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2 Yıl** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Kamu Hizmetleri Sektörü (Eğitim Sektörü dahil) - Bulut Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Ağ, donanım seviyeleri ile fiziksel saldırılar, yetkisiz erişim ve veri kaçağı siber tehdit unsurlarına yönelik, kamu ve özel sektör verilerinin depolanması ve paylaşımında kullanılmak üzere güvenli bulut teknolojilerinin ve ürünlerinin yerli olarak geliştirilmesi hedefine yönelik olarak **«Kamu ve özel sektör verilerinin ve servislerinin sunulabilmesi için IaaS, FaaS, PaaS ve SaaS bulut mimarilerinde güvenlik çözümleri geliştirilmesi»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | |
| **Kamu ve Özel Sektör Verileri için Güvenli Bulut Teknolojileri ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **3-9** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurumları, Kamu Araştırma Merkezleri, Büyük Ölçekli Kuruluşlar, KOBİ'ler, Teknopark Firmalar ve Üniversiteler | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Makine Öğrenmesi, Ağ ve Donanım, Kriptoloji, Yazılım Mühendisliği, Siber Güvenlik, Bulut Sistem Yönetimi, Hukuk, Blokzincir | |
| **Kamu ve Özel Sektör Verilerinin ve Servislerinin Sunulabilmesi için Iaas, Faas, Paas ve Saas Bulut Mimarilerinde Güvenlik Çözümleri Geliştirilmesi** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5 Yıl** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Ağ seviyesinde erişimin kesintisiz olması
- Yazılım seviyesinde güvenli uçtan uca ağ protokolü geliştirilmesi
- Yetkisiz erişim açısından güvenlik ve çok farktörlü doğrulama çözümlerinin iyileştirilmesi
- Veri kaçağı açısından sunucu güvenliğini sağlayacak, kişisel verilerin korunmasını ve verilerin şifreli olarak güvenli saklanmasını sağlayacak çözümler geliştirilmesi
- Uygun kriptolojik yaklaşımların geliştirilmesi ve kullanılması, ayrıca buna yönelik uzman denetimi yapılması
- Kimlik doğrulama ve parola güvenliği için uygun kriptolojik çözümlerin geliştirilmesi ve uygulanması
- "Çevrim içi eğitim sistemlerinde ve çözümlerinde" siber güvenlik ve kriptoloji teknolojileri ve "Güvenli video konferans çözümleri" için ölçeklenebilir ve uçtan uca güvenlik sağlayabilmesi
- Kamu veya özel sektörün çevrim içi hizmetlerinin bulut güvenlik servisleri kullanılarak hizmete sunması (Proxy olarak bulut ortamının kullanılarak hizmet vermesi, Cloudflare örneği gibi) ile güvenli veri depolama ve paylaşımı
- Kayıt tutma, kimlik doğrulama, yetkilendirme vb. servisleri ile teknoloji ve çözümlerin geliştirilmesi

