KTEAD

ISSUE 3

VOLUME/CİLT: 2
YEAR/YIL: 2024

Journal of Quantum Technologies and Informatics Research

International Peer-Reviewed and Open Access Electronic Journal
Uluslararası Hakemli ve Açık Erişimli Elektronik Dergi

Journal of Quantum Technologies and Informatics Research

JQTAIR

E-ISSN : 3023-4735
DOI: 10.70447/ktve

https:https://journals.gen.tr/index.php/jqtair/

HOLISTENCE publications

Journal of Quantum Technologies
and Informatics Research

JQTAIR

E-ISSN: 3023-4735
DOI: 10.70447/ktve

International Peer-Reviewed and Open Access Electronic Journal
Uluslararası Hakemli ve Açık Erişimli Elektronik Dergi

Volume/Cilt: 2
Issue/Sayı: 3
Year/Yıl: 2024

E-posta: jqtair@gmail.com
Web: https://journals.gen.tr/index.php/jqtair/
İletişim: Adres: Anafartalar Yerleşkesi, B2 Blok, Oda No: 8,
Çanakkale, Türkiye

HOLISTENCE
publications

"This page is left blank for typesetting"

Bu sayfa dizgiden dolayı boş bırakılmıştır

EDİTÖR'den

Değerli Bilim İnsanları, Araştırmacılar ve Okuyucular, Kuantum teknolojileri ve enformatik araştırmalarında bilgi birikimini zenginleştirmek, disiplinler arası iş birliğini artırmak ve yenilikçi çözümleri teşvik etmek amacıyla çıktığımız bu yolda, Kuantum Teknolojileri ve Enformatik Araştırmaları Dergisi (KTEAD) olarak ikinci yılımızın üçüncü sayısıyla karşınızdayız. Bu sayı, hem akademik camiayı hem de sektörel profesyonelleri hedef alan değerli makalelerle zenginleştirilmiştir.

Kuantum bilişim, yapay zeka, optimizasyon algoritmaları ve veri analitiği gibi günümüzün en dinamik ve yenilikçi alanlarında her geçen gün yeni ufuklar açılmaktadır. Bu hızlı gelişim süreci, yalnızca bilim dünyasını değil, aynı zamanda teknolojinin günlük yaşamlarımız üzerindeki etkisini de şekillendirmektedir. Dergimiz, bu alanlarda yapılan çalışmaların paylaşılmasına olanak tanıyarak, bilginin toplumla buluşmasını ve yeniliklerin daha geniş kitlelere ulaşmasını sağlamayı amaçlamaktadır.

Bu sayımızda, birbirinden değerli çalışmalarla dolu üç özgün makale yer almaktadır. Bu makaleler, **optimizasyon algoritmalarına genel bir bakıştan**, **meta-sezgisel yöntemler kullanılarak müzik popülarite sınıflandırmasında özellik seçimine** ve **kuantum teknolojilerinin gelecekteki istihbarat düzlemindeki yerine** geniş bir yelpazeye yayılmıştır. Bu içeriklerin, yalnızca akademik bilgiye katkıda bulunmakla kalmayıp, aynı zamanda uygulamalı çözümler üretmek isteyen araştırmacılar için de ilham kaynağı olacağını düşünüyoruz.

Derginin Misyonu ve Hedefleri

KTEAD, multidisipliner yaklaşımıyla kuantum teknolojileri ve enformatik araştırmaları arasındaki etkileşimi teşvik etmekte, farklı disiplinlerden bilim insanlarının bir araya gelmesini sağlamaktadır. Dergimiz, yalnızca akademik makalelerin yayımlandığı bir platform değil, aynı zamanda etik, bilimsel mükemmeliyet ve yenilikçilik ilkelerini ön planda tutan bir bilgi paylaşım ağıdır. Amacımız, teknoloji ve bilimin sınırlarını zorlayan çalışmalara ev sahipliği yaparak, akademik birikimi ve sektörel uygulamaları birbirine yaklaştırmaktır.

Bu sayımızda yer alan makalelerin her biri, araştırma dünyasına önemli katkılar sunmaktadır. Örneğin, **optimizasyon algoritmalarına genel bakış** üzerine yapılan bir çalışma, veri yoğun problemlere çözümler sunma potansiyeline sahiptir. Benzer şekilde, **meta-sezgisel yöntemler ile müzik popülarite sınıflandırmasında özellik seçimi**, veri analizinde yenilikçi yaklaşımlar sunmaktadır. **Kuantum teknolojilerinin gelecekteki istihbarat düzlemindeki yeri** ise teknolojinin gelişiminin güvenlik ve istihbarat alanlarındaki etkilerini araştırmaktadır.

Teşekkür ve Gelecek Perspektifi

Bu sayının hazırlanmasında emeği geçen tüm yazar, hakem, teknik ekip ve yayın kurulu üyelerine teşekkürü bir borç bilirim. Çalışmalarıyla dergimizin bilimsel niteliğini ve saygınlığını artıran bu değerli katkılar, KTEAD'ın bugün olduğu yere gelmesinde büyük bir rol oynamıştır. Ayrıca, araştırmacılarımızın bu alandaki yenilikçi çalışmalarını teşvik ederek, onların başarılarını uluslararası platformlara taşımayı da hedefliyoruz. Gelecek sayılarımızda da kuantum teknolojileri ve enformatik araştırmaları alanındaki en güncel ve etkili çalışmaları sizlerle paylaşmayı sürdüreceğiz. Araştırmacılarımızı, bilim insanlarını ve sektör temsilcilerini, dergimize katkıda bulunmaya davet ediyoruz. Birlikte, bilimin ve teknolojinin sınırlarını daha da ileriye taşıyabiliriz. Kuantum teknolojileri ve enformatik dünyasına dair yeni keşifler ve tartışmalar için sizleri dergimizin sayfalarına davet ederken, katkılarınızın bu alandaki ilerlemelere büyük bir ivme kazandıracağına olan inancımı paylaşmak isterim. Bilime ve bilgiye olan tutkumuzla, birlikte aydınlık bir geleceğe ilerlemeye devam edeceğiz.

Saygılarımla,

Dr. Öğr. Üyesi Sevdanur Genç

Editör Kuantum Teknolojileri ve Enformatik Araştırmaları Dergisi

Hakemler

Doç. Dr. Fatih AYDIN,
Balıkesir Üniversitesi – Bilgisayar Mühendisliği

Doç. Dr. Özkan ATAN,
Van Yüzüncüyıl Üniversitesi – Elektrik Elektronik Mühendisliği

Dr. Öğr. Üyesi Sevgi DEMİRCİOĞLU,
İstanbul Arel Üniversitesi – Bilgisayar Mühendisliği

Dr. Öğr. Üyesi Bayram KÖSE,
İzmir Bakırçay Üniversitesi – Elektrik Elektronik Mühendisliği

Dr. Öğr. Üyesi Alp KARADENİZ,
Balıkesir Üniversitesi – Elektrik Elektronik Mühendisliği

Dr. Çağatay KORKUÇ,
Opet Fuchs - IT Security Executive (BT Güvenlik Yöneticisi)

EDITORS/EDİTÖRLER

İletişim: Anafartalar Yerleşkesi,
B2 Blok, Oda No: 8, Çanakkale, Türkiye
Telefon: 5052423644
E-posta: jqtair@gmail.com
Web: https://journals.gen.tr/index.php/jqtair/

CONTENTS / İÇİNDEKİLER

"This page is left blank for typesetting"

Bu sayfa dizgiden dolayı boş bırakılmıştır

Journal of Quantum Technologies and Informatics Research
JQTAIR

KUANTUM TEKNOLOJİLERİ VE ENFORMATİK ARAŞTIRMALARI
Volume / Cilt: 2, Issue / Sayı: 3, 2024, pp. 105-113
E - ISSN: 3023-4735
URL: https://journals.gen.tr/index.php/jqtair/
DOI: https://doi.org/10.70447/ktve.2561

Received / Geliş: 27.09.2024
Acccepted / Kabul: 23.10.2024

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Optimizasyon Algoritmalarına Genel Bakış: Klasik ve Modern Yöntemler

Overview of Optimization Algorithms: Classical and Modern Methods

Güray Tonguç

Akdeniz Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Antalya, Türkiye, e-mail: guraytonguc@akdeniz.edu.tr

Öz

Günümüz dünyasındaki bilgi teknolojilerindeki gelişmeler daha büyük veriler içeren ve daha karmaşık sorunlara daha kesin ve doğru çözümler üretme gereksinimini arttırmıştır. Bu noktada araştırmacılara önemli faydalar sağlayan araçlardan birisi de optimizasyon algoritmalarıdır. Doğadaki olaylardan esinlenerek geliştirilmiş meta-sezgisel yöntemler de karmaşık problemler için hızlı ve etkili çözümler sunmaktadır. Bu çalışmada optimizasyon ve arama algoritmalarının temel prensipleri ve uygulama alanlarına odaklanılmaktadır. Optimizasyonun tanımı, karar değişkenleri, amaç fonksiyonu ve kısıtlar gibi temel kavramların verilmesinin ardından analitik, sezgisel ve meta-sezgisel yöntemlerden bahsedilmiştir. Dijkstra, Bellman-Ford, A*, Ateş Böceği, Karınca Koloni, Kurt Kolonisi ve Yapay Balık Sürüsü algoritmaları incelenerek, bu algoritmaların çeşitli uygulama alanlarındaki kullanım örnekleri ortaya konulmuştur.

Anahtar kelimeler: Optimizasyon, Meta-Sezgisel Algoritmalar, Doğa-Esinli Yaklaşımlar, Arama Algoritmaları

Abstract

Developments in information technologies in today's world have increased the need to produce more precise and accurate solutions to more complex problems that involve larger data. At this point, one of the tools that provide significant benefits to researchers is optimization algorithms. Meta-heuristic methods inspired by natural events also provide fast and effective solutions for complex problems. This study focuses on the basic principles and application areas of optimization and search algorithms. After giving basic concepts such as the definition of optimization, decision variables, objective function and constraints, analytical, heuristic and meta-heuristic methods are mentioned. Dijkstra, Bellman-Ford, A*, Firefly, Ant Colony, Wolf Colony and Artificial Fish Swarm algorithms are examined and examples of the use of these algorithms in various application areas are presented.

Keywords: Optimization, Meta-Heuristic Algorithms, Nature-Inspired Approaches, Search Algorithms

Citation/Atıf: TONGUÇ, G. (2024). Optimizasyon Algoritmalarına Genel Bakış: Klasik ve Modern Yöntemler. *Kuantum Teknolojileri ve Enformatik Araştırmaları*. 2(3): 105-113, DOI: 10.70447/ktve.2561

Corresponding Author/ Sorumlu Yazar:
Güray Tonguç
E-mail: guraytonguc@akdeniz.edu.tr

1. GİRİŞ

Kökeni Latince'deki "optimas" kelimesine dayan Optimizasyon, bir problemde belirli koşullar altında mümkün olan alternatifler içinden en iyisini seçme işlemidir. Diğer bir ifadeyle istenen bir çıktıyı elde etmek amacıyla, sistem girdilerinin veya bu girdilerin değerlerinin ne olacağını belirleme sürecidir.

Günümüz küresel ve teknolojik gelişmeleri karşısında optimizasyon yöntemleri veya algoritmaları mühendislik, yapay zeka, veri analitiği, sağlık ve lojistik gibi birçok alanda kullanım imkanı bulmaktadır (Adeniran, Efunniyi, Osundare, & Abhulimen, 2024; Javaid, Haleem, Singh, & Suman, 2022). Big data uygulamaları ve veri miktarındaki artış, daha karmaşık ve büyük hacimli problemlerin çözülmesini gerektirmektedir. Bu nedenle, modern optimizasyon yöntemlerinin önemi her geçen gün artmaktadır. Modern meta-sezgisel yöntemler, özellikle doğadan esinlenerek oluşturulan algoritmalar karmaşık problemlere hızlı ve etkili çözümler sunabilmektedir.

