

Siber Güvenlik Başkanlığı ve Yapısı

Av. Burak Üçüncü · 5 Mayıs 2026 · 11 dk okumaGüncelleme: 6 Mayıs 2026

19 Mart 2025 tarihinde yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türkiye'nin siber güvenlik mimarisinde köklü bir dönüşümün hukuki temelini oluşturmuştur. Bu dönüşümün merkezinde ise Siber Güvenlik Başkanlığı yer almaktadır. Kanun'un 4. maddesinde açıkça ifade edildiği üzere, siber güvenlik milli güvenliğin ayrılmaz bir parçasıdır ve bu ilkenin kurumsal karşılığı Siber Güvenlik Başkanlığı'dır.

Başkanlık, Türkiye'nin siber uzaydaki ulusal kapasitesinin korunması, geliştirilmesi ve yönetilmesinden sorumlu merkezi otorite olarak tasarlanmıştır. Strateji belirleme, politika oluşturma, denetim, sertifikasyon, olay müdahale ve yaptırım uygulama gibi geniş bir yetki yelpazesine sahip olan Başkanlık, Türkiye'deki siber güvenlik ekosisteminin en üst düzey koordinasyon ve karar alma merciidir.

BÖLÜM I

Kuruluş Amacı ve Hukuki Statü

Kanun'un 1. maddesi, düzenlemenin amacını şu şekilde ortaya koymaktadır: *"Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi, siber olayların muhtemel etkilerini azaltmaya yönelik esasların belirlenmesi."* Başkanlık, bu amacın gerçekleştirilmesinin birincil kurumsal aracıdır.

Başkanlığın hukuki statüsü bakımından dikkat çekici olan husus, kurumun doğrudan Cumhurbaşkanlığı teşkilat yapısı içinde konumlandırılmasıdır. Bu konumlandırma, Başkanlığa diğer düzenleyici ve denetleyici kurumlardan farklı bir nitelik kazandırmaktadır. Başkanlık, bağımsız bir idari otorite değil; yürütme organının doğrudan uzantısı olan bir kurumdur. Bu tercih, siber güvenliğin milli güvenlik boyutuyla doğrudan ilişkilidir. Milli güvenliğe ilişkin konularda hızlı karar alma ve yürütme kapasitesinin sağlanması, Cumhurbaşkanlığına bağlı bir yapılanmayla daha etkin biçimde gerçekleştirilebilir.

BÖLÜM II

Kanun'un Kapsamı ve Muafiyetler

Kanun'un 2. maddesi, kapsamı son derece geniş tutmuştur. Siber uzayda varlık gösteren, faaliyet yürüten veya hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, *gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların tamamı* Kanun'un kapsamındadır.

Ancak Kanun, belirli güvenlik ve istihbarat faaliyetlerini kapsam dışında bırakmıştır. 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbari faaliyetler ile 2937 sayılı Devlet İstihbarat Hizmetleri

ve Milli İstihbarat Teşkilatı Kanunu ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca yürütülen faaliyetler Kanun hükümlerinden istisna tutulmuştur.

Bu istisna düzenlemesi, siber güvenlik alanındaki sivil otorite ile askeri ve istihbarat faaliyetleri arasındaki yetki sınırını çizmektedir. Güvenlik ve istihbarat kurumlarının siber operasyonları, kendi özel mevzuatlarına tabi olmaya devam etmektedir. Bu tercih, uluslararası uygulamalarla da örtüşmektedir; zira pek çok ülkede sivil siber güvenlik otoritesi ile askeri/istihbarat siber operasyonları ayrı yetki alanları olarak düzenlenmektedir.

BÖLÜM III

Başkanlığın Görevleri

Kanun'un 5. maddesi, Başkanlığın görevlerini kapsamlı bir şekilde düzenlemektedir. Bu görevler, işlevsel olarak beş ana kategoride ele alınabilir.

A. Koruma ve Savunma Görevleri

Başkanlığın birincil görevi, Türkiye'nin siber uzaydaki varlığını korumaktır. Bu çerçevede Başkanlık, siber saldırıları tespit etmek ve önlemek, kritik altyapıların siber dayanıklılığını artırmak ve siber tehditlere karşı önleyici tedbirler almakla görevlidir.