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Kamu Hizmetleri Sektörü (Eğitim Sektörü dahil) - Bulut Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Ağ, donanım seviyeleri ile fiziksel saldırılar, yetkisiz erişim ve veri kaçağı siber tehdit unsurlarına yönelik, kamu ve özel sektör verilerinin depolanması ve paylaşımında kullanılmak üzere güvenli bulut teknolojilerinin ve ürünlerinin yerli olarak geliştirilmesi hedefine yönelik olarak **«Eğitim sektörü açısından çevrim içi eğitim sistemlerinde ve çözümlerinde siber güvenlik ve kriptoloji teknolojileri geliştirilmesi»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Kamu ve Özel Sektör Verileri için Güvenli Bulut Teknolojileri ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **3-9** | • Ağ seviyesinde erişimin kesintisiz olması<br>• Yazılım seviyesinde güvenli uçtan uca ağ protokolü geliştirilmesi<br>• Yetkisiz erişim açısından güvenlik ve çok farktörlü doğrulama çözümlerinin iyileştirilmesi<br>• Veri kaçağı açısından sunucu güvenliğini sağlayacak, kişisel verilerin korunmasını ve verilerin şifreli olarak güvenli saklanmasını sağlayacak çözümler geliştirilmesi<br>• Uygun kriptolojik yaklaşımların geliştirilmesi ve kullanılması, ayrıca buna yönelik uzman denetimi yapılması<br>• Kimlik doğrulama ve parola güvenliği için uygun kriptolojik çözümlerin geliştirilmesi ve uygulanması<br>• “Çevrim içi eğitim sistemlerinde ve çözümlerinde” siber güvenlik ve kriptoloji teknolojileri ve “Güvenli video konferans çözümleri” için ölçeklenebilir ve uçtan uca güvenlik sağlayabilmesi<br>• Kamu veya özel sektörün çevrim içi hizmetlerinin bulut güvenlik servisleri kullanılarak hizmete sunması (Proxy olarak bulut ortamının kullanılarak hizmet vermesi, Cloudflare örneği gibi) ile güvenli veri depolama ve paylaşımı<br>• Kayıt tutma, kimlik doğrulama, yetkilendirme vb. servisleri ile teknoloji ve çözümlerin geliştirilmesi |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurumları, Kamu Araştırma Merkezleri, Büyük Ölçekli Firmalar, KOBİ’ler, Teknopark Firmaları, Üniversiteler | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Makine Öğrenmesi, Ağ ve Donanım, Kriptoloji, Yazılım Mühendisliği, Siber Güvenlik, Bulut Sistem Yönetimi, Hukuk, Blokzincir | | |
| **Eğitim Sektörü Açısından Çevrim İçi Eğitim Sistemlerinde ve Çözümlerinde Siber Güvenlik ve Kriptoloji Teknolojileri Geliştirilmesi** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Finans ve Ticaret Sektörleri - Bulut Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle ağ ve yazılım seviyeleri siber tehdit unsurlarına yönelik, ülkemiz finansal hizmet sağlayıcılarının ihtiyaçlarını karşılayacak, özellikle yurt dışından gelen ataklara karşı operatörler seviyesinde yüksek kapasiteli, bulut tabanlı bir koruma sistemi oluşturulması ve finansal ağın (para trafiğinin) sürekliliğinin sağlanması hedeflenmektedir. Bunacyönelik olarak **«Finansal hizmet sağlayıcılarını yurt dışından gelen ataklara karşı koruyacak bulut tabanlı sistem»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Finansal Hizmet Sağlayıcılarının Ataklara Karşı Yüksek Kapasiteli, Bulut Tabanlı Korunması ve Finansal Ağın Sürekliliği** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri**: **2-7**<br><br>**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurumları, Kamu Araştırma Merkezleri, Büyük Ölçekli Firmalar, KOBİ'ler, Teknopark Firmaları, Üniversiteler | • Veri kaçağı açısından veri güvenliği amacıyla veri sızıntısı önleme çözümleri diğer güvenlik çözümleriyle de entegre olabilecek şekilde API destekli olması, davranış analiz tespiti çözümü içermesi anormal veri çıkışlarının tespit edilebilmesi<br>• İfşa/mahremiyet açısından kişisel verilerin ifşasını engellemek adına veri sızıntısını önleme çözümü veri