Batuhan Küpeli[1]
Politika Analisti

DEĞERLENDİRME NOTU

KUANTUM SONRASI DÜNYAYA HAZIR MIYIZ? Q-DAY

ABD hükümeti, 22 Haziran 2026'da kuantum teknolojisiyle ilgili iki önemli kararname yayımladı (Beyaz Saray, 2026a; 2026b). İlk kararname mevcut riske karşı koruma sağlamayı amaçlıyor. Kamu kurumlarının kullandığı şifreleme sistemleri, kuantum bilgisayarların çözemeyeceği yeni yöntemlerle değiştirilecek. Federal kurumların en kritik sistemlerinde bu dönüşümün 2030-2031'e kadar tamamlanması hedefleniyor. İkinci kararname ise kapasite geliştirmeye yönelik. ABD, kuantum bilgisayarları ve kuantum sensörleri için ulusal ölçekte bir araştırma ve yatırım programı başlatıyor. Amaç yalnızca korunmak değil, bu teknolojide dünya liderliğini elde tutmak.

Peki, bu acele neden? Kararların ardında iki gelişme var. Birincisi, bilim dünyası "şifre kırma günü" ne ilişkin tahminlerini öne çekti. Yakın tarihli çalışmalar, kuantum bilgisayarların bugünkü şifreleri kırma eşiğine sanılandan daha erken ulaşabileceğini gösteriyor. İkincisi, tehdit yalnızca gelecekte değil. Bugün şifreli biçimde iletilen veriler kaydedilip yıllarca saklanabiliyor. Yeterli kuantum gücü oluştuğunda bu veriler geriye dönük çözülebilecek. Oysa devlet yazışmaları, sağlık kayıtları ve finansal bilgiler uzun yıllar gizli kalmak zorunda. Bu nedenle hazırlığın bugünden başlaması gerekiyor.

Mesele yalnızca güvenlik de değil. Kuantum, yapay zekâ ile birlikte ilerleyen çok daha büyük bir teknoloji yarışının parçası. Donanımda öne geçen ülke, yazılımda da öne geçme şansı yakalıyor. Bu yüzden ABD, teknolojiyi yeniden devlet eliyle ve planlı biçimde geliştirmeye yöneliyor. İleride göreceğimiz gibi, bu tercihin Soğuk Savaş yıllarına uzanan bir geçmişi var. Üstelik yarışın etkileri iki büyük güçle sınırlı kalmıyor. Teknolojinin bloklara ayrıldığı bir düzen, Türkiye gibi üçüncü ülkeleri de doğrudan ilgilendiriyor.

İşin umut veren tarafı da var. Kuantum tehdidine karşı geliştirilen yeni şifreleme yöntemleri artık hazır. Asıl zorluk yeni bir teknoloji icat etmek değil, milyonlarca cihaz ve sistemi

[1] https://www.tepav.org.tr/tr/ekibimiz/s/1478

kapsayan bir dönüşümü yönetebilmek. Türkiye'de ise bu dönüşüm için kamuoyuna açıklanmış ulusal bir yol haritası henüz yok. Bu değerlendirme notunda dört soruya cevap arayacağız: Kuantum tehdidi ne kadar yakın? Dünya bu geçişe nasıl hazırlanıyor? Bu yarış küresel teknoloji düzenini nasıl yeniden şekillendiriyor? Türkiye bu tablonun neresinde duruyor?

Bu soruları yanıtlamanın ilk adımı, kuantum bilgisayarın ne olduğunu netleştirmek. Bildiğimiz bilgisayarlar bilgiyi "bit" adı verilen birimlerle işler. Bir bit ya 0 ya da 1 değerini alır. Kuantum bilgisayar ise "qubit" adı verilen birimleri kullanıyor. Qubit, "süperpozisyon" denen özellik sayesinde aynı anda hem 0 hem 1 olabiliyor. Böylece kuantum bilgisayar çok sayıda olasılığı aynı anda değerlendirebiliyor.

Ancak, bu özellik kuantum bilgisayarı her işte üstün kılmıyor. Belge açmak ya da tablo hesaplamak gibi gündelik işlerde sıradan bilgisayarlar daha hızlı. Kuantum bilgisayarın üstünlüğü, aynı anda çok sayıda olasılığın denenmesini gerektiren işlerde ortaya çıkıyor. Karmaşık optimizasyon problemleri, yeni ilaç ve malzeme tasarımı ile bazı yapay zekâ ve finans hesapları bu gruba giriyor.

Bu fikrin geçmişi kırk yılı aşıyor. Richard Feynman, 1982'de doğayı taklit edebilecek bir kuantum makinesinin kuramsal temelini attı (Feynman, 1982). Peter Shor, 1994'te böyle bir makinenin şifreleme için ciddi bir tehdit oluşturabileceğini gösterdi (Shor, 1994). Donanım da adım adım ilerledi. Google'ın Sycamore çipi 2019'da belirli bir testte klasik bilgisayarları geride bıraktı (Google, 2019). Aynı şirketin Willow çipi 2024'te hata düzeltmede kritik bir eşiği aştı (Google, 2024). Çin de kendi işlemcileriyle bu yarışa karşılık verdi (Global Times, 2026).

