Journal of Quantum Technologies and Informatics Research
JQTAIR

KUANTUM TEKNOLOJİLERİ VE ENFORMATİK ARAŞTIRMALARI
Volume / Cilt: 2, Issue / Sayı: 3, 2024, pp. 129-151
E - ISSN: 3023-4735
URL: https://journals.gen.tr/index.php/jqtair/
DOI: https://doi.org/10.70447/ktve.2576

Received / Geliş: 14.10.2024
Acccepted / Kabul: 25.10.2024

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

# Kuantum Teknolojilerinin İstihbarat Düzleminde Gelecekteki Yeri*

## *The Future Place of Quantum Technologies in the Intelligence Plane*

**Tuncay Doğantuna**

Gazi Üniversitesi, Bilgi Güvenliği Mühendisliği Doktora Öğrencisi, Ankara, Türkiye, e-mail: tidituna@gmail.com

**Öz**

Bu çalışma, Kuantum Teknolojilerinin (KUT) istihbarat ve ulusal güvenlik alanlarındaki potansiyel etkilerini incelemektedir. Yıkıcı inovasyon olarak isimlendirilen bu teknoloji, istihbarat disiplininde hem fırsatlar hem de riskler sunmaktadır. Özellikle Kuantum Bilgisayar ve Kuantum İnternet gibi çabalar, veri işleme, saklama ve iletme süreçlerinde devrim niteliğinde değişiklikler getirebilir. Kuantum teknolojilerinin aynı anda hem 0 hem de 1 değerine sahip olabildiği süperpozisyon özelliği, işlem hızını ve kapasitesini klasik bilgisayarların çok ötesine taşımaktadır. Bu teknoloji, özellikle güvenlik ve istihbarat sahasında büyük bir potansiyele sahiptir. Söz konusu çalışma, KUT'un istihbarat faaliyeti ve süreci üzerindeki etkilerini araştırırken, "Alternatif Gelecekler Analizi" ve "Kırmızı Takım Analizi" gibi yapılandırılmış analiz tekniklerinden yararlanmayı planlamaktadır. Bu analiz teknikleri, KUT'un belirsiz geleceğini değerlendirmek ve istihbarat faaliyetlerinde nasıl kullanılabileceğini öngörmek açısından faydalı olacağı değerlendirilmektedir.

**Anahtar kelimeler:** Kuantum Teknolojileri, Yıkıcı İnovasyon, İstihbarat, Ulusal Güvenlik, Siber Uzay

*Bu çalışma, Prof. Dr. Serhat Ahmet Erkmen'in danışmanlığında hazırlanmıştır.

**Citation/Atıf:** DOĞANTUNA, T. (2024). Kuantum Teknolojilerinin İstihbarat Düzleminde Gelecekteki Yeri. *Kuantum Teknolojileri ve Enformatik Araştırmaları*. 2(3): 129-151, DOI: 10.70447/ktve.2576

**Corresponding Author/ Sorumlu Yazar:**
Tuncay Doğantuna
E-mail: tidituna@gmail.com

**Abstract**

This study examines the potential impacts of Quantum Technologies in the fields of intelligence and national security. This technology, referred to as disruptive innovation, presents both opportunities and risks in the intelligence discipline. Efforts such as Quantum Computer and Quantum Internet in particular can bring revolutionary changes in data processing, storage and transmission processes. The superposition feature of quantum technologies, which can have both 0 and 1 values at the same time, increases processing speed and capacity far beyond classical computers. This technology has great potential, especially in the fields of cybersecurity and intelligence. While investigating the impacts of QUT on intelligence activities and processes, the study offers the use of structured analysis techniques such as "Alternative Futures Analysis" and "Red Team Analysis". It is evaluated that these analysis techniques will be useful in evaluating the uncertain future of QUT and predicting how it can be used in intelligence activities.

**Keywords:** Quantum Technologies, Disruptive Innovation, Intelligence, National Security, Cyberspace

## 1. GİRİŞ

Geleceği şekillendirme potansiyeli ve projeksiyonu olan yenilikçi ve fütüristik teknolojiler, yıkıcı inovasyon kabiliyetleriyle tahminlerden daha hızlı ve sürpriz bir şekilde ilerleme kaydetmektedir. Bu teknolojik dönüşüm, finanstan lojistiğe, iletişimden güvenliğe pek çok alan ve sektörlerde uzanan geniş bir yelpazeye oturmaktadır. Özellikle güvenlik alanında, teknolojik değişime ayak uydurmaya çalışan en önemli alanlardan birisi de Ulusal Güvenlik ve Strateji'nin olmazsa olmazı İstihbarat disiplini ve faaliyetleridir.

21. yüzyılın ilk çeyreğinde, hemen hemen her alanda etkili olan etkili olan dijital (sayısal) dönüşüm ve enformasyon (bilişim) teknolojileri, istihbarat disiplini için de muhtemel fırsat ve riskler sunmaktadır. Bu yüzden, geleceğin yıkıcı teknolojilerinin de benzer potansiyel etkilere neden olması beklenmektedir [1]. Bu noktada blokzincir teknolojisi [2], yapay zekâ [3], makine öğrenmesi [4], büyük veri analitiği [5] gibi teknolojiler, istihbarat alanı üzerinde dönüştürücü bir etkiye sahip olduğu değerlendirilmektedir. Diğer yandan, söz konusu bu teknolojilerin yanında istihbarata potansiyel etkileri olabilecek teknolojilerden biri de Kuantum Teknolojisi (KUT) olduğu belirtilebilir. Konunun arka planı açısından, başta ABD olmak üzere Batı merkezli istihbarat çalışmaları ve Çin'deki güvenlik odaklı akademik araştırmalar uzun yıllardır inovasyon, teknoloji ve siber faaliyetler bağlamında geliştiği ele alınmaktadır [6].

KUT, güvenliğin ana temalarından biri haline dönüşmeye başladığı son birkaç yıl içinde konunun önemi istihbarat örgütleri tarafından da öncelikli bir statüye yükselmeye başlamıştır. İstihbaratın hem önleyici hem de devletlere fırsat/avantaj sağlayabilecek açılımları öngörebilmesi boyutu, KUT ile istihbaratı beraber ele alan çalışmaların önemini artırmaktadır. Örneğin, istihbarat analizinin faydalı olduğu kadar riskli de bir boyutu olan veri ve analiz paylaşımı KUT çerçevesinde yeni boyutlar kazanabilecektir.

Mevcut dijital teknolojiler, verinin işlenmesi, saklanması ve iletilmesi gibi işlemler için büyük imkanlar sunmaktadır. Bu teknolojiler, bilgiyi bitler aracılığıyla işler ve her bit yalnızca 0 veya 1 değeri alabilir. Ancak kuantum teknolojisi, verinin en temel yapı taşı olan bit yerine "kübit" kullanır. Kübitler, aynı anda hem 0 hem de 1 değerine sahip olabilen, yani süperpozisyon durumunda olabilen veri birimleridir. Bu özellik, kuantum bilgisayarların klasik bilgisayarlardan çok daha hızlı ve karmaşık hesaplamalar yapmasını sağlar. Bu durum, atom altı parçacıkların kuantum fiziği ile öğrenilen özelliklerinin bir sonucudur. Kuantum bilgisayarlar, bu farklı çalışma prensibi sayesinde geleneksel bilgisayarlardan çok daha üstün bir işlem gücü ve kapasitesi sunar [7].

Tüm Dünya'da internet erişiminin giderek yaygınlaşmasıyla birlikte, siber uzaydaki veri transferi de pek çok farklı amaçla yapılır hale gelmiştir. Ancak, yenilikçi ve yıkıcı teknoloji olarak adlandırılan KUT, şu ana kadar henüz ciddi sonuçlar üretmemiştir. Henüz örnekleri sınırlı olsa da az sayıdaki çalışma, söz konusu bu teknolojinin güvenlik ve istihbarat alanlarında da önemli sonuçlar doğurabileceğini ileri sürmektedir [8].

Bu çalışmanın ana konusu, KUT'un sahip olduğu yenilikçi ve yıkıcı potansiyelin, istihbaratın geleceğinde faaliyet, organizasyon ve süreç bağlamında nasıl sonuçlar doğurabileceği üzerine değerlendirmeleri içermektedir. Kuantum Teknolojisi de verinin en temel formunun biçiminin değişimine, hesaplanmasına ve işlenmesine, yani "bilgi sayımına" olanak tanımaktadır. Burada asıl sorulması gereken, yenilikçi ve yıkıcı kapasiteye sahip fütüristik bir teknoloji olan KUT üzerine olan ilerlemenin birçok sektör, bilimsel alan ve disiplin için olduğu gibi; istihbaratı da önümüzdeki dönemde hangi şekilde ve ne seviyede dönüştüreceği üzerine olacaktır. Daha açık biçimde bu çalışmanın konusu, bu tür bir teknolojinin istihbarat faaliyetleri ve disiplini için sunduğu fırsat ve tehditleri değerlendirdikten sonra aşağıdaki yapılandırılmış istihbarat analiz teknikleriyle analizini irdelemektedir:

- Alternatif Gelecekler Analizi (AGA),
- Kırmızı Takım Analizi (KTA),

Yukarıda bahsi geçen yapılandırılmış analiz tekniği, ilgili teknolojinin kendine has şartları nedeniyle tercih edilmektedir. Kuantum teknolojisi, henüz ticari ve bireysel düzlemde kullanım imkânı olmasa da devletler, küresel firmalar ve akademik kuruluşlar nezdinde deneysel araştırmalara konu edilmesi itibariyle bu çalışmaların çıktılarından yararlanarak belirli senaryolar dahilinde kurgularla birlikte yararlanılabilir. Alternatif gelecekler analizi tekniği, bilhassa durumun karmaşık olarak düşünüldüğü veya çıktıların tek bir değerlendirmesine güvenilmesi yetersiz kabul edildiği noktada yararlı sonuçlar üretebilir. Bu analiz tekniği, KUT ve etkilerinin halen berrak olmayan gelecek tahminleri nedeniyle elverişli bulunarak seçilmiştir.

Bu çerçevede çalışmanın amacı, fütüristik ve teknolojik dönüşümün yıkıcı etkilerine yönelik literatürü referans alan bu araştırmayı, ilerideki çalışmalara farklı bir perspektiften temel sağlamaktır. İkinci amacı, belirlenmiş olan yapılandırılmış analiz tekniğiyle KUT'un istihbaratın yakın geleceğindeki yeri ve etkisine yönelik analizi ortaya çıkarmaktır. Bu minvalde, özellikle "Ulusal Güvenlik" temelinde ve "Stratejik İstihbarat" seviyesinde Kuantum teknolojilerinin dikkatle irdelenmesi ve değerlendirilmesi İstihbarat Topluluğu'nun bu konulardaki gelişmelere de odağını verebilmesi bir ülkenin istihbarat avantajı açısından elini güçlendireceği kayda değer çalışmalarda ele alınmaktadır [9].

Bunun yanı sıra KUT, istihbarat kurumları tarafından da önemi giderek anlaşılan teknolojiler arasına dahil edilmektedir. Nitekim bu yıkıcı teknolojilerin öneminin güvenlik kurumları tarafından anlaşıldığına pek çok örnek verilebilir. Amerikan İstihbarat Topluluğu'nun çatı kuruluşu olan Ulusal İstihbarat Direktörlüğü Ofisi (ODNI) tarafından kurulan İstihbarat Gelişmiş Araştırma Projeleri Etkinliği (IARPA), Kuantum Bilişim gibi yüksek riskli faaliyetleri finanse etmek için kurulduğu belirtilmektedir [10]. 2006 yılında ODNI tarafından yetkilendirilen IARPA, DARPA benzeri bir modeli temel alarak askeri ihtiyaçlardan ziyade ulusal istihbarat ihtiyaçlarına odaklanmaktadır.

Son olarak, KUT sadece istihbarat çalışmalarını değil, istihbarat alanında onlarca yıldır faaliyet gösterilen bazı alanları da etkilemektedir. Bunlardan birisi istihbarat faaliyetlerinde veri paylaşımı sorunudur. İstihbarat gibi hem hassas hem kıskançlıkla yapılan ve paylaşılan mekanizmaların ne kadar güvenli olursa olsun olanak verilen alanı, eskisine göre çok daha verimli hale getirebilecek teknolojik dönüşüm fırsatı olabilir. Üstelik kurumlar arası istihbarat paylaşımına dışarıdan sızmayı neredeyse imkânsız hale getirebilecek Kuantum İletişim, rakip ve hasım ülke servislerine yönelik istihbarat avantajı sağlayabiliyorsa, bu yol için her türlü çabaya değer görülecektir. İşte söz konusu bu teknolojiler yıkıcı olduğu kadar, yenilikçi bu özellikleri sayesinde, istihbarat topluluklarının geleceğinde kritik önemde yer alabilir.

Yukarıda bahsedilen faaliyetlerden bir başkası

ise, istihbarat analizi için kullanılan uygulamalar veya karşı istihbarat faaliyetleri çerçevesinde değerlendirilmektedir. İstihbarat topluluğunda, yıkıcı teknolojiler sadece verinin işlenmesi, saklanması ve paylaşılması noktasında değil, belli başlı istihbarat uygulamalarına yönelik; örneğin askeri istihbarat ya da jeouzamsal istihbarat (GEOINT) için de dönüştürücü etkiye sahip olacağı düşünülmektedir [11]. "*Kuantum Teknolojisi ve Ulusal Güvenliğe dair realist kılavuz*" başlıklı rapor ise, henüz ortaya çıkmış olsa bile KUT'un ulusal güvenlik için önemli etkilerine vurgu yapmaktadır [12]. Karar vericiler, bugünden itibaren basit pragmatik adımlar atarak kurumları ve organizasyonları kuantum geleceğe hazırlayabilirler.

## 2. YIKICI İNOVASYON TEORİSİ PERSPEKTİFİNDEN KUANTUM TEKNOLOJİSİ

Bu kısımda, çalışmanın arka planını ihtiva eden yenilikçi teknolojileri ilgilendiren yıkıcı inovasyon teorisi, Kuantum Teknolojisi (KUT), Sinyal İstihbaratı (SIGINT) ve siber istihbaratın dayandığı teknoloji ve kriptoloji ilişkisi anlatılacaktır.