sızıntılarını tespit için farklı veritabanlarına entegre olabilmesi, anahtar kelime (*keyword*) ve sıralı özel karakter (*regex*) tabanlı kural desteği ile birlikte farklı formattaki verileri tespit edebilmesi<br>• Verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünlerin geliştirilmesi<br>• Veri tabanı tarafında güvenlik, gizlilik ve doğruluğun sağlanmasına yönelik kriptolojik çözümlerin geliştirilmesi ve kullanılması<br>• Ağ seviyesinde yüksek kapasiteli saldırı tespit sistemlerine sahip (IPS, *Intrusion Prevention System*) ağ cihazları geliştirilmesi<br>• Yazılım seviyesinde saldırıları önleyecek web uygulamaları güvenlik duvarına sahip olması (WAF - *Web Application Firewall*)<br>• Sosyal mühendislik açısından oltalama saldırıları simülasyonları içermesi<br>• Yetkisiz erişim ve yetki yükseltme açısından hesap yönetim araçları içermesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Makine Öğrenmesi, Ağ ve Donanım, Kriptoloji, Yazılım Mühendisliği, Siber Güvenlik, Bulut Sistem Yönetimi, Hukuk, Blokzincir, Finans | |
| **Finansal Hizmet Sağlayıcılarını Yurt Dışından Gelen Ataklara Karşı Koruyacak Bulut Tabanlı Sistem** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu**: **5** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Finans ve Ticaret Sektörleri - Bulut Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Öncelikle ağ ve yazılım seviyeleri siber tehdit unsurlarına yönelik, ülkemiz finansal hizmet sağlayıcılarının ihtiyaçlarını karşılayacak, özellikle yurt dışından gelen ataklara karşı operatörler seviyesinde yüksek kapasiteli, bulut tabanlı bir koruma sistemi oluşturulması ve finansal ağın (para trafiğinin) sürekliliğinin sağlanması hedeflenmektedir. Buna yönelik olarak **«Finans ve Ticaret sektörleri için veri kaçağını engelleme ve veri mahremiyetini koruma ürünleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | |
| **Finansal Hizmet Sağlayıcılarının Ataklara Karşı Yüksek Kapasiteli, Bulut Tabanlı Korunması ve Finansal Ağın Sürekliliği** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **2-7** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Kamu Kurumları, Kamu Araştırma Merkezleri, Büyük Ölçekli Firmalar, KOBİ'ler, Teknopark Firmaları, Üniversiteler | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Makine Öğrenmesi, Ağ ve Donanım, Kriptoloji, Yazılım Mühendisliği, Siber Güvenlik, Bulut Sistem Yönetimi, Hukuk, Blokzincir, Finans | |
| **Finans ve Ticaret Sektörleri için Veri Kaçağını Engelleme ve Veri Mahremiyetini Koruma Ürünleri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Veri kaçağı açısından veri güvenliği amacıyla veri sızıntısı önleme çözümleri diğer güvenlik çözümleriyle de entegre olabilecek şekilde API destekli olması, davranış analiz tespiti çözümü içermesi anormal veri çıkışlarının tespit edilebilmesi
- İfşa/mahremiyet açısından kişisel verilerin ifşasını engellemek adına veri sızıntısını önleme çözümü veri sızıntılarını tespit için farklı veritabanlarına entegre olabilmesi, anahtar kelime (keyword) ve sıralı özel karakter (regex) tabanlı kural desteği ile birlikte farklı formattaki verileri tespit edebilmesi
- Verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünlerin geliştirilmesi
- Veri tabanı tarafında güvenlik, gizlilik ve doğruluğun sağlanmasına yönelik kriptolojik çözümlerin geliştirilmesi ve kullanılması
- Ağ seviyesinde yüksek kapasiteli saldırı tespit sistemlerine sahip (IPS, Intrusion Prevention System) ağ cihazları geliştirilmesi
- Yazılım seviyesinde saldırıları önleyecek web uygulamaları güvenlik duvarına sahip olması (WAF - Web Application Firewall)
- Sosyal mühendislik açısından oltalama saldırıları simülasyonları içermesi
- Yetkisiz erişim ve yetki yükseltme açısından hesap yönetim araçları içermesi