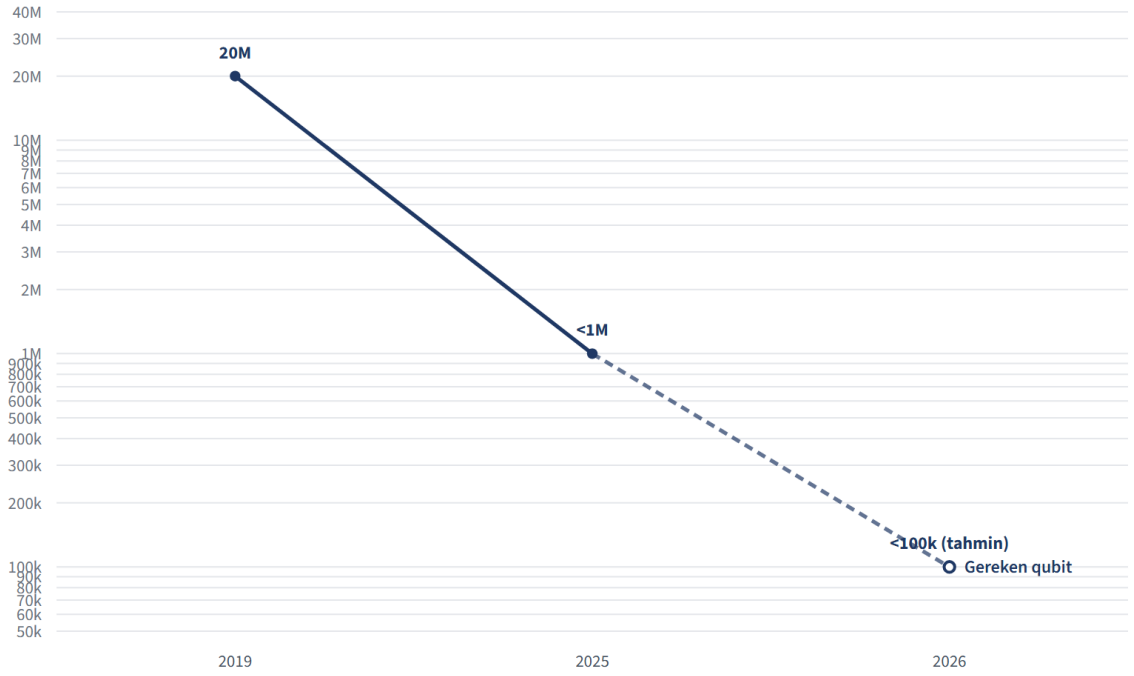
Kuantum bilgisayar şifrelemeyi neden tehdit ediyor? Modern şifreleme bir tür matematiksel dengesizliğe dayanır. Şifreyi kurmak kolaydır, geri çözmek ise pratikte imkânsızdır. Sıradan bir bilgisayarın bu işlemi tersine çevirmesi milyonlarca yıl sürer. İnternette en yaygın kullanılan sistemlerden biri RSA'dır. Banka hesaplarımızı, devlet yazışmalarını, mesajlarımızı ve kripto paraları koruyan kriptografik güvenliğin temelinde de bu hesaplama dengesizliği yatar.

Shor'un 1994'te gösterdiği tehdit tam bu noktada ortaya çıkıyor. Yeterince güçlü bir kuantum bilgisayar, normalde milyonlarca yıl sürecek bu çözme işlemini kısa sürede tamamlayabilir (Shor, 1994). Literatürde böyle bir makineye "kriptografik açıdan anlamlı kuantum bilgisayar" (CRQC) deniyor. Bu makinenin ortaya çıkacağı gün ise "Q-day" olarak adlandırılıyor. O gün geldiğinde, bugün güvendiğimiz şifrelemenin önemli bir bölümü bir anda savunmasız kalabilir.

Bugün için böyle bir kuantum bilgisayarı henüz mevcut değil. Var olan teknolojiyle kısa vadede üretilebilir de görünmüyor. Ancak bu hedefe doğru ilerleme beklenenden hızlı. Ayrıca son bir yılın en önemli gelişmesi donanımda değil, hesaplama yöntemlerinde yaşandı.

Uzun yıllar boyunca, yaygın kullanılan RSA-2048 şifresini kırmak için yaklaşık 20 milyon qubit'lik bir makine gerektiği hesaplanıyordu (Gidney ve Ekerå, 2021). Google araştırmacısı Craig Gidney, Mayıs 2025'te bu tabloyu değiştirdi. Gidney, yeni bir makine kurmadı. Yalnızca hesaplama yöntemini iyileştirerek bu sayıyı 1 milyonun altına indirdi (Gidney, 2025). Başka bir deyişle, aynı iş için gereken makine bir hamlede yaklaşık yirmide birine küçüldü. Cloudflare'dan Bas Westerbaan'ın yıllık "State of the post-quantum Internet" değerlendirmesine göre bu tek çalışma, tehdidi yaklaşık yedi yıl öne çekti (Cloudflare, 2025). Buna ek olarak Gidney'nin kullandığı hesap tekniğinin temeli, CRYPTO 2025'te sunulan ayrı bir çalışmadan geliyor (Chevignard vd., 2025). Düşüş burada da durmadı. Önerilen daha iddialı bir tasarım, aynı işi 100 binin altında qubit ile yapmayı öngörüyor (akt. PostQuantum.com, 2026) (Şekil 1).

Şekil 1. RSA-2048'i kırmak için gereken qubit sayısı, logaritmik ölçek, 2019-2026

