Güvenlik Savunma ve Emniyet Yönetişimi Akademisi

*Security & Defense Governance Academy*

# ANALİZ

GUSEYAD | AKADEMİ

*GUSEYAD | ACADEMY*

# Türkiye Güvenlik Tehditleri

## NATO Taahhütlerinin Zayıflığı ve Siber Güvenlik Perspektifi

### -İsrail'in Tahran / Doha / Sumud Filosu Saldırıları Sonrası-

**Eylül 2025**
**İstanbul / TÜRKİYE**

www.guseyadakademi.org

# Türkiye Güvenlik Tehditleri

## NATO Taahhütlerinin Zayıflığı ve Siber Güvenlik Perspektifi

### -İsrail'in Tahran / Doha / Sumud Filosu Saldırıları Sonrası-

Uzm. **Burak Soner BOZKURTLAR** *

**ANALİZ / EYLÜL 2025**

GUSEYAD | AKADEMİ

* İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi (AUZEF) Acil Yardım ve Afet Yönetimi (AYAY) Lisans Tamamlama Programı / Ders Veren Uzman

**Yayın Tarihi:** Eylül 2025



**GUSEYAD / AKADEMİ**

**E-Posta:** bilgi@guseyadakademi.org

**‘’Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5’inci maddesinin 2’nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir.’’**

# Türkiye Güvenlik Tehditleri

## NATO Taahhütlerinin Zayıflığı ve Siber Güvenlik Perspektifi

### -İsrail'in Tahran / Doha / Sumud Filosu Saldırıları Sonrası-

## İÇİNDEKİLER


YÖNETİCİ ÖZETİ.....2
GİRİŞ.....4
BÖLÜMLER.....6
1. Türkiye'nin Jeopolitik Güvenlik Ortamı .....7
2. NATO Taahhütlerinin Zayıflığı.....10
3. İsrail'in Tahran / Doha Sumud Filosu Saldırıları Sonrası Yeni Dinamikler.....12
4. Siber Güvenlik Perspektifi.....14
5. Ulusal Siber Savunma Stratejileri.....16
6. Uluslararası İş Birliği ve Siber Diplomasi.....19
7. Sivil Toplum, Özel Sektör ve Akademinin Rolü.....21
SONUÇ.....23
KAYNAKÇA.....,,,,,,,,,,,,,,,,25
İNTERNET LİNKLERİ.....28

# YÖNETİCİ ÖZETİ

Gazze işgalinde ve Türkiye' ye komşu bölgelerde, ardı sıra gerçekleştirilen nokta operasyonlarla görünür hale gelen ***"hibrit savaş yöntemleri"***, kamuoyunda, olası saldırılarda benzer tekniklerin kullanılacağı algısını pekiştirmekte ve nasıl önlemler alındığı veya alınması gerektiğine ilişkin olarak merak ve arayışları çoğaltmaktadır. Tatmin edici cevap bulunamayınca da ***"hibrit savaş"*** ın parçası olan ***"toplumsal kaygı"***, günlük hayat döngüsünü bozacak etkinlikte olabilmektedir.

Günlük hayatı kolaylaştıran ve vazgeçilmez hale gelmiş olan teknolojik iletişim ve güvenlik cihazlarının, *–belki de alt / üst kat / yan daire komşumuz olan üst düzey güvenlik görevlisine yapılabilecek nokta operasyon hazırlığı için-* aylar öncesinden bilgi toplamak için kullanılabileceği güncel örnekleri başlangıçta çarpıcı birer haber olmakta, kaygıya yol açmaktadır. Ancak, art arda yaşanan benzeri olaylar bir süre sonra, günlük döngü içinde ***"tehdide alışma ve kanıksama"*** sonucunu doğurmakta, ama ***"tehdit artarak sürmekte"*** dir.

İsrail' in Tahran / Doha / Sumud Filosu saldırıları, ***"sivil görünümlü güvenlik teknolojileri"*** nin ve lojistik tedarik zincirlerinin ***"siber istihbarat yöntemleri"*** nin *hibrid savaşa entegre edilmesiyle etkin olarak kullanıldığını daha da belirgin hale getirmiştir.* Sıralanan ve bilinenin dışında, *örtülü birçok nokta operasyonda güvenlik teknolojilerinin kullanıldığı gerçeği,* yıkıcı örnekler olarak ve günlük faaliyetlerimizi de sekteye uğratacak derecede hayatımıza girmiş haldedir.

Operasyon hazırlıklarının yıllar öncesinden yapıldığını *-savaş suçu kapsamında sivil kayıpları göze alarak, otonom silahlar ile-* nokta operasyon emri verdiğini açıkça söyleyen, uluslararası ceza mahkemesinde soykırım suçundan yargılanan kişi, en önemli istihbarat kaynaklarının ***"akıllı mobil iletişim cihazları"*** olduğunu *açıkça ve toplumsal algıyı yönetmek için söyleyebilmektedir.*

Türkiye güvenlik kurumları, tarihsel ve jeopolitik konumunun getirdiği stratejik yükümlülüklerle birlikte, artık yalnızca kara ve denizlerde değil, toplumun günlük hayatı ile iç içe olan ***"siber uzay"*** da da güvenliği sağlamalı, *toplumsal kaygıyı ortadan kaldıracak önlemleri görünür olarak almalıdır.*

***Siber güvenlik,*** yalnızca devlet kurumlarının sorumluluğuna bırakılabilecek bir alan değildir.

- *Kritik altyapıların büyük bölümünün özel sektör kontrolünde olduğu,*

-*Dijital inovasyonların üniversitelerden doğduğu,*

-*Toplumsal farkındalığın sivil toplum kuruluşları aracılığıyla geliştiği,*

göz önünde bulundurulduğunda; ***"bütüncül bir güvenlik anlayışı"*** kaçınılmaz hale gelmektedir.

Toplumun dijital okuryazarlık düzeyi artırılmalı, güvenlikte en zayıf halka sorunu ortadan kaldırılmalı, düzenlenecek ***"farkındalık kampanyaları"*** ile uzman kuruluşlar rol üstlenmeli, doğal afetlerde gönüllüler nasıl sahaya çıkıyorsa, siber kriz anlarında da uzman düzeyinde olmasa bile, her bir vatandaşın, *-farkında olmadan düşmanın haber elemanı olmasını engelleyecek-,* ***"siber gönüllü"*** olarak görünmez hibrit savaşın *doğru / dost tarafında olması sağlanmalıdır.*

ÖZCAN ÖZGEN

Dijital olarak imzalayan ÖZCAN ÖZGEN
Tarih: 2025.09.26 14:51:59 +03'00'

## GİRİŞ

Türkiye, jeopolitik konumu gereği tarih boyunca doğu ile batı arasında stratejik bir köprü olmuştur. Bugün ise bu rol, yalnızca kara ve deniz hatlarıyla değil; ***siber uzayda şekillenen yeni güvenlik denkleminde*** de devam etmektedir. Küresel ölçekte devletlerin güvenlik tehditleri artık yalnızca askeri unsurlardan ibaret değildir; *kritik altyapılara yönelik siber saldırılar, hibrit savaş teknikleri, yapay zekâ destekli istihbarat faaliyetleri ve sosyal medya manipülasyonları,* ***ulusal güvenliğin temel parametrelerini dönüştürmektedir.***

Özellikle ***"İsrail' in Tahran / Doha / Sumud Filosu Saldırıları"*** *sonrası ortaya çıkan* ***"yeni jeopolitik tablo",*** Türkiye açısından güvenlik kaygılarının çeşitlendiğini göstermektedir. Bölgedeki güç dengeleri hızla değişmekte, NATO' nun, Türkiye' ye yönelik güvenlik taahhütleri ise tartışmalı bir noktaya sürüklenmektedir. Bu durum, Türkiye' nin kendi ***"ulusal güvenlik mimarisi"*** ni, özellikle de ***"siber güvenlik perspektifi"*** temelinde yeniden kurgulamasını zorunlu hale getirmektedir.

***Bu çalışmanın amacı,***

1. *Türkiye' nin mevcut güvenlik tehditlerini jeopolitik ve siber boyutlarıyla analiz etmek,*
2. *NATO' nun zayıflayan güvenlik taahhütlerini değerlendirmek,*
3. *İsrail' in Tahran / Doha / Sumud Filosu saldırılarının ardından bölgesel ve küresel dengelerde oluşan yeni parametreleri incelemek,*
4. *Türkiye için siber güvenlik odaklı stratejik bir perspektif geliştirmektir.*

Çalışmada ***Milli İstihbarat Akademisi (MİA)*** *tarafından yayımlanan* ***"analiz ve raporlar"*** [1] referans kaynağı olarak kullanılacaktır. NATO' nun *"Five Eyes"* benzeri istihbarat ağlarıyla [2] karşılaştırmalı olarak, Türkiye' nin ve Türk Dünyası' nın ortak bir ***"siber güvenlik vizyonu"*** geliştirmesi, ***"9 Işık Teknolojileri"*** [3] çerçevesinde değerlendirilecektir.