Özellikle zafiyet ve sızma testleri yapma veya yaptırma görevi dikkat çekicidir. Başkanlık, kamu kurum ve kuruluşlarının ile kritik altyapıların bilişim sistemlerinde proaktif güvenlik testleri gerçekleştirebilmektedir. Bu yetki, siber güvenliğin reaktif değil proaktif bir yaklaşımla ele alınmasının kurumsal ifadesidir.

B. Olay Müdahale ve Koordinasyon Görevleri

Başkanlık, Siber Olaylara Müdahale Ekipleri (SOME) kurmak ve kurulmasını sağlamak, bu ekiplerin denetimini gerçekleştirmek ve tatbikatlarla müdahale kabiliyetlerini artırmakla görevlidir. SOME'ler, siber güvenlik olaylarının ilk müdahale aşamasında kritik rol oynamakta; saldırının tespiti, sınırlandırılması, bertaraf edilmesi ve ardından sistemlerin toparlanması süreçlerini yönetmektedir.

Ayrıca Başkanlık, siber saldırıya maruz kalan kurum ve kuruluşlara yerinde veya uzaktan müdahale desteği sağlamakta; saldırı izlerini takip ederek delil oluşturmakta ve suç teşkil eden durumları yetkili mercilerle paylaşmaktadır. Bu görev, Başkanlığın hem teknik hem de adli boyutta faaliyet yürütmesini gerektirmektedir.

C. Düzenleme ve Standartlaştırma Görevleri

Başkanlık, siber güvenlik alanında standartlar hazırlamak, kamu kurum ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün ve hizmetlerine yönelik teknik kriterler belirlemek ve mevzuat düzenlemeleri yapmakla görevlidir.

Bu görev kapsamında Başkanlık, siber güvenlik ürün, sistem ve hizmetlere yönelik test ve sertifikasyon işlemlerini yürütmekte; siber güvenlik uzmanları ve şirketlerine yönelik sertifikasyon, yetkilendirme ve belgelendirme işlemlerini ilgili kurumlarla koordineli olarak gerçekleştirmektedir. Bu sertifikasyon sistemi, siber güvenlik sektörünün kalite kontrolünü sağlama işlevi görmektedir.

D. Denetim ve Yaptırım Görevleri

Başkanlık, siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamakla görevlidir. Bu görev, Başkanlığa hem düzenleyici hem de yaptırım uygulayıcı bir rol yüklemektedir. Başkanlık, gerekli gördüğü hallerde doğrudan denetim yapabilmekte veya yetkilendirdiği bağımsız denetçi ve denetim kuruluşları aracılığıyla denetim yaptırabilmektedir.

E. Bilgi ve İstihbarat Görevleri

Siber tehdit istihbaratı elde etmek ve paylaşmak, Başkanlığın önemli görevleri arasındadır. Başkanlık, siber uzaydaki tehditleri izlemek, analiz etmek ve bu bilgileri ilgili kurum ve kuruluşlarla paylaşmak suretiyle proaktif bir savunma ağı oluşturmaktadır. Log kayıtlarını toplamak ve değerlendirmek de bu görevin operasyonel boyutunu oluşturmaktadır.

BÖLÜM IV

Başkanlığın Yetkileri

Kanun'un 6. maddesi, Başkanlığın görevlerini yerine getirirken kullanacağı yetkileri düzenlemektedir. Bu yetkiler, Başkanlığın operasyonel kapasitesinin hukuki çerçevesini çizmektedir.

A. Bilgi ve Belge Talep Etme Yetkisi

Başkanlığın en temel ve en geniş yetkilerinden biri, görev ve faaliyetleri kapsamında her türlü veri, bilgi, belge, donanım, yazılım ve diğer katkıları talep etme yetkisidir. Kanun'un 6. maddesinin birinci fıkrasının (ç) bendi, bu talebin muhataplarının kendi mevzuatlarındaki hükümleri gerekçe göstererek talebi reddedemeyeceklerini açıkça hükme bağlamıştır.