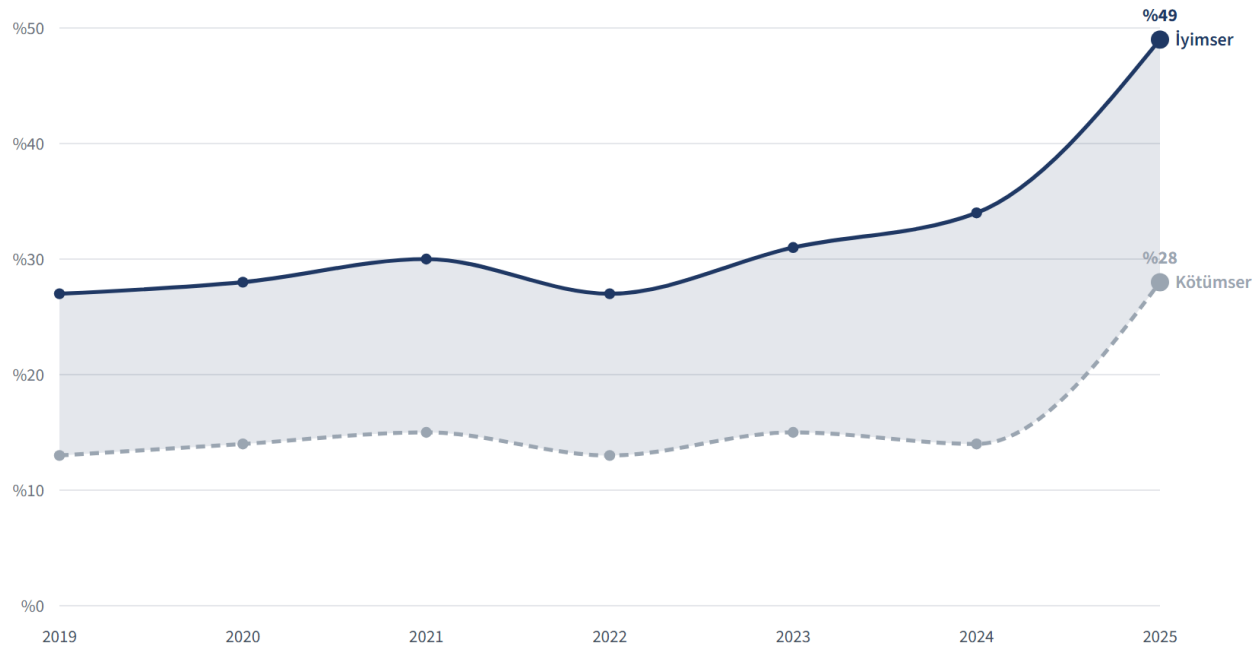


Kaynak: Gidney-Ekerå (2021), Gidney (2025), Pinnacle Architecture (2026), TEPAV görselleştirmeleri

Bu sıçrama sektörün büyük oyuncularını da harekete geçirdi. Google, kararnamelerden üç ay önce, Mart 2026'da iki açıklama birden yaptı. Şirket önce kendi sistemlerini 2029'a kadar kuantuma dayanıklı yeni şifrelemeye (post-quantum cryptography, PQC) taşıyacağını duyurdu (Google, 2026a). Ardından Google Quantum AI'dan Ryan Babbush ve Hartmut Neven, şifrelemedeki açığı özellikle kripto paralar üzerinden ortaya koyan teknik raporlarını yayımladı (Google, 2026b).

Q-day ne zaman gelecek? Bu sorunun kesin bir cevabı yok. Ancak uzmanların kanaati son yıllarda gözle görülür biçimde sertleşiyor. evolutionQ'dan Michele Mosca ve Marco Piani'nin Global Risk Institute için hazırladığı yıllık uzman anketi bu eğilimi gösteriyor. Ankete göre, uzman yanıtlarının iyimser okumasında böyle bir makinenin on yıl içinde ortaya çıkma olasılığı 2024'te yüzde 34 iken 2025'te yüzde 49'a yükseldi. Temkinli okuma bile yüzde 14'ten yüzde 28'e çıktı (Global Risk Institute ve evolutionQ, 2026). Kuşkusuz anket küçük bir uzman havuzuna dayanıyor. Bu yüzden rakamları ihtiyatla okumak gerekiyor. Yine de 2025 değeri yedi yıllık serinin en yükseği ve rapor, son üç yılın anketlerine göre belirgin bir sıçramaya işaret ediyor (Şekil 2).

Şekil 2. Uzman anketinde 10 yıl içinde kriptografik açıdan anlamlı kuantum bilgisayarın icat edilme olasılığı, 2019-2025

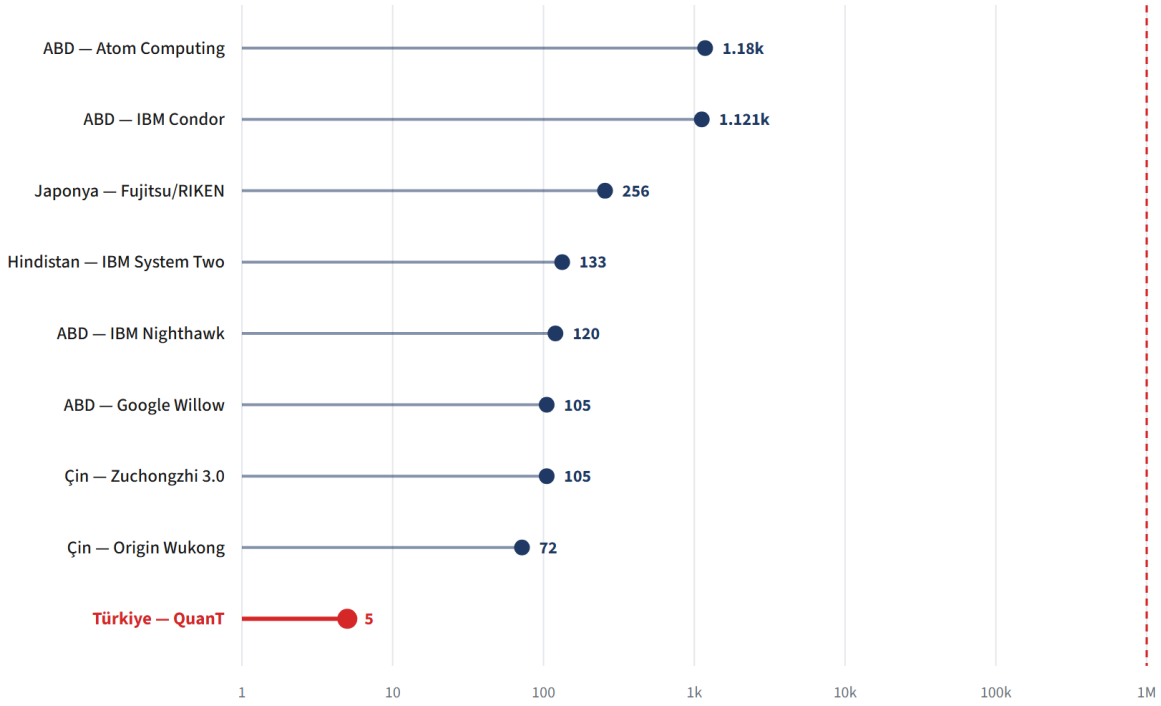


Kaynak: Global Risk Institute evolutionQ, Quantum Threat Timeline Report 2025, TEPAV görselleştirmeleri

Yine de önlem almak için kesin bir tarih beklememiz gerekmiyor. Çünkü tehdit, kuantum bilgisayarın icadını beklemiyor. Bunun nedeni "şimdi topla, sonra çöz" (harvest now, decrypt later) olarak bilinen saldırı yaklaşımı. Saldırganlar bugün ağlar üzerinden iletilen şifreli verileri kaydedip yıllarca saklayabiliyor. Yeterli kuantum kapasitesi oluştuğunda ise bu verileri geriye dönük çözebilecekler. Uzun süre gizli kalması gereken veriler için risk bu nedenle bugünden başlamış durumda. Geçişi kuantum bilgisayarın icadına kadar ertelemek, bu verilerin gelecekte açığa çıkmasını baştan kabullenmek anlamına geliyor.