*Son olarak,* ***"Siber Güvenlik Başkanlığı"*** nın kurumsal yapılanması ve gelecekte oynayabileceği rol, Türkiye' nin "*dijital savunma kapasitesi"* ni güçlendirme bağlamında ayrı bir başlık altında ele alınacaktır. Böylelikle, Türkiye' nin *yalnızca savunmada değil, ayni zamanda saldırı ve caydırıcılık unsurlarında da* ***"dijital seferberlik"*** anlayışıyla hareket etmesi gerektiği ortaya konulacaktır.

---

[1] **MİA (Milli İstihbarat Akademisi)**, 12 Gün Savaşı ve Türkiye İçin Dersler, Rapor, Ağustos 2025.

[2] **Mermer, C.T., Dr.,** Beş Göz: Anglosakson Dünyanın İstihbarat İş Birliği Mekanizması, Makale, TASAM Yayını, İstanbul, 2022. Makalenin tamamı için bkz., https://tasam.org/tr-TR/Icerik/70102/bes_goz_anglosakson_dunyanin_istihbarat_is_birligi_mekanizmasi, 24 Eylül 2025 tarihinde ziyaret edildi. Bir başka önemli kaynak için bkz.; **İrem Tabirlioğlu,** Dijital Çağda İttifakın Gözü: Five Eyes, Stratejik Gözetim ve Yeni Nesil Tehditler, İstihbarat ve Güvenlik Araştırmaları Merkezi, Makale, 2025. https://igam.org.tr/dijital-cagda-ittifakin-gozu-five-eyes-stratejik-gozetim-ve-yeni-nesil-tehditler/, 24 Eylül 2025 tarihinde ziyaret edildi.

[3] **Bozkurtlar, B.S.,** İslam Ülkeleri İçin Siber Güvenlik Başlığında Yeni Bir Kurgu Biçimi: Yapay Zekâ Destekli Sistem Yöneticisi, Bildiri, 3. ASSAM Kongresi, İstanbul, 2019.

## BÖLÜMLER

# 1. Türkiye' nin Jeopolitik Güvenlik Ortamı

Türkiye, bulunduğu coğrafi konum itibarıyla tarih boyunca çok boyutlu tehditlere maruz kalmış bir ülkedir. **Orta Doğu, Doğu Akdeniz, Karadeniz ve Kafkasya** üçgeninde yer alması, ülkenin güvenlik risklerini çeşitlendirmekte ve sürekli olarak dinamik bir tehdit algısı üretmektedir.[4]

## 1.1. Bölgesel Tehditler

İsrail-Filistin çatışmaları, Suriye iç savaşı ve İran' ın bölgesel politikaları nedeniyle Ortadoğu' da yaşanan istikrarsızlıklar, Türkiye' nin başta sınır güvenliği olmak üzere, iç istikrarına doğrudan etki etmektedir.[5]

Doğu Akdeniz' de yaşanan enerji rekabeti, "*deniz yetki alanları, enerji nakil hatları ve doğal gaz rezervleri*" üzerinden yürütülmekte ve Türkiye' nin stratejik çıkarlarını tehdit etmektedir.

Kafkasya ve Karadeniz hattına baktığımızda da, Azerbaycan-Ermenistan gerilimi, Rusya-Ukrayna Savaşı ve Karadeniz' in "*güvenlik, enerji ve ulaştırma koridoru*" olması itibarı ile kontrol çabalarıyla karşılaşıyoruz ki, bütün bunlar, Türkiye' nin doğrudan güvenlik öncelikleri arasında yer almaktadır.[6]

## 1.2. Hibrit Tehditler ve Siber Unsurlar

Geleneksel askeri tehditlerin yanı sıra, ***hibrit savaş unsurları*** giderek daha belirleyici hale gelmektedir.[7]

---

[4] Bu konuda detaylı bilgi için bkz., **Şahin, Güngör,** "Orta Doğu ve Doğu Akdeniz'in Önemi: Tehditler, Riskler, Fırsatlar ve Türkiye", Makale, Güvenlik Stratejileri Dergisi, 15, S.29, 2019, s.199-230. https://doi.org/10.17752/guvenlikstrtj.554061, 24 Eylül 2025 tarihinde ziyaret edildi.

[5] **Sumud Filosu' na Saldırı, İtalya ve İspanya Donanma Gemisi Gönderiyor,** BBC NEWS Türkçe, Haber, 2025. https://www.bbc.com/turkce/articles/c147vx16x18o, 25 Eylül 2025 tarihinde ziyaret edildi.

[6] **Şensoy, S.,** Karadeniz ve Kafkaslar: Ekonomi, Enerji ve Güvenlik, TASAM Yayını, 2017, bkz., Önsöz. https://tasam.org/tr-TR/Icerik/49136/karadeniz_ve_kafkaslar_ekonomi_enerji_ve_guvenlik, 24 Eylül 2025 tarihinde ziyaret edildi.

[7] "Hibrit Tehdit" kavramı ve örnekleri için bkz., **Havan, C.**, Hibrit Tehditler ve Sosyal Politika: Düzensiz Göçün Getirdiği Toplumsal Çatışmalar ve Çözüm Önerileri, Sosyal Güvence Dergisi, Özel Sayı, 2025, s.215-224., https://dergipark.org.tr/tr/download/article-file/4789424, 24 Eylül 2025 tarihinde ziyaret edildi.

*Enerji, finans, sağlık ve ulaşım altyapıları gibi kritik sektörlere* yönelik *siber saldırılar,* devletlerin zayıf noktalarını hedef almaktadır.[8]

Kitlesel *dezenformasyonu hedefleyen eylemler ve algı operasyonları, sosyal medya üzerinden yürütülen kampanyalar,* iç politik istikrarı zedeleme potansiyeli taşımaktadır.

PKK, DEAŞ ve benzeri terör örgütleri, her geçen gün biraz daha dijitalleşen dünyada, çağın gereklerine ve teknolojik gelişmelere uygun olarak, propaganda ve finansman için *kripto para, dark-web ağları ve yapay zekâ tabanlı araçları* kullanmaktadır.

### 1.3. Enerji, Su ve Göç Eksenli Kırılganlıklar

Enerji günlük hayatın, bağımlılık seviyesinde en önemli parçası haline gelmiş durumdadır ve enerji nakil hatlarına yönelik sabotaj veya siber saldırı riskleri, Türkiye' nin enerji arz güvenliğini kırılgan hale getirmektedir.

Dünya genelinde yaşanan susuzluk, su kaynaklarının giderek azalması, bu alandaki zorunlu güvenlik ihtiyacını ön plana çıkarmaktadır. Ortadoğu' da su kaynaklarının stratejik önemi, Türkiye' nin *Fırat-Dicle Havzası üzerindeki politikalarını doğrudan hedef haline getirmektedir.*

Tüm dünyada yaşanan *göç hareketleri,* savaşlar, çatışmalar ve iklim değişikliği kaynaklı *göç dalgaları,* yalnızca insani değil, aynı zamanda *güvenlik boyutuyla da Türkiye' nin önüne yeni tehditler çıkarmaktadır.*

### 1.4. İç Güvenlik Boyutu

Türkiye' nin güvenlik ortamı yalnızca dış tehditlerle sınırlı değildir. İç dinamikler de ulusal güvenlik üzerinde belirleyici etkiye sahiptir:

Etnik ve mezhepsel fay hatları, dış aktörlerin desteklediği ayrılıkçı faaliyetler, zaman zaman ülke içinde güvenlik boşlukları yaratmaktadır.

Radikalleşme ve terör tehdidi günümüzde tüm dünya ülkelerinin gündemi haline gelmiş durumdadır. Dini radikalizm veya siyasi aşırılıklar, iç güvenliğin zayıf noktaları arasında sayılmaktadır.[9]

---

Ayrıca, bkz., Sumud Filosuna Saldırı, agy. https://www.bbc.com/turkce/articles/c147vx16x18o, 25 Eylül 2025 tarihinde ziyaret edildi.

[8] İsrail ve İran arasında yaşanan 12 Gün Savaşı esnasında her iki ülke tarafından kullanılan, "siber saldırılar, dezenformasyonlar ve algı operasyonları" nın örnekleri için bkz.; **MİA (Milli İstihbarat Akademisi)**, 12 Gün Savaşı ve Türkiye İçin Dersler, Rapor, Ağustos 2025, 27-28.

[9] **Çakır, M.F.,; Aslan, Ö., ve Diğerleri,** Radikalleşme, Şiddet İçeren Aşırılık ve Terörizm, Rapor No.8, Polis Akademisi Yayını, Ankara, 2017.