### 2.1. Yıkıcı İnovasyon Teorisi

Yıkıcı inovasyon, endüstrilerde ve organizasyonlarda önemli değişimlere yol açan yeniliklerdir [13]. Bu tür yenilikler, mevcut sistemleri veya alışkanlıkları kökten değiştirerek yeni bir yapı oluşturur. Örneğin, otomobil, elektrik ve televizyon gibi buluşlar, ortaya çıktıklarında yıkıcı teknolojiler olarak görülmüştür. Daha sonraları e-ticaret, çevrimiçi haber siteleri ve GPS sistemleri de benzer bir etki yaratmıştır. Yıkıcı teknoloji, bir pazarın, faaliyet sahasının veya sektörün normal işleyişini etkileyen teknolojidir. Köklü bir ürün veya teknolojinin yerini alarak yeni bir endüstri veya pazar yaratır [14].

Clayton Christensen, yıkıcı inovasyon teorisini geliştirerek bu kavramı literatüre kazandırmıştır. Ona göre, inovasyonlar iki türdedir: Sürdürücü ve yıkıcı. Sürdürücü inovasyonlar, mevcut ürün veya hizmetlerdeki gelişmeleri ifade ederken; yıkıcı inovasyonlar, tamamen yeni bir teknolojiyle ortaya çıkar ve eskiyi ortadan kaldırır. Örneğin, dijital fotoğrafçılık, Kodak'ın film işini yok ederken; kişisel bilgisayarlar, Smith-Corona daktilo şirketini devre dışı bırakmıştır [15].

Yeni bir teknoloji, başlangıçta sürdürücü veya yıkıcı olabilir. Yıkıcı teknolojiler, genellikle büyük şirketler tarafından görmezden gelinir veya küçük bir pazarla sınırlı kalır. Ancak, bu teknolojiler hızla gelişerek geleneksel şirketler için büyük tehditler oluşturabilir. Örneğin, dijital kameralar, analog fotoğrafçılığı hızla devre dışı bırakmıştır. Yıkıcı inovasyona hazırlıklı olmayan kurumlar, yeni teknolojilere adapte olan rakipleri karşısında dezavantajlı duruma düşebilir. Yıkıcı teknolojinin etkilerini hesaba katamayan kurumlar, yıkıcı inovasyonu başarıyla entegre eden rakiplerine karşı avantaj kaybedebilir [13]. Bu tür teknolojiler, finanstan tedarik zincirine, ulaşımdan haberleşmeye birçok sektörü etkilemektedir.

Teknoloji ve inovasyon, Dünya tarihinin dönüm noktalarında mevcut düzeni dönüştürmüştür. Örneğin, 19. yüzyılda büyük sıçrama gösteren "Analog teknoloji" mevcut klasik düzen üzerinde "Analog Yıkım" etkisine sahip olduğu söylenebilir. Benzer bir durum analog cihaz ve teknoloji üstünde kuvvetli bir yıkım etkisi gösteren "Dijital teknoloji" için de söylenebilir. Daha doğrusu analog düzeni yıkan ve değişime zorlayacak olan "Dijital Yıkım" şeklinde ifade edilebilir. Dijital yıkım ise yerleşik organizasyon ve işletmelerin gelişmekte olan teknolojileri kullanan yeni iş modellerine yenik düşmesi olgusudur [16]. Dijital yıkım, bilhassa dijitalleşme ve gelişen teknolojiler nedeniyle beklenmedik bir şekilde başarısız olan Kodak gibi başarısız şirketler olgusunu tanımlamak için 1980 başlarında ortaya koyulmuştur. Bu özel durumun ironisi, Kodak'ın ilk dijital kamerayı geliştirmiş olmasına rağmen sonunda işlerini tasfiye etmelerine yol açan bu teknolojiden yararlanamamış olmasıdır [17]. Mevcut kuruluşlar, mevcut teknoloji, yapıları ve mirası ile mevcut bir çözüm alanında faaliyet gösterdikleri için, yıkıcı yeniliklere mesafeli duracaklardır. Bu bağlamda KUT, yıkıcı inovasyon ve teknolojileri arasında ele alınmaktadır.

### 2.2. Kuantum Teknolojileri (KUT)

Kuantum teknolojileri (KUT), genellikle "kuantum bilgi işleme ve iletişim teknolojileri" ya da "kuantum bilgi teknolojileri" gibi terimlerle ifade edilir ve belirli sınırları tam olarak çizilmemiş bir alanı kapsar. Bu alan, fizik temelli olmasına rağmen, farklı disiplinlerin de katkıda bulundu-

ğu, geniş kapsamlı ve hızla gelişen bir araştırma konusuna evrilmiştir. Alanla ilgili terimler henüz net bir şekilde tanımlanmamış olup, sıklıkla birbirlerinin yerine kullanılmaktadır [18]. Bunun nedeni, ikinci kuantum devriminin kapsamı konusunda henüz tam bir fikir birliğine varılamamış olmasıdır.

Birinci kuantum devrimi, kuantum fiziği ilkelerine dayalı klasik teknolojilerde önemli gelişmeler sağlamıştı. 2003 yılında Dowling ve Milburn, "İkinci Kuantum Devrimi" terimini kullanarak, kuantum teknolojisinin potansiyelini ve gelecek vaat eden bir alan olduğunu vurgulamıştır [19]. Bu devrim, başlangıçta sadece teorik bir yenilik olarak görülüyordu ve somut faydalar sağlama potansiyeli konusunda şüpheler vardı. Ancak, günümüzde bu alan büyük yatırımlarla desteklenerek ülkeler arasında ciddi bir rekabet ortamı yaratmış durumdadır.

İlk zamanlarda, bu bir yenilik ve yıkıcı inovasyon olarak görülmesine rağmen riske değecek bir fırsat olarak da değerlendirilmiyordu. İkinci kuantum devrimi ileri sürüldüğü ilk yıllardan kısa bir süre sonra popülerliği ivmelenmiş ve son birkaç yılda ona olan eğilimin artmasıyla milyarlarca dolarlık yatırım fırsatı ortaya çıkarmıştır. Diğer taraftan bu devrim, kuantum teknolojisine yönelik artan yatırım ve rekabetten dolayı ülkelerin geri kalmamak adına kendi ulusal ve uluslararası ortaklık girişimlerini oluşturmaya çabaladığı bir çağın habercisiydi.

KUT, bilişim (bilgi işleme ve hesaplama), iletişim, simülasyon ve algılama gibi alanlarda doğanın temel yasalarını kullanarak daha önce mümkün olmayan yetenekler sunmaktadır [20]. Bu teknolojiler, artık sadece teorik bir spekülasyon değil; büyük kamu ve özel sektör yatırımlarıyla laboratuvarların dışına taşınmaktadır [21]. Önümüzdeki 20 yıl içinde, özellikle nanoteknoloji, biyoteknoloji, yapay zekâ ve robotik gibi diğer gelişmekte olan teknolojilerle birleştirildiğinde bu teknolojilerin hayatımızı önemli ölçüde değiştirmesi beklenmektedir.

### 2.2.1. Kuantum Mekaniğine Dayalı Teorik Arkaplan

Kuantum mekaniği, aynı zamanda parçacık fiziği olarak da bilinen bir fizik dalıdır ve günümüzdeki formuna özellikle İkinci Dünya Savaşı'ndan sonra yaşanan bilimsel ve teknolojik gelişmelerle ulaşmıştır. Klasik fizik, Newton'un çalışmalarına dayanan ve makroskopik dünyadaki olayları açıklamada başarılı olan bir sistemdir [22]. Ancak, atom altı dünyaya inildikçe klasik fizik yasaları, gözlemlenen fenomenleri açıklamakta yetersiz kalmıştır. Bu nedenle, atom altı parçacıkların davranışlarını anlamak ve daha iyi tanımlamak için kuantum mekaniği ya da fiziği adı verilen yeni bir teorik alan geliştirilmiştir [23].

Kuantum fiziğinin temel ilkeleri, klasik fiziğin belirgin ve determinist yaklaşımından farklıdır. Klasik fizikte gözlemler ve ölçümler kesin ve tahmin edilebilirdir; fakat kuantum fiziğinde belirsizlik ve öngörülemezlik önemli bir yer tutar. Klasik fiziğin açıklamakta zorlandığı olaylara çözüm getiren kuantum fiziği, doğanın mikro düzeydeki yapısını anlamak için gereklidir. Örneğin, ışığın doğası hem dalga hem de parçacık özellikleri gösterebilir. Bu ikilik, 20. yüzyılın başlarında yapılan deneylerle ortaya konmuş ve kuantum fiziğinin temel taşlarından biri haline gelmiştir [24].

1900'lerin başında Max Planck'ın, enerjinin belirli miktarlarda yayılması gerektiğini öne süren teorisiyle başlayan bu yeni fizik anlayışı, Isaac Newton'un klasik mekaniğinin mikro düzeyde geçerli olmadığını göstermiştir. Planck'ın bu bulgusu, 1905 yılında Albert Einstein tarafından "fotoelektrik etki" yasası ile desteklenmiştir. Einstein, ışığın sadece bir dalga değil, aynı zamanda foton adı verilen enerji parçacıklarından oluştuğunu göstermiştir. Bu keşif, ışığın doğasına dair o güne kadar bilinen teorileri derinden sarsmış ve kuantum fiziğinin önemini pekiştirmiştir [25]. Bu yüzden Einstein, 1921 yılında Nobel Fizik Ödülü'nü görelilik teorisiyle değil, fotoelektrik etki üzerine yaptığı bu çalışma ile kazanmıştır.

Kuantum fiziğinin bir diğer önemli katkısı, dalga-parçacık ikiliği kavramıdır. Bu kavram, ışığın bazen dalga gibi (örneğin, girişim ve kırınım olaylarında), bazen ise parçacık gibi (örneğin, fotoelektrik etkide) davrandığını açıklar. Bu durum, sadece ışık için değil, tüm maddesel parçacıklar için geçerlidir [26]. 1920'lerde Louis de Broglie, elektron gibi parçacıkların da dalga

özellikleri gösterebileceğini öne sürmüştür ve bu hipotez daha sonra yapılan deneylerle doğrulanmıştır [27].

Kuantum mekaniğinin gelişimi, bilimsel paradigmanın değişmesine ve fizik dünyasında deterministik yaklaşımdan olasılıksal bir bakış açısına geçişe neden olmuştur. Bu değişim, klasik fizik ile açıklanamayan olayların (örneğin, atomların enerji seviyelerinin kesikli yapısı veya çift yarık deneyi) kuantum fiziği ile başarılı bir şekilde açıklanmasını sağlamıştır. Çift yarık deneyinde, tek bir elektron bile gönderildiğinde, bir dalga gibi davranarak girişim desenleri oluşturur. Bu deney, parçacıkların klasik fizikteki öngörülerle açıklanamayan davranışlar sergilediğini gösterir [28].

Einstein, Boris Podolsky ve Nathan Rosen tarafından 1935 yılında ortaya atılan EPR (Einstein-Podolsky-Rosen) paradoksu ise kuantum mekaniğinin belirsizlik ve yerel olmayan etkiler içerdiğine dikkat çekmiş ve bu alanın felsefi ve bilimsel tartışmalarını derinleştirmiştir. EPR paradoksu, bir parçacığın ölçümünün başka bir uzak parçacığın durumunu anında etkileyebileceğini savunmuş ve bu durum "kuantum dolanıklık" olarak adlandırılmıştır [29]. Bu olgu, klasik fizik ve kuantum fizik arasındaki farkı ciddi bir şekilde ortaya koyar. Sonuç olarak, kuantum mekaniği, klasik fiziğin açıklamakta yetersiz kaldığı mikro düzeydeki fenomenleri açıklamaya ve doğanın temel yapı taşlarını anlamaya yardımcı olmaktadır.

### 2.2.2. KUT Temelleri ve Çalışma Prensipleri

KUT, kuantum sistemlerinin durumlarını mühendislik yoluyla kullanarak işlev gösteren bir teknolojidir [19]. Bu yönüyle KUT, 20. yüzyıl fenomenine dayanan diğer teknolojilerden ayrılır. Ancak, kuantum sistemlerinin bireysel durumları doğrudan çalıştırılıp ölçülmemektedir. Bu bağlamda, kuantum fiziğine dair temel kavramların hem teorik hem de pratik olarak anlaşılması gerekmektedir.

Bir kuantum sistemi, kuantum fiziğindeki sıra dışı fiziksel yasalara göre elektronlar, fotonlar ve çekirdekler gibi mikroskobik dünyadaki parçacıklardan oluşan bir sistemdir [30]. Bu sistemin ölçümleri, olasılıklarına bağlı olarak rastgele değerlere sahiptir. Ölçüm sonrasında, kuantum sistemi, ölçüm mekanizması ve sonucu ile uyumlu bir duruma geçer. Kuantum sistemi, belirli bir andaki durumunu, bir ölçüm mekanizmasıyla ilişkili durumların üst üste binmesiyle (süperpozisyon) tanımlar. Bazı durumlarda, kuantum sistemi iki veya daha fazla alt sistemin dolanıklığını gösterir, bu da alt sistemler arasındaki ölçüm sonuçlarının istatistiksel korelasyonlara yol açmasını sağlar. Kuantum sistemi ve çevresi arasındaki etkileşimler, sistemin durumunu rastgele hale getirebilir. Bu sürece "kuantum bileşenleri arasındaki uyumun kaybı", yani dekoherans (decoherence) denir. Bu, sistemin durumunun hassas biçimde tasarlanmasını sınırlayan bir aşamadır [31].

Kübit, kuantum teknolojisinin temel yapı taşıdır ve en basit kuantum sistemini temsil eder. Kübitler genellikle iki durumdan birini, yani |0> ve |1> durumlarını alabilirler [32]. Kübit, farklı kuantum teknolojilerinin işleyişini ve bu teknolojilerin karşılaştırılmasını anlamaya yardımcı olan soyut bir kavramdır. Gerçek hayatta, çeşitli parçacık sistemleri veya bu sistemlerin farklı değişkenleri kübit rolünü üstlenebilir.

KUT, klasik cihazlar aracılığıyla kübitlerin durumlarını başlatma (örneğin lazer darbeleriyle), manipüle etme (örneğin mikrodalga darbeleriyle) ve ölçme (örneğin yayılan fotonların tespiti) işlevlerini gerçekleştirir. Bu süreçte, klasik bir bilgisayar, cihazları programlamak, kontrol etmek ve ölçüm verilerini kaydetmek için kullanılır. KUT, bilinen klasik bilgisayarlarla entegre bir şekilde çalışır. Kübitlerin fiziksel davranışları, klasik teknolojilere göre avantaj sağlar ve bu, kuantum teknolojisinin temel farkını oluşturur [31].