Ülkelerin elindeki makineler bu eşiğin neresinde? Devletler ve şirketler qubit sayısını artırma yarışında. Ancak asıl mesele kimin kaç qubit'e sahip olduğu değil, mevcut makinelerin şifre kırma eşiğine ne kadar yaklaştığı. Bugünün en güçlü sistemleri ancak bin qubit düzeyini aşabilmiş durumda. Oysa şifre kırmak için gereken kapasite bunun yüzlerce katı (Şekil 3). Yine de bu mesafeye güvenmek yanıltıcı olur. Çünkü aradaki fark bir makas gibi iki yönden birden kapanıyor. Bir yanda makineler her yıl büyüyor. Öbür yanda gereken qubit sayısı algoritmalardaki ilerlemeyle düşüyor (Gidney, 2025). Makas iki taraftan kapandığı için, bugünkü donanım sınırına bakıp "daha çok var" demek aldatıcı.

Şekil 3. Ulusal amiral gemisi kuantum bilgisayarları, qubit sayısı, logaritmik ölçek



Kaynak: Üretici ve ulusal program duyuruları, TEPAV görselleştirmeleri

Tehdide karşı elimizde ne var? Durum sanıldığından daha umut verici. Kuantuma dayanıklı şifreleme yöntemleri artık hazır. ABD'nin standart belirleyen kurumu NIST (Ulusal Standartlar ve Teknoloji Enstitüsü), 2024'te ilk kuantuma dayanıklı şifreleme standartlarını yayımladı. Anahtar değişimi için ML-KEM, dijital imza için ML-DSA ve SLH-DSA seçildi (NIST, 2024).

Bu standartların hayata geçirilmesi iki ayrı alanda ilerliyor. Ne var ki iki alandaki dönüşüm aynı hızda gitmiyor.

- İlk alan "anahtar değişimi". Bu mekanizma, iki tarafın ortak bir gizli anahtarı güvenli biçimde paylaşmasını sağlıyor. Buradaki dönüşüm görece hızlı ilerliyor. Çoğu durumda yazılım güncellemesi yeterli oluyor. Cloudflare'ın gözlemlediği kullanıcı trafiğinin yarısından fazlası bugün kuantuma dayanıklı şifrelemeyle akıyor (Cloudflare, 2025).
- İkinci ve daha zorlu alan, dijital imza sistemleri. Bu sistemler, bir mesajın gerçekten gönderildiği kişi ya da kurumdan geldiğini doğruluyor. Yeni nesil imza algoritmaları daha büyük anahtarlar ve imzalar gerektiriyor. Bu nedenle uygulama süreci daha yavaş ilerliyor. Standartların olgunlaşması da zaman alıyor.

Dijital imza tarafındaki güçlüklerin en somut örneğini kripto paralarda görüyoruz. Nitekim tartışmayı başlatan Google çalışması da doğrudan bu konuya odaklanıyordu (Google, 2026b). Bir kripto para cüzdanının sahipliği dijital imzayla doğrulanır. Yeterli kapasiteye sahip bir kuantum bilgisayar, ağda görünür hâle gelmiş açık anahtardan gizli anahtarı türetebilir. Bu durumda ilgili cüzdanın kontrolünü ele geçirmesi teorik olarak mümkün. Google'ın işaret ettiği başlıca risk alanı, uzun süredir hareketsiz duran ve sahipleri tarafından kullanılmayan eski adresler. Bununla birlikte bu senaryo kaçınılmaz bir sistem çöküşü anlamına gelmiyor. Aktif cüzdanlar kuantuma dayanıklı imza algoritmalarına geçebilir (Google, 2026b). Piyasalarda da

şimdilik yaygın bir panik gözlenmiyor. Bununla birlikte bazı analistler, kuantum endişesinin Bitcoin fiyatına şimdiden yansımaya başladığını savunuyor (CoinDesk, 2026).