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

# Kamu Hizmetleri Sektörü (Kritik Altyapılar ve Sağlık dahil) - Kriptoloji

| | |
|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Özellikle ağ seviyesi ve veri kaçağı siber tehdit unsurlarına yönelik, kamuda (öncelikle kritik kamu hizmetleri, e-devlet uygulamaları ve sağlık sektörü olmak üzere) verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünlerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Kamuda verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünler»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. |
| **Kamuda Veri Şifrelemesinde Güvenli Kriptografi Teknolojilerini Kullanan Ürünler** | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | |
| **Kamuda Verilerin Şifrelenmesinde Kuantum Ataklara Karşı Güvenli Kriptografi Teknolojilerini Kullanan Ürünler** | |

| | |
|---|---|
| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **3-7** |
| **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, KOBİ'ler, Araştırma Merkezleri, Kamu Kurumları | |
| **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Yazılım Mühendisliği, Adli Bilişim | |
| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **5** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Kamuda kullanılan kriptografik ürünlerin sertifikasyonu ve güvenlik/gizlilik ihtiyacı çalışmaları
- Kuantum/ Yan kanal ataklarına karşı güvenliği iyileştirilmiş yöntemler
- Kuantum sonrası algoritmaların standartlaşma öncesinde mevcut kriptografik ürünler için Göç Planı oluşturulması
    - Kritik konumda kullanılan şifreleme cihazlarındaki anahtar paylaşımı ve yönetiminin kuantum bilgisayarlara karşı dirençli bir hale getirilmesi,
    - Kritik konumda kullanılan simetrik şifreler için anahtar boyutlarının kuantum güvenlik düzeyine gelebilmesi için yeterliliğinin analiz edilmesi ve gerekli ise artırılması,
    - Kritik bilgilerin en kısa sürede kuantum bilgisayarlara karşı dirençli hale getirilmesi için çalışmalar yapılması
- Post kuantum öncesi-standartlaşma öncesi
    - Asimetrik şifreleme kullanan kuantum öncesi ürünlerin, post kuantum sonrası duruma göre güncellenmesi/adapte edilmesi ve gizlilik/güvenlik sağlama
    - Simetrik algoritma tabanlı sistemlerin anahtar boylarının yeterliliğinin analiz edilmesi gerekli ise arttırılması
- Post kuantum sonrası-standartlaşma sonrası
    - Standartlaşmanın sağlanması ve standartların gerçeklenmesine yönelik çalışmalar
    - Standartlaşan algoritmaların Donanım/İşlemciler üzerinde güvenli ve performanslı olarak tasarlanması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Kamu Hizmetleri Sektörü (Kritik Altyapılar ve Sağlık dahil) - Kriptoloji

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Özellikle ağ seviyesi ve veri kaçağı siber tehdit unsurlarına yönelik, kamuda (öncelikle kritik kamu hizmetleri, e-devlet uygulamaları ve sağlık sektörü olmak üzere) verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünlerin geliştirilmesi hedefine yönelik olarak **«Biyometrik ve çok aşamalı kimlik doğrulama teknolojileri (özellikle Kritik Kamu Hizmetleri)»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Kamuda Veri Şifrelemesinde Güvenli Kriptografi Teknolojilerini Kullanan Ürünler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, KOBİ'ler, Araştırma Merkezleri, Kamu Kurumları | |
| **Biyometrik ve Çok Aşamalı Kimlik Doğrulama Teknolojileri (Özellikle Kritik Kamu Hizmetleri)** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Yazılım Mühendisliği, Adli Bilişim | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Mahremiyet odaklı ve KVKK uyumlu yeni nesil mobil cihazlar (cep tel vb.) üzerinde kullanılabilen djital kimlik teknolojilerinin geliştirilmesi
- Kriptografik anahtarlar ve/veya verilerin korunacağı ve kriptografik anahtarlarla güvenli işlem yaparak verileri işleyecek Dijital cüzdan teknolojilerin geliştirilmesi ve güvenliklerinin test edilmesi
- Kamu kurumlarındaki verilen güvenliğinin arttırılması için Dijital cüzdan uygulamaları kapsamında kamunun kullanımı için uygun donanım güvenlik modülleri (HSM) geliştirilmesi
- Davranışsal biyometri araştırmaları
- Yapay zeka destekli biyometri çalışmaları (yüz tanıma teknolojileri vb.)
- Merkezi olarak toplanan verilerin gizliliğin ve güvenli depolama teknolojileri
- Dağıtık defter teknolojileri (distributed ledger) ve blokzincir gibi ademi merkezi (merkezi olmayan) sistemlerin güvenliğinin araştırılması ve kamunun kullanımı için bu sistemlerin geliştirilmesi
- Ademi merkezi anahtar yönetim sistemlerinin araştırılması ve kamuda kullanımın uygunluğunun araştırılması