Kuantum teknolojisine dayanan bir sistemde performans hem kübitlerin özelliklerine hem de klasik kontrol sistemlerine göre belirlenir. Performans, hassasiyet, doğruluk, hız ve dayanıklılık gibi ölçütlerle değerlendirilir. Kuantum teknolojilerinin farklı türleri için bu dört performans ölçütü bir araya getirilerek sistemin genel performansı değerlendirilir. Performans, yüksek kaliteli kübit sistemleri ve klasik kontrol yöntemleri kullanılarak geliştirilebilir. Yüksek kaliteli malzemeler, üretim teknikleri ve cihaz

mühendisliği, yüksek performanslı kuantum teknolojilerinin anahtarıdır [31].

Sonuç olarak, kuantum teknolojilerinin fiziksel temelleri "süperpozisyon" ve "dolanıklık" kavramları üzerine kuruludur. Kuantum nesneleri, birden fazla durumda süperpozisyon halinde olabilir. Örneğin, bir fotonun polarizasyon yönleri, yatay (H) ve dikey (V) olarak adlandırılır. H ve V süperpozisyonu, bir ölçüm sırasında doğanın bu iki durumdan yalnızca birini seçmesi ve bu seçimin rastgele gerçekleşmesi gibi özellikler gösterir. Bu durum, ölçüm öncesine kadar her iki durumun da aynı anda var olduğu anlamına gelir. Süperpozisyon kavramı, birden fazla parçacık için genişletildiğinde dolanıklık ortaya çıkar. Bu iki kavram genellikle aynı fenomeni ifade ettiği için karıştırılabilir.

### 2.2.3. KUT Sınıflandırması

Kuantum teknolojileri, AB Kuantum Amiral Gemisi girişimine göre dört ana kategoride incelenebilir [33]: Kuantum Bilişim, Kuantum İletişim, Kuantum Simülasyon ve Kuantum Algılama/Metroloji. Her bir kategori farklı özelliklere sahip olup, çeşitli uygulama alanları ve olgunluk seviyelerine göre değerlendirilmektedir.

**a. Kuantum Bilişim (Kuantum Bilgisayar Bilgisayım, Bilgi İşlem/Hesaplama)**: Kuantum bilgisayarlar, karmaşık problemleri çözmek amacıyla kuantum bitleri kullanarak süperpozisyon ve dolanıklık gibi kuantum fenomenlerinden yararlanır. Bu sayede, özellikle optimizasyon, sinyal işleme ve yapay zekâ gibi alanlarda klasik bilgisayarlardan çok daha hızlı çözümler sunar [34].

**b. Kuantum İletişim**: Kuantum iletişim sistemleri, veri güvenliği ve hassas ölçüm senkronizasyonu sağlar. Süperpozisyon ve dolanık kübitlerin kullanılması sayesinde, kuantum iletişimi kesintiye uğramadan güvenli bir şekilde veri aktarımı sağlar. Örneğin, tek fotonlar kullanılarak gerçekleştirilen iletişim kesilmesi imkânsız güvenlik sunar ve uçtan uca güvenli ağ oluşturur [35].

**c. Kuantum Simülasyon**: Kuantum sistemlerin simülasyonu, yeni malzeme, ilaç ve kimyasal tasarımları gibi birçok alanda devrim niteliğinde gelişmeler sağlayabilir. Kuantum simülatörleri, belirli problemler için özel tasarlanmış kuantum bilgisayarlar olabilir ya da aerodinamik modellemeye benzer şekilde, daha karmaşık sistemleri anlamak için basit kuantum sistemlerini kullanabilir [33].

**d. Kuantum Algılama ve Metroloji:** Kuantum sensörleri, olağanüstü hassasiyetle fiziksel büyüklükleri ölçebilir. Tıbbi teşhis, navigasyon ve IoT (Internet of Things) gibi pek çok farklı alanda yüksek doğrulukla veriler sağlayabilir. Kuantum metroloji, zaman, kuvvet ve elektromanyetik alan gibi değerlerin çok hassas ölçümüne olanak tanır [36].

Bu teknolojiler hem temel bilimlere dayanarak gelişmekte hem de mühendislik, yazılım, teori ve eğitim alanlarıyla desteklenmektedir. Böylece, kuantum teknolojilerinin tüm bileşenleri birbiriyle etkileşim halinde olup, gelişen teknoloji ekosistemine katkıda bulunmaktadır.

### 2.2.4. Kuantumda Güvenlik ve Şifreleme

**a. Kuantum Güvenli Sistemler**: Kuantum güvenli sistemler, kuantum teknolojilerini kullanarak geleneksel bilgi güvenliğini yeniden tanımlamayı amaçlar. Kuantum bilgisayarların sahip olduğu süperpozisyon ve dolanıklık özellikleri, veri güvenliği ve gizliliğini artıran yeni yaklaşımlar sunar. Bu sistemler, özellikle KAD (Kuantum Anahtar Dağıtımı) gibi protokollerle, iki taraf arasında iletilen verilerin üçüncü şahıslar tarafından kesintiye uğratılamayacağı güvenli bir iletişim sağlar [37].

**b. Kuantum Kriptografi**: Kuantum kriptografi, kuantum fiziği yasalarını kullanarak veri güvenliğini sağlamaya yönelik bir yaklaşımdır. Geleneksel kriptografik sistemler, genellikle matematiksel zorluklara dayalı algoritmalar kullanarak güvenlik sağlar; ancak bu algoritmalar kuantum bilgisayarlar tarafından hızlıca kırılabilir. Kuantum kriptografi ise, verilerin kübitler üzerinden iletilmesiyle güvenlik sağlar ve bilgiyi kopyalama veya değiştirme girişimlerini fiziksel olarak tespit etme imkânı sunar. Özellikle Kuantum Anahtar Dağıtımı (KAD), iki taraf arasında güvenli bir anahtar paylaşımını mümkün kılar ve herhangi bir dinleme girişimi anında fark edilebilir hale gelir [38].

**c. Post-Kuantum Kriptografi**: Kuantum Sonrası Kriptografi (KSK) olarak da ifade edilen, kuantum bilgisayarların klasik kriptografik sistemleri kırma yeteneğine karşı geliştirilmiş şifreleme tekniklerini ifade eder. Kuantum kriptografi ile farkı, kuantum bilgisayarların henüz yaygınlaşmadığı bir dünyada, klasik bilgisayarların işleyebileceği şekilde tasarlanmış olmasıdır. Bu yeni nesil kriptografik algoritmalar, kuantum bilgisayarların gelecekteki tehditlerine karşı hazırlıklı olmayı amaçlar. Özellikle RSA ve ECC gibi günümüzün yaygın şifreleme yöntemlerinin kuantum bilgisayarlar tarafından etkisiz hale getirilme riski göz önünde bulundurulduğunda, Post-Kuantum Kriptografi (KSK), daha güvenli ve kuantuma dayanıklı bir çözüm olarak önem kazanmaktadır.

### 2.3. Sinyal İstihbaratı Mücadelesinden Siber İstihbarat Çağı'na Kriptografi ve Kriptanaliz

Kriptografi (şifre yapma) ve kriptanaliz (şifre kırma), savaş ve kriz dönemlerinde istihbarat üzerinde önemli bir etkiye sahiptir. Örneğin, Zimmermann Telgrafı, ABD'yi I. Dünya Savaşı'na çekerken, II. Dünya Savaşı'nda Midway Muharebeleri ve Atlantik Savaşı'nda (Normandiya Çıkarması ve Overlord Harekâtı) da savaşın dönüm noktalarında önemli rol oynamıştır. SIGINT, zayıf operasyon güvenliğine sahip hedeflere karşı kritik avantajlar sağlamış ve Soğuk Savaş boyunca Batı'nın Sovyetlere karşı üstünlüğünü korumasına yardımcı olmuştur. Ancak diğer yandan, Pearl Harbor'dan önce Japon kodlarının kırılmasına rağmen istihbarat-politika işlevsizlikleri nedeniyle aynı SIGINT ve kriptanaliz başarısı stratejik bir avantaja dönüşmemiştir. General MacArthur gibi askeri karar vericilerin belirli stratejik önyargıları ve SIGINT çıktılarına olan ilgisi veya ilgisizliği, istihbarat üzerinde etkinliğini sınırlayan faktörlerdir. Bu yüzden kriptolojinin savaş üzerindeki etkisi her zaman açık ve net olmayabilir, hatta diplomasi alanında daha da belirsiz kalabilir [39].

Tarihsel süreç, kriptoloji uygulamalarındaki değişikliklere rağmen istihbarat dinamiklerinin statik kalabildiğini gözler önüne sermektedir. Bir SIGINT unsuru, değerli ve dikkatlice analiz edilmiş istihbarat üretip bunu doğru, ilgili ve gerekli müşterilere iletmek zorundadır. Zamanla sınırlı istihbarat söz konusu olduğunda, müşterilerin, bilgiyi olaylar yaşanmadan önce elde edip anlamlandırması gerekir. Ancak daha önce toplanmış veriler, hedefin davranışını değiştirmediği sürece yine de kullanılabilir nitelikte kalabilir. İstihbarat tarihçisi Michael Warner'a göre, KGB belgeleri, Venona projesi ile Batı karşı istihbaratı için onlarca yıl boyunca önemli bir rehber niteliği taşımıştır [39]. Benzer şekilde, günümüzde RSA gibi zayıf güvenlik önlemleriyle korunan veriler, hedeflerin kuantum anahtar dağıtımı (KAD) ya da post-kuantum kriptografi (KSK) sistemlerine geçişinden önce toplanırsa, büyük ölçekli bir kuantum bilgisayar geliştirildiğinde deşifre edilebilir hale gelebilecektir. Verilerin değerinin zamanla azaldığını göz önünde bulundurursak, istihbarat avantajının bağlamsal olduğunu ve birçok faktöre bağlı olarak değiştiğini söylemek mümkündür [40].

Dijital Bilgi Çağı'nda kriptografi ve kriptanaliz, siber güvenliğin ve istihbarat faaliyetlerinin merkezinde yer almaktadır. Modern siber tehdit ortamında hem devletler hem de özel sektör, kritik altyapılarını korumak ve hassas bilgilerini güvende tutmak için gelişmiş kriptografik protokollere başvurmaktadır. Özellikle siber casusluk, fidye yazılımları ve uluslararası organize siber saldırılar gibi tehditler, kriptografinin önemini daha da artırmaktadır. Öte yandan, kriptanaliz alanında, siber güvenlik uzmanları ve saldırganlar şifreleme sistemlerinin zayıf noktalarını bulmak ve bu sistemleri kırmak için sürekli çalışmaktadırlar. Siber istihbarat ya da güvenlik ekipleri, saldırganların iletişimlerini çözmek ve stratejik avantaj sağlamak için kriptanaliz tekniklerine başvurmaktadır. Ancak kuantum bilgisayarların ortaya çıkışı, mevcut kriptografi sistemlerinin güvenliğini tehdit etmektedir. Bu nedenle, post-kuantum kriptografi gibi yeni nesil şifreleme teknikleri, gelecekte siber güvenlik stratejilerinin önemli bir parçası olacaktır. Dijital Çağ'da kriptografi ve kriptanaliz arasındaki bu dinamik ilişki, siber uzay üzerindeki hakimiyeti şekillendirmeye devam edeceği varsayılmaktadır [41].

## 3. İSTİHBARAT VE TEKNOLOJİ İLİŞKİSİ BAĞLAMINDA KUANTUM TEKNOLOJİSİ

Bu bölümde ilk bölümdeki arka plan temel alınarak literatür ve güncel gelişmelere dayanan istihbarat ve yıkıcı inovasyon ilişkisi bağlamında kuantum teknolojisi ele alınmaktadır.

### 3.1. Modern Bilgi ve İletişim Döneminde İnovasyon Odaklı İstihbarat Rekabeti

Sanayii devrimi sonrası, bilimsel ve teknolojik ilerlemeler modern istihbarat organizasyonlarının şekillenmesinde önemli rol oynamıştır. Telgraf, telefon ve radyo gibi iletişim araçları, istihbarat toplama süreçlerini dönüştürerek önemli fırsatlar sunmuş, bu süreç I. Dünya Savaşı'ndaki Zimmerman Telegrafı olayıyla belirginleşmiştir. II. Dünya Savaşı'nda ise Enigma makinesi ve kriptografi çalışmaları, istihbarat ve teknoloji mücadelesinin temelinde dönüm noktası olmuştur. Bletchley Park'ta Alan Turing'in liderliğindeki ekip, bu şifreleme sistemini çözerek savaşın seyrini değiştirmiştir. Savaş, yalnızca silahlarla değil, aynı zamanda matematik, şifreleme ve bilgi harbi ile de kazanılmıştır [39].

Soğuk Savaş döneminde, Batı'nın SIGINT servisleri (NSA-GCHQ) sinyal istihbaratına, Sovyetler ise casuslara ağırlık vermiştir. Anglo-Amerikan iş birliği, özellikle Mart 1946'daki UKUSA anlaşması ile sinyal istihbaratı paylaşımını pekiştirmiştir. Bu dönemde, ABD U-2 uçakları ve uzaydan yapılan gözlemler Sovyet stratejik güçleri hakkında değerli bilgiler sağlamış, Moskova'nın blöflerini açığa çıkarmıştır. Uydu teknolojisi ile elde edilen büyük veri, ABD'nin istihbarat kapasitesini artırsa da veri işleme ve analiz konularında zorluklar yaşanmıştır. NSA, bu süreçte bilgisayar teknolojisine öncülük ederek, büyük veriyi analiz etmekte önemli aşamalar kaydetmiştir [39].