Özellikle büyük şehirlerde toplumsal olaylar, göç kaynaklı entegrasyon sorunları ve organize suç örgütleri, güvenlik güçlerinin sürekli teyakkuz halinde olmasını gerektirmektedir.

### 1.5. Savunma Sanayiinin Rolü

Türkiye' nin savunma sanayiindeki gelişmeleri, güvenlik ortamında ***caydırıcılık ve özerklik*** sağlamaktadır.

Yakın zamanda geliştirilen milli SİHA / İHA teknolojilerinin hem sınır ötesi operasyonlarda hem de iç güvenlikte etkin kullanımı sağlanmaktadır.[10]

Son dönemde savunma sanayii ihracatı artmıştır. Türk savunma ürünlerinin uluslararası pazarda tercih edilmesi, *diplomatik ve stratejik avantaj yaratmaktadır.*

Yerli yazılımlar, kriptografi çözümleri ve yapay zekâ destekli sistemler sayesinde gerçekleştirilen ***"Siber Savunma Entegrasyonu"*** faaliyetleri güvenlik altyapısının dayanıklılığını artırmaktadır.

*Tam bağımsızlık hedefinin* en önemli bileşenlerinden biri olan ***s****avunma sanayiinde dışa bağımlılığın azalması,* NATO' ya olan güvenlik bağımlılığını ***dengeleme potansiyeli*** taşımaktadır.

[10] Bu konuda daha detaylı bilgi için bkz., **Erdil, B.,** İnsansız Hava Araçlarının Kullanım Alanları ile Bu Araçların Türkiye' nin Yurtdışı Operasyonlarındaki Yeri ve Önemi, Makale, Bölgesel Araştırmalar Dergisi, 5 (2) Aralık 2021, s.581-607. https://dergipark.org.tr/en/download/article-file/1755805, 24 Eylül 2025 tarihinde ziyaret edildi.

## 2. NATO Taahhütlerinin Zayıflığı [11]

Türkiye, 1952 yılında NATO' ya katıldığından bu yana, ittifakın güneydoğu kanadında kritik bir rol üstlenmiştir. Ancak, özellikle "Soğuk Savaş" sonrası dönemde NATO' nun güvenlik taahhütleri ve Türkiye' ye bakışı, giderek daha tartışmalı hale gelmiştir.

### 2.1. Tarihsel Perspektif

Soğuk Savaş Dönemi' nde Türkiye, Sovyetler Birliği' ne karşı *NATO' nun ileri karakolu işlevi görmüş;* askeri üsleri ve stratejik konumu sayesinde *ittifakın vazgeçilmez bir üyesi olmuştur.*

Ancak*;* 1990 sonrası dönemde, NATO' nun tehdit algısının Balkanlar, Afganistan ve Orta Doğu' ya kaymasıyla, Türkiye' nin rolü *"lojistik destek"* ve *"kriz yönetimi"* ne indirgenmiştir.

Türkiye' nin güvenlik kaygıları, özellikle PKK Terör Örgütü bağlamında NATO tarafından yeterince dikkate alınmamış, bu da ittifaka olan güveni zedelemiş ve zaten var olan ***"çifte standart algısı"*** nın daha da güçlenmesinin yolunu açmıştır.

### 2.2. Güncel Çifte Standartlar

Türkiye, sınır ötesinden gelen *terör tehditlerine karşı NATO' dan somut destek görememekte* ve *terör tehdidi karşısında yalnız bırakılmaktadır.*

Türkiye hava savunma ihtiyaçları kapsamında müttefiklerden alamadığı desteği, Rus yapımı S-400 sistemleri ile aşmıştır. Bu tercih, F-35 Krizi ile sonuçlanmış ve *ülke savunmasına yönelik bu derece hayati bir konuda, NATO müttefikleri tarafından uygulanan yaptırımlar, güven krizini derinleştirmiştir.*

*Ege ve Doğu Akdeniz' de yakın dönemde yaşanan gerilimlerde, NATO üyesi Yunanistan ile yaşanan krizlerde ittifakın tarafsız davranmaması,* Türkiye' nin ***"stratejik yalnızlığını artırmaktadır."***

[11] NATO ile ilgili kapsamlı bir araştırma makalesi için bkz., **Çelik, S.,** Tarihsel Süreç İçerisinde Türkiye' de NATO Şüpheciliği, Makale, KTÜ-SBE, Sosyal Bilimler Dergisi, Yıl: 13, S.25, Haziran 2023, s.95-115. Ayrıca; İsrail' in İran' a karşı gerçekleştirdiği saldırı sonrasında yaşanan 12 gün savaşı bağlamında, NATO ile Türkiye iş birliğinde "*diplomasi ve ittifak ilişkileri*" nin ne kadar önemli olduğuna ilişkin İran örneği için bkz.; **MİA (Milli İstihbarat Akademisi)**, 12 Gün Savaşı ve Türkiye İçin Dersler, Rapor, Ağustos 2025, 32-33.

### 2.3. Ukrayna Savaşı ve NATO' nun Öncelikleri

Rusya-Ukrayna savaşı esnasında Ukrayna' ya odaklanan NATO savaşın ardından *tüm enerjisini Doğu Avrupa hattına yöneltmiştir.* Bu durum, Türkiye' nin güney sınırındaki tehditlerin ikinci planda kalmasına yol açmıştır.

*İstanbul Tahıl Anlaşması ve esir takasları* gibi girişimlerde, Türkiye' nin oynadığı ***"arabulucu rolü"*** saygınlıkla karşılanmış, önemi de ortaya çıkmış olmasına rağmen, *ittifak bu katkıları stratejik taahhütlere dönüştürememiştir.*

Türkiye, NATO üyesi olmasına rağmen[12], *güvenlik tehditleri karşısında çoğu zaman yalnız bırakılmakta ve* ***"jeopolitik yalnızlığa adeta itilmektedir."***

### 2.4. Güvenlik Garantilerinin Sorgulanması

Bu gelişmeler, Türkiye'de şu soruyu gündeme getirmektedir: *"**NATO gerçekten Türkiye' nin güvenliğini garanti ediyor mu?**"*

NATO Antlaşması' nın 5. maddesi, teoride *"kolektif savunma taahhüdü*" nü ifade etse de, pratikte söz konusu taahhüt, *siyasi çıkarlar ve öncelikler üzerinden şekillenmektedir.* Türkiye' nin yaşadığı tehditlerin çoğu, NATO tarafından *"ikincil öncelik"* olarak görülmekte, bu da *kolektif savunma ilkesinin etkinliğini tartışmalı hale getirmektedir.*

[12] Türkiye, NATO ile olan anlaşmasına sadık kalıp, yükümlülüklerine uyarken, benzer karşılığı görememektedir. Örneğin "*Türkiye, NATO ile Siber Güvenlik Anlaşması imzalayan ilk ülkedir.*" bkz. **Çiftçi, H.,** Her Yönüyle Siber Savaş, TÜBİTAK Popüler Bilim Kitapları, Ankara, 2023, s.42.

# 3. İsrail' in Tahran / Doha / Sumud Filosu Saldırıları Sonrası Yeni Dinamikler [13]

İsrail' in Tahran / Doha / Sumud Filosu' na yönelik saldırıları, *yalnızca askeri bir eylem olarak değil,* ***Ortadoğu ve Akdeniz bölgeleri güvenlik mimarilerinde yeni dengeler*** *yaratan bir gelişme olarak değerlendirilmelidir.* Bu saldırılar, İsrail' in, İran' ın ve Katar' ın bölgesel rollerini, Türkiye-İsrail, Türkiye-İran ve Türkiye-Katar ilişkilerini ve uluslararası güç dengelerini doğrudan etkilemiştir.

## 3.1. Askeri ve Psikolojik Etkiler

Askeri boyutuyla incelendiğinde, söz konusu saldırılar, bir taraftan *İsrail' in operasyonel kapasitesini göstermesinin* yanı sıra, diğer taraftan da *bölgesel caydırıcılığını artırmayı* hedeflemiştir. Ancak**, Katar gibi,** ***diplomatik merkez*** *niteliği taşıyan bir ülkeye yönelik hamlesi*, *uluslararası sulardaki bir insani yardım filosuna yönelik hamlesi,* ***uluslararası hukuk açısından*** *tartışma yaratmıştır.*

Saldırıların zamanlaması, *Tahran gibi bir ülke başkentini, Doha gibi küresel bir diplomasi merkezini, uluslararası sularda seyreden bir insani yardım filosunu hedef alması,* bölgede *"hiçbir yerin güvenli olmadığı"* algısını yaymayı amaçlayan bir ***"psikolojik savaş unsuru"*** olarak düşünülmelidir.