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Kamu Hizmetleri (Kritik Altyapılar ve Sağlık Sektörü dahil) - Kriptoloji

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Özellikle ağ seviyesi ve veri kaçağı siber tehdit unsurlarına yönelik, kamuda (öncelikle kritik kamu hizmetleri, e-devlet uygulamaları ve sağlık sektörü olmak üzere) verilerin şifrelenmesinde kuantum ataklara karşı güvenli kriptografi teknolojilerini kullanan ürünlerin geliştirilmesi hedeflenmektedir. Buna yönelik olarak **«Büyük veri dahil olmak üzere, veri koruma güvenlik teknolojileri, ürünleri ve kriptolojik çözümleri (özellikle Sağlık Sektörü)»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | |
| **Kamuda Veri Şifrelemesinde Güvenli Kriptografi Teknolojilerini Kullanan Ürünler** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **7-9** |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Büyük Ölçekli Firmalar, KOBİ'ler, Araştırma Merkezleri, Kamu Kurumları | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Fizik, Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Yazılım Mühendisliği, Adli Bilişim | |
| **Büyük Veri Dahil Olmak Üzere, Veri Koruma Güvenlik Teknolojileri, Ürünleri ve Kriptolojik Çözümleri (Özellikle Sağlık Sektörü)** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1** |

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Kamuda kullanılan kriptografik ürünlerin sertifikasyonu ve güvenlik/gizlilik ihtiyacı çalışmaları
- Kuantum/ Yan kanal ataklarına karşı güvenliği iyileştirilmiş
- Kuantum sonrası algoritmaların standartlaşma öncesinde mevcut kriptografik ürünler için Göç Planı oluşturulması
    - Kritik konumda kullanılan şifreleme cihazlarındaki anahtar paylaşımı ve yönetiminin kuantum bilgisayarlara karşı dirençli bir hale getirilmesi,
    - Kritik konumda kullanılan simetrik şifreler için anahtar boyutlarının kuantum güvenlik düzeyine gelebilmesi için yeterliliğinin analiz edilmesi ve gerekli ise artırılması,
    - Kritik bilgilerin en kısa sürede kuantum bilgisayarlara karşı dirençli hale getirilmesi için çalışmalar yapılması
- Post kuantum öncesi standartlaşma öncesi
    - Asimetrik şifreleme kullanan kuantum öncesi ürünlerin, post kuantum sonrası duruma göre güncellenmesi/adapte edilmesi ve gizlilik/güvenlik sağlama
    - Simetrik algoritma tabanlı sistemlerin anahtar boylarının yeterliliğinin analiz edilmesi gerekli ise arttırılması
- Post kuantum sonrası-standartlaşma sonrası
    - Standartlaşmanın sağlanması ve standartların gerçeklenmesine yönelik çalışmalar
    - Standartlaşan algoritmaların Donanım/İşlemciler üzerinde güvenli ve performanslı olarak tasarlanması
- Mahremiyet odaklı ve KVKK uyumlu sistemlerin geliştirilmesi (Verilerin gizliliği ve veri paylaşımı konuları özelinde)
- Sağlık sektörü için özellikle homomorfik şifreleme/kripto teknolojileri
- Şifreleme-imzalama teknolojileri ile sağlık sektöründe gizlilik/güvenliğin geliştirilmesi