Bu dönemde, Anglo-Amerikan ittifakı üstünlüğünü korumuş, ancak Sovyetler de başarılı sinyal istihbarat sistemleri geliştirmiştir. KGB, Batı istihbarat ağlarına sızarak önemli bilgiler elde etmiş, casusların yardımıyla Batı'daki gelişmeleri yakından takip etmiştir. Soğuk Savaş boyunca her iki taraf da teknik istihbarat araçlarını kullanarak stratejik dengeyi korumaya çalışmıştır. İstihbarat rekabeti diğer taraftan da uzay aracılığıyla devam etmekteydi. Uzaydan toplama, stratejik keşif için uzun vadeli bir çözüm sağlamıştır. Uyduların askeri kullanımları 1940'lardan beri tartışılıyordu, ancak Moskova'nın yörüngedeki ilk insan yapımı nesne olan Sputnik uydusunu fırlatması ABD'yi uydu geliştirme çılgınlığına yönlendirmiştir [39].

İstihbaratın, kriptoloji ve inovasyonla olan bağlantısı oldukça belirgindir [41]. 1970'lerden sonra 80'lerde bilgisayarların dijitalleşmesi ve internetin ticari kullanımına geçişi, bilgi ve iletişim teknolojilerinde büyük bir dönüşüm başlattı. 1989 yılı hem Berlin Duvarı'nın yıkılması hem de web teknolojisinin doğuşuyla bu sürecin dönüm noktasıdır. Milenyum, dijital gözetimin arttığı ve sosyal medya ile mobil cihazların tüm dünyaya yayıldığı bir dönem oldu. "Dijital Devrim" veya (Dijital Çağ), aynı zamanda "Bilgi ve İletişim Devrimi" (Bilgi Çağı) olarak da kullanılması normal hale gelmiştir [42]. Ancak kimilerine göre dijital çağın da sonu yaklaşmaktadır. Bilgi ve iletişim teknolojisinde yer alan gelişmeler hibrit hale geldikçe bu durum daha girift hale gelmektedir. Mevcut durumda, teknoloji, inovasyon, bilişim ve bilgi perspektifinde değerlendirme yapan uzmanlar "dijital bir yıkım" olmasını yakın bir gelecekte muhtemel görmektedir. Yıkıcı inovasyon teorisi bağlamında duruma baktığımızda, alternatif olarak sunulan "Kuantum Devrimi" olgusunu da dikkate alarak bunu ihtimal dışı görmek büyük bir ihmal sayılacaktır [42].

Bilgi ve iletişim teknolojilerinin tarihine baktığımızda, bunların istihbaratla yakından ilişkili olduğunu görüyoruz. Modern istihbaratın başlangıcını Fransız İhtilali veya Sanayi Devrimi'ne dayandırabiliriz. Matbaanın bilginin yayılmasını hızlandırması, modern istihbaratın ilk adımlarını atmasına yardımcı oldu. Telgraf ve telefon gibi analog teknolojiler Sanayi Devrimi'yle ortaya çıkmış ve dünya savaşları boyunca kullanılmıştır. Ancak dijital devrim, özellikle 1989'dan sonra hız kazanmıştır. Şimdi ise bilim insanları, "Kuantum Bilgi Devrimi" ile yeni bir dönemin kapıda olduğunu düşünmektedir [41]. Bu noktada bilgi ve iletişim dönemlerinin modern istihbarat tarihiyle paralel tasnifi aşağıdaki gibi ele alınabilir.

**Çizelge 1.** Bilgi ve İletişim Dönemlerinin Tasnifi [42]:

| | |
|---|---|
| Klasik Bilgi Dönemi (1660-1910) | Analog Bilgi ve İletişim Devri (1860-2001) |
| Dijital Bilgi ve İletişim Çağı (1989-2049) → | Kuantum Bilgi Devrimi (2030-?) |

### 3.2. KUT ve İstihbarat Perspektifi

Önceki bölümündeki kronolojik tasnif çalıması modern istihbarat dönemlerine göre bilgi ve iletişimin temel formu olan veri ve sinyalin baz alınmasıdır. Bilgi teknolojilerinin tarihsel klasik dönemini, yazılı basımın mekanik haline getirildiği matbaanın yaygınlaşması ile başlatıp işin içerisine radyo, telsiz, telefon, telgraf gibi analog teknolojinin dahil olduğu yirminci yüzyıl başında bitirilebilir. Lakin yine de bilginin şifrelenmesi için gereken teknikleri ihtiva eden kriptografi uygulamaları da klasik, analog veya dijital dönemlerinin hepsi bir bütün olarak klasik dönem başlığı altında toplanabilir. Zira kuantum sayesinde bilgi ve bilginin korunmasına yönelik olan kriptografi teknikleri de çok farklı bir boyuta geçmektedir. Bilgi güvenliği ve kriptoloji uygulamaları bağlamında, klasik bilgi ve kuantum bilgi güvenliği arasında henüz net bir sınır çizilmese bile aşağıdaki tablo ile izahı belli bir seviyede ele alınabilir.

20. yüzyıl başlarında "Birinci Kuantum Devrimi" süreci, ışık ve diğer elektromanyetik ışınımların doğasıyla ilgili temel sorunu istatiksel teknikleri kullanarak çözmesi yoluyla başlamıştır. İkinci Kuantum devrimi sayesinde ise, tamamen işlevsel kuantum bilgisayar, dijitale dayalı bilişim ve iletişim altyapısında siber güvenliği sağlayan kriptografik protokolleri kırabilir ve nihayetinde ulusal güvenlik, küresel ticaret ve kişisel veri mahremiyeti açısından yıkıcı sonuçlar doğurabilir. Son günlerde açık kaynaklarda sıklıkla iddia edilen diğer bir husus ise, kuantum bilgisayarların daha iyi performans gösterdiğine dair dönüm noktası olan "kübit sayısı" ile orantılı "kuantum üstünlüğü" gelişmeleridir [44]. Akademik bağlantılı laboratuvarlar ile Google, IBM, Intel ve Microsoft gibi küresel firmalar pratik uygulamalar ve prototipler üzerinde deneysel çalışmalarını hızla sürdürmektedirler. Literatürde son yıllarda kayda değer akademik çalışmalar bu çalışma kapsamında aşağıda incelenmektedir.

"Kuantum Tehdidinin Gizemini Açmak: Altyapı, Kurumlar ve İstihbarat Avantajı" başlıklı çalışmasıyla Lindsay, kuantum teknolojisindeki bilimsel yenilik ve kuantum bilişimdeki zorlu mühendislik zorluklarının üstesinden gelebileceğine dair iddiasını çalışmasına yansıtmaktadır [40]. Sonrasında savını devam ettirmektedir: "*Sinyal istihbaratı (SIGINT) toplayıcılarının yine de çok sayıda şifre çözmeyi analiz etmesi ve ilgili karar vericilere zamanında ve ilgili kararları vermesi gere-*

**Çizelge 2.** Klasik ve Kuantum Bilgi Güvenliğinin Karşılaştırılması [43]:

| Bilgi Güvenliği Uygulamaları | Klasik Bilgi Güvenliği | Kuantum Bilgi Güvenliği |
|---|---|---|
| Kriptografi | Özel sektör Akademi<br>Kamu<br>Askeri/Ordu<br>Diplomasi ve İstihbarat Toplulukları | Yeni hibrit disiplinler<br>Yıkıcı teknolojiler<br>Özelleştirilmiş OSINT Grupları<br>Özelleştirilmiş Analiz Firmaları |
| Kriptanaliz | Simetrik Şifreleme<br>Asimetrik Şifreleme veya<br>Açık Anahtar Kriptografisi | Shor ve Grover algoritmaları |
| Kuantum-Güvenli Kriptografi | Kuantum Sonrası Şifreleme (PQC: KSK) | Kuantum Anahtar Dağıtımı (QKD: KAD) |

*kir*." Ancak yarının kuantum ağları, zayıf operasyon güvenliği (OPSEC) uygulamalarına sahip karmaşık kuruluşlar için çok az koruma sağlayacaktır. Yazar, istihbarat pratiği için kuantum bilişimde klasik siyasetin hâkim olmasını beklemek gerektiğini ifade etmiştir [40].

"Kuantum Bilişim'in Ulusal Güvenliğe Karşı Siber Tehdidi" isimli diğer bir çalışmada, Amerika Birleşik Devletleri ve müttefiklerinin, Çin ve diğer jeopolitik rakipleriyle olan teknoloji yarışında, kuantum bilişimin bu rekabetin önemli bir cephesi haline geleceğini, hatta kaybetmeyi göze alınmaması gerekli bir mücadele olduğu üzerine durulmuştur [45]. Kuantum bilişimin güncel uygulanabilirliği üzerinde hâlâ birçok zorluk olmasına rağmen, bugün atılan adımların, gelecekte bir gün geldiğinde gerçek savunma üzerinde derin bir etkisi olacaktır. Ayrıca bu konuya yatırım yapan tüm aktörlerin, ABD teknolojisinin ve stratejik liderliğinin yerini almaya kararlı olduğunu anlamak gerektiğinden bahsedilmiştir. Grobman, kuantumun hem ulusal bir güvenlik tehdidi hem de potansiyel bir stratejik avantaj olduğunu vurgulayarak ABD'nin gelecekteki yerini garantilemek için bugün her iki unsura da odaklanmasını şiddetle önermiştir [45].

"Kuantum Teknolojileri, ABD-Çin Stratejik Rekabeti ve Siber İstikrarın Gelecekteki Dinamikleri" çalışmasında Kania ve Costello, siber alanda statükonun, kuantum iletişiminin ve kuantum bilişimin ortaya çıkmasıyla kökten bozulabileceğini, üstelik gelecekte siber güvenlik için oluşan zorlukların bu teknolojilerin derin bir analizini ve büyük güçlerin bu yönde eğilmesi gerektiğini vurgulamışlardır [46]. Kuantum Kriptografinin kullanımı, teorik olarak kırılamayan kuantum iletişim sistemleri yaratabileceği iddia edilse de daha uzak bir gelecekte, kuantum bilişimin gelişimi, mevcut siber yeteneklerin ötesine geçerek benzersiz saldırı gücünü mümkün kılacaktır. Bu yıkıcı teknolojilerin stratejik etkisi, ilgili teknolojik alanda lider hale gelen ABD ve Çin başta olmak üzere büyük güçlerin yaklaşımlarına bağlı olacağı belirtilmiştir [46].

"Kuantum Kripto Kıyamet'ten (Kriptokalips) Kurtulmak" makalesinde Lindsay, siber güvenliğe yönelik kuantum tehdidi meselesinde, deneysel makinelerin henüz açık şifrelemeyi ortadan kaldıracak kadar güçlü olmasa da kuantum bilgisayarların, gitgide en hızlı klasik süper bilgisayarlardan daha iyi performans gösterebileceğini vurgulamaktadır [43]. Lindsay, kuantum tehdidinin o denli inandırıcı hale geldiğini, böylece bilim topluluğunun yakında açık kullanımı için sertifikalandırılacak olan kriptografik karşı önlemler üzerinde çalıştığını ifade etmiştir. Dahası, kriptografik güvenliği artırabilecek yeni kuantum ağları üzerinde de araştırmaların devam ettiğini tekrarlamaktadır. Bunun yanında kuantum güvenlik açığı boyutunun, kuantum bilişim ve kuantuma dirençli alternatiflerdeki nispeten mühendislik başarısı yanında, sırların ne kadar süreyle korunması gerektiğine ilişkin politik düşüncelere bağlı olduğunu yazar öne sürmektedir. Ancak karşı önlemlerin tehditten daha hızlı olgunlaştığı hususunda ihtiyatlı bir iyimserlik olmasına rağmen kuantum tehdidi ciddiye alınmalıdır, ancak bu sayede bu tarz tehditler, yazara göre bir şekilde önlenecektir [43].

"Kuantum Bilişim Neden Uluslararası Güvenliği İstikrarsızlaştırmayacak: Kriptolojinin Politik Mantığı" makalesine göre, kuantum bilgi teknolojisinin siber güvenlik ve stratejik istikrar üzerindeki etkileri endişe verici göründüğü belirtilmiştir [47]. Teoride, kuantum bilgisayarı olan bir hasım, internet güvenliğini garanti altına alan asimetrik şifreleme protokollerini yenebilirken, fizik yasaları tarafından güvenliği garanti edilen kuantum iletişimlerini kullanan bir rakip, istihbaratın sürpriz saldırılarını önleyebildiği değerlendirilmiştir. Bu iddiaları değerlendiren makale, belirsizliği savaşın önemli bir nedeni olan kurumları önemli bir bilgi kaynağı şeklinde anlayan savaşın pazarlık modeline dayanan genel bir kriptoloji mantığı geliştirmektedir. Herhangi bir teknolojik dönemin kriptolojisi, stratejik istikrar için belirsiz çıkarımlarla birlikte bu mantığın her iki yönü tarafından şekillendirilir. Pratikte, hatalı insan organizasyonlarında uygulanan gerçek kuantum sistemlerini kullanan istihbarat rakipleri arasındaki stratejik etkileşim, kuantum bilişimin etkisini azaltacaktır. Sonuç olarak, kuantum bilişimin devrim niteliğindeki bilimsel yeniliği, kısmen kriptoloji ve bilişim alanlarının son yıllarda zaten önemli dönüşümlerden geçmesi nedeniyle muhtemelen yalnızca marjinal siyasi etkiye sahip olacaktır [47].

"Kuantum Bilgisayarların Toplum Üzerindeki Potansiyel Etkisi" adlı makale, kuantum bilişimin yeni gelişen teknolojisinin toplum üzerinde sahip olabileceği potansiyel etkiyi ele almaktadır [48]. Kriptografi, optimizasyon ve kuantum sistemlerinin simülasyonu olmak üzere üç alana odaklanan çalışma, ayrıca bu gelişmelerin bazı etik yönlerini ve riskleri azaltmanın yollarını tartışmaktadır. Başka bir çalışma olan "Kuantum Teknoloji Coşkusu ve Ulusal Güvenlik" ise, bir tür abartı veya beklenti söylemi olarak teknoloji coşkusu üzerine rasyonel ve eylemsel perspektifleri incelemektedir [49]. Buradan yola çıkan çalışma, coşku döngüleri, tehdit enflasyonu ve güvenlikleştirme teorisiyle kıyaslamaktadır.