Bölgesel aktörlere, İsrail' in *yalnızca askeri değil, aynı zamanda psikolojik üstünlük kurma kapasitesine sahip olduğu* mesajı verilerek ***"algı yönetimi"*** yapılmak istenmektedir. [14]

## 3.2. Katar-Türkiye İlişkileri Bağlamında Yansımalar

Türkiye ile Katar arasındaki *güvenlik ve savunma iş birliği (Örneğin, Katar' daki Türk Askeri Üssü) anlaşması* kapsamında yürütülen ***"stratejik ortaklık"***, saldırının ardından *daha kritik bir boyut* kazanmıştır.

---

[13] **Barrucho, L.,** İsrail' in Katar Saldırısı Ortadoğu' da Barış İhtimalini Tamamen Yok Mu Etti?, Haber / Analiz, BBC NEWS Türkçe, İstanbul, 2025. https://www.bbc.com/turkce/send/u50853841, 24 Eylül 2025 tarihinde ziyaret edildi.

[14] Sumud Filosuna Dron Saldırısı ve Ukrayna-Rusya Savaşı' nda Ukrayna' nın Dron Saldırısı ile ilgili bir değerlendirme için bkz., https://burakbozkurtlar.com/sumud-filosu-hedefte-dronlar-ve-siber-golge/, 25 Eylül 2025 tarihinde ziyaret edildi.

Saldırının yarattığı ekonomik etki bakımından, enerji piyasalarında Katar' ın LNG ihracatının hedef alınabileceği algısı, Türkiye' nin enerji arz güvenliği için risk oluşturmuştur.

Türkiye' nin saldırıya karşı Katar' la dayanışma göstermesinin ***"diplomatik sonucu"***, iki ülkenin bölgesel politikalarının daha da yakınlaşması olmuştur.

### 3.3. Ortadoğu ve Akdeniz Bölgeleri Güvenlik Mimarileri Üzerindeki Etkiler

Tahran / Doha / Sumud Filosu saldırıları, Körfez ülkeleri ile bazı Avrupa ülkelerinin güvenlik politikalarında kırılmalara ve yeni ittifak arayışlarına yol açmış ve *alternatif güvenlik ittifaklarının gündeme gelmesine sebep* olmuştur.

ABD ve Batı' nın genel olarak saldırıya yönelik *yetersiz tepkileri, Batı ittifakının bölgesel güvenlik algısını zayıflatmış, Türkiye ve Katar gibi aktörlerin bağımsız hareket etme eğilimini* güçlendirmiştir.

Ankara, bu süreçte *hem* ***arabulucu*** *hem de* ***bölgesel güvenlik sağlayıcı*** *rolleri* ile öne çıkmış; *"NATO' dan bağımsız güvenlik alternatifleri"* tartışmalarında ***etkin bir aktör*** haline gelmiştir.

### 3.4. Siber Boyut ve Yeni Tehdit Algısı

Tahran / Doha / Sumud Filosu saldırıları, ***"kritik altyapılar"*** a karşı gerçekleştirilecek *yalnızca kinetik saldırılar değil; siber saldırılarla da desteklenen* ***"hibrit bir stratejinin parçası"*** *olarak görülmüştür.*

*Başkentlerin / diplomatik merkezlerin / insani yardım filolarının hedef alınması*, uluslararası müzakerelere dair veri ve belgelerin, kısacası ***"veri güvenliği"*** nin *siber saldırılar yoluyla manipülasyonuna kapı aralamıştır.*

Bu saldırı, Ankara' nın ***siber diplomasi*** ve ***dijital savunma*** alanlarında – saldırıdan çıkardığı / çıkaracağı dersler ile - *daha güçlü refleksler geliştirmesi gerektiğini* ortaya koymuştur.[15]

[15] Detaylı bigi için bkz., **MİA (Milli İstihbarat Akademisi)**, 12 Gün Savaşı ve Türkiye İçin Dersler, Rapor, Ağustos 2025, 33-38.

# 4. Siber Güvenlik Perspektifi

Günümüzde güvenlik tehditlerinin en görünmez ama en etkili boyutlarından biri **siber uzayda yaşanmaktadır**. Devletlerarası *dengeleri değiştiren, toplumların psikolojisini hedef alan ve ekonomik istikrarı tehdit eden siber saldırılar,* Türkiye için de ***"ulusal güvenliğin merkezi"*** nde yer almaktadır. [16]

## 4.1. Kritik Altyapıların Korunması [17]

Günümüzde günlük yaşamın ayrılmaz bir parçası olan *enerji,* hemen hemen tüm dünyada önemli gündem maddelerinden biridir. Dolayısıyla *enerji üretimi ve enerji altyapıları* ile bu *tesislerin güvenliği* de aynı perspektif ile değerlendirilmektedir. Bu bağlamda; doğalgaz, petrol ve elektrik dağıtım sistemlerine yönelik saldırılar, *yalnızca ekonomik değil, toplumsal kaos potansiyeli* de taşımaktadır.

Benzer şekilde, havaalanları, metro sistemleri ve demiryolları gibi *kritik ulaşım altyapıları ve lojistik sistemleri de siber saldırılara karşı hedef* durumundadır.

Sağlık sistemleri de zaman zaman hedef alınmaktadır. Pandemi sürecinde görüldüğü üzere, *sağlık verilerinin çalınması ve hastane sistemlerine yönelik saldırılar, doğrudan insan hayatını tehdit* etmektedir.

## 4.2. Siber Saldırı Türleri [18]

Özellikle kritik dönemlerde (seçimler, uluslararası krizler) *yabancı istihbarat servislerinin yönlendirdiği* ***"devlet destekli saldırılar"*** öne çıkmaktadır.

Kamu kurumları ve belediyeler, *mali kazanç amaçlı fidye yazılımlarının* ***(Ransomware (MUSE) v.b. gibi)*** *sıkça hedefi* olmaktadır.

Liderlerin veya kritik figürlerin *dijital olarak* ***"derin sahtecilik (deepfake) yoluyla"*** *taklit edilmesi ve toplumun* ***"manipüle edilmesi"*** *siyasi krizleri tetikleme potansiyeli* taşımaktadır.

---

[16] Konu ile ilgili daha detaylı bilgi ve geniş kapsamlı araştırma için bkz.**; Türkiye Ulusal Siber Güvenlik Stratejisi (2024–2028),** T.C.UAB.lığı Yayını, Stratejik Eylem Planı, Ankara, 2024. Ayrıca; dünya genelindeki durum için bkz.; **Amerika' nın Siber Savunma Ajansı (CISA)** ve **AB Siber Güvenlik Ajansı (ENISA)** tarafından yıllık olarak yayımlanan **"Siber Güvenlik Raporları"**.

[17] Konu ile ilgili daha detaylı bilgi ve geniş kapsamlı araştırma için bkz.; **Kritik Altyapılı Tesis Yönetimi -I ve II,** Bilgi Notu-1 ve 2, GUSEYAD / AKADEMİ Yayınları, İstanbul, 2020.

[18] **Kritik Altyapılı Tesis Yönetiminde Siber Güvenlik**, Bilgi Notu-3, GUSEYAD / AKADEMİ Yayını, İstanbul, 2025, s.6-7.

Bilgiye erişimi olan kurum içi aktörlerin, *kasıtlı veya ihmalkâr davranışları, kritik güvenlik açıkları yaratmaktadır.*

### 4.3. Türkiye'nin Dijital Bağımlılıkları ve Zafiyetleri

Kamu kurumlarının kullandığı birçok sistem, hâlen *yabancı menşeli yazılımlara* dayanmaktadır. Bu durum, *veri güvenliği açısından zafiyet* oluşturmaktadır. [19]

Bilişim ve iletişim teknolojilerinde kullanılan donanımları ithal ediliyor olması, **y**erli çip ve sunucu altyapısı eksikliği, *siber güvenliğin stratejik bağımlılığını artırmaktadır.*

Bulut teknolojileri konusundaki yetersizlik, ulusal verilerin yabancı bulut servislerinde saklanması, *kritik bilgilerin üçüncü ülkeler tarafından erişilebilir* hale gelmesine yol açmaktadır.

İnsan kaynağı ve eğitimi konusundaki yetersizlikler, örneğin siber güvenlik uzmanı açığı, *Türkiye' nin savunma kapasitesini sınırlayan en önemli faktörlerden biridir.*

### 4.4. Ulusal Güvenlikte Siber Boyutun Önemi

Askeri operasyonlar açısından modern savaşlarda *siber saldırılar, kinetik operasyonlarla eşgüdümlü* şekilde kullanılmaktadır. [20]

Sosyal medya manipülasyonları ve bilgi kirliliği, tedbir almayan taraf için ciddi sorun haline gelirken, uygulayan taraf için ***"psikolojik üstünlük"*** sağlama vasıtası olmakta, *savaşmadan hasım ülkelerin iç istikrarını zedeleyebilmek imkânı doğmaktadır.*

Türkiye'nin *milli bir refleks göstererek* ***"siber vatan bilinci"*** ni güçlendirmesi, yalnızca *teknik bir zorunluluk değil; aynı zamanda ulusal güvenliğin stratejik dayanağıdır.* [21]

---

[19] Karaman, D. & Damar, M. (2021), Fikri mülkiyet haklarının yazılım sektörü açısından değerlendirilmesi: Usedsoft ve Verisil davaları, Makale, KAÜİİBFD, 12(24), 11651198, s.1169.