Optimizasyon yöntemleri antik dönemde geometri problemlerinden günümüzde doğadan esinlenen optimizasyon tekniklerine kadar pek çok süreçten geçmiştir (Kochenderfer, 2019). Alridha ve arkadaşlarının (2024) yaptığı bir inceleme, optimizasyon algoritmalarının makine öğrenimi, fizik, kimya ve mühendislik dahil olmak üzere çeşitli alanlarda giderek daha karmaşık sorunları çözmek için kullanıldığını ve yüksek doğruluk ve performans sağladığını vurgulamaktadır. Sanayi uygulamalarında, biyolojik esinli optimizasyon teknikleri karmaşık mühendislik problemlerine yönelik etkili çözümler sunmaktadır. Markov Karar Süreçleri (MDP) de robotik, radar takibi, tıbbi tedaviler ve karar verme uygulamaları gibi alanlarda geniş bir kullanım alanına sahiptir. Waqas (2024), MDP tabanlı tekniklerin özellikle pekiştirmeli öğrenmede etkili olduğunu ve dinamik ortamlarda karar verme süreçlerinde önemli bir rol oynadığını vurgulamaktadır.

Bu çalışmada çok geniş bir alan olan optimizasyon içerisinde özellikle doğadan esinlenen meta-sezgisel optimizasyon algoritmaları hakkında temel bilgileri ve güncel kullanım örneklerini sunmak ve ilgili kişilere temel düzeyde bilgiler vermek amaçlanmıştır.

1.1. Optimizasyonda Temel Kavramlar

Optimizasyonda temel kavramlar, bir problemin doğru bir şekilde tanımlanması, analiz edilmesi, modellenmesi ve çözülmesi için gereken unsurlardır. Karar değişkenleri, bir optimizasyon probleminde belirlenmesi gereken ve çözümün sonucunu doğrudan etkileyen faktörlerdir (Ma vd., 2015). Bir üretim problemi ele alındığında, üretilmesi gereken ürünlerin miktarı karar değişkenleri olarak kabul edilerek problemin yapısına göre belirli sınırlamalar ve koşullar altında optimum değerlere ulaşılır.

Bir optimizasyon probleminin çözüm sürecinde asıl hedef, amaç fonksiyonu adı verilen matematiksel ifadeyi en iyi şekilde optimize etmektir (Gunantara, 2018). Amaç fonksiyonu, problemde minimize veya maksimize edilmek istenen değeri temsil eder ve genellikle karar değişkenlerinin bir fonksiyonu olarak tanımlanır. Bir şirketin kârını maksimize etmeye çalışırken kârı temsil eden fonksiyon, problemin amaç fonksiyonudur.

Optimizasyon problemlerinde, karar değişkenlerinin belirli sınırlar içinde kalmasını sağlayan kısıtlar da önemli bir role sahiptir (Kaltinska, 2013). Kısıtlar, bir problemin gerçek dünya koşullarını yansıtan ve çözüm uzayını daraltan kurallardır. Bir fabrikanın belirli miktarda hammaddeye sahip olması ve bu durumun üretim miktarını sınırlandırması bir kısıt olarak işlev görür.

Çözüm uzayı, optimizasyon sürecinde karar değişkenlerinin alabileceği tüm olası kombinasyonların bir araya geldiği alanı ifade eder (Zimmermann & von Hoessle, 2013). Bu uzayda yer alan her bir çözüm, belirli bir kombinasyonu temsil eder. Eğer bir çözüm tüm kısıtları sağlıyorsa buna uygun çözüm denir. Örneğin, bir diyet programı oluşturulurken besinlerin günlük kalori ve besin değeri gereksinimlerini karşılayan her kombinasyon uygun çözümdür.

Optimizasyon sürecinin nihai hedefi, optimum çözüm olarak adlandırılan en iyi çözümü bulmaktır (Kernighan & Lin, 1973). Optimum

çözüm, uygun çözümler arasında amaç fonksiyonunun şartlarını en iyi şekilde karşılayan çözümdür. Çözüm uzayında bazen birden fazla yerel optimum (belirli bir bölgede en iyi çözüm) bulunabilir, ancak optimizasyonun nihai hedefi, tüm çözüm uzayında en iyi olan genel optimumu (global optimum) bulmaktır.

Son olarak, bir optimizasyon probleminin çözümü sırasında amaç fonksiyonunun aldığı en iyi değer hedef değeri olarak adlandırılır. Bu değer, problemde belirlenen tüm kısıtlar altında elde edilebilecek en iyi sonuçtur. Bir maliyet minimizasyon probleminde hedef değeri, elde edilebilecek minimum maliyettir.

2. OPTİMİZASYON YÖNTEMLERİ

Optimizasyon yöntemleri, bir problemin çözümünde en iyi sonuca ulaşmak için kullanılabilecek farklı yaklaşımları ifade eder. Problem yapısına, karmaşıklığına ve çözüm gereksinimlerine göre çeşitlilik gösterir. Bu yöntemler genel olarak şu şekilde gruplanabilir;

Analitik yöntemler (Matematiksel Modeller),
Sezgisel yöntemler,
Meta-sezgisel yöntemler.

Analitik yöntemler genellikle daha küçük ve basit problemler için uygunken, sezgisel ve meta-sezgisel yöntemler daha karmaşık ve büyük ölçekli problemler için kullanılır (Hatami, 2018).

Analitik yöntemler, problemin matematiksel olarak modellenmesiyle ve belirli denklemlerin çözümüyle elde edilen yöntemlerdir. Kesin çözümler sunarlar ancak büyük boyutlu ve karmaşık problemlerde çözüm süresi çok uzun olabilir veya sonuca ulaşmak zorlaşabilir (Bieniasz, 2015). Doğrusal Programlama, Kuvvet Yöntemi, Karma Tamsayılı Programlama, Newton-Raphson Yöntemi ve Dinamik Programlama Analitik yöntemlere örnek olarak verilebilir. Bu yöntemlerin her biri farklı problem yapıları ve çözüm gereksinimleri için uygun olabilir.

Sezgisel yöntemler, optimizasyon problemlerini çözmek için kullanılan ve belirli bir problemi tam olarak çözmek yerine, çözüm sürecini hızlandırmayı ve makul bir sürede "iyi" bir çözüm bulmayı amaçlayan yaklaşımlardır. Optimum çözümü her zaman garanti etmezler, ancak analitik yöntemlere kıyasla daha hızlı sonuçlar verirler. Bu yöntemler, belirli bir algoritmayı veya kural setini takip eder ve genellikle belirli bir problem tipi için özelleştirilmiş stratejiler kullanır (Ouassam, Hmina, Bouikhalene, & Hachimi, 2021). Sezgisel yöntemlere örnek olarak Johnson Algoritması, Pozisyon Ağırlığı Yöntemi, En Yakın Komşu Algoritması, Tabu Arama, Yerel Arama Algoritması, Simüle Tavlama (Simulated Anneaing), Genetik Algoritmalar, Kısmi Çözümleme ve Greedy (Açgözlü) Algoritması verilebilir.

Meta-sezgisel yöntemler, optimizasyon problemlerini çözmek için kullanılan ve çeşitli sezgisel yöntemleri birleştirerek daha genel ve esnek bir çözüm sunmak üzere tasarlanmış algoritmalardır. Meta-sezgisel yöntemlerin en önemli özelliklerinden birisi doğadaki canlıların karmaşık problemlere yaklaşımından ilham alarak geliştirilmiş olmalarıdır. Bu algoritmalar, ilgili canlının doğada bir problemi çözerken izlediği süreç ve ortaklaşa çalışma tekniklerini esas alır.

3. OPTİMİZASYON ALGORİTMALARI

Optimizasyon algoritmaları, bir problemi en iyi şekilde çözmek amacıyla hedef fonksiyonun minimum veya maksimum değerini bulmayı amaçlayan yöntemlerdir. Çeşitli problemlerde optimum çözümleri bulmak için uygulanır. Bu çalışmada yaygın olarak kullanılan şu optimizasyon algoritmaları hakkında bilgi verilerek güncel kullanım örnekleri sunulmuştur;

Dijkstra Algoritması
Bellman-Ford Algoritması
A* Arama Algoritması
Ateş Böceği Algoritması
Karınca Koloni Optimizasyonu
Kurt Kolonisi Algoritması
Yapay Balık Sürüsü Algoritması

3.1. Dijkstra Algoritması

Dijkstra Algoritması, bir kaynak noktadan bir grafik (graph) üzerindeki diğer tüm düğümlere (noktalar) olan en kısa yolları bulmayı amaçlar. Çalışma prensibi, başlangıç noktasından hareketle komşu düğümlerin maliyetini (mesafe) belirleyip, her adımda en düşük maliyetli düğümü

seçerek ilerlemektir. Bu işlem, tüm düğümler en kısa yolla ziyaret edilene kadar tekrarlanır ve böylece kaynak düğümden diğer tüm düğümlere en kısa yollar hesaplanır (Candra, Budiman, & Hartanto, 2020). Dijkstra Algoritması, pozitif ağırlıklı grafiklerde etkili bir şekilde çalışır.

Dijkstra Algoritması, en kısa yolu bulmadaki verimliliği nedeniyle çeşitli alanlarda pek çok uygulama örneğine sahiptir. Önemli bir kullanım örneği olan kentsel alanlarda araç yönlendirmesinde trafik sıkışıklığını, seyahat süresi güvenilirliğini ve eşdeğer yolların ağırlığını dikkate alarak en optimal rotayı oluşturur ve seyahat verimliliğini artırır (Utomo ve ark., 2023). Diğer bir uygulama ise turizm rota planlamasıdır. Talunohi, Sembiring, Khairina, Novita, Anisa ve Rambe (2023), birden fazla plaj konumunu ziyaret etmek için en verimli rotaları belirleyerek, Nias Adası'ndaki turistik noktalara en kısa yolu sunmaya çalışmıştır. Dijkstra Algoritması, quadrotor İHA›lar için yolculuk planlamasında kullanılmaktadır; minimum ivme/sn yaklaşımı ile entegre edilerek optimal yollar üretilir ve karmaşık ortamlardaki İHA hareketlerinin hassasiyetini arttırır (Cai ve ark., 2024). Lojistik sektöründe de Dijkstra Algoritması'ndan yararlanılarak teslimat rotaları optimize edilir. Endonezya'daki J&T Express uygulamasında paket teslimatları için seyahat mesafeleri ve süreleri uygun şekilde minimize edilmeye çalışılmıştır (Lusiani ve ark., 2023). Dijkstra Algoritması'nın modifiye edilmiş bir versiyonu, en kısa yolun kaza veya yol çalışması gibi kısıtlamalar nedeniyle ulaşılamaz olduğu durumlarda alternatif yollar bulmak için geliştirilmiştir ve bu sayede verimli navigasyon ve güvenlik sağlanmıştır (Gbadamosi & Aremu, 2023).

3.2. Bellman-Ford Algoritması

Bellman-Ford Algoritması, ağırlıklı bir grafikteki bir kaynaktan tüm diğer düğümlere en kısa yolu bulmayı amaçlar ve özellikle negatif ağırlıklı kenarların bulunduğu grafikleri de değerlendirebilmesiyle Dijkstra Algoritmasından ayrılır. Algoritma, her kenarı ve düğümü tekrarlı bir şekilde gözden geçirerek olası tüm yolların uzunluklarını güncelleyerek çalışır. Her döngüde (iterasyonda), bir düğümden diğerine olan uzaklıklar kontrol edilir ve daha kısa bir yol bulunursa bu yol güncellenir (Parimala, Broumi, Prakash, & Topal, 2021). Bu işlem, grafikteki düğüm sayısı kadar tekrarlandığında, en kısa yolların tamamı elde edilmiş olur.