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Finans ve Ticaret Sektörleri Sektörü - Kriptoloji

**Öncelikli Ürün ve Teknolojiler**

**E-ticaret ve Sanal Alışveriş için Dijital Varlıkların Kullanımına Yönelik Kriptografik Çözümler ve Bu Sistemlere Yönelik Siber Güvenlik Çözümleri**

E-ticaret ve sanal alışveriş için dijital varlıkların kullanımına yönelik kriptografik çözümler ve bu sistemlere yönelik siber güvenlik çözümleri hedefine yönelik olarak **«E-ticaret ve sanal alışveriş için dijital varlıkların kullanımına yönelik kriptografik çözümler»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir.

| **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-8** |
|---|---|

**Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**

Üniversiteler, Büyük Ölçekli Firmalar, KOBİ'ler, Araştırma Merkezleri, Kamu Kurumları

**Öncelikli Ar-Ge ve Yenilik Konusu**

**E-ticaret ve Sanal Alışveriş için Dijital Varlıkların Kullanımına Yönelik Kriptografik Çözümler**

**Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**

Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Yazılım Mühendisliği, Adli Bilişim

| **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **1** |
|---|---|

**Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar**

- Siber saldırılara karşı kriptografik çözümler geliştirilmesi ve yetkisiz erişim, veri kaçağı ve ifşa/mahremiyet açılarından KVKK'ya uyumlu koruma sağlanması
- Kimlik denetimi ve yetkilendirme, KVKK, veri mahremiyeti, uyumluluk, yasallık gibi pek çok konuda yaşanacak güvenlik problemlerine çözüm olabilecek uygun kriptografik ve Biyometrik çözümler ortaya konması
- Blokzincir temelli ve mahremiyet odaklı dijital kimlik teknolojileri geliştirilmesi (KVKK ve GDPR uyumlu)
- Uç cihazlardaki kriptografik anahtarların ve/veya verilerin güvenli saklanabileceği ve işleneceği yazılım/donanım Dijital Cüzdan'lar, genel anlamda mobil ortamda çalışan çözümler ve bunlara yönelik siber güvenlik çözümlerinin geliştirilmesi. Buna karşılık Servis sağlayıcılardaki verilerin güveliğinin arttırılmasına yönelik donanım destekli (örn: HSM) çözümlerin geliştirilmesi
- Blokzincir temelli dijital para teknolojileri alanında son kullanıcıya yönelik uygulamalar ve bunlara yönelik siber güvenliğine yönelik çözümler
- Mobil ortamlardaki kripto analiz çalışmaları ve beyaz kutu (whitebox) testlerinin geliştirilmesi

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler Teknoloji

# Finans ve Ticaret Sektörleri Sektörü - Kriptoloji

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | E-ticaret ve sanal alışveriş için dijital varlıkların kullanımına yönelik kriptografik çözümler ve bu sistemlere yönelik siber güvenlik çözümleri hedefine yönelik olarak **«E-ticaret ve sanal alışveriş için dijital varlıklara yönelik siber güvenlik çözümleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **E-ticaret ve Sanal Alışveriş için Dijital Varlıkların Kullanımına Yönelik Kriptografik Çözümler ve Bu Sistemlere Yönelik Siber Güvenlik Çözümleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **1-9** | • Uçtan uca siber güvenlik çözümleri/sistemlerinin geliştirilmesi<br>• Ağ seviyesinde sızma (penetration) ve diğer bilgi güvenliği saldırılarına karşı test sistemleri geliştirilmesi<br>• Dağıtık defter ve blokzincir güvenliğine yönelik çalışmalar<br>• Nesnelerin interneti ve implantlara yönelik siber güvenlik çalışmaları<br>• Bilgi güvenliği ürünlerinin test standartlarının belirlenmesi (Common Criteria Protection Profile vb.)<br>• Milli mobil işletim sistemi geliştirilmesi<br>• 3 boyutlu yazıcılarda copyright sorunları ve çıkan ürünlerin sertifikasyon sorunlarına ilişkin yenilikçi çözümler |
| | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Üniversiteler, Araştırma Merkezleri, Büyük Ölçekli Firmalar, KOBİ'ler, Kamu Kurumları | | |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Matematik, İstatistik, Elektrik Elektronik Mühendisliği, Bilgisayar Mühendisliği, Kontrol ve Haberleşme Mühendisliği, Yazılım Mühendisliği, Adli Bilişim | | |
| **E-ticaret ve Sanal Alışveriş için Dijital Varlıklara Yönelik Siber Güvenlik Çözümleri** | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **6** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