### 3.2.1. Yaklaşan Kuantum Kripto Kıyamet Beklentisi

Siber uzayda dijital bilgi ve iletişim güvenliğine yönelik kuantum tehdidi, muhtemel sonu belli bir kehanetin anlatımı gibi görülmektedir [43]. Tehdit anlatımı abartıldıkça, çareleri arayıp bulmak da o denli kıymetli hale gelmektedir. Deneysel kuantum makineler henüz yaygın şifrelemeyi ortadan kaldıracak kadar güçlü olmasa da kuantum bilgisayarların bazı koşullar altında en hızlı klasik süper bilgisayarlardan daha iyi performans gösterebildiği gözlenmektedir. Gerçekten de kuantum tehdidi o derece yaklaştı ki; bilim topluluğu son yıllarda kriptografik karşı önlemler üzerinde yoğun bir mesai göstermektedir. Kriptografik güvenliği artırabilecek yeni kuantum ağları üzerinde araştırmalar da aynı süreçte devam etmektedir.

Kuantum bilişimin olgunlaşması, tüm siber alanın gizliliği, bütünlüğü ve erişebilirliği için kategorik bir tehdit oluşturma potansiyeline sahiptir. Üstelik uygun türde makineye sahip bir istihbarat rakibi, potansiyel olarak RSA algoritmasını bozabilir, sınıflandırılmış verilerin şifresini çözebilir ve dijital imzalar oluşturabilir. Doğal olarak, bu ağlardaki açık ve özel, savunmasız kriptografi kullanan tüm ağlar ve uygulamalar riske atılacaktır. Tüm fiziksel ortamlardaki (kara, deniz, hava, uzay) askeri operasyonlar, küresel ekonomiye güç veren aynı bilgi teknolojilerinin ve ağların çoğuna dayandığından, siber alandaki sistematik bir güvenlik açığı, tüm alanlarda sistematik bir güvenlik açığı haline gelecektir. Böylece gizli bilgiler toplanabilir, değiştirilebilir veya silinebilir. Finansal, lojistik ve operasyonel veriler, taktik ve stratejik operasyonları etkilemek için manipüle edilebilir. Casusluğu etkinleştirmek veya kritik altyapıyı bozmak için istendiğinde kötü amaçlı yazılım yüklenebilir. Hassas teçhizatı ve silah stoklarını koruyan kimlik doğrulama kodları, silah kaçakçılığına yol açacak şekilde tahrif edilebilir. Siber uzayın her yerde bulunan önemi göz önüne alındığında, siber güvenlikten sistematik bir şekilde ödün verilmesi, birinci dereceden stratejik bir sorun olacaktır [43].

Kuantum bilişimdeki ilerlemeler, mevcut şifreleme sistemlerinin kırılmasına yönelik ciddi bir tehdit oluşturuyor; bu durum "Kriptokalips" anı olarak tanımlanmaktadır [43]. Bilim insanları ve karar vericilerin bu tehdidi engellemek için adımlar atmaları oldukça kritik görünmektedir. RSA gibi klasik şifreleme sistemlerine alternatif olarak, kuantum bilgisayarlar karşısında da güvenli olduğu düşünülen matematiksel problemlere dayanan kriptografik çözümler geliştirilmektedir. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bu çözümler üzerinde çalışmalarını sürdürüyor [50]. Ayrıca, kuantum mekaniğine dayalı yeni güvenli ağların geliştirilmesi de bu sürecin bir parçası olduğu bilinmektedir. Kuantum teknolojilerinde Çin'in ilerlemeleri, bu alandaki küresel rekabeti artırmakta ve yatırımları hızlandırmaktadır.

Kuantum tehdidi, siber güvenliğin geleceği açısından önemli risk ve fırsatları barındırmaktadır. Kuantum tehdidine rağmen, RSA, ECC ve benzeri şifreleme algoritmalar güvenli çalışır, çünkü açık anahtar çok büyük bir sayıya dayanır (yani, ), özel anahtar ise asal sayı çarpanlarına dayanır. Sıradan klasik bilgisayarlarda iki büyük asal sayıyı birbiriyle çarpmak kolaydır, ancak sonucu çarpanlara ayırmak katlanarak daha zordur. Tipik bir masaüstü bilgisayarın 2048-bit RSA'yı kırmak için altı katrilyon yıldan fazla zamana ihtiyacı olacaktır [43].

Kuantum sonrası kriptografi (KSK) ve kuantum anahtar dağıtımı (KAD) gibi çözümler, bu tehditlere karşı bir savunma geliştirme çabalarını yansıtmaktadır. Shor'un algoritması gibi kuantum algoritmaları, asimetrik şifreleme sistemle-

rini kolayca kırabilecek kapasiteye sahiptir. Bu algoritmanın, teorik olarak RSA ve benzeri şifreleme sistemlerini saniyeler içinde çözebileceği varsayılıyor. Ancak, bu senaryonun gerçekleşmesi için hâlâ kuantum bilgisayarların büyük bir mühendislik aşamasını geçmesi gerekiyor. Kuantum bilişimdeki mühendislik zorlukları ve belirsizlikler, büyük ölçekli kuantum bilgisayarların ne zaman ortaya çıkacağına dair tahminleri çeşitlendiriyor. Yine de bu süreçte kuantum bilgisayarların sunduğu muhtemel zorluklara karşı geliştirilen çözümler, siber güvenliğin geleceği için kritik öneme sahip olacaktır [40].

Kuantum bilişim açısından diğer bir kilometre taşı olan Grover algoritması, simetrik şifreleme algoritmaları olan Gelişmiş Şifreleme Standardı (AES) ve Güvenli Özet Algoritmaları (SHA) gibi sistemlere karşı polinom hızlanma sağlamaktadır. Shor'un algoritması, RSA, Diffie-Hellman (DH) ve Eliptik Eğri Kriptografisi (ECC) gibi asimetrik şifreleme sistemlerini üstel bir hızlanma ile çözebiliyor. Peter Shor, 1994 yılında, asal sayıların çarpanlarına ayrılmasını ve ayrık logaritmaların hesaplanmasını, bilinen klasik yöntemlerden çok daha hızlı bir şekilde yapabilen bir kuantum algoritması geliştirdi. Shor'un algoritması, yeterince güçlü bir kuantum bilgisayar varlığı durumunda, söz konusu asimetrik şifreleme algoritmalarını birkaç saat içinde kırma potansiyeline sahiptir. Oysa klasik süper bilgisayarlar, aynı işlemi gerçekleştirmek için neredeyse imkânsız denilebilecek bir süre, yani yaşam boyu çalışmak zorundadır. Bu da kuantum bilişimin kriptanaliz gücünün ne denli önemli olduğunu göstemektedir [41].

### 3.2.2. SIGINT ve Kripto Operasyonlarında Kuantum Bilişim ve İletişim Bağıntısı

Kuantum teknolojisindeki bilimsel yenilikler, istihbarat organizasyonları ve faaliyetleri üzerinde büyük bir etki yaratma potansiyeline sahiptir. Bu yenilikler, sinyal istihbaratı (SIGINT) toplama ve şifre çözme süreçlerinde devrim yaratabilir. Kuantum bilişim, özellikle zorlu mühendislik engelleri aşıldığında, kriptanaliz (şifre kırma) süreçlerini büyük ölçüde hızlandırabilir ve istihbarat toplayıcılarına avantaj sağlayabilir. Ancak, bu durum beraberinde yeni zorluklar da getirecektir. Örneğin, sinyal istihbaratı toplayıcıları kuantum teknolojisinin getirdiği yüksek şifre kırma kapasitesinde bile, çözülen şifreleri zamanında analiz ederek karar vericilere rapor yayacak kabiliyetten yoksun kalabilir [47].

Kuantum bilişim ve kuantum iletişim teknolojileri farklı olduğu kadar, aynı zamanda her ikisi de istihbarat toplama ve koruma süreçlerinde karşıt roller oynar. Kuantum bilişim, kriptanaliz yoluyla mevcut güvenlik protokollerini kırarak istihbarat toplama faaliyetlerini ileri taşıyabilirken, kuantum iletişim daha güvenli veri aktarımı sağlamak için kullanılabilir. Kuantum bilişim, şifreleme protokollerini kırarak büyük miktarda veri açığa çıkarma potansiyeline sahipken, kuantum iletişim, güvenli iletişim yolları oluşturarak karşı istihbarat veya istihbarata karşı koyma (İKK) faaliyetlerini güçlendirebilir [40]. Bu noktada karşı istihbarat faaliyetleri kuantum kriptografiyle birlikte ele alınabilir.

Bu çekişmede, kriptanaliz (şifre kırıcılar) ile kriptografi (şifre yapıcılar) arasında sürekli bir yarış vardır [48]. Kuantum bilişim sayesinde SIGINT, büyük miktarda veri şifre çözme ve analizini optimize edebilir, bu da istihbarat operasyonlarına stratejik bir avantaj sağlayabilir. Ancak, kuantum iletişim ve kuantum dirençli şifreleme yöntemleri (kuantum güvenli) operasyonel güvenliği (OPSEC) artırabilir, zayıf güvenlik uygulamaları olan kuruluşlar için koruma sağlayabilir. Özellikle kuantum bilişim donanımına ihtiyaç duymayan, matematiksel olarak geliştirilmiş kuantum dirençli şifreleme protokolleri, gelecekte hem klasik hem de kuantum tehditlerine karşı dayanıklı bir güvenlik katmanı oluşturabilir [47].

Kuantum bilişimin istihbarat dünyasına getirdiği potansiyel değişiklikler, sadece teknolojiyle sınırlı değildir. Aynı zamanda bu teknolojinin etkin bir şekilde kullanılması ve yönetilmesiyle de yakından ilişkilidir. Kuantum bilişim sayesinde kriptanaliz yeteneklerinde önemli ilerlemeler kaydedilebilse bile SIGINT'in etkinliği, sadece bu teknolojinin kullanılmasından ziyade, doğru zamanlamayla elde edilen bilgilerin analiz edilip karar vericilere aktarılmasında yatıyor [43]. Daha açık bir ifadeyle, Kuantum bilgisayarların ve diğer teknolojilerin doğrudan uygulamaya konulması, daimî stratejik bir avantaj sağlamanın garantisi olmayabilir. SIGINT'in değerli ola-

bilmesi için, elde edilen bilgilerin analiz edilmesi ve stratejik kararlarda doğru bir şekilde kullanılmaları gerekmektedir. Hatalı bir analiz ya da liderlerin istihbaratın değerini anlamaması, bu teknolojinin potansiyelini zayıflatabilir. Benzer şekilde, en güçlü kriptografik sistemler bile insan hatası ya da zayıf kurumsal uygulamalar nedeniyle tehlikeye girebilir [47].

Kuantum bilgisayarlar ve kuantum dirençli şifreleme arasındaki mücadelede, her iki tarafın da sürekli yenilik yapmak zorunda olması, istihbarat rekabetini dinamik bir hale getirecektir [45]. Kuantum güvenli şifreleme sistemleriyle beraber OPSEC'in güçlü bir şekilde uygulanması, bir kurumun güvenlik duruşunu önemli ölçüde güçlendirecektir. Ancak, zayıf protokollerin hatalı uygulandığı durumlarda, bu güvenlik avantajı kaybedilebilir. Ayrıca, kriptanalizdeki teknolojik yenilikler, bir kurumun OPSEC avantajını azaltabilir, ancak bu yeni teknolojilerden faydalanmak için kurumların yeterli kapasitelerini geliştirmesi de gerekecektir [43]. KUT ve istihbarat dünyası arasındaki etkileşimin dinamik olduğu bu süreçte, istihbarat toplama ve koruma stratejileri, teknolojinin sunduğu yeni fırsatlar ve riskler karşısında sürekli olarak yenilenmek zorundadır. Kuantum devrimi ile, istihbaratın toplanması, analiz edilmesi ve korunması arasındaki denge daha da karmaşık hale gelecek, ancak bu süreçte her iki taraf da kalıcı bir üstünlük sağlayamayacaktır [47].

### 3.2.3. Kuantum Üstünlük ve Hegemonya Bağlamında Uluslararası Güvenlik ve İstihbarat

Kuantum teknolojilerinin istihbarata etkisine yönelik genel yaklaşım, teknolojik altyapının ve organizasyonel yapıların bir araya gelerek istihbarat avantajını şekillendirdiğine odaklanmaktadır [40]. Bu, siyasi rekabet için kritik olan gizli bilgilerin toplanması veya korunması açısından büyük önem taşır. Tarihsel olarak, güçlü sinyal istihbarat kapasitesine sahip ülkeler, askeri çatışmalarda üstünlük sağlamış ve krizlerin tırmanmasını önleyerek önemli avantajlar elde etmişlerdir. Özellikle ABD, uzun yıllardır sinyal istihbaratında lider konumda olmuştur [39]. Bu pozisyonu, savaş sürelerini kısaltarak ve stratejik karar alma süreçlerini etkileyerek küresel jeopolitik dengeyi belirlemede kritik bir rol oynamıştır. II. Dünya Savaşı'nda Enigma kodunu kıran müttefik ülkelerin, bu başarıyla savaşın gidişatını değiştirdiği ve milyonlarca insanın hayatını kurtardığı tahmin edilmektedir [43].

Kuantum teknolojisi, bu tür tarihsel örneklerdeki gibi, gelecekte istihbarat üstünlüğünü yeniden şekillendirebilir. Ancak, kuantum kriptanaliz ve kuantum güvenli kriptografi, sadece teknolojik bir yenilik olarak değil, aynı zamanda bu teknolojiyi etkin bir şekilde kullanabilme kapasitesine sahip organizasyonlar tarafından yönetilen karmaşık bir süreçtir. Dolayısıyla, teknolojik avantajlar sosyal ve kurumsal faktörlerle şekillenir. Kuantum bilişim, bu süreçleri etkileyebilir, ancak onun gerçek etkisi büyük oranda organizasyonel adaptasyon ve kapasite geliştirme kabiliyetiyle sınırlı olacaktır [47].

Kuantum bilişim, istihbarat dünyasında yıkıcı bir etki yaratma potansiyeline sahiptir ve bu durum, gelecekteki güvenlik tehditleri hakkında ciddi uyarılar sunmaktadır. Tarihsel örneklere bakıldığında, Anglo-Amerikan Müttefiklerinin II. Dünya Savaşı sırasında Enigma şifreleme sistemini kırma başarısını gizli tutması, bu teknolojiyi kullanan diğer hükümetlerin on yıllar boyunca şifrelemelerinin güvenli olduğuna inanmalarına yol açtı. Soğuk Savaş boyunca İngiliz ve Amerikan istihbarat servisleri, bu gizli başarılarını kullanarak diğer hükümetlerin kritik iletişimlerini dinleyebildiler. Kuantum bilişim bağlamında da benzer bir riskle karşı karşıya olma durumu mevcuttur; rakip ülkeler, kuantum kriptanaliz yeteneklerini geliştirip kullanırken bu yeteneklerini gizleyebilir; nihayetinde kendilerini güvende varsayan ülkeler farkına varmadan sinyal istihbaratında yıllarca büyük bir dezavantajda kalabilir [45].