[20] Rusya-Ukrayna Savaşı' nda, savaş devam ederken, Ukrayna' nın Rusya derinliklerinde gerçekleştirdiği ***"dron saldırısı"*** bu konuda verilebilecek önemli örneklerden biridir. Bkz., https://www.hurriyet.com.tr/dunya/ukraynadan-film-gibi-dron-operasyonu-arktikten-sibiryaya-dort-ussu-vurdular-42824227, 25 Eylül 2025 tarihinde ziyaret edildi. Bir başka kaynakta aynı saldırı için bkz., https://dailymetin.com/ukraynadan-sibiryadaki-rus-hava-uslerine-tarihi-drone-saldirisi-40tan-fazla-savas-ucagi-vuruldu, 25 Eylül 2025 tarihinde ziyaret edildi.

[21] *"Yakın gelecekte "**Siber Vatan**" kavramını bütünleşik olarak değerlendirebilmek, başta Türk Dünyası olmak üzere NATO' dan bağımsız bir teknik alt yapı ile kurgulamak gerekmektedir. Aksi halde, ulus devletlerin **"Siber Vatan"** olarak ifade edebileceği bağımsız bir siber vatandan bahsetmek mümkün olmayacağı gibi, yerli ve milli olarak nitelendirilen çalışmaların dijital mandalıktan öteye geçebilen bir sonucu olmayacaktır."* Bkz., **Bozkurtlar, B.S., (2021),** Ulus Devletlerin Siber Güvenlik Stratejileri ve Siber Vatan, Makale, Academia, s.1

# 5. Ulusal Siber Savunma Stratejileri

Türkiye, 2010' lu yıllardan itibaren hazırladığı *ulusal strateji belgeleri* ve *kurumsal yapılanmalar'* la ***"siber güvenliği ulusal güvenliğin ayrılmaz bir parçası"*** haline getirmiştir. Ancak, değişen tehdit ortamı ve NATO' nun zayıflayan güvenlik taahhütleri, Türkiye' nin ***daha özerk, milli bir siber savunma modeli*** geliştirmesini zorunlu kılmaktadır. [22]

## 5.1. Mevcut Politikalar ve Strateji Belgeleri

***Ulusal Siber Güvenlik Stratejisi (2020–2024),*** Türkiye' nin ilk kapsamlı yol haritası olmuş, *kritik altyapıların korunması ve yerli yazılım kullanımına öncelik* verilmiştir.[23]

***Yeni Dönem Stratejisi (2024–2028),*** *yapay zekâ destekli güvenlik çözümleri, dijital bağımlılıkların azaltılması ve uluslararası iş birliği boyutu* ön plana çıkmıştır.[24]

Bu alanda ***"Milli Seferberlik"*** anlayışı ile hareket edilmelidir. Geç kalınacak olursa, geleceği kaybetmek söz konusu olacaktır. *Stratejiler, yalnızca devlet kurumlarını değil; özel sektör, üniversiteler ve sivil toplumu da kapsayan* ***"bütüncül bir güvenlik vizyonu"*** öngörmektedir.

## 5.2. Siber Güvenlik Başkanlığı' nın Rolü

2018' de Cumhurbaşkanlığı Hükümet Sistemi' ne geçişin ardından ***Siber Güvenlik Başkanlığı***, 8 Ocak 2025 tarihinde, Türkiye Cumhuriyeti Cumhurbaşkanlığı' na bağlı olarak resmen kurulan bir başkanlıktır. Amacı, devlet ve millet nezdinde siber istihbaratın derlenmesidir.

Başkanlığın hizmet birimleri arasında; *Siber Savunma Genel Müdürlüğü, Siber Mukavemet Genel Müdürlüğü, Ekosistem Geliştirme Genel Müdürlüğü, Dış İlişkiler Dairesi Başkanlığı, Yönetim Hizmetleri Dairesi Başkanlığı, Hukuk Müşavirliği, Basın ve Halkla İlişkiler Müşavirliği* yer almaktadır.

Kurumun görev ve sorumlulukları arasında, Başkanlık, siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planları hazırlamak, mevzuat çalışmalarını

[22] Konu ile ilgili daha detaylı bilgi ve geniş kapsamlı araştırma için bkz.; **Türkiye Ulusal Siber Güvenlik Stratejisi (2020–2023),** T.C.UAB.lığı Yayını, Stratejik Eylem Planı, Ankara, 2020. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.
Ayrıca; **TÜBİTAK BİLGEM** tarafından kurulmuş **Siber Güvenlik Enstitüsü (SGE)** ve çalışmaları için bkz., https://bilgem.tubitak.gov.tr/en/sge-corporate/#biz-kimiz, 25 Eylül 2025 tarihinde ziyaret edildi.
[23] **Türkiye Ulusal Siber Güvenlik Stratejisi (2020–2023),** agy., s.23-26.
[24] **Türkiye Ulusal Siber Güvenlik Stratejisi (2024–2028),** agy., s.25-28.

yürütmek, ilgili faaliyetlerin koordinasyonunu sağlamak, siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmalarını yürütmek, siber güvenlik ve bilgi güvenliğini destekleyici projeleri yürütmek, bu alanda kamu, özel sektör ve üniversiteler arasındaki iş birliğinin artırılmasına yönelik çalışmaları yapmaktır.

Bu çerçevede, siber güvenlik ekosistemi ile yerli ve milli ürün ve teknolojilerin geliştirilmesine ve yerli girişimcilerin dünya pazarında rekabet edebilecek konuma gelmesine yönelik çalışmalar yapılacak, siber güvenliğe ilişkin ihtiyaç duyulan alanlarda Ar-Ge ve teknoloji transferi sağlanacak, siber güvenlik zafiyetinin tespit edilmesi için çalışmalar yürütülecek, acil durum ve kriz yönetim planları oluşturulacak, mevzuatla verilen diğer görevler uygulanacaktır.

Ancak; kurumun henüz bağımsız bir *"siber komutanlık"* işlevi üstlenemediği; *personel kapasitesi ve bütçe imkanlarının sınırlı olduğu* değerlendirilmektedir.

Daha kurumsallaşmış bir yapıyla, ***Milli İstihbarat Akademisi*** *ve* ***Savunma Sanayii Başkanlığı*** ile *doğrudan entegre edilmesi gerektiği* düşünülmektedir. Ayrıca, MİA rapor ve analizlerinde yer alan regülasyon ihtiyaçlarını belirleyerek ***"dijital mütekabiliyet"*** tekniklerini ortaya koyacak, MİA rapor ve analizlerinde yer verilen tespitlerle alakalı görev, yetki ve sorumlulukları bulunan ilgili kurumlarla birlikte icra edilecek uygulamalarla, ***"yapay zeka destekli hükümet ve kamu yönetim modelleri"*** için şimdiden gerekli hazırlıkları yaptıracak ve böylece, kurumun ön alma kapasitesinin geliştirilmiş olacağı düşünülmektedir.[25]

### 5.3. NATO' ya Bağımlı Olmayan Modeller

Türkiye, ***"siber caydırıcılık"*** sağlayacak tedbirleri acilen almalı, ihtiyaç duyulan yöntemleri geliştirmelidir. *Yalnızca savunmada değil, gerektiğinde karşı saldırı için* de kapasitesini geliştirmelidir.

Milli yazılımlar yoluyla ve yerli üretim donanımlar kullanmak suretiyle,

*-Kriptografi yeteneği,*

*-Yapay zekâ güvenlik çözümleri geliştirilmeli,*

*-Yerli çip teknolojileri üretilmeli ve geliştirilmelidir.*

*Sıralanan konular* ***"stratejinin temel taşları"*** *dır.*

[25] Siber Güvenlik Başkanlığı hakkında yayımlanan 177 numaralı Cumhurbaşkanlığı Kararnamesi, ve başkanlık hakkında detaylı bilgi için bkz., https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

***Farkındalık yaratmak ve ilgili tüm personeli eğitmek maksadıyla,*** *yerel ve ulusal* ölçekte düzenli ***siber seferberlik tatbikatları*** yapılmalı, kamu-özel sektör iş birliği üzerinden ***geniş bir katılım*** sağlanmalıdır.

### 5.4. Yeni Nesil Kurumsal Yapılanma İhtiyacı

*Türk Silahlı Kuvvetleri, MİA ve Siber Güvenlik Başkanlığı' nın entegre edilmesiyle kurulacak (Örneğin;* **Milli Siber Güvenlik Komutanlığı)** *yeni bir yapı,* Türkiye' nin caydırıcılığını artıracaktır.