Bellman-Ford algoritması, negatif ağırlıklı döngüleri de tespit edebildiğinden dolayı finansal analizlerde (kâr fırsatları), yol bulma ve ağ analizlerinde kullanım alanı bulmaktadır. 2020 yılında yapılan bir çalışmada, Bellman-Ford algoritması kullanılarak sosyal medya ağlarındaki yalancı hesapların tespit edilmesi amaçlanmıştır (Liu vd., 2020). Çalışmada kullanıcılar arası etkileşim verileri kullanılarak oluşturulan ağ grafiğinde, yalancı hesapların gerçek kullanıcılardan farklı davranış sergilediği belirlenmiştir. Başka bir çalışmada Chen vd. (2021), eğitim verilerinin sezgisel olarak seçilmesinde, Zhang vd. (2021) makine öğrenme modellerinin hiperparametre optimizasyonunda bu algoritmadan faydalanmıştır.

3.3. A* Algoritması

A* Algoritması, en kısa yol problemlerini çözmek için kullanılan ve kaynak bir noktadan hedefe en hızlı şekilde ulaşmayı hedefleyen bir arama algoritmasıdır. Çalışma prensibi olarak yol maliyetini hesaplama içerdiğinden Dijkstra algoritmasına benzemektedir. Bunun yanı sıra hedefe olan tahmini uzaklığı da göz önünde bulundurur (heuristic). Algoritma her düğüm için yol maliyeti ve tahmini maliyetin toplamını hesaplar ve bu toplamı minimize ederek hedefe ulaşan en hızlı yolu bulmaya çalışır (XiangRong, Yukun ve XinXin, 2021). A* Algoritması, her adımda en düşük toplam maliyetli düğümü seçerek bir sonraki gideceği düğümü seçer ve böylece arama işlemini daha verimli hale getirir. Özellikle oyun geliştirme, robotik navigasyon, harita uygulamaları, GPS yönlendirme sistemleri ve rota belirlenmesi gibi alanlarda, bir kaynaktan hedefe en kısa veya en uygun yolun bulunması gereken problemlerde yaygın olarak kullanılır.

Yakın tarihli çalışmalar incelendiğinde A* algoritmasının güncel olarak birçok alanda etkin bir şekilde kullanıldığı görülmektedir. Navigasyon Sistemleri için geliştirilen bir uygulamada, altıgen grid tabanlı bir A* algoritması, hareket maliyetini optimize ederek navigasyon sistemlerin-

de daha verimli yol planlaması sağlar (Zehua & Rui, 2024). Dijital Kaya Fiziği üzerine yapılan bir çalışmada, kaya rezervuarlarının gözeneklilik ve geçirgenlik özelliklerinin belirlenmesi için kullanılmıştır (Raeli, Salina Borello, Panini, Serazio ve Viberti, 2024). Uydu Transfer Sistemleri için ise CubeSat uydu kümelerinin yörüngede daha etkin yer değiştirmesini sağlamak amacıyla A* algoritması kullanılarak platform kararlılığının korunması ve uydu transfer verimliliğinin arttırılması sağlanmıştır (Xu, Yue, Zhao, Yang, Wu, Pan, Tang ve Zhang, 2024). Otonom Sualtı Araçları (AUV) için A* algoritması enerji tüketimini optimize eder ve bu araçların daha verimli yol planlaması yapmalarını sağlar (Wu ve ark., 2024). Do ve ark. (2024) ise mobil robotların karmaşık ortamlarda hızlı hesaplama ve optimal yol planlaması işlemi için A* algoritmasını kullanarak robotun çeşitli engeller arasında en iyi rotayı bulmasına yardımcı olmuştur.

3.4. Ateş Böceği Algoritması

Ateş Böceği Algoritması (Firefly Algorithm), doğada ateş böceklerinin iletişim ve eş bulma davranışlarını taklit eden bir optimizasyon yöntemidir. Optimizasyon problemlerini çözmek için ateş böceklerinin birbirlerini çekme davranışını taklit eder. Çalışma prensibi, her bireyin bir «parlaklık» değeri ile temsil edilmesi ve bu değerlerin en yüksek olan bireylerin diğerleri tarafından çekici bulunarak daha fazla etkileşimde bulunmaları üzerine kuruludur. Ateş böcekleri parlaklıklarına göre birbirlerine doğru hareket ederler ve daha parlak olan ateş böceğine yaklaşarak optimum çözüme ulaşırlar (Jain, Sharma ve Sharma, 2021). Bu şekilde, bireyler en iyi çözümü bulmak için bir araya gelirler.

Ateş Böceği Algoritması farklı disiplinlerde çeşitli problemlerin çözümü için yaygın olarak kullanılmaktadır. Özellikle büyük veri analitiğinde, sağlık sektörü ve mühendislik alanlarında etkili bir optimizasyon aracı olarak öne çıkmaktadır (Rahul & Banyal, 2020). Bu algoritma, sağlık sektöründe hasta bakımı, kişiselleştirilmiş bakım ve sağlık sonuçlarının tahmini gibi uygulamalarda büyük veri analizini optimize etmek için kullanılmıştır. Ayrıca kesintisiz değişkenlere sahip olmayan optimizasyon problemleri için de kullanılmaktadır. İkili ve tamsayı değerli problemler gibi süreksiz değişkenli problemlerde algoritmanın çeşitli modifikasyonlarıyla etkili sonuçlar elde edilmiştir (Tilahun & Ngnotchouye, 2016). Öngörü ve hibrit örnek öğrenmeye dayalı modifikasyonlar, algoritmanın yakınsama hızını artırarak daha yüksek çözüm doğruluğu sağlamaktadır (Chen & Li, 2023).

3.5. Karınca Koloni Algoritması

Karınca Koloni Algoritması (KKA, Ant Colony Optimization, ACO), karınca kolonilerinin yiyecek arama davranışlarından esinlenerek geliştirilmiş bir optimizasyon yöntemidir. Algoritmanın temelinde karıncaların yiyecek bulmak için çevrede dolaşırken bıraktıkları feromon isimli kimyasal maddenin diğer karıncaların rotalarını etkilemesi vardır. Bu prensibe göre karıncaların en çok kullandığı yani en kısa veya en uygun yol üzerinde daha yoğun feromon birikimi olur, yol zamanla belirginleşir ve karıncalar bu yolu tercih eder (Singh, Meena ve Yang, 2020).

Karınca Koloni Algoritması, ulaştırma, telekomünikasyon, robotik ve veri madenciliği gibi birçok alanda kullanılmaktadır. Telekomünikasyon ağlarındaki uygulamalardan biri, ağ kaynaklarının tahsis edilmesidir. Berlíński ve arkadaşlarının (2023) çalışması algoritmanın 5G ağlarında ağ kapasitesini optimize etme, kayıpları azaltma ve verimliliği artırmadaki etkinliğini ortaya koymuştur. Geliştirilmiş bir KKA, Xiong ve Wang (2023) tarafından kablosuz iletişim ağlarında anormal sinyallerin tespiti için kullanılmış ve geleneksel algoritmalara göre daha yüksek performans göstermiştir. Bir diğer uygulamada, KKA, araç rotalama sorunlarının çözümünde kullanılmış ve şirketlerin taşıma maliyetlerini azaltmasına ve rotaları optimize etmesine yardımcı olmuştur. Bu süreçte, Graf Sinir Ağları (GNN) algoritmanın yakınsama hızını artırmada etkili olmuştur (Wang & Jin, 2023).

3.6. Kurt Kolonisi Algoritması

Kurt Koloni Algoritması (KKA), doğadaki kurtların avlanma ve sosyal davranışlarını örnek alarak geliştirilmiş bir algoritmadır. Doğada kurt sürüsü lider kurdu takip ederek hareket eder ve en iyi avlanma noktalarını keşfederler. Bu durumun bilgisayarda simüle edilmesi ile yazılım ta-

rafından çeşitli çözüm adayları oluşturulur ve en uygun olanlar seçilir (Wu ve Zhang, 2014).

Kurt Koloni Algoritması (Wolf Pack Algorithm - WPA), makine öğrenmesi, mühendislik tahmini, süreç kontrolü, uçak rotası planlaması ve enerji sistemleri gibi çeşitli alanlarda kullanılmaktadır. Peng ve arkadaşları (2024), WPA'nın Yapay Arı Koloni Algoritması (ABC) ile kıyaslandığında farklı özelliklere sahip CEC test fonksiyonlarında optimize etme yeteneğini ve hızlı yakınsama özelliğini göstermiştir. Ahmad ve arkadaşları (2024), Gri Kurt Algoritması'nın (Grey Wolf Optimization - GWO) WPA'nın unsurları ile birleştirilmesiyle elde edilen geliştirilmiş bir yöntemi kullanarak optimizasyon problemlerinde üstün performans elde etmişlerdir. WPA, ayrıca insansız hava araçları (UAV) için çok amaçlı rota planlamasında da kullanılmış ve karmaşık çevrelerde en kısa ve en optimize rotaların belirlenmesinde başarılı olmuştur (Li, Wei, Xie ve Wei, 2023).

3.7. Yapay Balık Sürüsü Algoritması (Artificial Fish Swarm Algorithm)

Bu algoritma optimizasyon problemlerini çözmek için doğadaki balıkların sürüler halinde hareket etme davranışını taklit eder ve sürünün yiyecek arama davranışlarını modellemeye çalışır. Balıklar, çevrelerindeki besin kaynaklarını ve diğer balıkları gözlemleyerek, en iyi çözümleri bulmak için birlikte hareket ederler. Her balık, belirli bir çözümü temsil eder ve besin kaynaklarına yakınlığına göre hareket eder. Çalışma adımları şu şekildedir; Her bir balık çevresini keşfeder ve daha iyi besin kaynağına doğru ilerler. Bir balık, çevresindeki diğer balıkların daha iyi bir konumda olduğunu fark ederse, onları takip eder (Darvishpoor, Darvishpour, Escarcega ve Hassanalian, 2023). Balıklar daha fazla besin kaynağı olan bölgelere doğru birlikte hareket ederler.

Yapay Balık Sürüsü Algoritması (YBSA) farklı uygulama alanlarında kullanılmaktadır. YBSA kullanılarak geliştirilen bir yöntemle akıllı ulaşım sistemlerinde trafik akışının optimize edilmesi hedeflenmiştir (Wang vd., 2015). Araştırmacılar, farklı senaryolar için algoritmanın performansını karşılaştırmışlardır. Huang vd. (2016) görüntü işleme alanında tanımlama problemlerine yönelik yaptığı çalışmalarında YBSA'yı kullanarak yüz tanıma gerçekleştirmişlerdir. Wang vd. (2019) derin sinir ağlarının eğitimi için, Zhang vd. (2020) ise veri madenciliği görevlerinde bu algoritmadan faydalanmışlardır.

4. SONUÇ

Bellman-Ford, A*, Ateş Böceği, Karınca Koloni ve Kurt Kolonisi algoritmaları, farklı yaklaşım ve prensiplerle çalışsalar da, hepsinin en iyi çözümü bulma süreçlerinde etkili araçlar olarak kullanıldığı ilgili literatürde görülmektedir. Bu algoritmalar, belirli bir probleme en iyi çözümü bulmak için doğadaki canlıların davranışlarından esinlenerek ya da taklit ederek geliştirilmiştir ve farklı problemlere göre uyarlanabilirler. Matematiksel ve sezgisel yaklaşımları birleştirerek karmaşık problemlere hızlı ve etkili çözümler sunabilirler. Bu algoritmalar, çeşitli türde problemler için başarılı sonuçlar elde ederek, yapay zekâ, robotik ve mühendislik gibi disiplinlerde geniş uygulama alanı bulmaktadır.

Bakteriyel Besin Arama, Kedi Sürüsü Optimizasyonu, Genetik Algoritma, Karınca Kolonisi Optimizasyonu, Parçacık Sürü Optimizasyonu, Yapay Arı Kolonisi, Diferansiyel Gelişim Algoritması, Benzetim Tavlama, Yerçekimi Arama Algoritması, Gaz Brownian Hareketi Optimizasyonu, Isı Transferi Arama, Elektromanyetik Alan Optimizasyonu, Optikten Esinlenen Optimizasyon, Ağırlıklı Süperpozisyon Çekimi, Orman Optimizasyonu Algoritması, Kasırga Temelli Optimizasyon Algoritması ve Ağaç-Tohum Algoritması gibi diğer algoritmalar da literatürde önemli bir yer tutmakla birlikte, bu çalışmada kapsam dışında bırakılmıştır. Gelecek çalışmalarda bu algoritmaların tekil veya kombinasyonlar halinde kullanılması üzerinde durmak faydalı olacaktır.