Kuantum bilişim, özellikle şifrelenmiş verilerin güvenliğine karşı ciddi bir tehdit oluşturmaktadır. Şu an için yakalanan şifreli veriler, kuantum kriptanaliz uygulamaları olgunlaştığında çözülebilir hale gelebilir. Bu da bugünün güvenlik önlemleri gelecekte yetersiz kalacağından, ulusal güvenlik açısından büyük bir tehdit anlamına gelir. ABD'nin, Çin gibi rakip devletlerle kuantum bilgisayar teknolojisi yarışında geri kalması durumunda, sinyal istihbaratında sahip olduğu liderliği kaybetmesi muhtemeldir [49].

Tıpkı Müttefiklerin II. Dünya Savaşı sonrası başarılarını gizlemeleri gibi, rakip devletler de kuantum üstünlüklerini saklayarak yıllar boyunca ABD'nin en hassas bilgilerine erişim sağlayabilir. Bu nedenle, kuantum kriptanaliz tekniklerinin geliştirilmesi ve uygulanması konusunda lider olamayan ülkeler, kendi veri güvenliklerini korumak için kuantuma dayanıklı şifreleme sistemlerine geçme zorluğuyla karşı karşıya kalacaktır. Kuantum bilgisayarların ortaya çıkışı, sadece askeri ve istihbarat sistemlerini değil, kamu ve özel sektörde kullanılan tüm güvenlik protokollerini tehdit eder hale getirebilir.

Kuantum teknolojilerinde, ABD'nin liderliği elinde tutma vizyonu hem ulusal güvenliğini hem de küresel jeopolitik üstünlüğünü koruması açısından kritik öneme sahiptir [51]. Diğer taraftan Çin'in bu alandaki erken adımları, küresel bir "kuantum hegemonyası" tartışmasını gündeme getirecektir [43]. Bu durum, Batı'nın istihbarat yeteneklerini zayıflatma ve sürpriz saldırılara karşı uyarı mekanizmalarını tehdit etme potansiyeliyle ilintilidir. Ancak, kuantum bilişim henüz uygulanabilir bir güvenlik açığı yaratacak kadar gelişmiş olmasa da bu teknolojinin gelecekteki etkilerini öngörmek ve buna göre stratejik hazırlık yapmak, ülkeler ve istihbarat kuruluşları için büyük önem taşımaktadır [40].

## 4. KUANTUM TEKNOLOJİLERİ VE İSTİHBARATIN GELECEĞİ: YAPILANDIRILMIŞ ANALİZ TEKNİKLERİ İLE BİR ÖNGÖRÜ

Bu kısımda kuantum teknolojilerinin kabiliyetlerinin, istihbaratın geleceğindeki rolünün anlaşılabilmesi adına, istihbarat analizinde sıkça kullanılan yapılandırılmış analiz tekniklerine başvurulmuştur.

### 4.1. İstihbarat Analizinde Yapılandırılmış Analiz Teknikleri

Yapılandırılmış analiz, analitik süreci şeffaf ve sistematik bir hale getirerek başkalarının inceleyip eleştirmesine olanak tanıyan bir mekanizmadır. Bu teknikler, bir problemin bileşenlerini ayırarak adım adım ele alınmasını sağlar ve de analistin genellikle karşılaştığı belirsiz veri yığınlarını düzenlemeye yardımcı olur [52]. Analistlere kesin bir çözüm sunmaz; daha çok sorunlar üzerinde düşünmeyi yönlendiren bir araç olarak kullanılır. Bu yöntem, belirsizliklerle uğraşan analistlerin düşüncelerini daha açık ve eleştirilebilir hale getiren ilkeler ve prosedürler sunar [53].

Yapılandırılmış analiz teknikleri, analistlerin eksik bilgi ve karmaşık uluslararası gelişmeler gibi istihbaratın sürekli sorunlarıyla başa çıkmalarına yardımcı olur. Düşmanların gizlenen niyet ve yeteneklerini anlamak zor olsa da bu teknikler, hata riskini azaltarak analistlerin bilişsel sınırlamaların üstesinden gelmesini sağlar [54]. Analistlerin önyargı ve varsayımlarını sorgulamalarına olanak tanıyarak, analitik problemlere daha disiplinli yaklaşmalarını teşvik eder ve daha sağlam kararlar almalarına yardımcı olur [55].

İstihbarat analizinde "zihinsel model" terimi, bir analistin olayları anlamlandırma biçimini ve karar alma sürecini şekillendiren anahtar bir kavramdır [52]. İstihbarat analistleri, tıpkı diğer insanlar gibi, olayları değerlendirmeye sıfırdan başlamazlar; geçmiş deneyimleri ve bilgi birikimleriyle hareket ederler. İyi bir zihinsel model, bir analiste neyin önemli olduğunu ve olayları nasıl yorumlayacağını gösterir. Bu modeller, analistlerin olayları anlama ve çözümleme süreçlerini etkilediği için, doğru zihniyetin geliştirilmesi önemlidir [56].

Zihniyetin esnek olmaması ya da güncel olmaması analitik süreçte bir sorun olarak görülebilir. Ancak bu durum, analiz sürecindeki zorlukların yalnızca bireysel hatalardan kaynaklanmadığını, zihinsel modellerin karmaşık ve belirsiz dünyayı tam olarak yansıtamayacağını gösterir. Daha doğru sonuçlar, farklı bakış açılarına sahip analistlerin işbirliği yapması ve yapılandırılmış analiz tekniklerinin kullanılmasıyla elde edilebilir. Bu yöntemler, yaratıcı ve sorgulayıcı bir yaklaşımla birleşmeli ve analizin yapıldığı organizasyonel çevre tarafından desteklenmelidir [52].

İstihbarat analistleri, analiz yaparken farklı yöntemler kullanır ve bu yöntemler genellikle nitel ve nicel, sezgisel ve ampirik veya bilimsel olarak sınıflandırılır. Bazı araştırmacılar üç ana yaklaşımı kabul eder [57]: sezgisel, yapılandırılmış ve bilimsel. Heuer ise istihbarat analizini dört ana kategoriye ayırır [58]: nicel yöntemlerle

deneysel veriler, uzman kaynaklı nicel yöntemler, kendi muhakeme süreçleri ve yapılandırılmış analiz. Akabinde yapılandırılmış analiz tekniklerini amaçlarına göre üç kategoriye ayırır [59]:

• Teşhis teknikleri: Tanı koyma odaklı yöntemdir.

• Karşıt teknikler: Meydan okuyan fikirleri baz alır.

• Yaratıcı düşünce teknikleri: Hayal gücünü ve senaryoyu temel alan teknikleri ifade eder.

Kuantum teknolojileri ve istihbarat ilişkisine dair henüz kamuoyuna yansıyan net bir vaka veya kesin bir istihbarî olay olmadığı için bu çalışmada, yapılandırılmış analiz tekniği olarak yaratıcı düşünce tekniklerinden alternatif gelecekler ve kırmızı takım analiz tekniklerinin uygulanması tercih edilmiştir.

#### 4.1.1. Alternatif Gelecekler Analizi (AGA)

Alternatif gelecekler analizi (AGA), karmaşık ve belirsiz bir durumun gelişebileceği yolları sistematik bir şekilde incelemeye yönelik bir tekniktir [54]. Bu analiz, çoklu senaryo üretimine dayansa da akademisyenler ve karar vericilerin katkılarıyla daha kapsamlı projelere dönüşebilir. AGA, bilgilendirilmiş bir kolaylaştırıcının rehberliğinde daha sistematik bir süreçle yürütülür ve ele alınan senaryoların sayısına göre çoklu senaryo üretiminden farklılık gösterir [52].

AGA, özellikle yüksek belirsizlik içeren ve sonuçların tek bir sonuca indirgenemeyeceği durumlarda kullanılır. Analistler, belirsizliği kabul edip çeşitli faktörleri dikkate alarak önyargısız bir şekilde bir dizi olası sonucu keşfetmeye hazır olmalıdır. Bu süreç, küçük ekiplerin birkaç saatlik çalışmalarından geniş katılımlı çalıştaylara kadar uzanabilir. Daha büyük projeler ise genellikle senaryo geliştirme konusunda uzman kişilerin özel becerilerine ihtiyaç duyar [54]. Alternatif gelecek geliştirme için yaygın olarak izlenen adımlar şunlardır [54]:

• Gelecek egzersizinin odak noktası ve hedefleri net bir şekilde belirlenir.

• Konunun uzmanlarıyla görüşülerek "odak sorunu" geliştirilir.

• Uzmanlarla kilit faktörleri tartışıp, sorunun gelişimini en çok etkileyen güçler, beyin fırtınasıyla belirlenir.

• En kritik ve belirsiz iki faktör seçilir, sonra bunları eksenler halinde gruplayarak bir 2×2 matris oluşturulur.

• Her faktör için uygun uç noktalar tanımlanır ve bu uç noktalar eksenlere yerleştirilir.

• Matrisin dört kadranında, iki faktörün kombinasyonlarıyla senaryolar oluşturulur ve isimlendirilir.

• Her senaryo için olayların nasıl gelişeceğini anlatan bir hikâye yazılır ve kronoloji eklenir.

• Her senaryonun etkileri açıklanır ve olası gelişmeleri gösteren anlatılar hazırlanır.

• Senaryoların gerçekleşme ihtimalini gösterecek işaretler ve göstergeler belirlenir.

• Bu göstergeler düzenli olarak takip edilir.

Politika yapıcılar, alternatif gelecek senaryoları üzerinde düşünerek, mevcut stratejilerin her bir olası senaryoda nasıl işleyeceğini değerlendirebilir. Bu sayede, stratejilerini daha esnek hale getirme veya değişimlere karşı hazırlıklı olma fırsatı bulurlar. Alternatif gelecekler analizi (AGA), sadece "bilinen bilinmeyenle" değil, özellikle yüksek belirsizlik içeren ve "bilinmeyen bilinmeyenlerle" barındıran durumlar için faydalı olabilir [52]. Analistler, bu belirsizliklerle başa çıkmak için yapılandırılmış teknikler kullanarak, gelecekte karşılaşabilecekleri beklenmedik durumlara hazırlıklı olur ve serbest görüş alışverişiyle geleceği daha yaratıcı biçimde hayal ederler [54].

#### 4.1.2. Kırmızı Takım Analizi (KTA)

Kırmızı Takım Analizi (KTA), bir rakibin veya hasmın bakış açısıyla düşünerek, onların strateji ve planlarına meydan okuma sürecidir [52]. ABD askerî ve savunma bürokrasisinde, KTA, bir organizasyonun stratejik, operasyonel ve taktiksel planlarına karşı alternatif bakış açılarını geliştirerek varsayımları test etmek için kullanılır [60].

KTA sadece rakiplerin perspektifini ele almakla kalmaz, aynı zamanda "şeytanın avukatlığını" yaparak yerleşik düşüncelere karşı alternatif yorumlar sunmayı hedefler. Bu yöntem, meydan okuma analizi veya alternatif analiz olarak da bilinir ve analitik becerilere sahip özel ekipler tarafından yürütülür. Böylece geleneksel bilgeliğe meydan okuyarak alternatif çözümleri araştırır [54].

Kırmızı Takım Analizi (KTA), yönetimin, geleneksel görüşe meydan okuma ihtiyacı hissettiğinde veya bir rakibin bakış açısını anlamak için yeterli kültürel bilgi eksikliği gördüğünde başlatılır. Mavi ekip dost güçleri temsil ederken, kırmızı takım düşman güçlerin perspektifinden çalışarak analistlerin kendi zihinsel modellerinden sıyrılmalarına ve rakiplerin kültürel ve politik bağlamlarını anlamalarına yardımcı olur [60].

KTA, mevcut kararları sorgulamak ve en güçlü eleştirileri geliştirmek amacıyla kullanılır. Bu teknik, rakibin düşünce yapısını anlamaya odaklanır ve kültürel uzmanlık gerektirir. KTA ekibi, hedefin dilini, kültürünü ve operasyonel çevresini bilen uzmanlardan oluşmalıdır, bu sayede rakibin bakış açısından durumu analiz edebilirler [52]. KTA ekibi, rakibin yerine kendini koyarak sorular sorar ve durumları onların bakış açısıyla değerlendirir. Ayrıca, rakip liderin veya grubun nasıl tepki vereceğini, hangi endişeleri olacağını ve hangi kararları alacağını simüle eden politika belgeleri hazırlar. Bu belgeler, hedefin kültürel ve kişisel normlarını yansıttıkça analize farklı bir perspektif kazandırır [61]:

• Düşmanın bakış açısı benimsenerek, onların dış uyarıcılara nasıl tepki vereceği simüle edilir.

• Düşmanın kendisine soracağı sorular belirlenir, örneğin: "Bu bilgiyi nasıl yorumlardım?" veya "Endişelerim neler olurdu?"

• Hedefin kültürel ve kişisel normlarına uygun politika belgeleri hazırlanır; bu belgeler farklı bir analitik bakış açısı sağlayacaktır.

• Kırmızı Takım analizi, genellikle "birinci şahıs" formatında, liderlere veya gruplara gönderilen taslak notlar şeklinde sunulur.

• Analiz, uyarı veya kesinlik sağlamaktan ziyade, düşünceyi kışkırtmayı ve rakiplerin düşünme biçimine dair yerleşik anlayışları sorgulamayı hedefler.

• Bu makaleler genelde diğer uzmanlarla koordine edilmez ve bir fikir birliğini temsil etmeyi amaçlamaz.

• Kırmızı Takım makaleleri, tüm eylem yollarını planlamak yerine, hedefin kişisel, örgütsel veya kültürel deneyimlerine dayalı tahminler sunar.