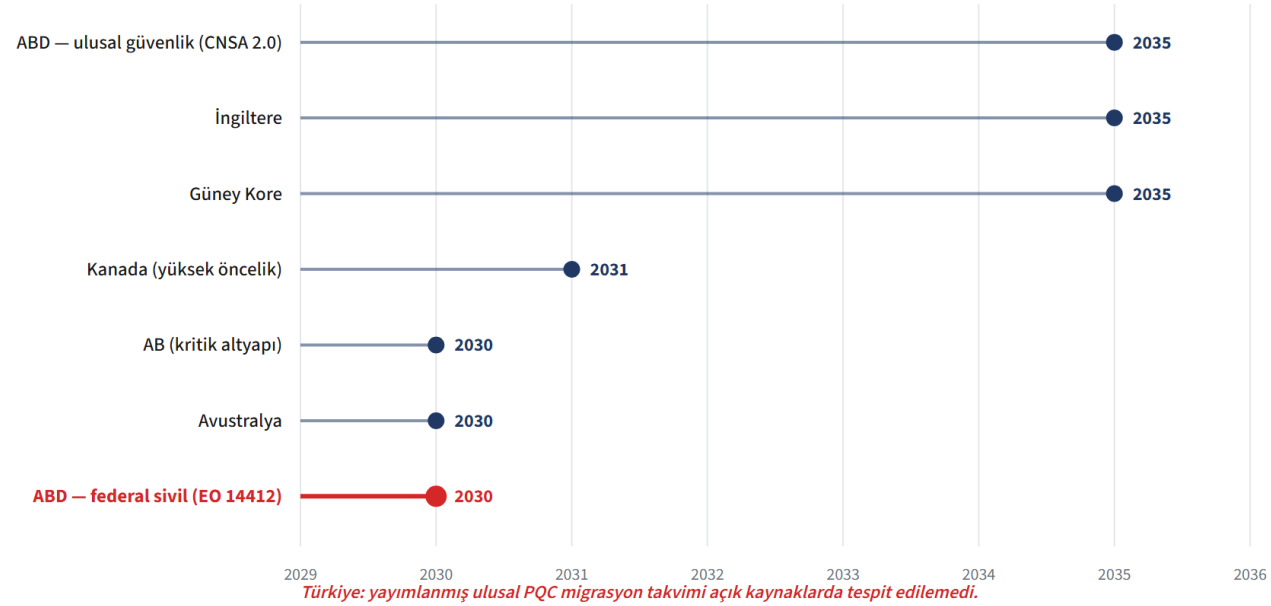
Bir diğer risk, yeni standartların büyük ölçüde aynı matematiksel aileye dayanması. Bu ortak temelde ciddi bir güvenlik açığı çıkarsa çok sayıda sistem aynı anda etkilenebilir. Nitekim Nisan 2024'te bu aileyi tehdit ettiği düşünülen bir yöntem ortaya atıldı. Yöntem yaklaşık on gün içinde geçerliliğini yitirdi. Ama bu deneyim önemli bir derse dönüştü. NIST, farklı bir matematiksel yaklaşıma dayanan yedek bir algoritma (HQC) seçti (Cloudflare, 2025; NIST, 2025). Amaç açık: gerektiğinde şifreleme yöntemini hızla değiştirebilmek.

Standartların hazır olması, her ülkenin aynı yoldan gideceği anlamına gelmiyor. Ortada iki farklı yaklaşım var. Batı ülkeleri geçişi açık ve tarihli takvimlere bağladı. ABD, ulusal güvenlik sistemleri için 2035 hedefini koydu (NSA, 2022). 22 Haziran 2026 kararnamesi buna sivil kurumların öncelikli sistemleri için 2030-2031 hedefini ekledi (Beyaz Saray, 2026a). İngiltere, Avrupa Birliği, Kanada, Avustralya ve Güney Kore de 2028-2035 aralığına yayılan kendi hedeflerini açıkladı (NCSC, 2025; Global Risk Institute ve evolutionQ, 2026; Reuters, 2026).

İkinci yaklaşım Çin'e ait ve mantığı tümüyle farklı. Önce bir yanlış anlamayı düzeltelim. Sık tekrarlanan "Çin üç yıl içinde kendi standardını çıkaracak" sözü resmi bir belgeye dayanmıyor. Bu söz, Tsinghua Üniversitesi'nden Profesör Wang Xiaoyun'un Reuters'a yaptığı bir değerlendirme (Reuters, 2026). Çin, Batı'nın hazır standardını benimsemek yerine kendi yöntemini geliştiriyor. Aradaki ayrım teknik ama özü basit. NIST'in seçtiği yöntemler, belirli bir matematiksel düzene oturan "cebirsel kafes" ailesine dayanıyor. Çinli araştırmacılar ise bu düzeni taşımayan "yapısız kafes" yöntemlerine, örneğin S-Cloud+'a yöneliyor. Wang'a göre düzenli aile küçük bir güvenlik zafiyeti taşıyor, düzensiz olan taşımıyor. Özetle Çin, Batı'nın standardını yeterince güvenli bulmuyor.

Üstelik Çin'in hamlesi standart tercihiyle sınırlı değil. Mart 2026'da açıklanan yeni beş yıllık plan, kuantumu çekirdek stratejik sanayilerden biri ilan etti. Geçişte öncelik, en hassas iki sektöre, finans ve enerjiye verildi (Reuters, 2026). Batı, tarihli bir NIST geçişi yürütüyor. Çin ise kendi standardını kuran ayrı bir yol izliyor. Ülkelerin hedef yılları arasındaki ayrışma Şekil 4'te görülebilir.

Şekil 4. Ülkelerin post-quantum kriptografi migrasyon hedef yılları



Türkiye: yayımlanmış ulusal PQC migrasyon takvimi açık kaynaklarda tespit edilemedi.

Kaynak: NSA CNSA 2.0, ABD EO 14412 (Haziran 2026), UK NCSC, AB Coordinated PQC Roadmap, Kanada, Avustralya, Güney Kore (Reuters), TEPAV görselleştirmeleri

Bu politikaların en kapsamlısını ise yarışın önünde giden ABD yürütüyor. Kuantum rekabeti artık yalnızca bilimsel araştırmaların konusu değil. Ulusal güvenlik ve teknoloji politikasının da temel başlıklarından biri hâline geldi. 22 Haziran'ın iki kararnamesi bu mantık içinde birbirini tamamlıyor. İlki (EO 14412) ülkenin kendi şifrelemesini korumaya alıyor. İkincisi (EO 14413) kuantum kapasitesini büyütüyor. İkinci kararnamenin gerekçesi de açık sözlü. Kararname, "diğer ülkelerin Amerikan liderliğine meydan okumak için hızla harekete geçtiğini" söylüyor ve öne geçmek için bütüncül bir devlet yaklaşımı çağrısı yapıyor (Beyaz Saray, 2026b).

EO 14413 yalnızca teknoloji hedefleri koymuyor. Devletin kuantumu baştan sona nasıl yöneteceğine dair bütün bir kurumsal model kuruyor. Modelin ilk ayağı üretim. Bilimsel keşiflere yetecek güçte bir kuantum bilgisayarı geliştirilecek ve en az bir makine Enerji Bakanlığı tesisine yerleştirilecek. Devletin bu süreçte özel sektörü kamu alım taahhüdü gibi araçlarla yönlendirmesi öngörülüyor. Böylece devlet yalnızca araştırmayı destekleyen değil, yeni teknolojiler için talep oluşturan bir aktör olarak konumlanıyor. Kararname ayrıca savunma alanındaki öncelikli kuantum sensör projelerinin 2028'e kadar sahaya çıkmasını hedefliyor.

