



T.B.M.M.

CUMHURİYET HALK PARTİSİ
Grup Başkanlığı

Tarih : 14 Ağustos 2025

Sayı : 13469

32718

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıda yer alan soruların, Cumhurbaşkanı Yardımcısı Cevdet YILMAZ tarafından Anayasanın 98. ve TBMM İçtüzüğü'nün 96. ve 99. Maddeleri uyarınca yazılı olarak cevaplandırılmasını talep ederim.

Eylem Ertuğ ERTUĞRUL
Zonguldak Milletvekili
Milli Savunma Komisyonu Üyesi

Siber güvenlik, günümüz dünyasında yalnızca teknolojik bir mesele değil, aynı zamanda ulusal güvenliğin, kamu düzeninin, ekonomik istikrarın ve bireysel hakların korunmasının da temel bileşenlerinden biridir. Türkiye'de son yıllarda artan veri sızıntıları, kimlik bilgisi hırsızlıkları ve kritik altyapılara yönelik siber saldırılar, bu alanda kurumsal kapasitenin güçlendirilmesi gerektiğini ortaya koymaktadır. Tam da bu noktada, son günlerde gündeme oturan sahte diploma skandalları bu kurumsal kapasitenin güçlendirilmediği ya da bir şekilde atıl bırakıldığı şüphelerini oluşturmaktadır.

Sahte diploma iddiaları pek çok kere gündeme gelmiştir. Kritik kurumlarımıza sızmak isteyen kişi ya da kişilerin sahte diplomalar yoluyla bu adımları attığı çeşitli soruşturma dosyalarına konu olmuş hatta meclis çatısı altında da araştırılması istenilmiştir. Diploma skandalı bir eğitim meselesi olmaktan öte, bir milli güvenlik sorunu haline gelmiştir.

Bu güvenlik sorununa yönelik olarak çözüm getirmek üzere Siber Güvenlik Başkanlığı, Cumhurbaşkanlığı'na bağlı olarak 08 Ocak 2025 tarihinde resmen kurulmuş bir başkanlıktır. Amacı ise devlet ve millet nezdinde siber istihbaratın derlenmesi olarak belirtilmiştir.

Hal böyleyken, Siber Güvenlik Başkanlığı'nın kendisine verilen kaynakları ve yetkiyi kullanarak devletimizin tüm kritik kurumlarına yönelen tehditlere karşı etkili bir mücadele vermesi elzemdir. Zira, son günlerde ortaya çıkan dijital imzaların kötüye kullanılarak sahte diploma, akademik unvan ve resmi belgeler üretildiğine dair iddialar, ülkemizin kritik sistemlerinin güvenilirliği konusunda ciddi endişeler doğurmuştur. MEB, YÖK, BTK ve Milli Emlak gibi sistemlere yetkisiz erişim sağlandığına dair iddialar yalnızca bir güvensizlik değil, devletin milli güvenliğine karşı ciddi bir tehdittir. Geçmiş dönemlerde, FETÖ mensuplarının Türk Silahlı Kuvvetlerimiz ve kritik kurumlarımıza sızmaları neticesinde yaşanan milli güvenlik sorunları hala hatırlardadır.

Siber Güvenlik Başkanlığı'nın kurulmasının ardından yine TBMM'de buna yönelik bir Siber Güvenlik Kanunu görüşülmüş ve kabul edilmiştir. Ancak o zamandan bu zamana gelindiğinde yani yaklaşık 8 aydır Siber Güvenlik Başkanlığı'na bir atamanın yapılmamış olduğu görülmektedir. Bu skandallar zinciri, Siber Güvenlik Başkanlığı'nın etkinliğini de sorgulamayı gerektirmiştir. Görevi, kritik altyapıları koruma; sorumluluğu, kurumlar arası koordinasyonu sağlama ve siber güvenlik politikalarını geliştirme olan bir başkanlığın bu tür zafiyetlerin önlenmesi için hayati önemde olduğu aşikardır.

Bu bağlamda;

1-)Türkiye'nin siber güvenliğinden ve bütün bakanlık ve devlet kuruluşlarının bu amaçla koordinasyonundan sorumlu olması amacıyla 08 Ocak 2025 tarihinde resmen kurulan Siber Güvenlik Başkanlığı'na bugüne kadar neden kimse atanmamıştır?

2-)Basında yer alan açıklamalara göre, soruşturmalar aslında aylar önce başlamıştır. Sahtecilik, sadece diploma ve ehliyetlerle mi sınırlıdır? Askeri ya da mali sisteme uzanan bir sahtecilik var mıdır?

3-) Ortaya çıkan iddialara göre, genellikle üst düzey ve yetki sahibi kamu görevlilerinin elektronik imzaları kopyalanmış bu sayede de kamu kurumlarında evrak üretilmeye çalışılmıştır. Kamu görevlilerinin neredeyse tamamı da elektronik imzalarını kamu kuruluşlarından özellikle TÜBİTAK'tan temin etmiştir. Konunun e-imza veren kamu kuruluşlarıyla bağlantısı var mıdır?

4-) Yetki sahibi kamu görevlilerinin elektronik imzaları klonlanırken ve kamu kurumlarının veri tabanlarında kullanılırken bunu tespit etmek mümkün değil midir?

5-)Eğer bu kadar çok sahteciliğe rağmen ilgili şirketler klonlama işlemlerini fark etmemişse bunun elektronik güvenlik kapasitesinin yeterli olmamasıyla ilgisi olduğunu düşünmez misiniz?

6-)Siber Güvenlik Başkanlığı ne iş yapmaktadır? Siber güvenliğin ulusal güvenliğin bir parçası olduğu yönünde güncel strateji belgeleri, eylem planları ve reform hazırlıkları var mıdır? Varsa bunlar kamuoyu ile paylaşılmış mıdır?

7-) Siber casusluk faaliyetlerine karşı gelişmiş tehdit istihbaratı ve analiz sistemlerinin geliştirilmesi için Siber Güvenlik Başkanlığı'nın planladığı veya yürüttüğü bir proje var mıdır?

8-)Hassas verilere yetkisiz erişim, bu bilgilerin iç ve dış kötü niyetli aktörler tarafından istismar edilme riskini doğurmaktadır. Sızan verilerin bireyleri hedef alabileceğine, kurumları manipüle edip kamu güvenini sarsma amacıyla kullanılabilmesine dair yakın geçmişte örnekler mevcuttur. Siber Güvenlik Başkanlığı, E-Devlet, YÖK, MEB, ÖSYM, SGK ve personel yönetim sistemleri gibi kritik veri tabanlarının çok katmanlı güvenlik duvarlarına, çapraz veri doğrulamasına ve içeriden sızmalara karşı aktif savunmaya yönelik bir çalışması yok mudur?