# Savunma, Havacılık ve Uzay sektörleri  Sektörü - Ağ ve İletişim Güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Savunma, Havacılık ve Uzay sektörleri ihtiyaçlarına yönelik siber güvenlik teknolojileri ve ürünleri hedefine yönelik olarak **«Savunma sistemlerinde merkezi olmayan otonom siber güvenlik çözümleri»** geliştirilmesi amacıyla **Teknoloji Geliştirme ve Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Savunma, Havacılık ve Uzay Sektörleri İhtiyaçlarına Yönelik Siber Güvenlik Teknolojileri ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **4-8** | • Kriptoloji destekli yüksek performanslı güvenlik duvarı içermesi<br>• Aviyonik sistemler ve saldırı ağaçlarının geliştirilmesi<br>• Yanıltma sinyali (spoofing) saldırılarına karşı sürekli algılaması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerini sürekli takip edip algılaması<br>• Kara delik (blackhole) saldırılarını algılama<br>• Mesh ağlarda karşılaşılabilecek saldırıların algılanması<br>• Sistemlerin yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması ve ulusal kripto sistemleri de desteklemesi<br>• Güvenli güncelleme ve bakım özelliği olması<br>• Elektromanyetik sızıntılara karşı dayanıklı olması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları, KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurumları, STK'lar | | |
| **Savunma Sistemlerinde Merkezi Olmayan Otonom Siber Güvenlik Çözümleri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik ve İstatistik, Uygulamalı Veri Bilimi, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **3** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Savunma, Havacılık ve Uzay sektörleri Sektörü – Otonom Hareketli Sistemleri Güvenliği

| | | |
|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Savunma, Havacılık ve Uzay sektörleri ihtiyaçlarına yönelik siber güvenlik teknolojileri ve ürünleri hedefine yönelik olarak **«İHA'lar için sağlayacak Elektronik Koruyucu Tedbirler (*Electronic Protective Measures* - EPM) teknolojileri ve ürünleri»** geliştirilmesi amacıyla **Temel/Uygulamalı Araştırma, Teknoloji Geliştirm ve Yenilik Projeleri** desteklenecektir. | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Savunma, Havacılık ve Uzay Sektörleri İhtiyaçlarına Yönelik Siber Güvenlik Teknolojileri Ve Ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri**: **3-8** | • Kriptoloji destekli yüksek performanslı güvenlik duvarı içermesi<br>• Aviyonik sistemler ve saldırı ağaçlarının geliştirilmesi<br>• Yanıltma sinyali (*spoofing*) saldırılarına karşı sürekli algılaması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerini sürekli takip edip algılaması<br>• Kara delik (*blackhole*) saldırılarını algılaması<br>• *Mesh* ağlarda karşılaşılabilecek saldırıların algılanması<br>• Sistemler yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması ve ulusal kripto sistemleri de desteklemesi<br>• Güvenli güncelleme ve bakım özelliği olması<br>• Elektromanyetik sızıntılara karşı dayanıklı olması<br>• Ağ seviyesinde karıştırılamaz ve bastırılamaz uydu iletişim sistemleri oluşturulması<br>• İleri seviye fiziksel katman güvenliği çözümleriyle desteklenmesi<br>• Ağ seviyesinde RF ağların denetlenmesi ve kontrolünün sağlanması |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları, KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurumları, STK'lar | |
| **İHA'lar için Sağlayacak Elektronik Koruyucu Tedbirler (*Electronic Protective Measures* - EPM) Teknolojileri Ve Ürünleri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik ve İstatistik, Uygulamalı Veri Bilimi, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu**: **3** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji

# Savunma, Havacılık ve Uzay sektörleri  Sektörü - Uygulama güvenliği

| | | | |
|---|---|---|---|
| **Öncelikli Ürün ve Teknolojiler** | Savunma, Havacılık ve Uzay sektörleri ihtiyaçlarına yönelik siber güvenlik teknolojileri ve ürünleri hedefine yönelik olarak **«Savunma sektörü ürünleri ve uygulamaları için kod güvenliği, veri kaçağını önleme, saldırı tespit ve önleme, vb. siber güvenlik çözümleri ve teknolojileri»** geliştirilmesi amacıyla **Yenilik Projeleri** desteklenecektir. | | **Projelerin Odaklanması Beklenen Yenilikçi Özellikler/Metrikler/Çalışmalar** |
| **Savunma, Havacılık ve Uzay sektörleri ihtiyaçlarına yönelik siber güvenlik teknolojileri ve ürünleri** | **Desteklenecek Projelerin Kapsayacağı Teknolojik Hazırlık Seviyeleri** | **6-9** | • Kriptoloji destekli yüksek performanslı güvenlik duvarı içermesi<br>• Aviyonik sistemler ve saldırı ağaçlarının geliştirilmesi<br>• Yanıltma sinyali (*spoofing*) saldırılarına karşı sürekli algılaması<br>• Sistem içi birimlerin ve sistem bütününün davranışsal anormalliklerini sürekli takip edip algılaması<br>• Kara delik (*blackhole*) saldırılarını algılaması<br>• *Mesh* ağlarda karşılaşılabilecek saldırıların algılanması<br>• Sistemler yapay zekâ ve makine öğrenmesi ile zenginleştirilmesi<br>• Kriptolojik yöntemlerin kullanılması ve ulusal kripto sistemleri de desteklemesi<br>• Güvenli güncelleme ve bakım özelliği olması<br>• Elektromanyetik sızıntılara karşı dayanıklı olması<br>• Ağ seviyesinde RF ağların denetlenmesi ve kontrolünün sağlanması<br>• İleri seviye / hedef odaklı saldırıların (*Advanced Threats / Targeted Attacks*) ve gelişmiş kalıcı tehditlerin (APT) tespitini ve önlenmesine yönelik ürünlerin yapay zekâ destekli olarak geliştirilmesi |
| **Öncelikli Ar-Ge ve Yenilik Konusu** | **Tavsiye Edilen Ar-Ge ve Yenilik İş Birliği/Modeli**<br>Büyük Sanayi Kuruluşları, KOBİ'ler, Üniversiteler, Kamu Araştırma Merkezleri, Teknopark Firmaları, Kamu Kurumları, STK'lar | | |
| **Savunma sektörü ürünleri ve uygulamaları için kod güvenliği, veri kaçağını önleme, saldırı tespit ve önleme, vb. siber güvenlik çözümleri ve teknolojileri** | **Ar-Ge ve Yenilik Sürecinde Bir Araya Gelmesi Gereken Disiplinler**<br>Elektronik Mühendisliği, Kontrol ve Haberleşme, Temel Mühendislik Alanları, Matematik ve İstatistik, Uygulamalı Veri Bilimi, Yapay Zekâ ve Makine Öğrenmesi, Ağ, Donanım, Algılama ve Tahmin Etme, Hukuk | | |
| | **Öngörülen Ar-Ge ve Yenilik Süreci Uzunluğu** | **2** | |

Bu konu, **Siber Güvenlik Teknoloji Yol Haritası** temel alınarak hazırlanmıştır.

Tüm Sektörler | Teknoloji