Optimizasyon algoritmaları gelecekte hızla artan veri miktarı ve günümüz dünyasındaki gelişmelere paralel olarak önemli bir evrim geçirecektir. Özellikle meta-sezgisel ve doğadan esinlenen algoritmalar, karmaşık dünya problemlerine daha etkili çözümler sunma potansiyeline sahiptir.

5. KAYNAKÇA

Adeniran, I. A., Efunniyi, C. P., Osundare, O. S., & Abhulimen, A. O. (2024). Optimizing logistics and supply chain management through advanced analytics: Insights from industries. Engineering Science & Technology Journal, 5(8).

Ahmad, I., Qayum, F., Ur Rahman, S., & Srivastava, G. (2024). Using Improved Hybrid Grey Wolf Algorithm Based on Artificial Bee Colony Algorithm Onlooker and Scout Bee Operators for Solving Optimization Problems. *International Journal of Computational Intelligence Systems*. https://doi.org/10.1007/s44196-024-00497-6

An, Z., Rui, X., & Gao, C. (2024). Improved A* Navigation Path-Planning Algorithm Based on Hexagonal Grid. ISPRS Int. J. Geo-Inf., 13(5), 166. doi: 10.3390/ijgi13050166

Berliński, M., Rasmus, M., Kopertowski, Z., & Kozdrowski, S. (2023). Ant Colony Algorithms Application for Telco Networks Performance with Multi-criteria Optimization.

Bieniasz, L. (2015). Analytical Solution Methods. https://doi.org/10.1007/978-3-662-44882-3_11

Cai, Z., Selezneva, M. S., & Yang, M. (2024). Dijkstra algorithm based minimum acceleration/snap quadrotor UAV trajectory planning. *J. Phys. Conf. Ser.*, 2746(1), 012028. doi: 10.1088/1742-6596/2746/1/012028

Candra, A., Budiman, M. A., & Hartanto, K. (2020, July). Dijkstra's and a-star in finding the shortest path: A tutorial. In 2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA) (pp. 28-32). IEEE.

Chen, L., & Li, J. (2023). A Firefly Algorithm Based on Prediction and Hybrid Samples Learning. In *Lecture Notes in Computer Science*.

Chen, S., Zhang, H., Xu, Z., He, X., Kang, S., & Li, M. (2021). A review of deep learning for big data. *Information Fusion*, 76, 15-38. https://doi.org/10.1016/j.inffus.2021.03.006

Darvishpoor, S., Darvishpour, A., Escarcega, M., & Hassanalian, M. (2023). Nature-inspired algorithms from oceans to space: A comprehensive review of heuristic and meta-heuristic optimization algorithms and their potential applications in drones. Drones, 7(7), 427.

Derrick, D., Utomo, M., Aurelia, S. M., Tanasia, N., Nurhasanah, A. T., & Handoyo, T. (2023). Implementation of Dijkstra Algorithm in Vehicle Routing to Improve Traffic Issues in Urban Areas, 73-78. 2023 3rd International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS). https://doi.org/10.1109/icon-sonics59898.2023.10435225

Do, Q. V., Bui, T. A., & Nguyen, T. H. (2024). An Efficient Improved A* Algorithm for Mobile Robot Path Planning in Complex Environments. *Proceedings of IEEE ICCC*.

Gbadamosi, O. A., & Aremu, D. R. (2023, February). Modification of Dijkstra's Algorithm for Best Alternative Routes. In International Congress on Information and Communication Technology (pp. 245-264). Singapore: Springer Nature Singapore.

Gunantara, N. (2018). A review of multi-objective optimization: Methods and its applications. Cogent Engineering, 5(1), 1502242.

Hasan, A., Alsharify, F., & Al-Khafaji, Z. (2024). A Review of Optimization Techniques: Applications and Comparative Analysis. Iraqi Journal For Computer Science and Mathematics, 5(2), 122–134. doi: 10.52866/ijcsm.2024.05.02.011

Hatami, M. (2018). Introduction to Analytical Methods. https://doi.org/10.1016/B978-0-12-813218-0.00001-7

Huang, X., Li, L., & Wang, M. (2016). Face recognition based on artificial fish swarm algorithm. *Neurocomputing*, 171, 623-632. https://doi.org/10.1016/j.neucom.2015.02.034

Jain, A., Sharma, S., & Sharma, S. (2021). Firefly algorithm. Nature-Inspired Algorithms Applications, 157-180.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2022). Artificial intelligence applications for industry 4.0: A literature-based study. Journal of Industrial Integration and Management, 7(01), 83-111.

Jeprin, T., Zulfikar, S., Khairina, N., Novita, N., Anisa, Y., & Rambe, S. (2023). Analysis of the Dijkstra Algorithm in Determining The Shortest Route to Tour the Beaches of Nias Island. 2023 International *Conference of Computer Science and Information Technology (ICOSNIKOM).* https://doi.org/10.1109/icosnikom60230.2023.10364421

Kaltinska, R. (2013). Optimizing under constraints. Bringing Mathematics To Earth, 53.

Kernighan, B. W., & Lin, S. (1973). Heuristic solution of a signal design optimization problem. The Bell System Technical Journal, 52(7), 1145-1159.

Khan, Q. W. (2024). Exploring Markov Decision Processes: A Comprehensive Survey of Optimization Applications and Techniques. Igmin Research, 2(7), 508–517. https://www.igminresearch.com/articles/html/igmin210 adresinden alınmıştır.

Kochenderfer, M. J. (2019). *Algorithms for Optimization*. The MIT Press Cambridge.

Li, G. G., Wei, J. J., Xie, F. X., & Wei, S. S. (2023). Multi-objective UAV Trajectory Planning Based on Improved Wolf Pack Algorithm Improved Wolf Pack Algorithm. ACM Other conferences. Association for Computing Machinery. doi: 10.1145/3625403.3625429

Liu, L.-s., Lin, J.-f., Yao, J.-x., He, D.-w., Zheng, J.-s., Huang, J., & Shi, P. (2021). Path Planning for Smart Car Based on Dijkstra Algorithm and Dynamic Window Approach. *Wireless Communications and Mobile Computing*, 2021(1), 8881684. https://doi.org/10.1155/2021/8881684

Liu, Q., Chen, E., Chen, C., & Jiang, X. (2020). Detecting fake accounts in online social networks using graph topological features. *Information Processing & Management*, 57(4), 102236. https://doi.org/10.1016/j.ipm.2020.102236

Lusiani, A., Purwaningsih, S. S., & Sartika, E. (2023). Dijkstra Algorithm In Determining The Shortest Route For Delivery Service By J&T Express In Bandung. Jurnal Lebesgue: Jurnal Ilmiah Pendidikan Matematika, Matematika dan Statistika, 4(2), 940-948.

Ma, X., Liu, F., Qi, Y., Wang, X., Li, L., Jiao, L., ... & Gong, M. (2015). A multiobjective evolutionary algorithm based on decision variable analyses for multiobjective optimization problems with large-scale variables. IEEE Transactions on Evolutionary Computation, 20(2), 275-298.

Ouassam, E., Hmina, N., Bouikhalene, B., & Hachimi, H. (2021). Heuristic Methods: Application to Complex Systems. https://doi.org/10.1109/ICOA51614.2021.9442647

Parimala, M., Broumi, S., Prakash, K., & Topal, S. (2021). Bellman–Ford algorithm for solving shortest path problem of a network under picture fuzzy environment. Complex & Intelligent Systems, 7, 2373-2381.

Peng, Q., Zhan, R., Wu, H., & Shi, M. (2024). Comparative Study of Wolf Pack Algorithm and Artificial Bee Colony Algorithm. *International Journal of Swarm Intelligence Research*. https://doi.org/10.4018/ijsir.352061

Raeli, A., Salina Borello, E., Panini, F., Serazio, C., & Viberti, D. (2024). A parallel programming application of the A* algorithm in digital rock physics. Comput. Geosci., 187, 105578. doi: 10.1016/j.cageo.2024.105578

Rahul, K., & Banyal, R. K. (2020). Firefly algorithm: an optimization solution in big data processing for the healthcare and engineering sector. Int. J. Speech Technol., 24(3), 581–592. doi: 10.1007/s10772-020-09783-y

Singh, P., Meena, N. K., & Yang, J. (2020). Ant colony optimization, modifications, and application. In Swarm Intelligence Algorithms (pp. 1-14). CRC Press.

Talunohi, J., Sembiring, Z., Khairina, N., Novita, N., Anisa, Y., & Rambe, Y. S. (2023, November). Analysis of the Dijkstra Algorithm in Determining The Shortest Route to Tour the Beaches of Nias Island. In 2023 International Conference of Computer Science and Information Technology (ICOSNIKOM) (pp. 1-5). IEEE.

Tilahun, S. L., & Ngnotchouye, J. M. T. (2016). Firefly Algorithm for optimization problems with non-continuous variables: A Review and Analysis. arXiv, 1602.07884. https://arxiv.org/abs/1602.07884v1 adresinden alınmıştır.

Wang, G., Zhang, X., & Wang, J. (2019). Artificial fish swarm algorithm optimized deep belief networks for intrusion detection. *Knowledge-Based Systems*, 163, 848-861. https://doi.org/10.1016/j.knosys.2018.08.017

Wang, J., Liang, Y., & Huang, H. J. (2015). Traffic signal optimization selection using artificial fish swarm algorithm. *Transportation Research Part C: Emerging Technologies*, 55, 460-473. https://doi.org/10.1016/j.trc.2015.03.014

Wang, X., & Jin, Y. (2023). An Ant Colony Algorithm Assisted by Graph Neural Networks for Solving Vehicle Routing Problems. ACM Conferences. Association for Computing Machinery. doi: 10.1145/3583133.3596424

Wu, G., Li, W., Li, J., Jiang, G., & Cheng, Y. . Improved A* Algorithm AUV Path Planning Based on Multi-Thread Parallelism and CUDA Optimization. 2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE. doi: 10.1109/AINIT61980.2024.10581438

Wu, H. S., & Zhang, F. M. (2014). Wolf pack algorithm for unconstrained global optimization. Mathematical Problems in Engineering, 2014(1),

465082.

XiangRong, T., Yukun, Z., & XinXin, J. (2021, February). Improved A-star algorithm for robot path planning in static environment. In Journal of Physics: Conference Series (Vol. 1792, No. 1, p. 012067). IOP Publishing.

Xu, D., Yue, H., Zhao, Y., Yang, F., Wu, J., Pan, X., ...Zhang, Y. (2024). Improved A* Algorithm for Path Planning Based on CubeSats In-Orbit Electromagnetic Transfer System. Aerospace, 11(5), 394. doi: 10.3390/aerospace11050394

Zhang, H., Cui, L., Neumann, M., & Chen, Z. (2021). An overview of deep learning in big data. *Information Fusion*, 76, 87-106. https://doi.org/10.1016/j.inffus.2021.03.006

Zhang, H., Liu, S., Liu, Y., & Wang, X. (2020). Artificial fish swarm algorithm optimized support vector machine for data classification. *Knowledge-Based Systems*, 195, 105708. https://doi.org/10.1016/j.knosys.2020.105708

Zimmermann, M., & von Hoessle, J. E. (2013). Computing solution spaces for robust design. International Journal for Numerical Methods in Engineering, 94(3), 290-307.