Bu düzenleme, bankacılık sırrı, ticari sır, kişisel verilerin korunması gibi sektörel mevzuatlardaki koruma hükümlerinin Başkanlık talebi karşısında ileri sürülemeyeceği anlamına gelmektedir. Kanun koyucu, siber güvenliğin korunması amacını, diğer mevzuatlardaki gizlilik ve koruma amaçlarının üzerinde tutmuştur. Bu tercih, Kanun'un siber güvenliği milli güvenliğin parçası olarak nitelendirmesiyle tutarlıdır.

B. Önleyici ve Müdahale Yetkileri

Başkanlık, siber saldırılara karşı gerekli tedbirleri almaya veya aldırmaya yetkilidir. Siber olaylara müdahale desteği sağlama, saldırı izlerini takip ederek delil oluşturma ve suç teşkil eden durumları yetkili mercilerle paylaşma yetkileri bu kapsamdadır.

Bu yetkilerin operasyonel boyutu son derece geniştir. Başkanlık, bir siber saldırı tespitinde doğrudan müdahale edebilmekte, saldırıyı durdurma ve sınırlandırma tedbirleri alabilmekte, adli delil toplama sürecini yönetebilmekte ve gerektiğinde uluslararası koordinasyonu sağlayabilmektedir.

C. Denetim ve Arama-El Koyma Yetkileri

Kanun'un 8. maddesi, Başkanlığın denetim yetkisini somutlaştırmaktadır. Denetimle görevlendirilen personel, elektronik ortamdaki verilerin, belgelerin, elektronik altyapının, cihaz, sistem, yazılım ve donanımların incelenmesi, bunlardan kopya, dijital suret veya örnek alınması ve yazılı veya sözlü açıklama istenmesi yetkilerine sahiptir.

Daha da önemlisi, milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesinin gerektirdiği hallerde hâkim kararıyla veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının emriyle arama ve el koyma işlemleri yapılabilir. Hâkimin kararını kırk sekiz saat içinde açıklaması gerekmekte; aksi hâlde çıkarılan kopyalar ve çözümü yapılan metinler derhal imha edilmekte ve el koyma kendiliğinden kalkmaktadır.

Bu düzenlemede iki önemli istisna bulunmaktadır. İlk olarak, yetkilendirilmiş veri merkezi işletmecilerinin veri merkezlerinde sadece hâkim kararıyla arama, kopya çıkarma ve el koyma işlemi yapılabilir. İkinci olarak, kamu kurum ve kuruluşları bakımından hâkim kararı aranmamaktadır. Bu fıkra kapsamındaki talepler bakımından Ankara sulh ceza hâkimliği yetkili ve görevlidir.

D. Sınıflandırma ve Düzenleme Yetkisi

Başkanlık, Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları sınıflandırabilmekte; faaliyetlerini icra ederken gerektiğinde sadece belirli bir kısmını kapsayan hükümler oluşturabilmektedir. Bu yetki, Başkanlığa risk bazlı bir düzenleme yaklaşımı benimseme esnekliği tanımaktadır.

E. Uluslararası İlişkiler Yetkisi

Başkanlık, görev alanına giren konularda uluslararası kuruluşlar ve ülkelerle ilişkiler yürütebilmekte, bilgi alışverişinde bulunabilmekte ve Türkiye'yi temsil edebilmektedir. Siber güvenliğin sınır ötesi niteliği göz önünde bulundurulduğunda, bu yetki Başkanlığın etkinliği bakımından hayati öneme sahiptir.