### 4.2. KUT ve İstihbarat Bağıntısına AGA Tekniği Uygulamak

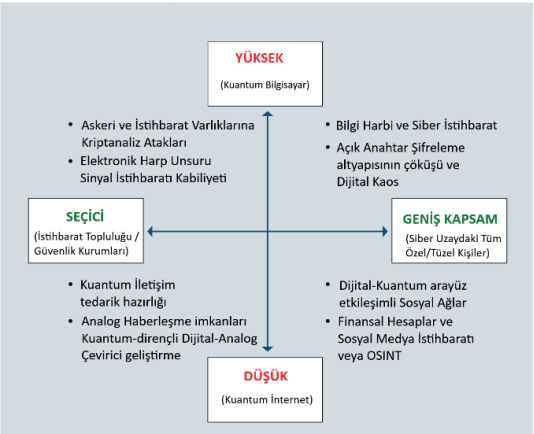
Kuantum teknolojilerinin istihbarat disiplini üzerindeki yenilikçi ve yıkıcı etkileri göz önüne alındığında, Kuantum Bilişim ve Kuantum İletişim alanları özelinde ilerlemek, istihbarat düzleminde alternatif geleceklerin netleştirilmesinde bir fikir verebilir. Daha önce de belirtildiği üzere, Kuantum Bilişim'in yol açabileceği "Kriptokalips" (yani kuantum kripto kıyameti), mevcut çevrimiçi güvenlik sistemlerini geçersiz kılarak gizliliğin bilinen tüm boyutlarını sona erdirme potansiyeline sahiptir [43].

Kuantum bilişimdeki hızlı ilerlemeler ve bu alandaki yenilik beklentileri, "Kriptokalips" anının giderek yaklaştığına işaret ederken, bilim insanları ve politika yapıcılar bu yaklaşan tehdidi önlemek için adımlar atmaya çalışmaktadır. Özellikle Çin'in kuantum teknolojilerine yönelik bilimsel ve politik kararlılığı, ABD hükümeti için ciddi bir endişe kaynağı haline gelmiştir. İki ülke de tehdit algılamalarına paralel olarak bu alandaki yatırımlarını hızla artırmaktadır. Bu yatırımların en öncelikli hedefi, tehdit edici bir kuantum bilgisayardan önce "kuantum güvenli" çözümleri geliştirmektir.

Kuantum güvenli ya da dirençli sistemler bakımından Kuantum iletişim altyapısına sahip olabilecek revizyonist aktörler, önemli stratejik avantajlar elde edebilirler [40]. Örneğin, hasım bir aktör tarafından planlanan sürpriz bir saldırının Batı'nın SIGINT birimleri tarafından tespit edilmesi neredeyse imkânsız hale gelebilir. Çin'in kuantum iletişimdeki erken hamleleri ve hızlı ilerleyişi, bu alandaki Kuantum Hegemonyasının, belirleyici askeri ve istihbarî bir üstünlük sağlayabileceğine dair spekülasyonları artırmaktadır [49].

ABD, Çin gibi rakip ulus devletler karşısında kuantum bilgisayar yarışını kaybederse, yalnızca sinyal istihbaratındaki liderliğini değil, aynı zamanda siber uzaydaki stratejik üstünlüğünü de kaybetme riskiyle karşı karşıya kalacaktır [49]. II. Dünya Savaşı sonrasında Batılı Müttefikler'in elde ettiği avantajlara benzer şekilde, ABD'nin rakipleri de kuantum teknolojisindeki kritik atılımlarını gizleyebilir ve fark edilmeden şifreleme sistemlerini kırarak ülkenin en hassas bilgilerine yıllar boyunca erişim sağlayabilir [45].

Mevcut literatür ve gelişmeler ışığında ortaya çıkan senaryolarda, ABD ve Çin arasında kuantum üstünlük yarışı sürerken kuantum hegemonyayı belirleyebilecek sürpriz olayların gelişmesi düşünülebilir. Örneğin, Çin Kuantum Bilişim yarışında kuantum üstünlüğü belirleyecek olan kübit işleme sayısında rekabet eder görünüyorken, daha hızlı bir şekilde Kuantum İletişim altyapısını tesis ederek kırılması imkânsız bir iletişim altyapısına sahip olabilir. Böylece ABD ve Batılı müttefiklerin kübit üstünlüğüne dayanan kuantum bilgisayar sahipliği sayesinde gerçekleştireceği ofansif istihbarat ve siber espiyonaj operasyonları temelindeki sürpriz etkisi boşa çıkarılması olası olacaktır. Bu bağlamda, aşağıdaki senaryo ve matris görseli ele alınabilir:




**Şekil 1.** Alternatif Gelecek Analizi Tekniğinin Kuantum Gelecek Senaryosunda Görselleştirilmesi [62]

***Gelecek Egzersizi:*** Görsel, KUT sayesinde yeni nesil kuantum saldırı seviyesine erişmiş rakip bir gücün (devletin), henüz böyle bir seviyede olmayan klasik bilişimin dijital bilgi ve iletişim kabiliyetleriyle yetinen başka bir güce (devlete) nasıl bir saldırı gerçekleştirebileceğini anlamaya yönelik dört olası geleceği ele almaktadır. Bir beyin fırtınası egzersizi, analistlerin iki temel belirsizliği (rakip güç tarafından kullanılacak teknolojinin karmaşıklığı ve saldırının amaçlanan etkisi) belirlemesine yardımcı olabilir. Böylece bu faktörler, görselde "x" ve "y" eksenleri olarak sıralanır. 2 x 2 matrisindeki dört sonuç kadranı, analistlerin çeşitli kombinasyonlardan (teknolojinin düşük ila yüksek karmaşıklığı ve bir saldırının seçici ila geniş kapsamlı amaçlanan etkisi) potansiyel hedefleri görselleştirmesine olanak sağlayabilir.

Örneğin, söz konusu rakip son derece sofistikte kuantum bilgisayara sahipse ve hedef aldığı hasmına geniş bir saldırı planlıyorsa, olası hedefler arasında kamu/özel bilişim ağları ve askeri/istihbarat unsurları olabilir. Veyahut kamusal Kuantum İnternet ağı yerine özel Kuantum İletişim ağı için çeşitli geçici çözümlerin ortaya atılması ele alınabilir. Bu çalışma kapsamında tasarlanan yukarıdaki görselde bu hususta muhtemel senaryolar geliştirilmiştir. Yine bu kapsamda Kuantum Bilişim, "Kuantum Bilgisayar" olarak ve de Kuantum İletişim ise "Kuantum İnternet" olarak kurgulanmıştır. Görselde yer alan 2 x 2 matrisinde yer alan hayali senaryodaki analiz çıktıları aşağıdaki gibi listelenebilir:

- Yüksek – Geniş Kapsam:

⇒ Kamu ve özel bilişim ağlarına yönelik bilgi harbi ve siber istihbarat faaliyeti neticesinde tüm kurum ve bireylerin kritik verilerine erişim.

⇒ Mevcut Açık Anahtar Şifreleme (PKI) altyapısının sekteye uğraması akabinde ortaya çıkabilecek "Dijital Kaos".

- Yüksek – Seçici:

⇒ Hedef odaklı gerçekleştirilen askeri ve istihbarat varlıklarının kritik bilgilerine yönelik kriptanaliz saldırıları.

⇒ Rakip devletin elektronik harp unsurunu sekteye uğratmak ve sinyal istihbaratı sürecinde rakibe asimetrik üstünlük kurmak.

- Düşük – Geniş Kapsam:

⇒ Küresel teknoloji devlerinin siber uzaydaki yeni duruma uygun olarak milyonlarca kullanıcıyı Kuantum İnternet altyapısı üzerinden Dijital-Kuantum arayüz etkileşimli sosyal ağlara yönlendirmesi.

⇒ Klasik İnternet ağından Kuantum İnternet'e geçerken bankacılık ve finans hizmetlerinin yeni ortama adaptasyonu, ayrıca sosyal medya ve açık kaynak istihbaratının bu noktada evrilmesi.

- Düşük – Seçici:

⇒ Güvenlik ve istihbarat kurumlarının kamusal Kuantum İletişim ağı yerine özel Kuantum İletişim ağı tedarik hazırlığı.

⇒ Özel Kuantum İletişim ağı tedariki gecikmesi durumda kuantum-dirençli dijital-analog çevirici modüllerle mevcut sistemlerin güçlendirilmesi.

### 4.3. KUT ve İstihbarat Bağıntısına KTA Tekniği Uygulamak

KUT'un geleceğin istihbarat düzleminde olası dönüştürücü rolünü saptamak için bu kısımda kırmızı takım analizi uygulamasına başvurulmuştur. Ancak, pratik açıdan henüz net bir teknolojik vaka ortaya çıkmadığı için kırmızı takım analizinde daha anlaşılır bir denklem tercih edilmiştir. KUT ve istihbarat bağıntısı, teknolojik altyapı ve örgütsel kurumlar bağlamında incelendiğinde, kuantum bilişim ve kuantum iletişim alt alanlarının stratejik düzlemde zıt uçlarda konumlandığı söylenebilir. Bu zıtlık, kuantum kriptanalizi ve kuantum kriptografinin dijital dünyadaki geleneksel sınırları aşarak bilgi işlemeyi ve iletimini yeniden tanımlama potansiyelinden kaynaklanmaktadır. Klasik bilişimdeki makro ölçekli ekonomik gerçekler, kuantum bilişimin sunduğu mikro ölçekli gelecek projeksiyonlarını tamamen değiştirebilir [43].

Bir istihbarat hasmı, kuantum bilişimin kritik eşiği olan kübit sayısına ulaşarak, asimetrik şifreleme algoritmalarını çözme kapasitesine sahip bir makine geliştirdiğinde, bu durum önemli stratejik tehditler doğuracaktır [40]. Bu tür bir teknolojiyle, askeri operasyonlarda kullanılan kritik verilerin şifreleri kırılabilir ve siber güvenlik açıkları fiziksel ortamlara yayılacak şekilde genişleyebilir [43]. Ayrıca, üst düzey devlet yetkililerinin hesaplarının ele geçirilmesi ve bu hesaplar üzerinden yanlış bilgi yayılması, hasımların propaganda ve manipülasyon çabalarına fırsat sunacaktır [47]. Siber uzayda mevcut konjonktür ve devletler arası siber istihbarat/espiyonaj düzlemi, kuantum bilişim veya kuantum iletişimin bir anda ortaya çıkmasıyla bozulma riskiyle karşı karşıya kalacaktır. Kuantum kriptografinin ciddi şekilde kullanımı, prensipte sızılması mümkün olmayan kuantum iletişim sistemlerini oluşturacağı öngörülmektedir [46].

Öngörülebilir gelecekte kuantum bilişim, günümüzün gelişmiş şifreleme tekniklerinin çoğunun üstesinden gelmesi mümkün olduğu için hükümet ve askeri sistemlerin çoğunu benzeri görülmemiş derecede savunmasız hale getirecektir. Siber mücadelede öne çıkacak kuantum teknolojileri olan bilişim ve iletişim, sırasıyla siber alanda saldırı ve savunma avantajı sağlama eğiliminde olacaktır. Kuantum iletişimin çalıştırılacağı bilgi ağları üzerinde sağlayacağı güçlü bir koruma, teknolojik caydırıcılığa katkıda bulunabilir. Ancak daha uzak bir gelecekte, kuantum bilişime yapılan daha ciddi yatırımlar, kuantum iletişimin sağlayacağı korumayı boşa çıkarabilir [49]. Bu çalışmada KTA açısından en belirgin saptama, geleceğin istihbarat düzleminde kuantum bilişim ve iletişimin rolleri ve bulundukları pozisyonları üzerine olacaktır:

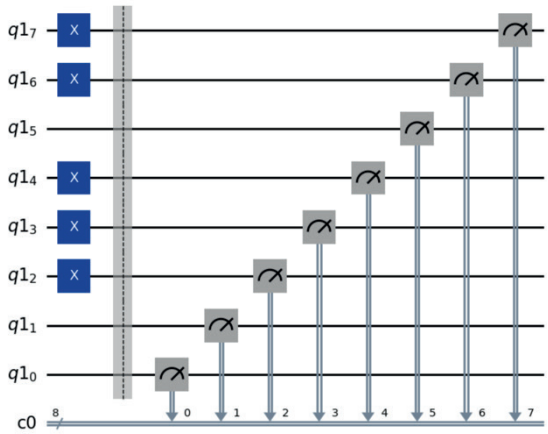
- Kuantum Bilişim → Kırmızı Takım (Ofansif)
- Kuantum İletişim → Mavi Takım (Defansif)

Bu çalışma dahilinde referans alınan çalışmalarda, istihbarat ve siber uzay açısından kuantum bilişimin kriptanalizle, kuantum iletişimin de kriptografiyle ilintili olduğu tekraren vurgulamaktadırlar. Bilhassa, şu ifade söz konusu saptamayı doğrulamaktadır [63]:

*"Neyse ki, kuantum mekaniği bir eliyle aldığını, diğer eliyle geri veriyor." (Kuantum Anahtar Dağıtımı üzerine kırılamaz Kuantum İnternet veya Kuantum İletişim hakkındaki beklenti söylemine göre)*

Kuantum bilişimin KTA uygulaması için her ne kadar istihbarat açısından uygun bir senaryo veya vaka tespit edilmemiş olsa da kuantum bil-

gisayarların geliştirilmesinde önemli bir aşama olan kuantum programlama platformları kullanımı son günlerde giderek daha fazla revaçta olmaya başladığı söylenebilir. Bir kuantum bilgisayarın programlanması için gerekli devrenin ve devre kapılarının uygun bir biçimde entegre edilmesinde IBM Qiskit, Google Cirq, Microsoft Q# ve D-Wave Leap popüler programlama platformlarından öne çıkanlardır. Aşağıdaki görsel Qiskit platformu kütüphanesinde Python ile kodlanarak basit şekilde tasarlanan bir kuantum devresini yansıtmaktadır:




**Şekil 2.** Qiskit ile tasarlanan kuantum devresi örneği [64]

Yukarıdaki devre örneği, rastgele 8 bitlik ikilik sayı seçilerek 8 kübit ve 8 klasik bit ile bir kuantum devresi tasarlanmasını göstermektedir. Her kübit için Python ile yazı tura atılır ve sonuç yazı gelirse X-kapısı uygulanır. Kübit ölçümü sonrasında, devre 10 kez çalıştırılır [64]. Bunun sonucunda 2, 3, 4, 6 ve 7 sıralı X kapıları kübite uygulanır. Tekrarlanan 10 işlem sonrasında ikilikten onluk sisteme çevrilen rastgele çıktı şu şekilde elde edilebilir: {‹11001100›: 128}

## 5. SONUÇ

Kuantum teknolojilerinin gelişimi, yıkıcı inovasyon bağlamında istihbarat düzleminde gelecekteki dengeleri derinden etkileme potansiyeline sahip olacağı bu çalışmada irdelenmiştir. Özellikle kuantum bilişim ve kuantum iletişim alanlarında kaydedilen ilerlemeler hem bilgi güvenliği hem de istihbarat toplama yöntemlerinde köklü değişikliklere yol açabileceği tahmin edilmektedir. Kuantum bilişim, mevcut asimetrik şifreleme algoritmalarını kırma yeteneğiyle kritik verilerin güvenliğini tehdit ederken, kuantum iletişim neredeyse kırılmaz güvenlik sağlayan bir ortam sunmaktadır. Bu çelişen dinamikler, istihbarat teşkilatları ve devletler arası rekabette stratejik avantajların yeniden tanımlanması gerektiğini düşündürtmektedir.