"This page is left blank for typesetting"

Bu sayfa dizgiden dolayı boş bırakılmıştır

Journal of Quantum Technologies and Informatics Research
JQTAIR

KUANTUM TEKNOLOJİLERİ VE ENFORMATİK ARAŞTIRMALARI
Volume / Cilt: 2, Issue / Sayı: 3, 2024, pp. 115-128
E - ISSN: 3023-4735
URL: https://journals.gen.tr/index.php/jqtair/
DOI: https://doi.org/10.70447/ktve.2573

Received / Geliş: 12.10.2024
Acccepted / Kabul: 25.10.2024

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Meta-Sezgisel Yöntemler ile Müzik Popülarite Sınıflandırması için Özellik Seçimi

Feature Selection with Meta-Heuristics for Music Popularity Classification

Abdurrahim Hüseyin Ezirmik[1] **İdiris Dağ**[2]

[1] Balıkesir Üniversitesi, Bilgisayar Mühendisliği Bölümü, Balıkesir, Türkiye, e-mail: huseyin.ezirmik@balikesir.edu.tr
[2] Eskişehir Osmangazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Eskişehir, Türkiye, e-mail: idag@ogu.edu.tr

Öz

Günümüzde multimedya içerik üretimi büyük bir hızla artmış, bu da değerli bilgilere erişimi zorlaştırmıştır. Anlamlı verilere ulaşımı kolaylaştırmak amacıyla veri madenciliği kritik bir hale gelmiştir ve bu süreçte önemli bir adım, veri boyutunun azaltılmasıdır. Özellik seçimi, veri kümesindeki ilgisiz, gürültülü veya eksik verilerin çıkarılmasıyla veri boyutunu küçülterek, veri analizinde kullanılan yöntemlerin daha hızlı ve verimli çalışmasını sağlar. Bu çalışmada, doğadan ilham alınan meta-sezgisel algoritmalar kullanılarak özellik seçimi gerçekleştirilmiştir. Belirlenen özellikler, makine öğrenimi algoritmaları ve yapay sinir ağları ile müzik verilerini şarkı popülerliğine göre sınıflandırmak için kullanılmıştır. Müzik veri seti üzerinde yapılan iyileştirmeler ile sınıflandırma başarımı %3.2 oranında artırılmış ve sonuç olarak %88 doğruluk elde edilmiştir. Kullanılan yöntemler karşılaştırmalı olarak sunulmuş ve elde edilen bulgular değerlendirilmiştir.

Anahtar kelimeler: Yapay sinir ağları, Metasezgisel algoritmalar, Özellik seçimi, Sınıflandırma

Abstract

In today's world, the rapid increase in multimedia content production has made accessing valuable information more challenging. Data mining has become critical to facilitate access to meaningful data, and an important step in this process is reducing the size of the data. Feature selection reduces the data size by eliminating irrelevant, noisy, or missing data from the dataset, allowing the methods used in data analysis to operate faster and more efficiently. In this study, feature selection was performed using nature-inspired metaheuristic algorithms. The selected features were used to classify music data by song popularity with machine learning algorithms and artificial neural networks. Improvements made on the dataset increased classification performance by 3.2%, achieving an accuracy of 88%. The methods used were presented comparatively, and the findings were evaluated.

Keywords: Artificial neural networks, Metaheuristic algorithms, Feature selection, Classification

Citation/Atıf: EZİRMİK, A. H. & DAĞ, İ. (2024). Meta-Sezgisel Yöntemler ile Müzik Popülarite Sınıflandırması için Özellik Seçimi. *Kuantum Teknolojileri ve Enformatik Araştırmaları*. 2(3): 115-128, DOI: 10.70447/ktve.2573

Corresponding Author/ Sorumlu Yazar:
Abdurrahim Hüseyin Ezirmik
E-mail: huseyin.ezirmik@balikesir.edu.tr

1. INTRODUCTION

In today's world, music is present in every aspect of human life. With the growing influence of the entertainment industry, the volume of music data produced is increasing over time, making it difficult for listeners to access all this data [1]. Without a good method for discovering music, a significant portion of the music produced may go unnoticed. As multimedia content expands and digital libraries continue to grow, information retrieval and access are becoming increasingly important. The aim for this work is to tackle the challenge of extracting valuable insights from audio datasets. By using feature selection with metaheuristic algorithms, the study attempts to improve computational efficiency and enhance the accuracy of music popularity prediction models.

Music data consists of several audio files. To analyze an audio file, it is first necessary to determine the type of information provided [2]. Much research has been conducted on music, speech, and sound. However, studies on songs are relatively fewer and still ongoing. Information about songs, such as lyrics, genre, and era, is shared online. Digital music serves as a source for information such as artist, track name, and year. Many operations can be performed using this information. Examples of this include track classification and song recommendation systems [3].

Recently, research on feature selection has increased for various reasons [4]. This is due to the development of new applications dealing with large amounts of data, such as data mining, medical data processing, and multimedia information retrieval. Feature selection is efficiently and widely used in classification systems [5]. Identifying distinctive features enhances recognition success. In classification using selected features, fewer operations are required, noisy and irrelevant features are removed from the original data, classification success is improved, and classification based on features becomes easier to interpret. Training time is reduced, fewer measurements are made, and less memory is used. These factors provide meaningful and easier classification.

This article is organized into several key sections that provide a comprehensive overview of the research. The Related Works section reviews existing literature on feature selection and categorization, identifying domains and advancements. The Metaheuristic Algorithms section outlines the specific algorithms used, explaining their principles and selection criteria. The Material and Methods section details the dataset and experimental procedures to ensure transparency and reproducibility. In the Results and Discussion section, findings are presented. Finally, the Conclusion summarizes the key contributions and suggests directions for future research in feature selection using metaheuristic methods.

2. RELATED WORKS

This section provides a thorough review of the contributions from numerous works on meta-heuristic algorithms and feature selection in many fields. The contributions in meta-heuristic algorithms cover a wide range of applications. For example, Tayarani et al. (2014) provided a state-of-the-art overview of meta-heuristic strategies for vehicle engine design [6], while methodologies outlining their advantages and disadvantages in dealing with reactive power planning difficulties [7] were discussed by Shaheen et al. (2018). The use of meta-heuristics in parallel computing scheduling, along with obstacles and future research prospects [8], was focused on by Memeti et al. (2018). Furthermore, the significance of meta-heuristic strategies in academic scheduling difficulties [9] was investigated by Teoh et al. (2015), and a comparative analysis of five techniques —ACO, PSO, GA, BA, and LCA— was conducted by Kalra and Singh (2015) to demonstrate their effectiveness in task scheduling for grid and cloud frameworks [10].

In the domain of feature selection, the application of feature selection in mobile malware detection was examined by Feizollah et al. (2015), providing a detailed overview of its significance [11]. Feature selection strategies used in sentiment analysis and their application in opinion mining [12] were briefly reviewed by Asghar et al. (2014). Finally, Saeys et al. (2007) concentrated on bioinformatics, offering a basic taxonomy of feature selection approaches and discussing

their usefulness in both classic and developing bioinformatics applications [13].

Recent studies using metaheuristic methods in the field of music are generally based on music generation [14-16]. This work stands out by applying nature-inspired meta-heuristic algorithms specifically for feature selection in music data, focusing on song popularity prediction. Unlike previous studies that cover various fields, this research targets a unique challenge in the music domain.

3. METAHEURISTIC ALGORITHMS

The term metaheuristic refers to an algorithmic framework that provides guidance or strategies for the development of different heuristic optimization algorithms, independent of the problem at hand [17]. This term is also used to describe the specific application of a heuristic optimization algorithm to a given problem. Technically, the term metaheuristic was first introduced by Fred Glover in 1986, combining the Greek word "meta" with "heuristic," meaning higher-level heuristic [18].

A higher-level heuristic approach involves methods that perform a probabilistic yet conscious search in the solution space [19]. These methods generate new solutions by starting from the set of solutions created at each step. Thus, by searching near the points that are closest to the optimum in the search space, they aim to reach the optimal solution while avoiding local optima selection [20].

Metaheuristic methods are techniques that direct the search process. They aim to explore the search space efficiently to obtain the best or near-optimal results. These methods span from local search techniques to complex learning processes. Typically, they offer an approximate solution that is non-deterministic. They are not limited to solving a specific problem but provide solutions to different types of problems. They are designed in a way that prevents convergence to local solutions in the search space.

For metaheuristic algorithms to produce good results, it is essential that the fundamental concepts of the method are well adapted to the problem. There are many types of metaheuristic algorithms [21]. Algorithms inspired by nature imitate the behavior patterns of living beings in natural environments. Some are population-based, while others are individual-based. Their objective functions can be either static or dynamic. They can be classified based on whether or not they use neighborhood structures or memory. These methods are seen as the nature-inspired extensions of classical heuristic algorithms. The variety of algorithms has increased as they have been developed for optimization purposes based on various scientific fields.

3.1. Ant Colony Algorithm

Ant Colony Optimization (ACO) is a metaheuristic method developed to solve difficult optimization problems. It is inspired by the behavior of real ants, which use the pheromone hormone they secrete in their natural environment as a means of communication [22]. Similar to the biological example, this optimization method is based on the indirect communication established through pheromone trails in an artificial ant colony. Pheromones serve as distributed, numerical information that ants use to probabilistically generate solutions to a problem, reflecting their search experience and adapting during the execution of the algorithm.

Real ants perform complex tasks, such as finding the shortest path to food sources and transporting the obtained food back to the nest, through collective behavior. The ant colony algorithm mimics the principle of how an ant colony can find the shortest path between two points using a simple communication mechanism [23]. There is a path that ants with poor vision can travel between the nest and the food source. During their trips, ants leave a chemical trail (pheromone) on the ground. Pheromone is a volatile substance with a distinct smell. This trail plays a role in guiding other ants toward the target point [24]. As the amount of pheromone on a certain path increases, the probability of ants choosing that path also increases.

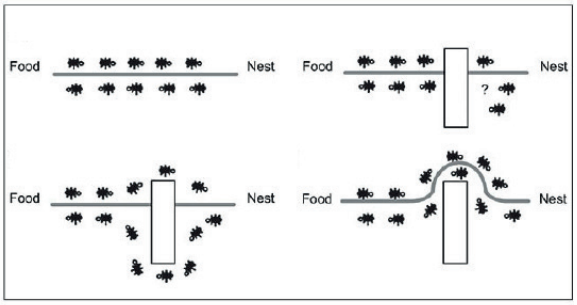


Figure 1. An ant colony searching for the best path between food and the nest [25]

Additionally, this chemical substance has a diminishing effect over time as it evaporates, and the amount of this substance secreted by an ant depends on the amount of food in the environment. As shown in Figure 1, when faced with an obstacle, each ant has an equal probability of choosing either the left or right path. Since the left trail is shorter than the right one and requires less travel time, the ant will leave a higher amount of pheromone. The more ants use a path, the more pheromone accumulates on that path. Thus, the shortest path is eventually determined.

3.2. Particle Swarm Optimization

Particle Swarm Optimization (PSO) is another population-based, stochastic metaheuristic optimization method inspired by swarm intelligence [26]. It imitates the behaviors exhibited by natural organisms, such as birds and fish, when searching for a place with sufficient food. In these swarms, coordinated behaviors in Figure 2 using local movements emerge without any central control. PSO has been successfully designed to solve continuous optimization problems.

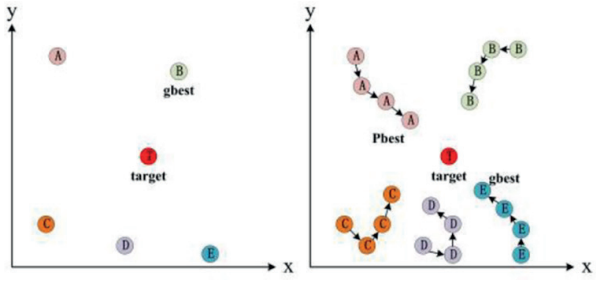


Figure-2. Geometrical illustration for PSO algorithm [27]

3.3. Simulated Annealing

In computer science, particularly in the field of optimization, one of the algorithms used is inspired by the annealing process applied during iron processing, which involves heating the iron and then allowing it to cool. The goal of the Simulated Annealing (SA) algorithm is to achieve overall improvement for any given problem [28]. In other words, it aims to find the global minimum or maximum value of any function or measure.