BÖLÜM V

Siber Güvenlik Kurulu

A. Yapısı

Kanun'un 9. maddesi, siber güvenlik alanında en üst düzey karar alma organı olarak Siber Güvenlik Kurulu'nu düzenlemektedir. Kurul'un yapısı, siber güvenliğin devlet nezdindeki stratejik önemini açıkça yansıtmaktadır. Kurul üyeleri şunlardır:

- Cumhurbaşkanı (Başkan)
- Cumhurbaşkanı Yardımcısı
- Adalet Bakanı
- Dışişleri Bakanı
- İçişleri Bakanı
- Milli Savunma Bakanı
- Sanayi ve Teknoloji Bakanı
- Ulaştırma ve Altyapı Bakanı
- Milli Güvenlik Kurulu Genel Sekreteri
- Milli İstihbarat Teşkilatı Başkanı
- Savunma Sanayii Başkanı
- Siber Güvenlik Başkanı

Cumhurbaşkanının katılmadığı hallerde Kurula Cumhurbaşkanı Yardımcısı başkanlık etmektedir. Bu bileşim, siber güvenliğin yalnızca teknik bir mesele olmayıp, askeri, diplomatik, istihbari, ekonomik ve hukuki boyutları olan çok disiplinli bir alan olduğunu teyit etmektedir.

B. Görevleri

Siber Güvenlik Kurulu'nun görevleri, stratejik niteliktedir. Kurul, siber güvenlikle ilgili politika ve strateji kararları almak, teknoloji yol haritasını uygulamak, teşvik edilecek alanları belirlemek, kritik altyapı sektörlerini tespit etmek ve Başkanlık ile kamu kurumları arasındaki ihtilafları çözmekle görevlidir.

Kurul'un kritik altyapı sektörlerini belirleme görevi, Kanun'un uygulamasında belirleyici bir işlev üstlenmektedir. Hangi sektörlerin kritik altyapı kapsamında olduğunun Kurul tarafından belirlenmesi, Kanun'un cezai hükümlerinin uygulama alanını da doğrudan etkilemektedir.

BÖLÜM VI —

Personel Rejimi

A. Sözleşmeli Uzman Personel

Kanun'un 10. maddesi, Başkanlıkta siber güvenliğin sağlanması ile ilgili görevleri yürütmek üzere sözleşmeli uzman personel istihdamına imkân tanımaktadır. Bu personelin sayısı Cumhurbaşkanınca belirlenmektedir.

Ücret rejimi bakımından son derece önemli bir düzenleme yapılmıştır: sözleşmeli uzman personele verilecek net ücretler, 657 sayılı Devlet Memurları Kanunu'nun 4/B kapsamında çalıştırılanlar için uygulanmakta olan sözleşme ücret tavanının beş katını aşmamak üzere Siber Güvenlik Kurulu tarafından belirlenmektedir. Bu düzenleme, Başkanlığın özel sektörle rekabet edebilecek ücret düzeylerinde nitelikli siber güvenlik uzmanı istihdam etmesine olanak tanımaktadır.

Siber güvenlik alanında nitelikli personel temininin global ölçekte en büyük sorunlardan biri olduğu göz önüne alındığında, bu esnekliğin stratejik önemi açıkça ortadadır. Ancak beş katı aşmama sınırının pratikte yeterli olup olmadığı, özel sektördeki siber güvenlik uzmanı maaş düzeyleri gözetilerek değerlendirilmelidir.

B. Güvenlik Soruşturması ve Arşiv Araştırması

Başkanlıkta görev alacak tüm personele (geçici görevlendirmeler dahil) güvenlik soruşturması ve arşiv araştırması yapılmaktadır. Bu gereklilik, Başkanlık bünyesinde erişilecek bilgilerin hassasiyeti ile doğrudan ilişkilidir. Kritik altyapılara, devlet sırlarına ve kişisel verilere erişim imkânı bulunan personelin güvenilirliğinin teyit edilmesi, kurumsal güvenliğin temel gerekliliklerindendir.

C. Zorunlu Hizmet Muafiyeti

Diğer kamu kurumlarında zorunlu hizmet yükümlülüğü bulunan personelin Başkanlıktaki hizmet süreleri, bu yükümlülükten düşülebilmektedir. Bu düzenleme, nitelikli kamu personelinin Başkanlığa çekilmesini kolaylaştırmaya yönelik bir teşvik mekanizması niteliğindedir.