Modelin ikinci ayağı güvenlik. Kararname, istihbarat ve savunma kurumlarına düzenli bir değerlendirme görevi veriyor. Bu kurumlar ticari kuantum bilgisayarların gelişimini izleyecek. Gelişmelerin kuantuma dayanıklı şifrelemeye geçiş üzerindeki etkilerini de raporlayacak. Başka bir ifadeyle ABD, teknolojiyi geliştirmeyi ve risklerine karşı önlem almayı aynı stratejinin içinde ele alıyor.

Üçüncü ayak ise kurumsal yapılanma. Kuantum stratejisinin koordinasyonu Beyaz Saray düzeyine taşınıyor. Performans ölçümü, ortak araştırma altyapıları, iş gücü programları, danışma mekanizmaları ve karşı istihbarat kapasitesi tek bir çerçevede toplanıyor. Böylece dağınık destek programlarından merkezî olarak yönetilen bir yapıya geçiliyor.

ABD, kuantumu neden bu kadar stratejik görüyor? Bu devlet öncülüğünün arkasında teknik bir gerçek var. Güven Sak'ın 2024'te dikkat çektiği gibi, artan veri hacmi donanım ve yazılım yeniliğini aynı anda tetikliyor (Sak, 2024). Bir yanda çipler küçülüp hızlanıyor ve kuantum işlem gücü büyüyor. Öbür yanda yapay zekâ bu veriyi işleyecek olgunluğa yaklaşıyor. Kuantum bu nedenle tek başına bir donanım yarışı değil. Yapay zekâ ile birlikte ilerleyen tek bir teknoloji cephesinin donanım ayağı. Donanımı elinde tutan ülke, yazılımda da öne geçme şansı yakalıyor. Nitekim Washington üç hafta içinde üç kararname imzaladı. 2 Haziran'da yapay zekâ, 22 Haziran'da kuantum ve kriptografi kararnameleri geldi (Beyaz Saray, 2026a; 2026b; 2026c). Bu sıralama, üç alanın tek bir stratejik bütün olarak görüldüğüne işaret ediyor.

Teknolojiyi devlet eliyle ve planlı biçimde geliştirme yaklaşımı, yeni bir tartışmanın da parçası. Palantir yöneticileri Alexander Karp ve Nicholas Zamiska, 2025'te yayımladıkları "Teknolojik Cumhuriyet" (The Technological Republic) kitabında bu tartışmayı açtı. Yazarlara göre ABD, son kırk yılda teknolojiyi tüketiciye yönelik açık pazara bıraktı. Oysa rekabeti kazanmak için devletin yön verdiği kapalı devre bir buluş düzenine dönmek gerekiyor (Karp ve Zamiska, 2025).

Güven Sak'ın "Çin Rekabetini Ciddiye Alın" başlıklı yazısı, bu modelin kökenini hatırlatıyor (Sak, 2026). Sovyetler Birliği 1957'de ilk uydu Sputnik'i fırlatınca ABD, bir yıl sonra DARPA'yı (Savunma İleri Araştırma Projeleri Ajansı) kurdu. DARPA'nın kendi laboratuvarı yoktu. Ajans, projeleri üniversitelere ve şirketlere veriyor, sonuçları kendi çatısında topluyordu. Bugünkü internetin atası ARPANET de bu düzenden çıktı. Ancak 1973'teki Mansfield düzenlemesi,

ajansı yalnızca doğrudan askeri projelerle sınırladı. Dönemin bütçe ve petrol krizleri de eklenince DARPA'nın sivil teknolojiye öncülük rolü sona erdi. Buluşlar devletin denetiminden çıkıp önce tüketici pazarına, oradan bütün dünyaya yayıldı. Kuantum kararnamesinin amiral gemisi bilgisayarı devlet eliyle kurma ve şirketleri alım taahhütleriyle yönlendirme yaklaşımı, tam da bu DARPA tarzı düzene bir dönüş olarak okunabilir.

Bu yeni yaklaşımın hedefi açık. Yapay zekâ ve kuantum gibi sınır teknolojileri kapalı tutulacak. Rakibin, yani Çin'in, bakarak öğrenip kopyalaması zorlaştırılacak. Ancak Sak, bu girişimin Çin'in kapasitesini hafife alabileceğini ve başarı şansının tartışmalı olduğunu da vurguluyor (Sak, 2026). Stratejinin bir yan etkisi de var. Teknolojiyi tek elde tutma çabası, tıpkı ABD-Çin ticaret gerginliğinde olduğu gibi, üçüncü ülkeleri Çin ile daha fazla iş birliğine itebilir. Türkiye de bu üçüncü ülkelerden biri. Yine de üçüncü ülkelerin eli tümüyle bağlı değil. Belirleyici olan yalnızca teknolojiyi kimin ürettiği değil, geçişi kimin zamanında ve kararlı biçimde yönetebildiği. Buradan Türkiye'nin çıkaracağı ders şu: Kapasitesini somut bir taahhüde ve takvime bağlayabilen ülke, bu yeni düzende kendine yer bulur.

Türkiye bu tabloda nerede?

Türkiye'de kuantum teknolojisine ilgi de var, kapasite de. Ama kriptografik geçiş için açıklanmış, tarihli bir plan yok. Kurumsal taraf hareketli ancak dağınık. TÜBİTAK BİLGEM bünyesinde 2023'te Kuantum Teknolojileri Bölümü kuruldu. 2025'te sözü verilen Ulusal Kuantum Enstitüsü ise henüz kurulmadı (Anadolu Ajansı, 2025). TSE çatısı altında 2024'te, Turkcell öncülüğünde Kuantum Ayna Komitesi kuruldu (TSE, 2024). Savunma Sanayii Başkanlığı 2026'da Türkiye Kuantum Platformu'nu duyurdu (SSB, 2026). Bu dört yapı birbirinden ayrı çalışıyor. Tek elden işleyen bir ulusal post-quantum otoritesi ise yok.