3.4. Genetic Algorithms

Genetic Algorithms (GA) are a very popular class of evolutionary algorithms. A GA typically applies a crossover operator to two solutions, which plays a significant role, and a mutation operator that randomly alters individual content to increase diversity [29]. GA use probabilistic selection, which is proportional selection. The replacement that determines selection is generational, meaning parents are systematically replaced by their offspring. The crossover operator is based on n-point or uniform crossover, while the mutation operator alters bits [30]. A fixed probability is applied to the mutation operator.

The main search components for designing an evolutionary algorithm are: gene representation, population initialization, objective (fitness) function, selection, mutation and crossover for reproduction, generational replacement, and stopping criteria in Figure 3.

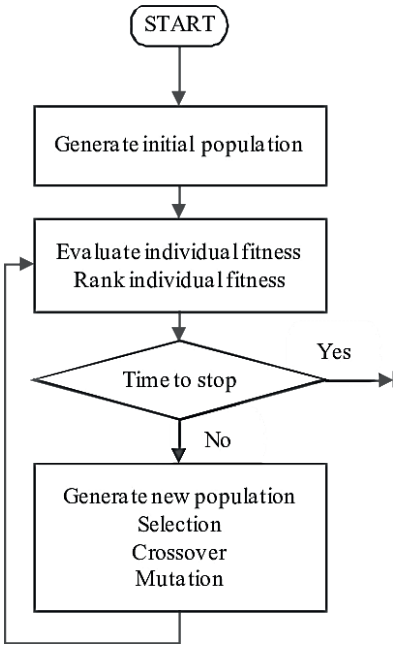


Figure 3. Genetic algorithm flowchart [31]

4. MATERIAL AND METHODS

4.1. Music Dataset

The open library used in this research, created by the Echo Nest company in collaboration with LabROSA, a laboratory for intelligent machine listening, aims to gather data on approximately one million contemporary and popular songs under the name Million Song Dataset [32]. The data includes standard information about songs, such as the artist's name, album, and year of release. Additionally, it contains more advanced information, such as the length of the song, the number of musical bars, and the fade-out duration.

The Million Song Dataset will be analyzed for classification purposes. The original dataset is 280GB in size and consists of one million tracks. In this study, a subset of 10.000 pieces has been used to reduce computational costs. The reduced dataset consists of 22 features, including artist name, title, duration, and tempo.

In the original dataset, there is a song popularity feature. The "song_hotttnesss" tag represents the song popularity. However, this feature does not include values for approximately 4.500 songs, which is almost half of the total number of data entries. Therefore, the BillBoard Top 100 list is used to determine popularity. If a song reaches the BillBoard Top 100 at least once, it is defined as a hit song. Of the 10.000 songs in the dataset, 1.192 songs are classified as popular songs. Popular tracks are represented by 1, while non-popular ones are represented by 0.

As shown in Figures 4 and 5, artist similarities and song loudness are related to the song's popularity. The similarity between artists shows a positive correlation, as expected. However, surprisingly, song loudness exhibits a negative correlation with popularity. It was anticipated that more popular songs would be louder, but this appears to be the opposite, as the overall average loudness of songs tends to be slightly higher. In Figure 5, loudness is plotted on the x-axis, while popularity is plotted on the y-axis. The reason more popular songs seem to be quieter could be due to the presence of exceptionally loud songs in the data, which lowers the overall popularity average of the songs.

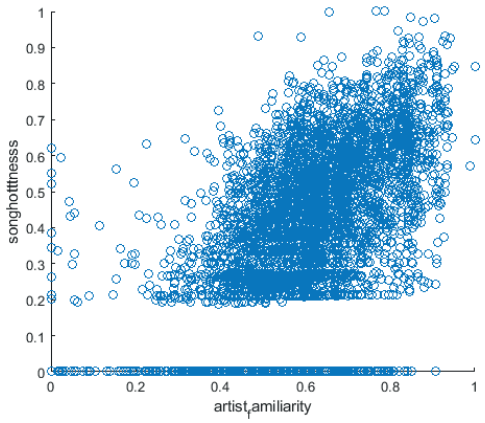


Figure 4. Artist similarity-popularity distribution graph

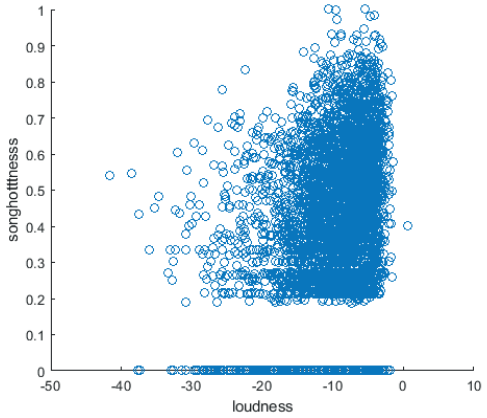


Figure 5. Loudness-popularity distribution graph

Data preprocessing has been performed on the music dataset to achieve more efficient results. Textual data, such as song titles and artist locations, has been removed from the feature set, allowing for the extraction of numerical data in Table 3 that can be computed using algorithms. The data numbers entered in the rows are given as count. Cells with no value in the dataset are entered as NaN. The means, standard deviations and minimum-maximum values of these data are presented in the table.

The data under the "year" tag, which stores the release year of pieces, shows an imbalance due to the high frequency of pieces with unknown release years, where a value of 0 was entered. To prevent this distribution from causing deviations, the year feature column was removed from the processed data. After data cleaning, a dataset with 16 numeric features and a target column (popularity class) was obtained. In its final state, the data consists of 16x10001 inputs and 1x100001 target. Based on this information, the comma-separated values (.csv) file on which feature selection will be performed was converted into formats (.mat, .arff) suitable for the software used.

4.2. Feature Selection

Feature selection is the process of determining a subset that represents a dataset and isolating the variables that best express this data [33]. This process selects the best k features from n features by scanning them according to the algorithm being used, thereby reducing the number of features and providing various benefits in problem-solving. Feature selection reduces the size of the attribute set, allowing the algorithm used for data analysis to run faster. It improves data quality by isolating noisy or incomplete data and prevents complexity by simplifying the dataset [34]. Additionally, it provides storage savings by reducing the data size.

Feature selection processes have been carried out using algorithms designed with MATLAB 2018a software, which enables effective and fast mathematical computations in areas such as statistics, optimization, and numerical analysis [35]. To measure classification performance, desired features were extracted using ACO, PSO, SA, and GA metaheuristic methods.

The Ant Colony Optimization algorithm was used to reduce the dimensionality by performing feature extraction on data containing inputs and targets. In the application phase, the desired number of features was specified as 4. The problem was defined, and a fitness function was created. The parameter values to be used in ant colony optimization were entered in Table 1.

Table 1. ACO parameter values

Parameter	Value
Number of ants (population)	50
Initial pheromone value	1
Pheromone trail information (alpha)	1
Heuristic parameter (beta)	1
Evaporation rate	0.05

In the feature selection process, a matrix is first created to store the tour, cost, and output values of 50 ants. In the loop, which will run for the number of iterations determined at the start, the feature where the tour will begin is randomly selected, starting with the first ant. Then, the probability of this ant moving to other features is calculated. Positions are subjected to roulette wheel selection based on pheromone values, and the next feature the ant will visit is determined [36]. Once the ant completes its tour, the obtained values are sent to the fitness function, and the cost value is calculated. The order of features in the ant's tour, the cost value of the tour, and the structure containing the desired number of

features are recorded as output. Afterward, the pheromone values left by the ant are updated. The loop moves to the next ant, and the same processes are repeated. For each iteration, pheromone is evaporated by 0.05, and the best cost value found is recorded.

When feature selection is performed using Particle Swarm Optimization, the population size consists of 50 particles in total. The values of the Fi (phi) constants are taken as 2.05, and their sum is passed through the chi-square method to equal the inertia weight. The damping ratio of this weight is 0.99. The individual and social learning coefficients (c1, c2) are found by multiplying the Fi constants with the value obtained from the chi-square formula. Velocity limits are set, and the minimum limit is adjusted to be the negative of the maximum limit.

In Simulated Annealing, initial positions are determined using a random permutation function, which returns a random vector composed of the entered features. The positions found are evaluated using the fitness function, and the best solution is assigned. A list containing as many elements as the number of iterations is created to store the best cost values. The initial temperature is set to 10. In the main loop, which runs for the total number of iterations of the Simulated Annealing process, there is an inner loop that runs for the number of sub-iterations. A new solution is generated using the neighbor generation function. In this function, the swap, return, and join rates are applied as 0.2, 0.5, and 0.3, respectively. These rates are subjected to roulette wheel selection, and based on the result, one of these operations is applied to the initially determined tour. After determining the new tour in this way, the cost value for this tour is calculated. If the found value is better, the solution is updated. Once the sub-iteration is completed, the best cost value is retained in the loop for the main iteration, and the temperature is updated based on the cooling rate.

When using a Genetic Algorithm for feature selection, the initial phase was initiated after defining the parameters found in Table 2. An empty structure was defined to hold the positions and costs of the individuals. An array containing as many elements as the population size of individuals was created. In the loop, which runs for the number of individuals, genes consisting of bits were assigned to the elements using a discrete uniform distribution. The individuals were evaluated using the fitness function, and the obtained values were recorded. All individuals in

Table 3. Basic statistics on numerical data

Feature	Count	Mean	Std. dev.	Min.	Max.
artist_familiarity	9997	0.565	0.16	0	1
artist_hotttnesss	10001	0.386	0.144	0	1.083
artist_latitude	3742	37.157	15.599	-41.281	69.651
artist_longitude	3742	-63.934	50.508	-162.44	174.77
duration	10001	238.512	114.133	1.044	1819.8
end_of_fade_in	10001	0.759	1.868	0	43.119
key	10001	5.276	3.554	0	11
key_confidence	10001	0.45	0.275	0	1
loudness	10001	-10.485	5.4	-51.643	0.566
mode	10001	0.691	0.462	0	1
mode_confidence	10001	0.478	0.191	0	1
song_hotttnesss	5649	0.343	0.247	0	1
start_of_fade_out	10001	229.98	112.191	1.044	1813.4
tempo	10001	122.921	35.186	0	262.83
time_signature	10001	3.565	1.266	0	7
time_signature_confidence	10001	0.51	0.373	0	1
year	10001	935	996.651	0	2010

the population were ranked according to their fitness. The best solution was recorded, and an array was created to hold the cost values.

Table 2. Parameters used in genetic algorithm

nPop=50	Population size
pc=0.7	Crossover percentage
nc=2*round(pc*nPop/2)	Number of offspring
pm=0.3	Mutation percentage
nm=round(pm*nPop)	Number of mutants
mu=0.1	Mutation rate
beta=8	Selection pressure

4.3. Classification Algorithms

The data classification problem has countless applications across a wide range of data mining fields [37]. This is because the problem attempts to learn the relationship between a set of feature variables and a target variable of interest. In practice, since many issues can be expressed as relationships between features and target variables, this model provides broad applicability. The concept of classification simply involves distributing data among various classes defined on a dataset. Classification algorithms learn this distribution pattern from the given training set and then attempt to classify correctly when test data arrives, for which the class is not specified.

Classification algorithms typically consist of two stages: the training phase, in which a model is constructed from training examples, and the testing phase, which is used to assign labels to unlabeled test examples. The values that specify these classes on the dataset are referred to as label names and are used during both training and testing to determine the class of the data. In some cases, the training phase may be entirely skipped, and classification is performed directly based on the relationship between training examples and test examples. Instance-based methods, such as nearest neighbor classifiers, are an example of such a scenario [38]. Even in these cases, a preprocessing stage may be carried out to ensure efficiency during the testing phase.

The output of a classification algorithm can be presented in one of two ways. In one, a direct label is found for the test example. In the other, a numerical score is returned for each class label and the combination with the test example. This numerical score can be converted into a separate label by selecting the class with the highest score for a test example. The advantage of this scoring system is that it allows for the comparison of the tendency of different test examples to belong to a certain importance class and enables their ranking when necessary.

To test the classification performance of the obtained features, various classifiers were used. The open-source Weka 3 machine learning software, which contains many different clustering and classification algorithms and enables data mining applications, was utilized.