Geliştirilecek bir **Dijital Seferberlik Modeli** ile üniversiteler, özel sektör ve kamu kurumları içinde *"siber milis"* benzeri *"gönüllü ağlar"* oluşturulmalıdır.

**Siber Güvenlik Başkanlığı** süratle güçlendirilmeli ve sağlanacak *stratejik bütçe, nitelikli uzman kadrolar* ve *uluslararası diplomasi* rolü ile ***daha etkin hale*** getirilmelidir.

# 6. Uluslararası İş Birliği ve Siber Diplomasi

Siber tehditler sınır tanımadığı için, hiçbir devlet tek başına bu alanı güvence altına alamaz. Türkiye açısından siber güvenlik, yalnızca ulusal bir mesele değil; aynı zamanda ***uluslararası iş birliği ve diplomasi konusu*** haline gelmiştir. Örneğin; "*Türkiye, NATO ile Siber Güvenlik Anlaşması imzalayan ilk ülkedir.*" [26]

## 6.1. Türkiye' nin Uluslararası Arenadaki Konumu

Türkiye, *NATO Siber Savunma Mükemmeliyet Merkezi'* nin (Estonya) çalışmalarına [27] katılsa da *ittifak içindeki çifte standartlar güven ilişkisini zedelemektedir.*

Birleşmiş Milletler çatısı altında yürütülen *siber güvenlik normları tartışmaları,* Türkiye' nin küresel düzeyde *norm belirleyici bir aktör* olma ihtimalini gündeme getirmektedir.

Türkiye, gözlemci statüsünde olduğu, Şanghay İş Birliği Örgütü (ŞİÖ) üzerinden Çin ve Rusya ile *siber güvenlik konusunda sınırlı iş birlikleri* geliştirmektedir.

## 6.2. Siber Diplomasi: Caydırıcılık ve İş Birliği

Türkiye, siber saldırılara karşı *yalnızca savunmada değil,* gerektiğinde *misilleme kapasitesine sahip* olduğunu diplomatik dille vurgulamalı, ***"caydırıcılık boyutu"*** nu da kullanmalıdır.

Türk Devletleri Teşkilatı başta olmak üzere, bölgesel örgütlerle ***"ortak siber tatbikatlar",*** Türkiye' nin *diplomatik etkinliğini* artırmaktadır.

Türkiye, *"siber savaşın sınırları"* ve *"kritik altyapıların korunması"* konularında *uluslararası alanda* ***"dijital normların geliştirilmesi"*** *nde öncü rol* üstlenebilir.

## 6.3. "Five Eyes" Karşısında Yeni Model: "9 Işık Teknolojileri"

Batı merkezli "**Five Eyes"** istihbarat ittifakı (*ABD, İngiltere, Kanada, Avustralya, Yeni Zelanda*), *bilgi paylaşımı ve siber istihbarat koordinasyonunda uzun süredir* ***etkin bir model***

[26] Türkiye' nin "Siber Diplomasi" konusunda uluslararası alanda gerçekleştirdiği iş birliğine güzel bir örnek için bkz. **Çiftçi, H.,** Her Yönüyle Siber Savaş, TÜBİTAK Popüler Bilim Kitapları, Ankara, 2023, s.42.
[27] https://ccdcoe.org/about-us/, 25 Eylül 2025 tarihinde ziyaret edildi.

olarak işlemektedir. Ancak bu yapı, Türkiye ve benzeri ülkeler açısından *dışlayıcı bir nitelik* taşımaktadır.[28]

Türkiye' nin öncülüğünde geliştirilebilecek alternatif bir vizyon ise, ***"9 Işık Teknolojileri"*** modeli olabilir.

***9 Işık Teknolojileri*** kavramı, **ASSAM Kongresi** çerçevesinde, İslam İş Birliği Teşkilatı üyesi ülkelerin ve "Five Eyes" tan gelen gözlemcilerin katılımıyla, ilk kez kayıtlara geçmiştir. [29]

Burada ***"temel hedef",*** Türk Dünyası' nın (*Türkiye, Azerbaycan, Kazakistan, Kırgızistan, Özbekistan, Türkmenistan, KKTC, Macaristan –Türk kökenli kabul– ve potansiyel diğer müttefikler*) ortak bir ***siber güvenlik ittifakı*** oluşturmasıdır.

Kritik tehditlere karşı *anlık bilgi paylaşımı, ortak veri merkezleri ve yerli yapay zekâ tabanlı analiz sistemleri* aracılığı ile istihbarat paylaşımı sağlanacaktır.

Ortak *5G / 6G, uydu sistemleri ve kriptografi projeleri* üzerinden *bağımsız bir teknolojik ekosistem* inşa edilecek, ihtiyaç duyulan *"teknolojiler geliştirilecek"* tir.

Bu yapı, belki NATO' ya alternatif olmayacak, ancak; yine de Batı dışı bir ***siber caydırıcılık*** ve ***dayanışma platformu*** işlevi görebilecektir.

### 6.4. Türkiye' nin Stratejik Hamleleri

***9 Işık vizyonu,*** *Türk Devletleri Teşkilatı ile entegre edildiği takdirde,* mevcut TDT iş birliklerinin *siber güvenlik boyutunu* güçlendirecektir.

Tahran / Doha / Sumud Filosu saldırılarının ardından, Bazı Avrupa ülkeleri ile Katar ve Körfez ülkelerinin *alternatif güvenlik mekanizmalarına ilgisi* artmıştır. Türkiye bu süreçte, iş birlikleri geliştirecek ve *lider rolü* üstlenebilecektir.

Macaristan' ın bu ittifakta yer alması, AB ile bağları koparmadan ***yeni bir güvenlik hattı*** kurulmasını sağlayacaktır.

[28] Bu konuda detaylı bilgi için bkz. **İrem Tabirlioğlu,** agy. https://igam.org.tr/dijital-cagda-ittifakin-gozu-five-eyes-stratejik-gozetim-ve-yeni-nesil-tehditler/, 24 Eylül 2025 tarihinde ziyaret edildi.
[29] Bu konuda detaylı bilgi için bkz. **Bozkurtlar, B.S.,** agy.

# 7. Sivil Toplum, Özel Sektör ve Akademinin Rolü

Siber güvenlik, yalnızca devlet kurumlarının sorumluluğuna bırakılabilecek bir alan değildir. Kritik altyapıların büyük bölümünün özel sektör kontrolünde olduğu, dijital inovasyonların üniversitelerden doğduğu ve toplumsal farkındalığın sivil toplum aracılığıyla geliştiği göz önünde bulundurulduğunda; ***bütüncül bir güvenlik anlayışı*** kaçınılmaz hale gelmektedir.

## 7.1. Kamu-Özel Sektör İş Birliği

Enerji, telekomünikasyon, bankacılık ve ulaşım sektörleri ile bunlara ait ***"kritik altyapılar"*** çoğunlukla özel şirketlerin elindedir. Bu alanlarda ulusal güvenlik standartlarının uygulanması, *devlet-özel sektör koordinasyonuyla mümkündür.* [30]

Özel şirketlerin *USOM ve Siber Güvenlik Başkanlığı* ile "*düzenli ortak tatbikatlar" a dahil edilmesi ve sertifikasyona tabi tutulması, tehditlere karşı refleksleri artıracaktır.* [31]

*Saldırı ve zafiyet bilgisi,* kamu kurumlarıyla *eş zamanlı paylaşılmalıdır.* ABD' deki ***Information Sharing and Analysis Centers (ISACs)*** modeline *benzer yapılar Türkiye' de geliştirilebilir.* [32]

## 7.2. Üniversiteler ve Akademinin Katkıları [33]

*Yapay zekâ, kriptografi ve siber savunma yazılımları* üzerine odaklanacak *üniversitelerin araştırma merkezleri, yapacakları buluş, üretim ve geliştirmeler sayesinde, Türkiye' nin teknolojik bağımsızlığını* destekleyecektir.

---

[30] **Özgen, Ö.,** agy.-I., s.3-5.

[31] **Güvenlik Savunma ve Emniyet Yönetişimi,** Masaüstü Yayın-I, GUSEYAD / AKADEMİ Yayını, İstanbul, 2018, s.16-19.; https://guseyadakademi.org/wp-content/uploads/2025/09/guseyad-masa-ustu-yayin-1.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

[32] **Bilgi Paylaşımı ve Analiz Merkezi (ISAC),** kritik altyapıya yönelik siber ve ilgili tehditler hakkında bilgi toplamak ve özel ve kamu sektörleri arasında iki yönlü bilgi paylaşımı sağlamak için merkezi bir kaynak sağlayan bir kuruluştur. ABD ve dünyanın diğer ülkelerindeki çalışmalar hakkında detaylı bilgi için bkz., https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center , 24 Eylül 2025 tarihinde ziyaret edildi.