Türkiye'nin en somut gücü yazılımda değil, fiziksel donanımda. TOBB ETÜ'de geliştirilen QuanT (5 qubit), ülkenin ilk kuantum bilgisayarı (Daily Sabah, 2024). Asıl öne çıkan alan ise kuantum anahtar dağıtımı (QKD). Bu teknoloji, şifreleme anahtarını fiziğin kurallarıyla dinlenemez biçimde paylaştırıyor. Bu alanda özel sektör öne geçmiş durumda. Turkcell kıtalararası karasal bir QKD bağlantısı kurdu (Turkcell, 2025). Türkiye çıkışlı girişim Qubitrium ise kuantum haberleşme yükünü yörüngeye taşıdı (Qubitrium, 2026).

Peki, "şimdi topla, sonra çöz" tehdidine asıl yanıt verecek olan kriptografik yazılım tarafında durum ne? Türkiye bu alanda da sıfırdan başlamıyor. Google'ın 2016'daki Chrome deneylerinde kullandığı kafes tabanlı öncü şema NewHope'un baş tasarımcılarından biri Türkiye'den: bugün Dokuz Eylül Üniversitesi'nde çalışan Erdem Alkım (Alkım vd., 2019). Türkiye'den akademisyenler NIST yarışmasındaki başka aday algoritmalarda da yer aldı. ODTÜ Uygulamalı Matematik Enstitüsü 2018'de Post-Kuantum Kriptografi Grubu'nu kurdu (ODTÜ UME, 2018). Sabancı ve Ondokuz Mayıs üniversitelerinde de bu alanda çalışan ekipler var. Ancak bu yetkinlik hâlâ sınırlı. Birikim ağırlıklı olarak kafes tabanlı yöntemlerde yoğunlaşıyor. Kurumsal süreklilik açısından da kırılgan görünüyor.

Bütün bu kapasiteye rağmen eksik olan tek halka, yayımlanmış, tarihli ve bağlayıcı bir ulusal geçiş takvimi. Resmî belgeler bu boşluğu doğruluyor. On İkinci Kalkınma Planı'nda "post-kuantum" ya da "kriptografi" hiç geçmiyor (Kalkınma Planı, 2023). Ulusal Siber Güvenlik Stratejisi'nde "kuantum" yalnızca bir kez anılıyor (Cumhurbaşkanlığı, 2024). Bankacılık, sermaye piyasası, kişisel veri ve telekom düzenleyicilerinin hiçbirinde PQC'ye dair bir rehber yok. Kısacası Türkiye kuantumu bir teknoloji üretim fırsatı olarak ele alıyor. Ama bugünün şifreli verisini yarının kuantum bilgisayarından koruma çerçevesine henüz geçmedi. Oysa "şimdi topla, sonra çöz" tehdidine bugün cevap veren şey, tam da bu geçiş ve onun takvimi.

Öneriler

Bu tablo, ertelenmemesi gereken beş somut adımı öne çıkarıyor.

- İlgili kamu otoriteleri, TÜBİTAK BİLGEM öncülüğünde, tarihli bir ulusal post-quantum geçiş takvimini 2027 yılı içinde açıklamalıdır. Takvim, kamu kurumlarını ve kritik altyapıyı kapsamalı ve NIST standartlarına dayanmalıdır. Anahtar değişimi ve dijital imza ayakları ayrı ele alınmalıdır. Batı ülkelerinin politikalarının merkezine koyduğu ve Türkiye'de eksik olan tek halka budur.
- Kamu kurumları ve kritik altyapı işletmecileri, ilk adım olarak kısa vadede kriptografik envanter çıkarmalıdır. Bu envanter, hangi sistemin hangi şifrelemeye bağlı olduğunu göstermelidir. "Şimdi topla, sonra çöz" tehdidi nedeniyle, en uzun süre gizli kalması gereken veriler geçişte önceliklendirilmelidir.
- Türkiye, kuantum girişimlerini ABD'nin bugün kurduğu modele benzer, görev odaklı tek bir yapıda toplamalıdır. Bu modelde devlet somut bir hedef koyuyor, işi tek bir amiral gemisi kuruma emanet ediyor ve talebi kamu alım taahhüdüyle garanti ediyor. Projeler ise üniversiteler ve şirketler eliyle yürütülüyor. Türkiye'de modelin parçaları bugün de mevcut. TÜBİTAK araştırmayı fonluyor ve kendi enstitülerinde yürütüyor. Savunma Sanayii Başkanlığı projeleri sözleşmelerle şirketlere veriyor ve tedarik gücüyle yönlendiriyor. Eksik olan, bu parçaları tek çatıda birleştirmek. Bu çatı, daha yalın bir DARPA tarzında da kurulabilir: kendi laboratuvarı olmayan, süreli ve iddialı hedefler koyan bir program ajansı.
- Kurulacak yapı, donanım ve yazılımı birlikte ele almalıdır. Türkiye'nin QKD ile öne çıkan donanım gücü ile NewHope mirasına dayanan yazılım birikimi aynı programda buluşturulmalıdır. Donanım ile yazılımın birbirini beslediği bir çağda, iki alandan birini ihmal eden strateji eksik kalır.
- Türkiye bu geçişi yalnızca teknik bir güncelleme olarak görmemelidir. Teknolojinin yeniden devletlerin denetimine ve bloklara çekildiği bir çağda geçiş, aynı zamanda stratejik bir konumlanmadır. Geçiş takvimi tek bir standarda, tedarikçiye veya teknoloji blokuna kilitlenmeden tasarlanmalıdır. Şifreleme yöntemini gerektiğinde hızla değiştirebilme yeteneği (kripto-çeviklik) korunmalıdır. Bunu başaran ülke, Q-day sonrası düzende güvenilir ve esnek bir taraf olarak kendine yer bulur.