BÖLÜM VII —

Başkanlıkla İlgili Yasak ve Sınırlama Hükümleri

A. Görevden Ayrılan Personele Yönelik Yasaklar

Kanun'un 12. maddesi, Başkanlıkla ilişkisi kesilen personele yönelik kapsamlı yasaklar öngörmüştür. Kadrolu veya sözleşmeli statüde görev yapanlardan Başkanlıkla herhangi bir nedenle ilişkisi kesilenler, Başkanlıktan muvafakat almadan iki yıl süreyle yurt içi veya yurt dışında siber güvenlik alanında resmi veya özel görev alamamakta, ticaretle uğraşamamakta, serbest meslek faaliyetinde bulunamamakta ve siber güvenlik şirketlerinde hissedar veya yönetici olamamaktadır.

Bu yasağın soğuma dönemi (cooling-off period) olarak adlandırılan uluslararası uygulamanın bir yansıması olduğu açıktır. Yasağın ihlali, Kanun'un 16/8 hükmü uyarınca üç yıldan beş yıla kadar hapis cezasıyla yaptırıma bağlanmıştır.

B. Sır Saklama Yükümlülüğü

Kanun'un 13. maddesi, Başkanlık faaliyetleri kapsamında edinilen gizli bilgilerin, kişisel verilerin, ticari sırların ve bunlara ait belgelerin, mevzuat gereği yetkili kılınan mercilerden başkasına açıklanmasını ve gerçek veya tüzel kişilerin menfaatine kullanılmasını yasaklamaktadır. İkinci fıkra ise bu bilgilerin her türlü medya aracıyla yayımlanması veya açıklanmasını yasaklamaktadır.

Bu yükümlülüğün ihlali, Kanun'un 16/3 hükmü uyarınca dört yıldan sekiz yıla kadar hapis cezasıyla yaptırıma bağlanmıştır. Cezanın ağırlığı, korunan bilgilerin hassasiyetiyle doğru orantılıdır.

BÖLÜM VIII

Kişisel Verilerin İşlenmesi ve Korunması

Kanun'un 6. maddesinin ikinci fıkrası, Başkanlık tarafından yürütülen işlemler kapsamındaki kişisel verilerin hukuka uygun şekilde işlenmesini zorunlu kılmaktadır. İlgili sebeplerin ortadan kalkmasıyla birlikte kişisel veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Bu düzenleme, Başkanlığın geniş veri toplama yetkilerinin KVKK ilkeleriyle dengelenmesini sağlamaktadır. Başkanlık, sınırsız bir veri biriktirme yetkisine sahip değildir; toplanan verilerin amacın ortadan kalkmasıyla birlikte tasfiye edilmesi zorunludur. Amaçla sınırlılık ve veri minimizasyonu ilkelerinin, Başkanlık faaliyetleri bakımından da geçerli olduğu açıkça vurgulanmıştır.

Bununla birlikte, 6. maddenin birinci fıkrasının (ç) bendindeki "kendi mevzuatlarındaki hükümleri gerekçe göstererek kaçınamaz" kaydı, KVKK'daki veri işleme şartlarının Başkanlık talepleri karşısında ileri sürülemeyeceğini göstermektedir. Bu durum, Başkanlığın veri toplama yetkisi ile veri sahiplerinin hakları arasında bir gerilim alanı oluşturmaktadır.

BÖLÜM IX

Başkanlığın Mali Yapısı

Kanun'un 14. maddesi, Başkanlığın gelirlerini düzenlemektedir. Gelir kaynakları arasında genel bütçe yardımları, faaliyet gelirleri, uygulanan idari para cezaları, ilgili fonlardan aktarılacak tutarlar ve diğer gelirler yer almaktadır.

İdari para cezalarının Başkanlığın gelir kaynakları arasında sayılması dikkat çekicidir. Kanun'un 16. maddesinin onuncu ve on birinci fıkralarında öngörülen idari para cezaları (bir milyon TL'den yüz milyon TL'ye kadar uzanan geniş bir aralıkta) Başkanlığın bütçesine doğrudan katkı sağlamaktadır.

Başkanlık ayrıca belirli vergi ve harç muafiyetlerinden yararlanmaktadır. Bu muafiyetler, Başkanlığın operasyonel esnekliğini ve mali sürdürülebilirliğini güçlendirmeye yöneliktir.