[33] Akademik katkılara bir örnek, bkz., **Özgen, Ö.; Eren, M.; Bozkurtlar, B.S.,** *Acil Yardım ve Afet Yönetiminde Çağdaş Yaklaşımlar*, İstanbul Üniversitesi AUZEF Yayınları, İstanbul, 2025. Bir başka örnek; **Sağıroğlu, Ş. (Ed.),** Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar, Bilgi Güvenliği Derneği Yayını, Havelsan Katkısıyla, Grafiker Yayınları, Ankara, 2019., https://bilgiguvenligi.org.tr/BGD/Siber_Guvenlik_ve_Savunma_Kitap_Serisi_3_Standartlar%20ve%20Uygulamalar.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

***Milli İstihbarat Akademisi (MİA),*** görevi ve sorumluluk alanı itibarı ile yalnızca istihbarat personeli değil; aynı zamanda *stratejik düşünce üreten, politika yapıcıları bilgilendiren bir kurum* olarak daha da öne çıkacaktır.

Yetkin insan kaynağı sağlamak ve nitelikli eğitim süreçlerini gerçekleştirmek için**,** üniversitelerde açılacak *siber güvenlik bölümleri*, *yüksek lisans ve doktora programları, nitelikli uzman açığını kapatmaya katkı* sunacaktır.

### 7.3. Sivil Toplumun Gücü [34]

Toplumun *dijital okuryazarlık düzeyi*, güvenlikte en zayıf halka sorununu ortadan kaldıracak, düzenlenecek ***"farkındalık kampanyaları"*** *ile STK' lar bu noktada kritik rol üstlenecektir.*

Doğal afetlerde AFAD gönüllüleri nasıl sahaya çıkıyorsa, *siber kriz anlarında* da, ***"gönüllü siber uzmanlar"*** *ın devreye gireceği bir model* geliştirilmelidir.

Siber saldırılarla mücadele yalnızca teknik değil; aynı zamanda *etik ve hukuki bir meseledir*. *Sivil toplum,* bu alanda *toplumun bilinçlendirilmesini sağlayacaktır.*

### 7.4. Dijital Seferberlikte Üçlü Dayanak

Türkiye' nin ulusal güvenlik vizyonu; ***devlet, özel sektör ve toplum*** sacayağı üzerine oturtulmalıdır. Bu bağlamda:

- *Devlet → Strateji ve kurumsal koordinasyon sağlayacak,*
- *Özel sektör → Teknik kapasite ve inovasyon oluşturacak,*
- *Akademi / STK → İnsan kaynağı ve farkındalık yaratacaktır.*

*Bu üç aktörün eşgüdümü,* ***"siber vatan bilinci"*** *nin* ***toplumsal tabana yayılmasını*** *mümkün kılacaktır.* [35]

---

[34] Tehlikenin farkında olan ve alanı sahiplenen bir avuç gönüllü tarafından yürütülen etkinlikler için bkz., https://siberguvenilirturkiye.com/, 24 Eylül 2025 tarihinde ziyaret edildi.

[35] https://burakbozkurtlar.com/siber-vatan-ve-egemenlik/, 24 Eylül 2025 tarihinde ziyaret edildi. Konu ile ilgili daha detaylı bilgi ve geniş kapsamlı araştırma için ilgili kaynaklar aşağıdadır. Bkz., **12. Kalkınma Planı Öncelikli ve Kilit Teknoloji Alanları,** https://tubitak.gov.tr/tr/kurumsal/politikalar/tubitak-2024-2025-oncelikli-ar-ge-ve-yenilik-konulari, 24 Eylül 2025 tarihinde ziyaret edildi.

## SONUÇ

Türkiye, tarihsel ve jeopolitik konumunun getirdiği stratejik yükümlülüklerle birlikte, artık yalnızca kara ve denizlerde değil, ***siber uzayda da güvenliğini sağlamak zorundadır.*** İsrail' in Tahran / Doha / Sumud Filosu saldırıları sonrasında ortaya çıkan yeni güvenlik dinamikleri, NATO' nun zayıflayan güvenlik taahhütleri ve hibrit savaşın görünmez boyutları, Türkiye için ***"bağımsız ve milli bir güvenlik mimarisi geliştirme gerekliliği"*** ni açıkça ortaya koymaktadır.

Çalışmanın önceki bölümlerinde görüldüğü üzere:

> *Türkiye'nin **jeopolitik güvenlik ortamı**, yalnızca dış tehditlerle değil, iç güvenlik boyutu ve kaynak temelli kırılganlıklarla da şekillenmektedir.*
>
> ***NATO' nun çifte standartlı yaklaşımı**, Türkiye' yi çoğu zaman yalnız bırakmakta, kolektif savunma ilkesinin pratikte sorgulanmasına yol açmaktadır.*
>
> ***Tahran / Doha / Sumud Filo saldırıları**, bölgede hiçbir yerin güvenli olmadığı mesajını vermiş; Türkiye-Katar ortaklığı başta olmak üzere alternatif güvenlik ittifaklarını öne çıkarmıştır.*
>
> ***Siber güvenlik perspektifi**, kritik altyapılardan seçim güvenliğine kadar, tüm alanlarda Türkiye 'nin "**ulusal güvenlik gündeminin merkezi**" ne oturmuştur.*

Bu bağlamda Türkiye' nin *güvenlik vizyonu, **üç temel sütun** üzerine inşa edilmelidir:*

> *Siber Güvenlik Başkanlığı'nın kurumsal olarak güçlendirilmesi ve kapasitesinin artırılması, Milli İstihbarat Akademisi ile doğrudan entegre edilmesi ve bağımsız bir **Milli Siber Güvenlik Komutanlığı** yapılanmasının kurulması.*
>
> *NATO' ya bağımlı kalmadan, Türk Devletleri Teşkilatı, Körfez ülkeleri ve stratejik müttefiklerle iş birliği yaparak, uluslararası dayanışmanın sağlanması. Bu çerçevede, "**Five Eyes"** karşılığı **"9 Işık Teknolojileri"** modelinin hayata geçirilmesi, Türkiye'nin bölgesel ve küresel caydırıcılığının güçlendirilmesi.*
>
> *Özel sektör, akademi ve sivil toplumun dahil olacağı, toplumsal katılımın sağlandığı, **dijital seferberlik modeli, "siber vatan bilinci"** ni topluma yayarak "**ulusal direnç**" in artırılması.*

Türkiye 'nin gelecekteki güvenlik mimarisi, yalnızca tank, tüfek veya füze ile değil; ***"algoritmalar, yapay zekâ sistemleri, veri merkezleri ve dijital ittifaklar"*** ile şekillenecektir. Bu nedenle, ulusal güvenlik stratejileri yeniden tanımlanırken, ***"siber vatan"*** kavramı yalnızca bir slogan değil, ***"yeni nesil caydırıcılığın temeli"*** olarak kabul edilmelidir.

Sonuç olarak, Türkiye' nin karşı karşıya olduğu tehditler büyüktür; fakat aynı ölçüde fırsatlar da vardır. Eğer doğru kurumsallaşma, "*güçlü uluslararası iş birlikleri ve toplumsal farkındalık"* la hareket edilirse, Türkiye yalnızca *kendini savunan değil*, aynı zamanda ***dijital çağın güvenlik mimarisini inşa eden öncü devletlerden biri*** olabilir.

## KAYNAKÇA

1. **Annual Report 2023,** NATO Headquarters, Brussels, 2023.

2. **Barrucho, L.,** İsrail' in Katar Saldırısı Ortadoğu' da Barış İhtimalini Tamamen Yok Mu Etti?, Haber / Analiz, BBC NEWS Türkçe, İstanbul, 2025.

3. **Bozkurtlar, B.S.,** İslam Ülkeleri İçin Siber Güvenlik Başlığında Yeni Bir Kurgu Biçimi: Yapay Zekâ Destekli Sistem Yöneticisi, Bildiri, 3. ASSAM Kongresi, İstanbul, 2019.

4. **Bozkurtlar, B.S.,** Kritik Altyapılı Tesis Yönetiminde Siber Güvenlik, Bilgi Notu-3, GUSEYAD / AKADEMİ Yayını, İstanbul, 2025.

5. **Çifçi, H.,** Her Yönüyle Siber Savaş, TÜBİTAK Popüler Bilim Kitapları, Ankara, 2023.

6. **Erdil, B.,** İnsansız Hava Araçlarının Kullanım Alanları ile Bu Araçların Türkiye' nin Yurtdışı Operasyonlarındaki Yeri ve Önemi, Makale, Bölgesel Araştırmalar Dergisi, 5 (2), Ankara, 2021.

7. **Güvenlik Savunma ve Emniyet Yönetişimi,** Masaüstü Yayın-I, GUSEYAD / AKADEMİ Yayını, İstanbul, 2018, s.16-19.;

8. **Havan, C.**, Hibrit Tehditler ve Sosyal Politika: Düzensiz Göçün Getirdiği Toplumsal Çatışmalar ve Çözüm Önerileri, Sosyal Güvence Dergisi, Özel Sayı, 2025, s.215-224.