Kaynakça

Alkım, E. vd. (2019). NewHope: kafes-tabanlı anahtar değişimi (NIST PQC standardizasyonu, 2. Tur adayı). https://newhopecrypto.org

Anadolu Ajansı (2025). Kuantum teknolojileri TÜBİTAK Ulusal Kuantum Enstitüsü ile desteklenecek. 28 Mart 2025. https://www.aa.com.tr/tr/bilim-teknoloji/kuantum-teknolojileri-tubitak-ulusal-kuantum-enstitusu-ile-desteklenecek/3522214

Beyaz Saray (The White House) (2026a). Securing the Nation Against Advanced Cryptographic Attacks (Executive Order 14412). 22 Haziran 2026. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

Beyaz Saray (The White House) (2026b). Ushering in the Next Frontier of Quantum Innovation (Executive Order 14413). 22 Haziran 2026. https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

Beyaz Saray (The White House) (2026c). Promoting Advanced Artificial Intelligence Innovation and Security (Executive Order 14409). 2 Haziran 2026. https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/

Chevignard, C., Fouque, P. A. ve Schrottenloher, A. (2025). Reducing the Number of Qubits in Quantum Factoring. CRYPTO 2025.

Cloudflare (2025). State of the post-quantum Internet in 2025 (Bas Westerbaan). 28 Ekim 2025. https://blog.cloudflare.com/pq-2025/

CoinDesk (2026). Quantum-resistant tokens jump 50% as Google flags risks to Bitcoin security (Omkar Godbole). 1 Nisan 2026. https://www.coindesk.com/markets/2026/04/01/the-first-winners-of-the-quantum-crypto-debate-are-already-clear-and-some-of-them-are-up-50

Cumhurbaşkanlığı (2024). 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (Cumhurbaşkanlığı Genelgesi 2024/11). Resmî Gazete, 7 Eylül 2024.

Daily Sabah (2024). Türkiye marks tech milestone as it unveils first quantum computer. 21 Kasım 2024. https://www.dailysabah.com/business/tech/turkiye-marks-tech-milestone-as-it-unveils-first-quantum-computer

Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6), 467-488.

Gidney, C. (2025). How to Factor 2048 Bit RSA Integers With Less Than a Million Noisy Qubits. arXiv:2505.15917. https://arxiv.org/abs/2505.15917

Gidney, C. ve Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.22331/q-2021-04-15-433

Global Risk Institute ve evolutionQ (2026). Quantum Threat Timeline Report 2025 (Michele Mosca, Marco Piani). Mart 2026. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

Global Times (2026). China's homegrown Origin Wukong superconducting quantum computer. 15 Haziran 2026. https://www.globaltimes.cn/page/202606/1363573.shtml

Google (2019). Quantum supremacy using a programmable superconducting processor (Sycamore). Nature, 574, 505-510.

Google (2024). Meet Willow, our state-of-the-art quantum chip. Aralık 2024.

Google (2026a). Quantum frontiers may be closer than they appear (Heather Adkins, Sophie Schmieg). 25 Mart 2026. https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

Google (2026b). Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly (Ryan Babbush, Hartmut Neven). Google Research, 31 Mart 2026. https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

Kalkınma Planı (2023). On İkinci Kalkınma Planı (2024-2028). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. https://www.sbb.gov.tr

Karp, A. C. ve Zamiska, N. W. (2025). The Technological Republic: Hard Power, Soft Belief, and the Future of the West. Crown.

NCSC (2025). Timelines for migration to post-quantum cryptography. 20 Mart 2025. https://web.archive.org/web/20250401031349/https://www.ncsc.gov.uk/pdfs/news/pqc-migration-roadmap-unveiled.pdf

NIST (2024). Post-Quantum Cryptography Standards (FIPS 203, 204, 205). https://csrc.nist.gov/projects/post-quantum-cryptography

NIST (2025). HQC'nin yedek anahtar kapsülleme mekanizması olarak seçilmesi. Mart 2025. https://csrc.nist.gov/projects/post-quantum-cryptography

NSA (2022). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).

ODTÜ UME (2018). Post-Quantum Cryptography Research Group. ODTÜ Uygulamalı Matematik Enstitüsü. https://iam.metu.edu.tr/en/post-quantum-cryptography-research-group

PostQuantum.com (Ivezić, M.) (2026). Quantum Threat Timeline Report 2025: Record Predictions. 5 Nisan 2026. https://postquantum.com/security-pqc/quantum-threat-timeline-report-2025/

Qubitrium (2026). QubitCore: yörüngeye ulaşan ticari kuantum haberleşme yükü. The Quantum Insider, 14 Nisan 2026. https://thequantuminsider.com/2026/04/14/a-quantum-payload-reaches-orbit-commercial-quantum-communication-is-on-the-horizon/

Reuters (2026). China likely to have standards for post-quantum cryptography in 3 years, expert says. 19 Mart 2026. https://www.reuters.com/world/asia-pacific/china-likely-have-standards-post-quantum-crytography-3-years-expert-says-2026-03-19/

Sak, G. (2024). Yapay zekâ yatırımları yavaşlatır mı? TEPAV Blog (Nasıl Bir Ekonomi Gazetesi), 30 Ocak 2024. https://www.tepav.org.tr/tr/blog/s/7315

Sak, G. (2026). Çin rekabetini ciddiye alın. Medium, Haziran 2026. https://guvsak.medium.com/çin-rekabetini-ciddiye-alın-630432e092e3

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. FOCS 1994, 124-134.

SSB (2026). Türkiye Kuantum Teknolojileri Yol Haritası ve Türkiye Kuantum Platformu. Savunma Sanayii Başkanlığı. https://kuantum.ssb.gov.tr

TSE (2024). Kuantum Teknolojileri Ayna Komitesi kuruldu (Turkcell ve TÜBİTAK BİLGEM iş birliği). Türk Standardları Enstitüsü, 19 Eylül 2024.

Turkcell (2025). Turkcell, kıtalararası karasal kuantum anahtar dağıtımını gerçekleştirdi. 25 Şubat 2025. https://medya.turkcell.com.tr