BÖLÜM X

Kanun Kapsamındaki Kişi ve Kuruluşların Başkanlığa Karşı Sorumlulukları

Kanun'un 7. maddesi, bilişim sistemleriyle hizmet sunan, veri toplayan ve işleyen tüm kişi ve kuruluşlara önemli sorumluluklar yüklemektedir. Bu sorumluluklar şöyle özetlenebilir:

Bilgi ve veri sağlama sorumluluğu

Başkanlığın görev ve faaliyetleri kapsamında talep ettiği her türlü veri, bilgi, belge, donanım, yazılım ve diğer her türlü katkıyı öncelikle ve zamanında Başkanlığa iletmek.

Olay bildirme sorumluluğu

Hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek.

Yetkili tedarikçilerden ürün ve hizmet temini

Kamu kurumları ve kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetlerini Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanlarından, üreticilerden veya şirketlerden tedarik etmek.

Sertifikasyon zorunluluğu

Sertifikasyon, yetkilendirme ve belgelendirmeye tabi siber güvenlik şirketlerince faaliyete başlamadan önce Başkanlığın onayını almak.

Bu sorumlulukların yerine getirilmemesi, Kanun'un 16. maddesindeki cezai hükümler ve idari para cezaları ile yaptırıma bağlanmıştır.

BÖLÜM XII

Değerlendirme ve Sonuç

7545 sayılı Siber Güvenlik Kanunu ile kurulan Siber Güvenlik Başkanlığı, Türkiye'nin siber güvenlik ekosisteminde paradigma değişikliği yaratacak bir kurumsallaşmadır. Başkanlığın, [Siber Güvenlik Kanunundaki suçlarla](#) kapsamı korunan geniş görev ve yetki yelpazesi, Cumhurbaşkanlığına bağlı konumu, esnek personel rejimi ve güçlü denetim-yaptırım mekanizmaları, bu kurumun merkezi ve etkin bir siber güvenlik otoritesi olarak tasarlandığını açıkça ortaya koymaktadır.

Bununla birlikte, bu kurumsal tasarımın başarısı büyük ölçüde uygulamaya bağlı olacaktır. Özellikle şu hususlar, Başkanlığın etkinliği bakımından belirleyici olacaktır:

Kanun'un Geçici 1. maddesi, uygulama düzenlemelerinin bir yıl içinde yürürlüğe konulmasını öngörmektedir. Sertifikasyon kriterleri, denetim usulleri, bildirim prosedürleri ve sınıflandırma esasları gibi ikincil

düzenlemelerin zamanında ve yeterli açıklıkta çıkarılması kritik öneme sahiptir.

Siber güvenlik alanında global ölçekte yaşanan yetenek açığı göz önüne alındığında, Başkanlığın yeterli sayıda ve nitelikte uzman personel istihdam edebilmesi, kurumun operasyonel kapasitesinin temel belirleyicisi olacaktır.

Başkanlığın düzenleyici ve denetleyici rolü ile özel sektörün inovasyon ve rekabet kapasitesi arasında sağlıklı bir denge kurulması gerekmektedir. Aşırı düzenlemenin sektörü kısıtlaması, yetersiz düzenlemenin ise güvenlik açıkları yaratması riski her zaman mevcuttur.

Siber tehditlerin sınır ötesi niteliği, Başkanlığın uluslararası iş birliği mekanizmalarını etkin şekilde kullanmasını zorunlu kılmaktadır. Budapeşte Sözleşmesi çerçevesindeki adli yardım mekanizmaları, ikili iş birliği anlaşmaları bu kapsamda önem taşımaktadır.

Siber Güvenlik Başkanlığı, kuruluş amacı ve sahip olduğu yetkiler itibarıyla, Türkiye'nin dijital çağıdaki güvenlik ihtiyaçlarına yanıt verme potansiyeline sahip güçlü bir kurumsal yapıdır. Bu potansiyelin gerçeğe dönüştürülmesi, kurumun operasyonel olarak güçlendirilmesine, hukuki çerçevenin netleştirilmesine ve tüm paydaşların aktif katılımına bağlıdır.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/siber-guvenlik-baskanligi-ve-yapisi>