9. **İrem Tabirlioğlu,** Dijital Çağda İttifakın Gözü: Five Eyes, Stratejik Gözetim ve Yeni Nesil Tehditler, İstihbarat ve Güvenlik Araştırmaları Merkezi, Makale, 2025.

10. **Karaman, D. & Damar, M. (2021),** Fikri Mülkiyet Haklarının Yazılım Sektörü Açısından Değerlendirilmesi: Usedsoft ve Verisil Davaları, Makale, KAÜİİBFD, 12(24), 11651198.

11. **Mermer, C.T.,** Beş Göz: Anglosakson Dünyanın İstihbarat İş Birliği Mekanizması, Makale, TASAM Yayını, İstanbul, 2022.

12. **MİA (Milli İstihbarat Akademisi),** 12 Gün Savaşı ve Türkiye İçin Dersler, Rapor, Ankara, 2025.

13. **MSB 2024 Yılı Faaliyet Raporu,** Türkiye Cumhuriyeti Millî Savunma Bakanlığı, Ankara, 2024.

14. **Özgen, Ö.; Eren, M.; Bozkurtlar, B.S.,** *Acil Yardım ve Afet Yönetiminde Çağdaş Yaklaşımlar*, İstanbul Üniversitesi AUZEF Yayınları, İstanbul, 2025.

15. **Özgen, Ö.,** Kritik Altyapılı Tesis Yönetimi -I, Bilgi Notu-1, GUSEYAD / AKADEMİ Yayını, İstanbul, 2020.

16. **Özgen, Ö.,** Kritik Altyapılı Tesis Yönetimi -II, Bilgi Notu-2, GUSEYAD / AKADEMİ Yayını, İstanbul, 2007.

17. **Sağıroğlu, Ş. (Ed.),** Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar, Bilgi Güvenliği Derneği Yayını, Havelsan Katkısıyla, Grafiker Yayınları, Ankara, 2019.

18. **Siber Güvenlik Enstitüsü (SGE)**, TÜBİTAK BİLGEM, Ankara, 2012.

19. **Siber Güvenlik Raporu (2024),** AB Siber Güvenlik Ajansı (ENISA), 2024.

20. **Siber Güvenlik Raporu (2024),** Amerikan Siber Savunma Ajansı (CISA), 2024.

21. **Strategic Concept 2022,** NATO Summit, Madrid, 2022.

22. **Şahin, Güngör,** "Orta Doğu ve Doğu Akdeniz'in Önemi: Tehditler, Riskler, Fırsatlar ve Türkiye", Güvenlik Stratejileri Dergisi 15, S.29, 2019.

23**. Türkiye Ulusal Siber Güvenlik Stratejisi (2020–2023),** T.C.UAB.lığı Yayını, Stratejik Eylem Planı, Ankara, 2020.

24. **Türkiye Ulusal Siber Güvenlik Stratejisi (2024–2028),** T.C.UAB.lığı Yayını, Stratejik Eylem Planı, Ankara, 2024.

## İNTERNET LİNKLERİ

https://www.nato.int/strategic-concept/, 22 Eylül 2025 tarihinde ziyaret edildi.

https://www.nato.int/cps/en/natohq/news_221644.htm, 22 Eylül 2025 tarihinde ziyaret edildi.

https://guseyadakademi.org/?page_id=2, 22 Eylül 2025 tarihinde ziyaret edildi.

https://cbddo.gov.tr/ulusal-siber-guvenlik-stratejisi-2019-2023, 22 Eylül 2025 tarihinde ziyaret edildi.

https://mia.edu.tr/uploads/f/12-gn-savasi-ve-trkiye-iin-dersler_1.pdf?v=1754026418, 22 Eylül 2025 tarihinde ziyaret edildi.

https://www.msb.gov.tr/Content/Upload/Docs/2024%20YILI%20MSB%20FAAL%C4%B0YET%20RAPORU.pdf, 22 Eylül 2025 tarihinde ziyaret edildi.

https://mia.edu.tr/uploads/f/topic_5.pdf?v=1745819827, 22 Eylül 2025 tarihinde ziyaret edildi.

https://assamcongress.com/ar/burak-bozkurtlar-ar/, 22 Eylül 2025 tarihinde ziyaret edildi.

https://mia.edu.tr/uploads/f/12-gn-savasi-ve-trkiye-iin-dersler_1.pdf?v=1754026418, 22 Eylül 2025 tarihinde ziyaret edildi.

https://www.msb.gov.tr/Content/Upload/Docs/2024%20YILI%20MSB%20FAAL%C4%B0YET%20RAPORU.pdf, 22 Eylül 2025 tarihinde ziyaret edildi.

https://mia.edu.tr/uploads/f/topic_5.pdf?v=1745819827, 22 Eylül 2025 tarihinde ziyaret edildi.

https://assamcongress.com/ar/burak-bozkurtlar-ar/, 22 Eylül 2025 tarihinde ziyaret edildi.

https://assamcongress.com/tr/asrika-ortak-savunma-sanayi-uretimi-kongre-programi/, 22 Eylül 2025 tarihinde ziyaret edildi.

https://siberguvenilirturkiye.com/, 24 Eylül 2025 tarihinde ziyaret edildi.

https://burakbozkurtlar.com/siber-vatan-ve-egemenlik/, 24 Eylül 2025 tarihinde ziyaret edildi.

https://www.msb.gov.tr/Content/Upload/Docs/Katar%20ile%20Asker%C3%AE%20%C3%87er%C3%A7eve%20Anla%C5%9Fmas%C4%B1.pdf 24 Eylül 2025 tarihinde ziyaret edildi.

https://turkicstates.org/u/tdt-budapes%CC%A7te-bildiri.pdf 24 Eylül 2025 tarihinde ziyaret edildi.

https://www.researchgate.net/publication/390764144_The_Five_Eyes_Allies_and_China_Assessing_Threat_Perceptions_and_Power_Dynamics, 24 Eylül 2025 tarihinde ziyaret edildi.

https://archive.org/details/the-palestine-laboratory-how-israel-exports-the-technology-of-occupation-around-, 24 Eylül 2025 tarihinde ziyaret edildi.

https://tubitak.gov.tr/tr/kurumsal/politikalar/tubitak-2024-2025-oncelikli-ar-ge-ve-yenilik-konulari, 24 Eylül 2025 tarihinde ziyaret edildi.

https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center , 24 Eylül 2025 tarihinde ziyaret edildi.

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, 24 Eylül 2025 tarihinde ziyaret edildi.

https://doi.org/10.17752/guvenlikstrtj.554061, 24 Eylül 2025 tarihinde ziyaret edildi.

https://dergipark.org.tr/tr/download/article-file/4789424, 24 Eylül 2025 tarihinde ziyaret edildi.

https://dergipark.org.tr/en/download/article-file/1755805, 24 Eylül 2025 tarihinde ziyaret edildi.

https://tasam.org/trTR/Icerik/70102/bes_goz_anglosakson_dunyanin_istihbarat_is_birligi_mekanizmasi, 24 Eylül 2025 tarihinde ziyaret edildi.

https://www.bbc.com/turkce/send/u50853841, 24 Eylül 2025 tarihinde ziyaret edildi.

https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

https://bilgem.tubitak.gov.tr/en/sge-corporate/#biz-kimiz, 25 Eylül 2025 tarihinde ziyaret edildi.

https://bilgiguvenligi.org.tr/BGD/Siber_Guvenlik_ve_Savunma_Kitap_Serisi_3_Standartlar%20ve%20Uygulamalar.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

https://guseyadakademi.org/wp-content/uploads/2025/09/guseyad-masa-ustu-yayin-1.pdf, 25 Eylül 2025 tarihinde ziyaret edildi.

https://www.bbc.com/turkce/articles/c147vx16x18o, 25 Eylül 2025 tarihinde ziyaret edildi.

https://burakbozkurtlar.com/sumud-filosu-hedefte-dronlar-ve-siber-golge/, 25 Eylül 2025 tarihinde ziyaret edildi.

# Türkiye Güvenlik Tehditleri

## NATO Taahhütlerinin Zayıflığı ve Siber Güvenlik Perspektifi

## İsrail'in Tahran / Doha / Sumud Filosu Saldırıları Sonrası

EYLÜL 2025

# Güvenlik Savunma ve Emniyet Yönetişimi Akademisi

*Security & Defense Governance Academy*

GUSEYAD | AKADEMİ

*GUSEYAD | ACADEMY*

Barbaros Mh. Sırmaperde Sk. Nu.2 A-Blok D.1

Üsküdar / İSTANBUL

Tel: +90 212 906 09 56

Gsm: +90 532 062 72 10

Fax: +90 212 906 09 57

E-Posta: bilgi@guseyadakademi.org