Kuantum Devrimiyle beraber Kuantum kriptanaliz tehdidine karşı Kuantum sonrası kriptografi (KSK) ve Kuantum anahtar dağıtımı (KAD) gibi yenilikçi çözümler, siber güvenlik ve istihbarat sistemleri için gelecekte temel yapı taşları olacaktır. Bu bağlamda, ülkelerin kuantum teknolojilerine yapacağı yatırımlar, istihbarat avantajlarını belirleyecek kilit unsurlardan biri haline getirmiştir. Çin'in bu alandaki öncü adımları, ABD ve diğer Batılı müttefikler için önemli bir stratejik tehdit oluşturmaktadır. Kuantum üstünlüğünü yakalayan devletler hem siber güvenlikte hem de istihbarat toplamada belirleyici bir avantaja sahip olacaktır. Ancak, tüm teknolojiler gibi, yanlış ellerde kuantum bilişim tehlikeli bir araç olabilir. Siber uzayın geniş bir alanını güvence altına alan açık anahtar şifreleme sistemlerini kırmak için kuantum teknolojisini kullanabilecektir [45].

Kuantum anahtar dağıtımı (KAD) sayesinde oluşturulacak "kırılamaz bir kuantum internet", kuantum bilgisayarların neden olduğu güvenlik açıklarına yönelik teknik bir çözüm olarak sunulmaktadır. Böylece, yıkıcı inovasyon ve yenilikçi teknoloji yarışında, kuantum tabanlı saldırılara karşı, yine kuantum bazlı savunma ile "kuantum ağlarına" ihtiyaç duyulacaktır [65]. Sonuç olarak, kuantum bilişim ve iletişim teknolojilerinin istihbarat düzlemindeki etkileri, ulus devletler arasındaki güç dengelerini yeniden şekillendirecek ve istihbarat toplama, bilgi güvenliği, siber operasyonlar gibi kritik alanlarda yeni fırsatlar ve tehditler yaratacaktır.

Yıkıcı inovasyon ve yenilikçi teknolojilerin birçok farklı alanı akademik ve teorik kabullerin dışına çıkarak gündelik pratik hayatta ve çeşitli sektörlerde yerleşmeye başlamıştır. Bu noktada, yapay zekâ, makine öğrenmesi ve robotik gibi blokzincir teknolojisi de belli bir aşamaya ulaşmış durumdadır. Blokzincir teknolojisi de güvenlik ve benzer alanlarda ofansif [66] ve de-

fansif [67] yaklaşımla kurgulanarak süreçlere entegre edilebilir. Gelecek çalışmalarına temel olması açısından, blokzincirin sağladığı özellikler KUT ile ele alınarak yeniden geliştirilebilir. Bir diğer gelecek çalışma önerisi ise, yapılandırılmış analiz tekniklerinin diğer yöntemlerinin yeni vaka veya senaryolarla KUT için uygulanması biçiminde olacaktır. Orijinal ve yeni analiz çıktıları sayesinde stratejik aktörlerin, kuantum teknolojilerinin sunduğu fırsat ve riskleri dikkatle değerlendirerek uzun vadeli politikalar geliştirmesi mümkün hale gelecektir.

## KAYNAKÇA


[1] Zohar, Eran. "Intelligence analysis as a manifestation of a grounded theory." International Journal of Intelligence and CounterIntelligence 26.1 (2013): 130-160.

[2] Razali, Noor Afiza Mat, et al. "Secure blockchain-based data-sharing model and adoption among intelligence communities." IAENG International Journal of Computer Science 48.1 (2021).

[3] Regens, James L. "Augmenting human cognition to enhance strategic, operational, and tactical intelligence." Intelligence and National Security 34.5 (2019): 673-687.

[4] Brantly, Aaron F. "When everything becomes intelligence: machine learning and the connected world." Developing Intelligence Theory. Routledge, 2020. 96-107.

[5] Lim, Kevjn. "Big data and strategic intelligence." Intelligence and National Security 31.4 (2016): 619-635.

[6] Schneier, Bruce. "NSA plans for a post-quantum world." Schneier on Security 21 (2015).

[7] STM, 2018. "Bir Devrimin Ayak Sesleri: Kuantum Bilgisayarlar" URL: https://thinktech.stm.com.tr/detay.aspx?id=159, Erişim Tarihi: 16.03.2024.

[8] Lindsay, Jon R. "Quantum computing and classical politics: The ambiguity of advantage in signals intelligence." Cyber Security Politics. Routledge, 2022. 80-94.

[9] GENÇOĞLU, Muharrem Tuncay. "İstihbarat Alanında Kuantum Teknolojilerinin Kullanımı."(2024). URL Adresi: https://tasam.org/tr-TR/Yazar/18350/doc-dr-muharrem-tuncay-gencoglu Erişim Tarihi: 14.07.2024.

[10] Liman, Anders, and Kate Weber. "Quantum Computing: Bridging the National Security–Digital Sovereignty Divide." European Journal of Risk Regulation 14.3 (2023): 476-483.

[11] Europe Defence Agency, 2017. "Europe Defence Matters: 10 Upcoming Disruptive Defense Innovations". URL: https://eda.europa.eu/docs/default-source/eda-magazine/edm-issue-14_web.pdf Erişim Tarihi: 15.06.2024.

[12] Deloitte, 2020 URL: https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html, Erişim Tarihi: 16.03.2021.

[13] Christensen, Clayton M. The innovator's dilemma: when new technologies cause great firms to fail. Harvard Business Review Press, 2015.

[14] Christensen, Clayton M. "The innovator's dilemma. Harvard Business School Press." Boston, MA (1997).

[15] Christensen, Clayton M. "The ongoing process of building a theory of disruption." Journal of Product innovation management 23.1 (2006).

[16] Gerber, Aurona, and Machdel Matthee. "Design thinking for pre-empting digital disruption." Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18. Springer International Publishing, 2019.

[17] Usborne, David. "The moment it all went wrong for Kodak." The Independent 20 (2012).

[18] Seskir, Zeki Can, and Arsev Umur Aydınoğlu. "The landscape of academic literature in quantum information technologies." (2019).

[19] Dowling, Jonathan P., and Gerard J. Milburn. "Quantum technology: the second quantum revolution." Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 361.1809 (2003): 1655-1674.

[20] Martin, Vicente, et al. "Quantum technologies in the telecommunications industry." EPJ Quantum Technology 8.1 (2021): 19.

[21] Gibney, Elizabeth. "Hello quantum world! Google publishes landmark quantum supremacy claim." Nature 574.7779 (2019): 461-463.

[22] Baggott, James Edward. The quantum story: a history in 40 moments. Oxford University Press, USA, 2011.

[23] Ford, Kenneth W. The quantum world: Quantum physics for everyone. Harvard University Press, 2009.

[24] Kleppner, Daniel, and Roman Jackiw. "One hundred years of quantum physics." Science 289.5481 (2000): 893-898.

[25] Rempe, G. "Quantum physics of entangled systems: Wave-particle duality and atom-photon molecules." Annalen der Physik 512.11-12 (2000): 843-850.

[26] Rashkovskiy, Sergey A. "Quantum mechanics without quanta: the nature of the wave–particle duality of light." Quantum Studies: Mathematics and Foundations 3 (2016): 147-160.

[27] Brooks, Juliana HJ. "Hidden variables: the elementary quantum of light." The Nature of Light: What are Photons? III. Vol. 7421. SPIE, 2009.

[28] Casati, Giulio, and Tomaž Prosen. "Quantum chaos and the double-slit experiment." Physical Review A—Atomic, Molecular, and Optical Physics 72.3 (2005): 032111.

[29] Laloë, Franck. "Do we really understand quantum mechanics? Strange correlations, paradoxes, and theorems." American Journal of Physics 69.6 (2001): 655-701.

[30] Susskind, Leonard, and Art Friedman. Quantum mechanics: the theoretical minimum. Basic Books, 2014.

[31] Doherty, M. (2020) "Quantum Technology: An Introduction". URL: https://researchcentre.army.gov.au/library/land-power-forum/quantum-technology-introduction, Erişim Tarihi: 16.06.2024.

[32] Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Cambridge university press, 2010.

[33] AB Kuantum Amiral Gemisi (2024). URL: https://qt.eu/

Erişim Tarihi: 09.05.2024.

[34] Preskill, John. "Quantum computing in the NISQ era and beyond." Quantum 2 (2018): 79.

[35] Wehner, Stephanie, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead." Science 362.6412 (2018): eaam9288.

[36] Cartlidge, Edwin. "Quantum sensors: a revolution in the offing?." Optics and Photonics News 30.9 (2019): 24-31.

[37] Yi, Haibo. "A post-quantum secure communication system for cloud manufacturing safety." Journal of Intelligent Manufacturing 32.3 (2021): 679-688.

[38] Wolf, Ramona. "Quantum key distribution." Lecture notes in physics 988 (2021).

[39] Warner, Michael. The Rise and Fall of Intelligence: an international security History. Georgetown University Press, 2014.

[40] Lindsay, J. R. (2020). Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. Security Studies, 29(2), 335-361.

[41] Era, Snowden, and Bart Preneel. "Cryptography and information security in the post-snowden era." Proc. TELERISE@ ICSE. 2015.

[42] Doğantuna, Tuncay. "Dönüşen Bilgi ve İletişim Dönemleri Boyunca Entelektüel Rekabet ve Statü Sınıfları Yaklaşımıyla İstihbarat." İstihbarat Çalışmaları ve Araştırmaları Dergisi 1.1 (2022): 99-128.

[43] Lindsay, Jon R. "Surviving the quantum cryptocalypse." Strategic Studies Quarterly 14.2 (2020): 49-73.

[44] Nature, (2024). URL: https://www.nature.com/articles/d41586-024-03288-3 Erişim Tarihi: 10.10.2024.

[45] Grobman, Steve. "Quantum computing's cyber-threat to national security." PRISM 9.1 (2020): 52-67.

[46] Kania, Elsa B., and John K. Costello. "Quantum hegemony." China's ambitions and the challenge to US innovation leadership. Washington, DC: Center for New American Security (2018).

[47] Lindsay, Jon. "Why quantum computing will not destabilize international security: The political logic of cryptology." Available at SSRN 3205507 (2018).

[48] De Wolf, Ronald. "The potential impact of quantum computers on society." Ethics and Information Technology 19 (2017): 271-276.

[49] Smith III, Frank L. "Quantum technology hype and national security." Security dialogue 51.5 (2020): 499-516.

[50] NIST, (2024). URL: https://csrc.nist.gov/projects/post-quantum-cryptography Erişim Tarihi: 30.09.2024.

[51] Raymer, Michael G., and Christopher Monroe. "The US national quantum initiative." Quantum Science and Technology 4.2 (2019): 020504.

[52] Pherson, Randolph H., and Richards J. Heuer Jr. Structured analytic techniques for intelligence analysis. Cq Press, 2020.

[53] Heuer Jr, Richards J. "The evolution of structured analytic techniques." Presentation to the national academy of science, national research council committee on behavioral and social science research to improve intelligence analysis for national security (2009): 529-545.

[54] Primer, A. Tradecraft. "Structured analytic techniques for improving intelligence analysis." CIA Center for the study of intelligence (2009).

[55] Heuer, R. J. "The future of 'alternative analysis'." Director of National Intelligence conference on Improving Intelligence Analysis: What Works. 2007.

[56] Pherson, Randolph H. "The Five Habits of the Master Thinker." Journal of Strategic Security 6.3 (2013): 54-60.

[57] Wirtz, J. J. (2012). The Science of Artful Analysis: Richards J. Heuer Jr. and Randolph H. Pherson: Structured Analytic Techniques for Intelligence Analysis CQ Press, Washington, DC, 2011, 343 p.

[58] Heuer Jr, Richards J., Randolph Pherson, and Sarah M. Beebe. "Use of Analytic Tools and Techniques in the Homeland Security Classroom." (2012).

[59] Heuer, Richards J. "Taxonomy of structured analytic techniques." International Studies Association Annual Convention. 2008.

[60] DoD "DoD Red Teaming Activities, IRP Federation of American Scientists" (2003). URL: https://irp.fas.org/agency/dod/dsb/redteam.pdf Erişim Tarihi: 03.05.2024.

[61] HEUER, RJ. "Rethinking Challenge Analysis." Conference on Learning the Lessons of All Source Intelligence Analysis. 2008.

[62] Bu çalışma kapsamında elde edilen bulgular; "Primer, A. Tradecraft" belgesindeki talimatlara ve görsele göre çalışılarak hazırlanmıştır.

[63] Nielsen, Michael A., and I. L. Chuang. "Quantum Computation." (2011).

[64] QWorld Gitlab (2024). URL: https://gitlab.com/qworld/bronze-qiskit Erişim Tarihi: 20.10.2024.

[65] MIT Technology Review, (2017). URL: https://www.technologyreview.com/2017/10/25/105219/new-twists-in-the-road-to-quantum-supremacy/ Erişim Tarihi: 02.10.2024.

[66] Korkuc, Cagatay, et al. "BLOCKBOX: Blockchain based black box designing and modeling." Concurrency and Computation: Practice and Experience 36.13 (2024): e8057.

[67] Korkuc, Cagatay, et al. "Blockchain based network access control (NAC) management solution and architecture Blokzincir tabanli a erişim kontrol (NAC) yönetim çözümü ve mimarisi."