4.3.1. Naive Bayes Classifier

The Naive Bayes classifier (NB) is a classification technique based on Bayes' Theorem, named after the English mathematician Thomas Bayes, which assumes independence among predictions [39]. In simple terms, it assumes that the presence of a particular feature in a class is independent of the presence of any other feature. Even if these features are dependent on each other or on the presence of other features, all of these features contribute to the probabilities independently [40]. The Naive Bayes model is easy to construct and is particularly useful for very large datasets. Along with its simplicity, it is known to perform better than even highly complex classification methods.

$$P(c|x) = \frac{P(C|X)P(c)}{P(x)} \quad (1)$$

$$P(c|x) = P(x_1|c) \times \ldots \times P(x_n|c) \times P(c) \quad (2)$$

- $P(c\,|\,x)$ The asymptotic probability distribution of a given predictor for a class
- $P(c)$ The prior probability distribution for a parameter or parameter vector
- $P(x\,|\,c)$ The likelihood function of a given class
- $P(x)$ The prior probability of the predictor

4.3.2 K-Nearest Neighbors

The K-Nearest Neighbor (KNN) algorithms are a classification algorithm proposed by T. M. Cover and P. E. Hart in 1967 [41]. It takes multiple labeled points and uses them to learn how to label

other points. To label a new point, it looks at the k nearest labeled points to that new point and uses the labels of these neighbors. Therefore, the label that appears most frequently among the neighbors becomes the label for the new point.

When determining the neighborhood condition, the distance of a point from other points is considered [42]. Typically, three different distance functions are used for distance calculations:

- Euclidean Distance

$$d(x,y) = \sqrt{\sum_{i=1}^{k}(x_i - y_i)^2} \quad (3)$$

- Manhattan Distance

$$d(x,y) = \sum_{i=1}^{k}|x_i - y_i| \quad (4)$$

- Minkowski Distance

$$d(x,y) = \left(\sum_{i=1}^{k}(|x_i - y_i|)^q\right)^{\frac{1}{q}} \quad (5)$$

IBk (Instance Based Learner), a derivative of KNN, is a pattern recognition method that classifies test data based on the nearest training examples in the feature space [43]. This algorithm performs classification based on the class of the k nearest neighbors. In the IBk algorithm, the classification of a vector is done using known class vectors. In this study, the value of k indicating the neighborhood was set to 3. The linear search algorithm was used in the neighbor finding process [44].

4.3.3. Decision Tree

A decision tree creates classification or regression models in the form of a tree structure [45]. As it divides a dataset into smaller subsets, a corresponding decision tree is developed step by step. The result is a tree with decision nodes and leaf nodes. A decision node has two or more branches, while a leaf node represents a classification or decision. The top decision node in the tree corresponds to the best prediction and is called the root node. Decision trees can handle both categorical and numerical data. The J48 decision tree, based on the C4.5 algorithm, was used in this study [46]. J48 utilizes information gain for attribute selection and includes pruning techniques to mitigate overfitting, ensuring robust model performance.

4.3.4. Support Vector Machines

It is possible to separate labeled groups located in a plane by drawing a boundary between them. The location where this decision boundary is drawn should be the point that is farthest from the members of the groups. Support Vector Machines (SVM) determine these boundaries. This method was developed in 1995 by Vladimir Vapnik, Bernhard Boser, and Isabelle Guyon [47]. Today, SVM is used in various classification problems, ranging from face recognition systems to text categorization. SMO (Sequential Minimal Optimization) is an algorithm that operates by using John Platt's sequential minimal optimization algorithm to train a support vector classifier [48].

4.3.5. Artificial Neural Networks

Artificial neural networks are developed by drawing inspiration from the way nerve system cells function in living organisms [49]. Their aim is to impart the learning ability of a living brain to computers. A neural network consists of units (neurons) organized in layers that transform an input vector into an output. Each unit receives an input, applies a typically nonlinear function to it, and then passes the output to the next layer. Networks are generally defined to feed forward [50]. A unit feeds its output to all units in the next layer but does not transmit feedback to the previous layer. Weights are applied to the signals that pass from one unit to another, and these weights are adjusted during the training phase to adapt the artificial neural network to the specific problem at hand [51].

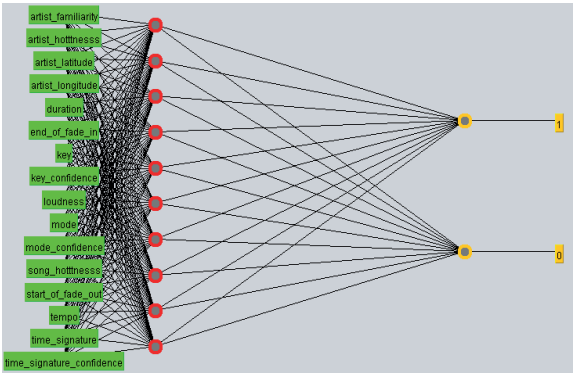


Figure 6. A Multi-layer Perceptron with 10 hidden layers

The most commonly used model of artificial neural networks is the Multi-layer Perceptron (MLP) [52]. Multilayer artificial neurons fundamentally consist of three parts in Figure 6. The input layer does not perform any information processing; it simply receives information and transmits it to the hidden layers. Each element in the input layer is connected to all processing units in the hidden layer. In this part, the information from the input layer is processed. A single hidden layer can solve many problems, but multiple hidden layers can also be utilized. The number of hidden layers varies depending on the type of problem. The output layer processes the information coming from the hidden layer and transmits it to the outside.

$$f(x) = b + \sum_{i=1}^{n}(x_i\, w_i) \tag{6}$$

Here:

b = bias, x = neuron input, w = weights, n = number of inputs from the previous layer, i = counter from 0 to n.

In artificial neural networks, the values of the inputs are multiplied by the weights of the connections, and the results are combined to find the net input of the network [53]. Once the net inputs are passed through an activation function, the net output of the network is obtained.

During the classification process, 10-fold cross-validation was used. Cross-validation divides the dataset into 10 random subsets, using 9 for testing and 1 for training. This process is repeated 10 times until all permutations are used for training and testing.

4.4 Performance Metrics

The most commonly used method for measuring classification performance is accuracy. It is calculated by dividing the number of correctly classified instances by the total number of instances.

$$A = \frac{(TP+TN)}{(TP+FP+FN+TN)} \tag{7}$$

TP (True Positive): This is used when the value in the test data matches the class predicted by the model. The classification is correct.

FN (False Negative): This occurs when the value in the test data is different from the class produced by the model, where a positive instance is incorrectly classified as negative. The classification is incorrect.

FP (False Positive): This occurs when the actual value is negative but is incorrectly classified as positive.

TN (True Negative): This is when the value is correctly classified as negative when it is actually negative.

Precision is the ratio of the number of true positives (TP) predicted as positive to the total number of instances predicted as class 1.

$$P = \frac{TP}{(TP+FP)} \tag{8}$$

The metric that indicates how many of all positive classes were correctly predicted is defined as sensitivity.

$$R = \frac{TP}{(TP+FN)} \tag{9}$$

In cases where sensitivity and precision metrics are not sufficient to produce meaningful results, it is necessary to evaluate these two metrics together. Therefore, the F-measure has been defined. This metric is the harmonic mean of precision and sensitivity.

$$F = \frac{2RP}{(R+P)} \tag{10}$$

5. RESULTS AND DISCUSSION

Through studies conducted using metaheuristic methods, feature selection was performed on the data in the music dataset to enhance classification performance. The most important features for the classification process were identified. A current dataset containing features that meaningfully represent the data was created, and the data was classified according to track popularity using various classifiers. It was observed that the artist_hotttnesss label, which represents artist popularity, was a significant feature in all the algorithms used. This indicates that an artist's recognition is an important factor in a song's popularity. Furthermore, it was concluded that the features tempo and loudness, which indicate the track's tempo and volume, are significant factors in determining song popularity. After 100 iterations, the lowest error value in Table 4 was achieved using the ant colony algorithm.

The results obtained from classification using different classifiers were compared after feature selection was performed using metaheuristic methods, as well as without feature selection. Initially, the best performance in the classification of raw data was achieved with the SMO algorithm among five different classifiers. According to Table 5, it was observed that the success rate increased after feature selection using metaheuristic methods compared to the raw dataset. In classifications using fewer features, the success rates of decision trees, Naive Bayes, kNN, and artificial neural networks increased compared to the previous state of the data, while there was no change in the success rate for classifications performed with support vector machines. Based on these results, the highest success obtained through feature selection was achieved with the J48 algorithm, which is a decision tree algorithm. The highest performance increase compared to the raw dataset was 3.23%, which was obtained using features selected by a genetic algorithm and the Naive Bayes classifier. The error rates obtained with this classifier are presented in Table 6.

Table 4. Algorithm comparison results according to iteration number

Method	Iteration	Feature Set	Min. Error
ACO	20	artist_hotttnesss, loudness, mode, mode_confidence	0.10172
	50	artist_hotttnesss, loudness, tempo, time_signature_confidence	0.10153
	100	artist_hotttnesss, loudness, tempo, start_of_fade_out	0.10109
PSO	20	artist_hotttnesss, loudness, tempo, key	0.10122
	50	artist_hotttnesss, artist_familiarity, tempo, start_of_fade_out	0.10113
	100	artist_hotttnesss, duration, tempo, end_of_fade_in	0.10119
SA	20	artist_hotttnesss, loudness, duration, time_signature	0.10227
	50	artist_hotttnesss, loudness, key, mode	0.10193
	100	artist_hotttnesss, loudness, key, mode_confidence	0.10149
GA	20	artist_hotttnesss	0.10541
	50	artist_hotttnesss	0.10517
	100	artist_hotttnesss	0.10507

Table 5. Classification results

Classifier	Raw (%)	ACO (%)	PSO (%)	SA (%)	GA (%)
IBk	84.53	84.96	85.04	84.83	85.48
NB	84.77	87.86	87.75	87.97	88.00
MLP	87.74	88.08	88.02	88.04	88.07
J48	88.02	88.08	88.08	88.08	88.08
SMO	88.08	88.08	88.08	88.08	88.08

Table 6. Naive Bayes classifier error rates

Metric	ACO	PSO	SA	GA
TP Rate	0.879	0.878	0.880	0.880
FP Rate	0.862	0.858	0.867	0.871
Precision	0.820	0.817	0.823	0.823
Recall	0.879	0.878	0.880	0.880
F-Measure	0.829	0.829	0.828	0.827

6. CONCLUSION

This study addresses the significant issue of improving machine learning classification performance through the use of efficient feature selection techniques. Finding the most relevant features in multimedia datasets is crucial, especially when it comes to music data analysis. In order to improve the accuracy and efficiency of predictive models, this research attempts to enhance the feature selection process by investigating different nature-inspired metaheuristic algorithms.

The results of this study show that using four different metaheuristic techniques greatly improves the ability to extract relevant features from the dataset. It has been demonstrated through comparative evaluations that these metaheuristic techniques not only improve classification accuracy but also make model training more effective. Furthermore, the use of artificial neural networks to assess the appropriateness of particular features highlights the potential for synergy between machine learning classification methods and reliable feature selection processes.

In future studies, the speed performance of the currently applied algorithms can be tested. It appears feasible to make improvements in terms of time and cost with different parameter values. Furthermore, it is believed that new studies could be conducted to measure the success of other metaheuristic algorithms in feature selection. The use of hybrid versions of heuristic optimization methods is also recommended for this purpose.

Acknowledgments

This article has been prepared based on master's thesis, *Meta-Heuristic Methods for Feature Selection and Categorization on Music Data* [54]. I would like to express my sincere gratitude to my thesis advisor Prof. İdiris Dağ for his exceptional guidance, insightful feedback, and unwavering support throughout this research journey.

REFERENCES

[1] M. A. Casey, R. Veltkamp, M. Goto, M. Leman, C. Rhodes, and M. Slaney, "Content-based music information retrieval: Current directions and future challenges," *Proceedings of the IEEE,* vol. 96, no. 4, pp. 668-696, 2008.

[2] A. Lerch, *An introduction to audio content analysis: Music Information Retrieval tasks and applications*. John Wiley & Sons, 2022.

[3] P. Knees and M. Schedl, "A survey of music similarity and recommendation from music context data," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* vol. 10, no. 1, pp. 1-21, 2013.

[4] T. Dokeroglu, A. Deniz, and H. E. Kiziloz, "A comprehensive survey on recent metaheuristics for feature selection," *Neurocomputing,* vol. 494, pp. 269-296, 2022.

[5] R.-C. Chen, C. Dewi, S.-W. Huang, and R. E. Caraka, "Selecting critical features for data classification based on machine learning methods," *Journal of Big Data,* vol. 7, no. 1, p. 52, 2020.

[6] M.-H. Tayarani-N, X. Yao, and H. Xu, "Meta-heuristic algorithms in car engine design: A literature survey," *IEEE Transactions on Evolutionary Computation,* vol. 19, no. 5, pp. 609-629, 2014.

[7] A. M. Shaheen, S. R. Spea, S. M. Farrag, and M. A. Abido, "A review of meta-heuristic algo-

rithms for reactive power planning problem," *Ain Shams Engineering Journal,* vol. 9, no. 2, pp. 215-231, 2018.

[8] S. Memeti, S. Pllana, A. Binotto, J. Kołodziej, and I. Brandic, "A review of machine learning and meta-heuristic methods for scheduling parallel computing systems," in *Proceedings of the International Conference on Learning and Optimization Algorithms: Theory and Applications*, 2018, pp. 1-6.

[9] C. K. Teoh, A. Wibowo, and M. S. Ngadiman, "Review of state of the art for metaheuristic techniques in Academic Scheduling Problems," *Artificial Intelligence Review,* vol. 44, pp. 1-21, 2015.

[10] M. Kalra and S. Singh, "A review of metaheuristic scheduling techniques in cloud computing," *Egyptian informatics journal,* vol. 16, no. 3, pp. 275-295, 2015.

[11] A. Feizollah, N. B. Anuar, R. Salleh, and A. W. A. Wahab, "A review on feature selection in mobile malware detection," *Digital investigation,* vol. 13, pp. 22-37, 2015.

[12] M. Z. Asghar, A. Khan, S. Ahmad, and F. M. Kundi, "A review of feature extraction in sentiment analysis," *Journal of Basic and Applied Scientific Research,* vol. 4, no. 3, pp. 181-186, 2014.

[13] Y. Saeys, I. Inza, and P. Larranaga, "A review of feature selection techniques in bioinformatics," *bioinformatics,* vol. 23, no. 19, pp. 2507-2517, 2007.

[14] L. Dong, "Using deep learning and genetic algorithms for melody generation and optimization in music," *Soft Computing,* vol. 27, no. 22, pp. 17419-17433, 2023.

[15] U. Boryczka, M. Boryczka, and P. Chmielarski, "ACO and generative art–artificial music," *Procedia Computer Science,* vol. 225, pp. 2624-2633, 2023.

[16] Q. Zhu, A. Shankar, and C. Maple, "Grey wolf optimizer based deep learning mechanism for music composition with data analysis," *Applied Soft Computing,* vol. 153, p. 111294, 2024.

[17] J. A. Parejo, A. Ruiz-Cortés, S. Lozano, and P. Fernandez, "Metaheuristic optimization frameworks: a survey and benchmarking," *Soft Computing,* vol. 16, pp. 527-561, 2012.

[18] F. Glover and K. Sörensen, "Metaheuristics," *Scholarpedia,* vol. 10, no. 4, p. 6532, 2015.

[19] G. Keren and K. H. Teigen, "Yet another look at the heuristics and biases approach," *Blackwell handbook of judgment and decision making,* pp. 89-109, 2004.

[20] J. D. Knowles, R. A. Watson, and D. W. Corne, "Reducing local optima in single-objective problems by multi-objectivization," in *International conference on evolutionary multi-criterion optimization*, 2001, pp. 269-283: Springer.

[21] M. Abdel-Basset, L. Abdel-Fatah, and A. K. Sangaiah, "Metaheuristic algorithms: A comprehensive review," *Computational intelligence for multimedia big data on the cloud with engineering applications,* pp. 185-231, 2018.

[22] M. Dorigo, M. Birattari, and T. Stutzle, "Ant colony optimization," *IEEE computational intelligence magazine,* vol. 1, no. 4, pp. 28-39, 2006.

[23] M. Dorigo and T. Stützle, *Ant colony optimization: overview and recent advances*. Springer, 2019.

[24] E. Talbi, "Metaheuristics: From Design to Implementation," *John Wiley & Sons google schola,* vol. 2, pp. 268-308, 2009.

[25] E. Flórez, W. Gómez, and L. Bautista, "An ant colony optimization algorithm for job shop scheduling problem," *arXiv preprint arXiv:1309.5110,* 2013.

[26] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95-international conference on neural networks*, 1995, vol. 4, pp. 1942-1948: ieee.

[27] H. Liu, X. Wang, and M. Li, "External force estimation for robotic manipulator base on particle swarm optimization," *International Journal of Advanced Robotic Systems,* vol. 18, no. 6, p. 17298814211063744, 2021.

[28] D. Bertsimas and J. Tsitsiklis, "Simulated annealing," *Statistical science,* vol. 8, no. 1, pp. 10-15, 1993.

[29] A. Hassanat, K. Almohammadi, E. a. Alkafaween, E. Abunawas, A. Hammouri, and V. S. Prasath, "Choosing mutation and crossover ratios for genetic algorithms—a review with a new dynamic approach," *Information,* vol. 10, no. 12, p. 390, 2019.

[30] K. A. De Jong and W. M. Spears, "A formal analysis of the role of multi-point crossover in genetic algorithms," *Annals of mathematics and Artificial intelligence,* vol. 5, pp. 1-26, 1992.

[31] V. Kachitvichyanukul, "Comparison of three evolutionary algorithms: GA, PSO, and DE,"

Industrial Engineering and Management Systems, vol. 11, no. 3, pp. 215-223, 2012.

[32] T. Bertin-Mahieux, D. P. Ellis, B. Whitman, and P. Lamere, "The million song dataset," 2011.

[33] H. Liu and H. Motoda, *Feature extraction, construction and selection: A data mining perspective*. Springer Science & Business Media, 1998.

[34] W. Fan, F. Geerts, and X. Jia, "Improving data quality: Consistency and accuracy," 2007: ACM.

[35] G. Ciaburro, *MATLAB for machine learning*. Packt Publishing Ltd, 2017.

[36] A. Lipowski and D. Lipowska, "Roulette-wheel selection via stochastic acceptance," *Physica A: Statistical Mechanics and its Applications,* vol. 391, no. 6, pp. 2193-2196, 2012.

[37] G. Kesavaraj and S. Sukumaran, "A study on classification techniques in data mining," in *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)*, 2013, pp. 1-7: IEEE.

[38] B. Martin, "Instance-based learning: nearest neighbour with generalisation," 1995.

[39] J. Joyce, "Bayes' theorem," 2003.

[40] M.-L. Zhang, J. M. Peña, and V. Robles, "Feature selection for multi-label naive Bayes classification," *Information Sciences,* vol. 179, no. 19, pp. 3218-3229, 2009.

[41] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE transactions on information theory,* vol. 13, no. 1, pp. 21-27, 1967.

[42] L. E. Peterson, "K-nearest neighbor," *Scholarpedia,* vol. 4, no. 2, p. 1883, 2009.

[43] R. Ade and P. Deshmukh, "Instance-based vs batch-based incremental learning approach for students classification," *International Journal of Computer Applications,* vol. 106, no. 3, 2014.

[44] M. R. Abbasifard, B. Ghahremani, and H. Naderi, "A survey on nearest neighbor search methods," *International Journal of Computer Applications,* vol. 95, no. 25, 2014.

[45] W. Y. Loh, "Classification and regression trees," *Wiley interdisciplinary reviews: data mining and knowledge discovery,* vol. 1, no. 1, pp. 14-23, 2011.

[46] N. Bhargava, G. Sharma, R. Bhargava, and M. Mathuria, "Decision tree analysis on j48 algorithm for data mining," *Proceedings of international journal of advanced research in computer science and software engineering,* vol. 3, no. 6, 2013.

[47] V. Vapnik, *The nature of statistical learning theory*. Springer science & business media, 2013.

[48] J. Platt, "Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Machines," 1998.

[49] A. Abraham, "Artificial neural networks," *Handbook of measuring system design,* 2005.

[50] T. L. Fine, *Feedforward neural network methodology*. Springer Science & Business Media, 2006.

[51] K. Jadav and M. Panchal, "Optimizing weights of artificial neural networks using genetic algorithms," *Int J Adv Res Comput Sci Electron Eng,* vol. 1, no. 10, pp. 47-51, 2012.

[52] M. Riedmiller and A. Lernen, "Multi layer perceptron," *Machine Learning Lab Special Lecture, University of Freiburg,* vol. 24, 2014.

[53] S. Han, J. Pool, J. Tran, and W. Dally, "Learning both weights and connections for efficient neural network," *Advances in neural information processing systems,* vol. 28, 2015.

[54] A. H. Ezirmik, "Meta-sezgisel yöntemler ile müzik verisi üzerinde özellik seçimi ve kategorizasyon," *Eskişehir Osmangazi Üniversitesi, Fen Bilimleri Enstitüsü,* 2020.

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 Kamu Askeri/Ordu Diplomasi ve İstihbarat Toplulukları	Yeni hibrit disiplinler Yıkıcı teknolojiler Özelleştirilmiş OSINT Grupları Özelleştirilmiş Analiz Firmaları
Kriptanaliz	Simetrik Şifreleme Asimetrik Şifreleme veya 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

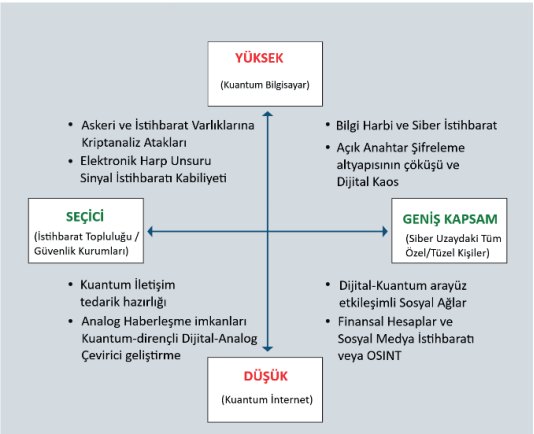
Kuantum teknolojilerinin istihbarat disiplini üzerindeki yenilikçi ve yıkıcı etkileri göz önüne alındığında, Kuantum Bilişim ve Kuantum İletişim alanları özelinde ilerlemek, istihbarat düzleminde alternatif geleceklerin netleştirilmesinde bir fikir verebilir. Daha önce de belirtildiği üzere, Kuantum 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:

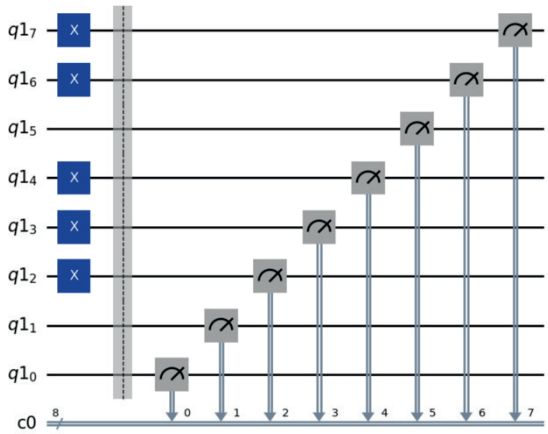
- Kuantum Bilişim → Kırmızı Takım (Ofansif)
- Kuantum İletişim → Mavi Takım (Defansif)

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."

E-ISSN : 3023-4735
DOI: 10.70447/ktve

Journal of Quantum Technologies and Informatics Research

JQTAIR

HOLISTENCE publications